Information & Security Volume 4, 2000

Dialectics of Information Security

Edited by Veselin Tselkov and Dragomir Pargov

Editorial
Dialectics of Information Security

The Dialectics of Information

Deyan Gotchev
Kaleidoscopic Approach to Security Shadows in the Age of Information Warfare Abstract

Andrew Borden
The Dialectics of Information – A Framework Abstract

Information Assurance

Veselin Tselkov, Dragomir Pargov
Information Assurance in C4I Systems Abstract

Eugene Nickolov
Contemporary Trends in the Development of Information Security and Computer Virology Abstract

Metodi Popov
Security Aspects of the Cellular Communications Abstract

Information Security Solutions

Veselin Tselkov

Cryptographic Software Solution for Information Protection in a Corporate Intranet Abstract

Atanas Nachev
Electromagnetic Radiation and the Computer Systems Data Security Problem Abstract

I&S Monitor

I&S Library Update

Information Warfare and Security

Information Security Architecture: An Integrated Approach to Security in the Organization

Information Security Management Handbook

Coding in Cellular Communications

Network Security Fundamentals

LAN Times Guide to Security and Data Integrity

Network Intrusion Detection: An Analyst’s Handbook

I&S Reference Files

Common Criteria for IT Security Evaluation

Network Security Roadmap

Starting Points for Antivirus Software

Notes on Internet Security

Acronyms

I&S News

Swedish-Bulgarian Government IT Security Conference "Information Security in the 21st Century: Global Convergence"

I&S Research Centers

National Laboratory of Computer Virology

Research and Demonstration Centre of the Institute for Advanced Defence Research

Author: **Editorial**
Title: **Dialectics of Information Security.**
Year of issuance: **2000**
Issue: **Information & Security. Volume 4, 2000**
Hard copy: **ISSN 1311-1493**

DIALECTICS OF INFORMATION SECURITY

At the transition between two millennia a new era is born - the information age. Information technology is our means of reinforcing human knowledge and communications. It opens up a new revolutionary world to mankind. The envisioned revolution in the field is slowly progressing, and thus not always easily distinguished. Information age and information technology create dependencies, capabilities, and vulnerabilities that have to be understood and managed.

Information and knowledge have always been - and are now more than ever – inherent in any economy, corporation, or family. In the information society, being informed becomes more important than any tangible asset. As information age evolves, society will face new threats. People take information systems for granted and do not realize their total dependence on them. They do not understand clearly the extent of their vulnerability, and consequences of possible malfunction or disruption. Previously, unless public, all information was strictly confidential. Today, unless strictly confidential, all information is made public. Immensely sophisticated information systems have so far been created on insecure foundations. Network capabilities simply outpace information protection.

Data traffic is tripling every year and will overtake voice as the dominant type of traffic over the worldwide telecommunication networks by 2005. 75 million new customers signed up for the cellular phone service in 1998, bringing the worldwide untethered population to roughly 285 million. In 1998, an average of five million e-mails were sent every minute. Users can listen to e-mail messages over the phone and then reply with voice messages. Or they can have e-mail messages and attachments printed as faxes by a fax machine. Intelligent software agents will sort and filter incoming messages and allow callers to retrieve and manage voice mail using spoken commands rather than a telephone keypad.

Today there are more than 100 million users of the Internet and a new Web site is created every four seconds. Internet traffic is doubling every 100 days. By 2005 there might be about one billion people using the Internet. An enormous number of Web sites and information will be available and at risk of unauthorized access. The real assets will be symbols and bytes, not cash. Time, as well as information, is money but high-speed filtering of information for special purposes is even more valuable. The Internet is changing the way the world economy functions. By 2005 sales over the Internet are expected to reach 5 trillion US dollars in the United States and Europe collectively.

It is obvious that the revolution in information technology and the new global information economy and knowledge will create new risks unparalleled to past criminal acts. We do not yet know the outcome of the changing circumstances but we will need to rapidly create and mobilize means of information protection in order to encounter expected cyber crimes. Even the US President Bill

Clinton stated that our *"vulnerability, particularly to cyber attacks, is real and growing."*

Billions in proprietary secrets have been stolen from high-tech corporations. Most corporations have been penetrated electronically by cyber-criminals. In the United States the FBI estimates that damages from electronic crimes amount to about 10 billion dollars a year. The importance of customer confidence and shareholder value is the reason why companies report to law enforcement agencies only a fraction of the intrusions. Furthermore, it is estimated that only a small fraction of all intrusions are detected by systems under attack.

We have already experienced an arsenal of information warfare weapons such as computer viruses, Trojan horses, logic bombs and software for denial of service. Compromising high-powered scanners and sniffers proliferate and are being used to intercept mobile phones, faxes, and satellite and landline communications. A number of new methods are being used and further developed in order to steal information and camouflage where attacks originate. There is also a large arsenal of tools for destruction of information and information infrastructure. For example, telephone lines can be overloaded by special software, thus air, sea and land traffic control can be disrupted or given false information. Financial institutions', emergency services and other government services' software can be scrambled, electric power and pipeline industrial processes can be altered by remote control and even stock exchanges sabotaged by using the same technique.

Peace does not really exist in the information age and the threat spectrum is constantly changing. Malicious tools are constantly improving and changing. Password-cracking programs are widely available. Programs detecting weak points in system security now can also automate attacks against the identified vulnerabilities. Computer chips with malicious codes, i.e., trapdoors, backdoors, logic bombs, are available and affordable. World Wide Web home page editing programs can be used for attacking network servers. Powerful high capacity malicious servers can attack information systems connected to the Internet.

Preliminary Observations

Historically, the term Information Security was used to refer to the combination of computer security (COMPUSEC) and communications security (COMSEC). During the past several years, a new term has been developed to encompass a broader aspect of security concerns. This term is "Information Assurance." It covers not only the traditional areas of COMPUSEC and COMSEC but also includes protection, detection and reaction capabilities as well as technical, personnel, physical and procedural security.

All of these disciplines are essential to an effective security posture in today's highly networked world. In summary, Information Assurance includes all information operations that protect and defend information and information systems by ensuring their availability, integrity, confidentiality and non-repudiation.

The Need for Security

Why is security needed? The answer is simple—there is a threat out there and it is real and growing each and every day. A later paragraph will give examples of the types of threats and the magnitude of the problem.

Given the severity of the threat, it is clear that unprotected communications and information systems (CIS) are at risk. If they are not protected, a country may experience:

- unauthorized access to classified information;
- destruction of critical data or, just as bad, loss of confidence in the correctness of the data;
- a potential loss of control over military forces.

Finally, the performance of inadequately protected CIS can be degraded or reduced to zero at critical points in time by adversaries.

Security is Important to NATO

As an alliance of independent sovereign states, NATO depends on the cooperation of its members to ensure adequate levels of security for shared information. The foundation of this approach is *C-M(55)15 Final* entitled "Security Within the North Atlantic Treaty Organization" which has been unanimously agreed by the nations. This document lays out the minimum security requirements which the nations have agreed to meet in protecting NATO classified information. It establishes the basic requirements for physical, personnel, procedural and technical security. By agreeing to C-M(55)15 Final each nation is making a national-level commitment to ensure the adequate protection of NATO classified information—it is not just a MOD issue. When a nation joins NATO it agrees to this common commitment to adequately protect NATO classified information. Each nation makes its own assessment of how the other nations are living up to this shared commitment and based on that assessment determines what information it will share with the Alliance. Thus, any failure on the part of one or more nations to meet their security commitments can lead to a reduction in the quantity and quality of defense information that is shared.

In the focus of I&S

In an attempt to cover the broad area of Information Security we chose a set of articles in the current volume of I&S.

The first two articles deal with security challenges in the age of information warfare and a framework for studying the dialectics of information.

The first paper by Deyan Gotchev studies a number of outgrowths of Information Warfare (IW). Society is analysed as a set of interdependent infrastructure elements. Their functional contradictions lead to conflict, crisis, and catastrophe (C3). They could involve dramatic shifts in political power and attitudes toward authority. The C3 activity incarnates as information warfare and cyber-terrorism. This paper describes the multidirectional holographic-like construction of the IW space. Special attention is paid on intelligence. In order not to loose orientation in "fuzzy" IW functioning one should try to balance among previous experience, hard reason and a feeling of transformation during a self-organizing process. The prosecution of IW is not limited to established national and transnational architectures. Security in the age of information warfare will be characterized by operations in the obscurant boundary region between real, often incomprehensible phenomena, and dominating bluff. Nevertheless, it is important to discuss the problems of protection in IW in order to help the security professional and military planner not to forget to be on a cool alert and cautiously to search for newly emerging and interwoven features of the information space. According to the comments made in this paper, the commander in future combat variants should not expect to exist and act relying entirely on a "comprehensive, stable, predictable" scheme.

In the next paper a framework for studying dialectics of information is presented. The dialectics of information applies whenever there is a human conflict or competition in which information (1) is a commodity that is not shared; and (2) is subject to attack. The purpose of this paper is to present a generic, domain-independent, framework of information dialectics and to show how the framework can be applied to any selected domain. The program for doing so is straightforward: defines the generic tasks relevant to the development of information; identifies the generic types of attack that can be mounted against these tasks (Identify Attack measures); shows how the performance of the tasks can be protected against these Attack Measures (Identity Protect Measures). This framework will be developed in the context of an analog to the Shannon-Hartley channel capacity theorem. The use of a standard design method for situation assessment strategies makes this evaluation possible.

The second group of articles is concerned with various problems of Information Assurance. The first paper of this group discusses information assurance in C4I systems. Information Assurance should be a key aspect of any C4I architecture and system design. With that fact in mind, the paper develops a broader definition of security, information assurance architecture and a set of policy and implementation recommendations. The paper presents three distinct aspects of computer security: confidentiality (secrecy), integrity and availability. In some systems or application environments, one security aspect may be more important than another. Your own assessment of what type of security your organization requires will influence your choice of the particular security techniques and products needed to meet those requirements. A security policy is the set of rules and practices that regulate how an organization manages, protects, and distributes sensitive information. It is the framework in which the system provides trust. A security policy is typically stated in terms of subjects and objects.

The second paper deals with computer viruses. The information and its security have been a subject of a special attention through the ages. All the achievements in this area were estimated highly and found immediate application. During the last few years the development of the contemporary society is connected to the continuously growing information activity. Some of the main effects on information security of a given information object are computer viruses and their derivatives. The science of computer virology appeared as a response to these challenges. It deals with analysis and synthesis of virus signatures used by antivirus programs for detection, blocking and removal of computer viruses. In the contemporary information society computer virology turns into one of the most important agents for mastery of ‘malicious thinking’ and for guaranteeing the necessary information security. Computer virology is a contemporary dynamically developing science branch, in which the peak achievements of mathematics, informatics, physics, chemistry, biology, genetics, etc., are combined. Nowadays, it is extremely important for guaranteeing the necessary information security in the conditions of global and mobile communications.

The third paper refers to information security in cellular communications and shows the applicability of cryptographic technologies. In it Prof. Metodi Popov describes functions, architectures, security procedures and means in the rapidly developing field of cellular communications, concentrating on implementation issues in the GSM standard.

The third group of articles presents some solutions for information security.

The first paper of this group presents a cryptographic software system for information protection in a corporate Intranet. The architecture, functional features, and components of the system are explained. CSSW is a Windows based software system for cryptographic protection. It uses symmetrical and asymmetrical algorithms and provides the following services: identification and authentication of users; identification and authentication of applications; cryptographic protection on file and block data levels; digital signature; access control to cryptographic functions; logs; and cryptographic application program interface.

The next paper answers some questions about electromagnetic radiation and computer system data security. A major information security issue is the emission of electromagnetic field. The paper presents the threats and basic solutions of information assurance. The problem arising from the emission of electromagnetic field in different types and classes of working electronic equipment has been present for more than twenty years. Its solution is particularly urgent for emissions from computer systems. The experience of using computer systems for processing classified information in special conditions shows that special attention needs to be paid to insuring the security of sensitive information. The electromagnetic emission of working computer systems is extremely revealing. The original methods for solving the problem of electromagnetic field emissions are presented.

For those, interested in learning more about information security, several books are presented. The first one deals in a comprehensive manner with information warfare and security. The second presents information on security architecture in an integrated approach to security in organizations. One handbook on information security management is also presented, as well as a recent book on coding in cellular communications. Presentations of three fundamental books on network security are also included in this volume: *LAN Times Guide to Security and Data Integrity* By Marc Farley, Tom Stearns, and Jeffrey Hsu; *Network Security Fundamentals* By Peter Norton and Mike Stockman, and *Network Intrusion Detection, An Analyst’s Handbook* by Stephen Northcutt, Judy Novak and Donald McLachlan.

For the lay reader, a brief definition of information assurance is given. Two research centers are also presented.

We hope this issue will help the reader to develop new interrelations from various areas of scientific research. The common interest in solving information security problems could provide new opportunities for fruitful cooperation and consideration of future implementation and joint R&D projects.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Author: **Deyan Gotchev**
Title: **Kaleidoscopic Approach to Security Shadows in the Age of Information Warfare**
Year of issuance: **2000**
Issue: **Information & Security. Volume 4, 2000**
Hard copy: **ISSN 1311-1493**

KALEIDOSCOPIC APPROACH TO SECURITY SHADOWS IN THE AGE OF INFORMATION WARFARE

Deyan GOTCHEV

Table Of Contents:

Introduction
Society
Cyberterrorism
Essence of IW
Means of Conducting IW
Intelligence
Protection
Prognosis
Conclusions
Notes

Introduction

In order to learn the necessary rules of the new era one can not usually skip the long period of disorientation and confusion characteristic of all periods of transition. In this paper society is analysed as a set of interdependent infrastructure elements. Their functional contradictions lead to conflict-crisis-catastrophe (C3).[1] They could involve dramatic shifts in political power and attitudes toward authority, in the means and the burden of conflict and defence. The C3 activity incarnates as information warfare (IW) and cyber-terrorism.

The aim of this paper is to present one idea about the multidirectional holographic-like construction of the IW space. Special attention is focused on intelligence. In order not to loose orientation in "fuzzy" IW functioning one should try to balance among previous experience, hard reason and the feeling of transformation during a self-organising process. The problems of protection in IW are discussed in order to help the military planner not to forget to be on a cool alert and cautiously to search for newly emerging and interwoven features of the information space. According to the comments made in this paper, the commander in future combat variants should not expect to exist and act relying entirely on a "comprehensive, stable, predictable" scheme.

Society

Some societies and cultures have developed considerable infrastructure to support the elements of the social contract between members of the society. A *"dependency infrastructure"* is created for an economy of scale and to optimise the level of complexity in society. Its successive stages insulate the advanced levels from the details of the previous stages. Dependency infrastructures closely parallel a hierarchy of needs. Elements of the dependency infrastructure include macro- and micro-administration, transportation systems and communication mechanisms.[2]

The infrastructure on which society depends, in sectors such as transportation, finance, energy, and telecommunications, is becoming increasingly automated as advances in information technology open up new possibilities for greater service efficiency. A *National Information Infrastructure (NII)* today is more than just a larger, more modern and complex version of the Roman road and aqueduct systems. All sectors have components distributed over wide geographic areas. The NII sectors are owned and operated predominantly by private companies interrelated with various sector-specific interfaces among themselves, as well as with federal, state, and local governments. Varying degrees of co-ordination exist among providers within a sector, but *there is no complete central authority within or among sectors.*[3]

In the net, a domain of ever-shifting patterns of links and nodes, parties are exchanging things that may either represent the real world, or have no worldly connection whatsoever. The might of the networks comes from their redundancy, or multiple pathways between any two points. Value is added only at nodes. Management of the net becomes functionally based. With secure communications and coherent information sharing, the net's hierarchy and overall organisation have a good memory about the participants and avoid a weak central repository of authority. Immediacy provides that a command is always 'forward'; that's why for a perspective in tactical situation hierarchies should be relied on with great precaution and only temporally.

By using quantitative symbols to represent typical value relations between various resources, the *economy* allows efficient distribution of signals in the social system. Its subsystems carrying representations of situational knowledge may be implemented in both completely automated environments and those involving humans. The information age brings a new level of personalisation to our world that changes the value of consumer products and services. Topologically, the effect of fast signal transports is equivalent to *the collapse of the social space dimensions along established social connections*. We can customise the item to our needs, desires, and even our own physical measurements. No longer do we have to accept the statistical norm. The value added to a product customised to personal preference is the value of knowledge. Now the information-based market can tap this added value.

Today's economic indicators do a decent job in reflecting quantitative changes in the structurally stable areas while using questionable methods to disguise small structural changes as quantitative, and totally failing to account for the new products constituting the essence of real economic progress. As a result, rigorous economic methods become confined to a rapid, relatively shrinking and no longer isolated domain of stable production, and so *fail to reflect long-term growth* in social wealth, let alone guide it.

For either nation-state or business, private concern to ignore the networked global markets is a risky business, if not impossible.[4] The information age empowers individuals with access, mobility, and ability to effect change anywhere, instantaneously. The value that we place on personalising and individual rights affects the way we view the world and our expectations of nation-states.

The NII components are not synonymous with commerce, profit, and communications. The organisations that have become dependent on the net in order to reduce, if not to avoid, the conflict-crisis-catastrophe triad have placed their trust in the net's systems, even though they are insecure and not always reliable. Data should not be accepted as a mirror-like image of the structure supporting the traffic. Information traffic, partly due to its relatively low cost, often unpredictably becomes inefficient. Whether the forces of the market will continue to provide infrastructure services with acceptable reliability in this environment remains to be seen.[5]

Spurred by information age technologies, our highly personalised social and political processes have become interconnected and non-linear, making it almost impossible to distinguish cause from effect. Consequential benefits of the information revolution include greater economic efficiency, faster growth, demise of territorial sovereignty, and shift of importance to functional power centres and nodes of influence. Our cyber-future will feature direct participation by the individual as opposed to group representation. As a result, *the relevance of authority and sovereignty has diminished.*[6]

The former monolithic threat is now enlarged and complicated by the fast changing diversity of actors, i.e., the increasing role of international corporations in comparison to nations. Coalitions are difficult to construct and even more difficult to maintain.[7] It is impossible to be sure about the direction of these changes.

Conflict is chaotic, confusing, and messy. Internal and expansionistic conflicts have to do with the selection and control over the leverage points of the social contract and dependency infrastructure. The priority of a target is dependent on its value to the other side.

As conflicts migrate from territorial to functional structures, weapons change from guns to words and bank accounts. Virtual money assists economic intelligence and attacks, control of clandestine assets, money laundering, insider trading. Counter-economic espionage is focused on supporting negotiators in trade talks and stopping foreign practices that hurt firms.[8]

Total agreement on national economic objectives is virtually impossible due to the emergent global and networked nature of markets. In the information age *national security strategies will depend less on confrontation with opponents and more on co-operation and trust among competitors*. A sovereign nation might effectively pursue its interests only as it paradoxically subordinates those interests to the common interests of all networked partners. Just like the non-zero-sum game where "win-win" results are not only expected but are required for information-based economies to flourish.[9]

Cyberterrorism [10]

The globalisation and personalising of electronic communications system appear to be undermining the authority of nation-states and facilitating a devolution of power to sub-national and transnational movements, especially those that tap ethnic, religious or cultural loyalties.

As knowledge disseminates the number and locality of the threats and cyber-civil disobedience will increase. "New tribalism" demands for "self rule" and decentralisation gain momentum. The non-state opposition force should be the more frightening potential of IW because of varying motive to target government and civilian sectors, using technology to recruit, organise, communicate, fund, gather intelligence, plan, and even launch operations.

Technology is complex, abstract and indirect in its impact on individuals. It is feared as a result of the following factors:

- the concept of convergence - technology has the ability to become the master and humanity the servant;
- the increase of the "connectivity absurd" according to which the entire world will soon be controlled by a single computer system;
- the sense of chaos and insecurity without computers, their low cost, the opportunity to attack anonymously due to non-specific location make information warfare and information terrorism attractive;
- the means to disrupt or destroy digital equipment are relatively inexpensive, easily smuggled from one place to another, can be used from a distance, and are virtually untraceable.

An unintended consequence of the technological developments is the emergence of new opportunities for terrorists. Because the risk of detection is low, and the risks of apprehension and punishment are even lower, a cyber-space attack can be cheap and rather risk-free. Although less sanguinary, such information warfare type of attack may cause much greater impact.

Furthermore, the aim of terrorism is not to destroy the enemy's armed might, but to undermine his will to fight. *Designed to be feared, terrorism is perceived as being random, incomprehensible and uncontrollable*. These features are in the fundament of its real power. Terrorism warfare is shifting more and more toward civilian targets. Potential targets of cyberterrorism are banks, international financial transactions and stock exchanges, traffic control systems, medication formulas at pharmaceutical manufacturers and power grids. The logic of NII activities makes possible the deliberate abuse such as theft of services and assets, acquisition or alteration of data, corruption or disruption of data in storage or motion, disruption of information services.

Essence of IW

War is a human contest that rewards innovation, learning, adaptability and flexibility. The changes in human society as a whole will entail changes in the way to wage war. The latter are characterised by the use of overwhelming force and a search for technological advantage that is not guaranteed at the commencement of hostilities. IW is a new wrinkle in the geopolitical game -- a game presumably impossible to be prosecuted in terms of the national and transnational architectures already established.

In the current military establishment information warfare is the hottest term used as if it were indicative of something precise and analysable. Information warfare could be defined as "actions taken to achieve relatively greater understanding of the strengths, weaknesses, and centres of gravity of an adversary's military, political, social, and economic infrastructure in order to deny, exploit, influence, corrupt, or destroy those adversary information-based activities thorough command and control warfare and information attack." [11]

The precise meaning of IW is elusive, in part because it describes a wide range of seemingly unrelated phenomena. A central obstacle to a future information warfare capability is that the words and definitions currently used among the armed forces to guide future development in IW are unclear, confused, and often contradictory. For some defence analysts, IW refers primarily to the military application of computers and other information technologies, and the implication for the military establishments of organisational, operational and doctrinal changes. For other writers IW is a much broader idea, relating to the emergence of "Information Age" civilisation and the development of associated modes of political and social conflict which point toward the gradual erosion of nation-states and their monopoly of organised violence.[12]

While information systems are still subject to "territorialisation," *space within modern communication and computing environments is effectively non-metric,* i.e., its dynamics are unlike that of the physical space. Information defies constraint by parameters such as unique locus or finite production. This means that most space-related laws of all previous functional spaces would not apply to "digital" systems. The latter have lower replication costs of agents than execution costs, which makes them dramatically different from all systems more essentially embedded in their physical substrates. As a result, the means for leveraging one's own interests, e.g., tools, tactics, etc., in the information realm will be (or at least can be) qualitatively different from the means applied to leverage the physical space. Another reason for such a focus is that the degree to which warfare becomes innate to everyday life will be directly proportional to the degree to which warfare is conducted exclusively within the information realm. For IW negative experience could not be pre-played in an abstract form, i.e. *time cannot be reversed or compressed*. Another difficulty in information evaluation is generated by the *irregular scale frame of causality*.

Advances in surveillance, communications, and information-processing technologies are all driving the *"Military-Technical Revolution" (MTR)*.[13] Modern society has real-time demands for immediacy. It is required by the change in the range of potential military operations and the constraints consequent of both downsizing and the ever-increasing costs of traditional platforms. In future operating environments marked by ambiguity, speed, and precision effect information warfare breaks the platform-to-platform long-range strategic thinking.[14]

MTR creates the possibility of charging the "information loop of warfare" with unprecedented accuracy and speed, thereby sometimes a possibility of achieving *"information dominance" (ID)* over less capable adversaries. ID is the capability to reshape organisations and revise strategies based upon a systematic analysis of the opponent. ID is the ability to identify vulnerabilities and *centres of gravity* of an enemy, a competitor or even a customer. Where there is cohesion, the analogy of the centre of gravity can be applied.[15] The first characteristic of a centre of gravity is that it remains the enemy's principal strength. The second characteristic of a centre of gravity is that each enemy has only one of them, at least at each war level. The third characteristic of a centre of gravity is that it is the most important one for a given war level and normally depends on the nature of the war itself. A fourth characteristic of centres of gravity is that to some extent they are limited or defined by strategy. ID is achieved by transforming knowledge into capability. The first task in planning for a war is to identify the enemy's centres of gravity, and if possible trace them back to a single one. The proliferation of information technologies has led to the impression that information is itself a centre of gravity. The goal of ID is greater understanding, not total understanding. [16]

Another related concept is that of *Dominant Battlespace Knowledge (DBK)*. In a conventional war, the benefits of DBK are that it removes uncertainty as to whether an attack is underway; gives the location, composition, and status of the attacking units; ensures sufficient knowledge on friendly units.[17] The major problems of achieving *dominant battle space knowledge* are of organising information storage or processing and factorising the decision making. DBK would allow the military to change from a vertical, serial, hierarchical decision making to flattened, parallel, virtual decision making and still be able to turn inside out any potential adversary's decision making loop. A possible exploitation of functional vulnerabilities could be reduced if DBK is built on decentralised decision making.

DBK assumes higher level of situational awareness. Situational awareness has different dimensions, gives the time horizon and the nature of the resources likely to be available, but *"total" or perfect situation awareness is beyond our reach.*

Information about phenomena dynamics deals with dependencies and their thresholds. Dependencies are dynamic and have thresholds. Since the MTR is seen as a long-term process that presupposes threats which have not yet materialised, its relevance to current defence needs is open to question. DBK alone is meaningless. The gap between DBK and actual targeting may require additional local information, man-in-the-loop, or very intelligent weapons with terminal guidance capability. Technology may be pursued to create a force multiplier, but it can also limit opportunity for the development of new ideas or for societal change. Enforced trust in machine data and operation in real-time places human judgement secondary or out of loop entirely.[18]

Information warfare will provide an essential component of the global presence through which national security objectives will be met.[19] As a preliminary step in a state versus state conventional conflicts IW will most likely be used to negate the opponents' weapons-of-mass-destruction, impair their command and control, attack their industry, financial systems, and run propaganda campaigns. This sort of conceptual warfare model by a Pareto simplification is a force multiplier in achieving the intent or mission. Information technology multidimensionality blurs traditional boundaries, changes the whole vision of military operations. *Combat is increasingly assuming the pattern of a continuous flow* rather than a sequence of moves and counter moves. Unlike conventional ways, IW defies the military principle of mass. Its primary objectives are control and paralysis. In future information wars, virtual reconnaissance, strike, and defence would be co-ordinated in battles fought as "meeting engagements" where both sides are on the offence.

Sometimes the narrow margin for the "victory" is based on a very small differential of talent, performance, or luck. It is the relative performance in the above mentioned activities which makes being "the second-best" (even at lower cost) inadequate. The relative and differential advantage in information, information processing, communications and information security will provide for *asymmetric strategic response* [20] often in the form of Information Operations (IOs).

Information operations' use should be conditioned by operational, organisational, legal, and moral factors. Among the vexing issues is the intellectual separation of the use of force or IO among nation-states, from that in the context of interpersonal relations. IOs can be conducted by other than military means. Some information operations do not involve the use of force: psychological operations, applications of deception, a variety of computer "code bombs," viruses, and "chipping." The more routine "information operations" like "counter-terrorism" can be understood as self-defence not involving use of force.

Unlike economic actions, sanctioning the activities of other states, generally considered as slow-acting and blunt information operations can quickly impose severe damage with low levels of violence. Recently IOs have tended to be judged by the following guidelines governing the use of force: necessity, discrimination, proportionality, and humanity. There have been no specific arms control agreements directed at limiting IOs. In fact, however, with its emphasis on confidence-building measures and operational transparency, arms control has acted to hobble effective information operations. Whether IOs that involve civilian satellite systems are always to be regarded as "non-peaceful" is a fundamental issue that has not yet been settled. It is difficult even to articulate a moral code in such circumstances, let alone to follow one consistently. If, no sort of IO can be brought out from under the "use of force" mantle, for a country with the great capability to conduct information operations, this would forfeit what could be a decisive advantage in peace, crisis, and war.

Information operations have both offensive and defensive aspects and should be fully integrated into overall national security policy. In peacetime they can contribute to the prevention of conflict, or they can be used to respond to crises and overt hostilities. In times of crisis, information operations can be employed to resolve disagreements, fortify deterrence, or prepare for the possibility of open conflict. In war they can directly achieve strategic, operational, and tactical objectives or underwrite other means to achieve such objectives.

Means of Conducting IW

They include: electronic warfare; military deception; physical destruction; security measures. Offensive and defensive information operations can use a common variety of means. The net's functionality without ideology offers prime destructive opportunities. It is a bluff that IW scenarios are being studied at present mostly with an eye toward defense rather than offence. Information technology is being developed by strategic planners both as an offensive battlefield weapon, and as a weapon for "logistics attack." It is designed to disrupt the civilian infrastructure on which an enemy's military apparatus depends. Offensive actions using information operations include those that move information from one place to another, destroy it, promulgate disinformation, and corrupt, degrade, interrupt, or deny data flows without visibly changing the physical entity where it resides. Possible offensive weapons are computer viruses; logic bombs; "chipping"; worms; Trojan horses; back doors and trap doors. Devices for damaging entire systems over a wide area are high energy radio frequency guns, which focus a high power radio signal on target equipment, putting it out of action; as well as electromagnetic pulse devices, which can be detonated in the vicinity of a target system.

Denial •f Service Attacks (DOS) are carried in order to hamper, distort and prohibit access, utilisation, or benefit from material (M) infrastructure (DOS-M). DOS are realised through various forms of warfare which focus on different elements of dependencies in society

Information attack will be employed as an expression of global power made possible through global awareness and global reach.[21] Targeting the information infrastructure (V) IW is rapidly polarising along a massive, sneak (DOS-V/M) attack predominantly as orientation management.

The other direction, *political warfare*, is more difficult to accomplish than DOS attacks. Political warfare creates an alternative social contract and dependency infrastructure and induces their common adoption. This is usually achieved through efforts of subversion, rioting and diversionary diplomacy.

Psychological warfare (psyops) requires a human touch to debase human decisions. Psychological warfare is the attempt to warp the opponent's view of reality, to project a false view of things, or to influence his will to engage in hostile activities. It can be divided up into categories according to their targets: operations against troops, operations against opposing commanders, operations against the national will, and operations designed to impose a particular culture upon another. From a psyops perspective one of the 'problems' of the net is rooted in the users' scepticism generated by their education and experience.

The information revolution has led to information overload, and people respond to this pressure by trying to process messages more quickly and, when possible, by taking mental shortcuts. Propagandists short-circuit rational thought by agitating emotions, by exploiting insecurities, by capitalising on the ambiguity of language, and by bending the rules of logic, i.e. by limited and specifically targeted DOS attacks.[22]

Intelligence [23]

The best weapons, those that make men dangerous, are tools of thought i.e.system analysis, operations research, game theory, cybernetics, general semantics, etc. Iintelligence, is all about information. The more we know about the other side, the more economical our strikes against it can be. Intelligence can be the discovered or acquired variety from espionage and the domain of operations. Cognitive intelligence creates new ways of thinking. The cognitive hierarchy phases are: correlated data becomes information; information converted into situational awareness becomes knowledge; knowledge used to predict the consequences of actions leads to understanding. The act of data gathering should not trigger "Heisenberg's effect" (intelligence gathering effects target). Embedded knowledge is hard, if not impossible, to steal. Operationally speaking, knowledge and understanding of the opposition is the most important sort of information to possess (some even thought it more important to control information regarding themselves over espionage against enemy targets).

For an insurgency to work, there needs to be an alternative social contract and dependency infrastructure established. The net already comprises such a system. Building and testing models is one of the primary functions of the net. This is what makes it such a potent intelligence tool. Game theory can be used to create and test scenarios, for factoring in operational risks and consequences.

Information creates and then degrades *models*. A model is created to answer questions generated by logic. It is artificial and often out-of-date. Models are based on formalization of quantities. During phenomena observations the measured characteristic values become quickly polarised and unstable, even irrelevant to "sound reason", and so new types of numbers are created in an attempt to overcome the paradox. The same is valid for data processing methods. The great obstacle in model construction is the impossibility to create an absolute, universal and final model. This is due to inadequate degree of abstraction based on real observation.

Information mechanisms create new abilities for *deception, blackmail and sabotage*, the creation and manipulation of "truths", through monitoring and manipulating message traffic. Operational organisations will tend to be small, tightly directed, well camouflaged and hard to detect and stop. The information environment can accommodate any number of them 'inside' the same virtual territory. They require a high degree of security and trust- the cornerstone of such relationships is the proper selection of personnel. Weeding out of potential members through a thorough background investigation is possible as never before. The reversal of this process is also important--"legends" can be created and seeded across the relevant databases.

*Counterintelligenc*e must be viewed not as an annoying intrusion but rather as an integral part of the intelligence process. It must focus not only on protecting our own sensitive information, but equally on external efforts to manipulate our collection and analysis. This requires certain openness of mind and willingness continually to balance the conclusions drawn from intelligence with the possibility of deliberate deception by a target. Intelligence analysts who are familiar with the totality of information on a particular topic are often in a position to detect anomalies. This comes from building cognitive models of the objectives, constraints, assumptions, dependencies, patterns, and complexities of your opponent.

In the international community the "slippery slope" of the move to *open source and competitive intelligence* has become one of espionage (by definition espionage is illegal) and sabotage. The net is becoming a well defined entry point to the media cycle. Deliberate sensitive figure manipulation especially in speculative areas like finance, natural disasters, crime and migration extremely hampers noise filtration. The unbalanced presentation and analysis of facts could cause close to fatal deviations in the decision loop.

The net offers unprecedented opportunities for synergism among information-charged paradigm sets like religions, global conspiracies, meta-knowledge, etc.

For intelligence and counterintelligence applications subliminally implanted posthypnotic suggestions and scripts use acoustically delivered and phonetically accelerated posthypnotic commands without somnambulistic preparation of the subject. Additional applications include misinformation dissemination, confusing and confounding leaders during critical decision moments, distorting significance of various facts to sway decisions and actions, behavioural modification and self initiated executions. This technology is used to develop and control spies, political candidates, and other public figures through psychological intimidation, fear and extortion. This technology is the perfect intelligence tool. The subject does not know the source of the technology or the technology itself, the subject has no proof or evidence, only their perception, suffering, and isolation.

Information effects *risk*. For the ease of risk evaluation sometimes the very essence of logic restrictions of the math constraints embedded in the calculation techniques are neglected. The situation analysis is overloaded with psychological and civilisational nuances inconsistent with the embedded calculation technique. This makes the results not-trust-worthy especially for scenarios' crossroads. The societies' multidimensional interactions' non-definable and with a not-fixed topology space of states makes prognosis to surpass a normal challenge. A discussion about the need to use and rely on intuitive para-techniques unrelated to objective schematisation is underway.

Is it possible with responsiveness and efficiency to manage the problem of information synergy and intelligence? In the game of strategies' testing the choosing of the moment to publish/activate pieces if information rarely coincides with the moment of data assessment. Parallel intelligence cells and multi-level not-contacting functional scenarios, tightly compartmentalised information exchange and manipulation with archives' secrecy contribute a great deal to the artificially distorted for political aims picture. As a result of the balance among humint, osint, sigint and imint interpretation new *rules for dealing with "floating" fuzzy truth are generated during real time operations*. Maybe a set of not-contacting, and even contradicting variants represent an alternative for an optimal functional medium.

Protection

Albert Einstein once observed "The Lord God is subtle, but malicious he is not." During information warfare, demand for information will dramatically increase while the capacity of the information infrastructure will most certainly decrease. Critical areas in need of protection are: information, communications, electrical power systems, gas, oil, banking and finance, transportation, water supply systems, emergency services and governmental services.

Is there enough military gain from a concerted attack on the civilian infrastructure to warrant the risks? Considerable interest in the politico-military potential of cyberspace has devolved into planning and acquisition focused on *the integrity of specific nodes* or regions within the realm of perspectives, approaches and tactics. This reduces all of IW to a unimodal defensive posture, i.e. addressing all cyberspace risks through guarding and patrolling those systems within one's own zone of control.

Security and information assurance as it applies to telecommunications in defensive information warfare could be viewed as a classical quality problem. Infrastructure information networks face a lot of *reliability challenges*. Network failures can be classified in terms of the mechanisms by which they are manifested and by their causes. Mechanisms range from chain reactions, in which small faults propagate and result in widespread disruptions, to the direct, independent failure of key components that in themselves represent major disruptions. Causes range from natural disasters to human error, and from equipment failure to deliberate destructive acts by person's intent. From a technical standpoint, these are not different problems; they are different parts of the same problem.

Fragility is an inherent inability, realised or not, to respond to changes in external conditions. In the context of mission accomplishment, fragility is a substantial source of risk, and therefore its identification, reduction and control are critical. Fragility may occur from either the overt actions of the enemy or the natural occurrences which sap energy and resources during the course of military operations. [24]

We theorise about our own information technology vulnerability and then assume it is the same for others. No one really knows how vulnerable is the national information infrastructure. We do not know what *normalcy* in the infrastructure is and how it varies with such things as season, world events, national holidays, etc. We need to establish the "noise level" in the infrastructure--namely, the day-to-day abnormal or accidental events that occur as a matter of routine operation. At the operational level, network intrusions are difficult to detect because they can disguise as legitimate transactions or go unnoticed in a busy network. In many networks today, successful intrusions are more likely to be detected by their effects rather than by any discernible telltale signature.

The propagating *"chain reaction"* failure mechanism is characteristic of complex systems with tightly coupled subsystems. Seemingly inconsequential events trigger an unanticipated multiple interaction of anomalous operating modes among subsystems. The problems can be exacerbated by the very features and procedures intended to protect against failures. Systems should be designed to be redundant and to fail gracefully rather than catastrophically.

Little evidence exists of *recovery or protection synergy* which cuts across sectors under attack. It is usually necessary to find specific defences against specific attacks. These defences, in turn, become targets for future attack. Currently there is much about this threat that is not known. Currently, the security solutions lag far behind the potential threat. This situation is likely to continue until the threat becomes reality, forcing a reassessment of the preventive measures.[25]

Surprise works because it hits from unexpected directions, forces an unexpected and disruptive phase-change with the attendant loss of coherence while re-orientation is taking place. In information operations, as in terrorism, the possibility exists that a devastating attack will be made without the perpetrator being identified. Even if an attacker can be identified, questions arise about the proper form of retaliatory action. Such questions enervate deterrence by reducing the certainty of retaliation. If one can formulate no appropriate and effective form of retaliation, one is obliged to rely on deterrence by denial. Moreover, because information operations can take place at very high speed and without warning, the implications of surprise are potentially serious at all levels of information warfare. If this distinction about the operational acceptability of information operations is recognised, decision makers must assess the possibilities for the adversary to retaliate, and also they must determine whether they can defend against or tolerate that retaliation.

There are indications that, in order to avoid the inevitable difficulties, superpowers try to test the possibilities of a strategy that shapes the environment. In its preliminary stages the basic efficiency paradigm is suspicious.

We do not possess the omnipotent assessment-decision tools to steer an opponent via ID. Thus, against an adversary dealing with the most ambiguous defence topics, a pre-emptive, quick and simultaneously applied *full-spectrum strike* focused on the very sensitive points of control should not be ruled out, too. The resulting stress for the decision makers could lead to time-disruptions and errors in the planning phase, logic deficiency, paralysis and subordination of will.

Defence-in-Depth is an approach to design, implement, and operate where each and every component, system, subsystem, process, procedure, etc. is looked at to see what threat could occur at that level, and then addressing the threat at that level. The targets' spectrum ranges over international political and economic competition, military operations other than war, crises, overt conflict, termination of conflict, and restoration of normal political and economic competition. Defensive actions seek to protect one's own information frame from similar actions of an adversary and to avoid promoting paranoia and the resulting dissipation of responsibility.

The threat of massive disruption through information warfare has been posited as a potential successor to massive destruction by nuclear warfare. General *deterrence* stems from maintaining the capability and will to inflict severe damage in retaliation against adversaries. Its effectiveness relies on the presence of an arsenal of tangible capabilities. "Focused" deterrence operating by threat of punishment of identifiable targets is "stronger" than general deterrence. Aside from punishment, general deterrence based on very strong defences can work through denial. Since no defence is stronger than its weakest point, the ability of open societies to deter an information attack by a strategy of denial always will be uncertain. Deterrent to information warfare could be economic interdependence, fear of escalation, lack of technical expertise (it is the weakest factor and is eroding fast).

Protection is to be sought through:

a) *Degree of access*. Technology, and especially information technology, is best understood in its societal context. Can the operational utility of the net be limited? People represent both the strongest and the weakest links in the reliability chain. An enemy "mole" with precise and accurate knowledge and understanding of how decisions to respond to a crisis are made and how information is passed within the military might get inside the cycle and do real damage.

Attacking a system whose interfaces are publicly available and thus well-understood is far easier than attacking a system whose parameters and interfaces are proprietary trade. For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. Although 95 percent of US DOD unclassified communications depend on the NII, *the net is rarely used for mission-critical tasks*. An attack on the NII, that left an opening for strategic mischief, could be far more damaging than one that merely caused damage. Co-ordinated cyber attacks are focused, organised, and carefully calculated to yield a specific outcome. The case for assigning cyberspace defence to the DOD arises from the prediction that cyberspace attacks could become the predominant feature of 21-st century warfare.

The net is not the sort of place that can be 'occupied' in a military sense. It could be shut down, but nobody can 'take' the net and hold or police it. The technologies to re-establish it, even in a covert form, are spread enough to make an 'official' shutdown improbable. *For the net to exist, it has to remain freely accessible.* No good alternative exists to having system owners attend to their own protection. Government restrictive regulation of cryptography removes the technology from the legal users, since it is a defensive technology, not an 'armament' as many wish to classify it.

IW opens new opportunities for bureaucrats and "black" programs. The *"privacy versus encryption"* discussion signals that society does not trust the government to fight terrorism. At its extreme end some people are afraid of an elite-sponsored form of new world order imposition attempt.

b) *Resources spent on sophistication*. Infrastructure information networks are inherently dependent on *software.* Every software performance enhancement carries the possibility of introducing logical errors, undoing previous algorithm corrections, changing software and timing performance. It is even possible for malicious code, deliberately and surreptitiously included in critical software during production, to go undetected in installation. All these can increase system vulnerabilities. Competition can pressure developers to rush software to market without sufficient testing. Software-developing companies are increasingly contracting with others, i.e. system integrators are left with little insight into the development and validation of critical control software. Long-term maintenance of software is made difficult by changing preferences in programming languages and lack of support tools for obsolete or orphaned systems.

Some innovations carry new security risks, but the emphasis on adopting today's security practices may keep systems astray from taking advantages of tomorrow's innovation. In security, the primitive is often superior to the sophisticated, but the complexity of systems often constitutes in itself a barrier to attack. A system that is easy to abuse in one way may be difficult to abuse in another. *Heterogeneity* makes co-ordinated disruption harder to achieve and preserves alternative paths. Even insiders can rarely count on knowing how information is routed into a decision. In an age in which hierarchical information flow is giving way to networked information flow, the importance of any one predestined route is doubtful.

Threats to the infrastructure are challenging existing boundaries between the national defence, intelligence, law enforcement, and regulatory roles of the government. Clarification of missions, responsibilities, and authorities in this new context are needed, and will necessarily involve all the executive, legislative and judicial branches of government.

International law is currently ambiguous regarding criminality and acts of war on information infrastructures. In political science, national security studies have been divided into realism and liberalism. Reality needs non-lethal approaches, reversible effects, keeping open the channels of communication and opening up pathways to conflict resolution. Global liberal institutions and agreements would be a step in the right direction. There isn't any traditional way to dominate, control, protect in the IW space. An alternative, or at least partial, essence core should be integrated amidst the background-level noise, i.e., kept as a back-up copy out of view and reach. Maybe a simplification of clearance procedures will increase security effectiveness. However, we must always accept the realist presumption that information warfare in one form or another is inevitable.

Prognosis

Parallel with IW a new form of "Low Intensity Conflict" emerges. Human tragedies will be used to camouflage truth in power games (e.g. Caucasus, Balkans). Simple facts will be of no help to reconstruct even a possible causality. The technology-empowered media and the proliferation of personal information/communication devices will have the effect of limiting the practical ability of casualty-adverse democracies to engage in combat for much more than a couple of weeks (e.g. UN/US/ "human rights" activities in Africa). Planners for information-age conflicts ought to consider, therefore, training and equipping forces for extremely intense, hyper- or *"blitzkrieg" style warfare flow of combat operations* (e.g. US Marines).[26]

"Low Intensity Conflict" operations cause failure of parts of a dependency infrastructure. Guerrillas and terrorists operate beneath low-intensity conflicts' "sophistication threshold." Especially in the post-Cold War context, few of the small wars currently engage the vital interests of major powers or seem likely to bring about immediate changes in the international balance of power. War represents the most imitative activity known to man. In order to wage low-intensity conflicts with any hope of success, conventional armies may have to adopt the organisational methods, and perhaps even the mentality of their opponents. *Distinctions will thus erode* between military and police forces, and ultimately among soldiers, terrorists and criminals who are responsible for combating.

While forecasts of a *"coming anarchy" or "clash of civilisations"* may be overdrawn now, war in the Information Age could well spill outside of the Clausewitzian framework where it functions as a "rational" instrument of state policy. Different cultures have shaped war into bizarre and self-destructive forms whose warrior practitioners, unlike modern soldiers, often looked upon combat as a means of self-expression, recreation or religious sanctification. Such peoples are hardly the type to capitulate solely as a result of the "bloodless" information warfare techniques touted by so many as the future of war following the purported "revolution in military affairs".

Information-age warfare will likely see both new techno-weapons and more traditional arms used in *innovative and unexpected ways*. Enhanced communications can release potent psychological energy to produce violent results. It is dangerous to underestimate how significantly emerging technologies will empower warrior peoples. This kind of technology does not depend upon the physical presence of foreign military trainers who might otherwise be able to influence and moderate warrior societies' actions. Some adversaries may abandon whole classes of weapons that require highly trained operators in favour of fully automated, easy-to-use systems. By using technology to replace the intellectual achievement that could previously be obtained only through laborious and time-consuming courses of study, the combatants on future battlefields will become much more equal than has historically been the case.

All generations of warfare coexist, because technological transformation does not occur everywhere simultaneously. As society has become more complex (not even modern), the traditional means for society to police itself have become susceptible to new frailties which at least complicate, and possibly compromise, maintaining that society (e.g. IRA, ETA; Indonesia).[27] In a post-Clausewitzian world war couldn't be clean and short which makes high-tech armies' effectivity doubtful (e.g. US anti-drug campaign in Latin America).

Conclusions

Instead of unrealistic and quixotic seeking of ID on tomorrow's battlefield, the focus must be on developing doctrine and strategies for operating in an environment of "information equality" based more on "information fuzziness" than on partial "information transparency". A main feature will become operation in the obscurant boundary region between real and often not-understandable phenomena and dominating bluff. *The optimal aim should be to try to keep a full-scale and range contact with the environment in order at least to define a set of questions for the observed puzzle.*

Notes:

1. Deyan Gotchev, "IC3 – The Informativeness of the Conflict-Crisis-Catastrophe Trad," *Information & Security: An International Journal* 1, 2 (Fall, Winter 1998), 43-55.
2. Alexander Chislenko, "Automated Collaborative Filtering and Semantic Transports" < *sasha1@netcom.com* >; Michael Wilson, "Infrastructural Warfare," *Presentation at the receipt of 1997 Sun Tzu Award from the US NDU*, Available at http://www.7pillars.com/
3. John H. Gibbons, Assistant to the President for Science and Technology, *Cybernation - The American Infrastructure in the Information Age. A Technical Primer on Risks and Reliability* (Office of Science and Technology Policy, Executive Office of the President, internal date April, 1997, embargoed until November 12, 1997); *NII Security: The Federal Role* (Office of Management and Budget, 1995).
4. Robert R. Tomes, "Boon or Threat? The Information Revolution and U.S. National Security," *Naval War College Review* 53, 3 (Summer 2000), 39-59.
5. R. H. Anderson and A. C. Hearn, *The Day After in Cyberspace II,* RAND report MR-797-DARPA (Santa Monica, CA: RAND Corporation, 1996); "Science and Technology Assuring Our Preparedness and Improving Global Stability", in *National Security and Global Stability* (Washington, DC: The White House), Chapter 3.
6. Alexander Chislenko, *Some Thoughts on Multi-agent Systems and Hypereconomy* (1997).
7. Alvin M. Saperstein, "War and Chaos," *American Scientist* 83 (November-December 1995), 548 - 555.
8. Nick Kotz, "Mission Impossible," *Washingtonian* (December 1995), 145.
9. Sir Leon Brittan, "EU Pursues Global Answers: International Economic Instability is New Threat," *Defense News* 10, 48 (4 December 1995).
10. Matthew Devost, "Political Aspects of Class III Information Warfare: Global Conflict and Terrorism," *Second International Conference on Information Warfare* (Montreal, Canada: January 18-19, 1995); Barry Collin, "The Future of CyberTerrorism," in *Proceedings of 11th Annual International Symposium on Criminal Justice Issues* (1996). Available also at http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm; *Patterns of Global Terrorism* (Washington, DC: United States Dept. of State, 1996).
11. Randall Whitaker, *Information Warfare* (Umee: Institutionen för Informatik Umeå Universitet, 1998); Todor Tagarev, "Evolution of the Notion of 'Information War'," *Military Journal* 105, 3 (1998), 80-86.
12. Gunilla Ivefors, *Defeat the enemy before battle - a warfare revolution in the 21-st century?* (October 22, 1996). Available at http://www.ida.liu.se/~guniv/Infowar ; D. Magsig, *Information warfare will dominate 21st century conflict* (1995). Available at http://www.seas.gwu.edu/student/dmagsig/infowar.html.
13. William Owens, "The Emerging U.S. System of Systems," *Military Review* 75, 3 (May-June 1995), 15-19.
14. Michael Mazarr, et. al., *The Military Technical Revolution - A Structural Framework* (Washington, D.C.: Center for Strategic and International Studies, March 1993).
15. *DOD Dictionary of Military and Associated Terms*, Office of the Joint Chiefs of Staff, Joint Publication 1-02 (Washington, D.C. 1984), 188; Carl von Clausewitz, *On War*, eds. Michael Howard and Peter Paret (Princeton, N.J.: Princeton Univ. Press, 1984), 595-6, 617-9; Lisa Bennett and Bruce Niedrauer, "Center of Gravity," *Military Intelligence Professional Bulletin* (April-June 1995), 25; William W. Mendel and Lamar Tooke, "Operational Logic: Selecting the Center of Gravity," *Military Review*, (June 1993), 25.
16. Owen Jensen, "Information Warfare: Principles of Third-Wave War," *Airpower Journal* 8, 4 (Winter 1994), 35-

43; John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review* 22 (Summer 1994), 24-30.

17. Stuart Johnson and Martin Libicki, eds., *Dominant Battlespace Awareness* (Washington: NDU Press, 1995).
18. Paul Bracken, "The Significance of DBK," in *Dominant Battlespace Awareness,* ed. Stuart Johnson and Martin Libicki, (Washington, DC: NDU Press, 1995), pp. 51-65.
19. For a comprehensive study of one particular aspect the reader may refer to Robert D. Critchlow, "Whom the Gods Would Destroy: An Information Warfare Alternative for Deterrence and Compellence," *Naval War College Review* 53, 3 (Summer 2000), 21-38.
20. Richard Szafranski, "A Theory of Information Warfare. Preparing for 2020," *Airpower Journal* 9, 1 (Spring 1995), 56-65.
21. George J. Stein, "Information Warfare In 2025," A Research Paper presented to *Air Force 2025* (Air War College, August 1996). Available at http://www.au.af.mil/au/2025/volume3/chap03/v3c3-1.htm.
22. Aaron Delwiche (March 12, 1995) < *redwood@u.washington.edu* >.
23. John Deutch, "Remarks at CIA Town Meeting," < *http://www.odci.gov/cia/public_affairs* >, (May 11, 1995); John M. Deutch, "Speech at NDU", < *http://www.odci.gov/cia/public_affair* > (June 14, 1995); James Woolsey, on NBC, "The Future Director of Intelligence," *NBC News Transcript* (July 18, 1994), 3.
24. Carl von Clausewitz, "Friction in War," Chapter Seven in Book One of *On War*, eds. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1984).
25. Thomas P.M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *Proceedings of the U.S. Naval Institute* (January 1999). Available at http://www.usni.org/Proceedings/Articles99/PRObarnett.htm.
26. Richard Chilcoat, *Strategic Art: The New Discipline for 21st Century Leaders* (Carlisle, PA: U.S. Army War College, 1995).
27. Charles William Maynes, "The World in the Year 2000: Prospects for Order or Disorder" in *The Nature of the Post-Cold War World* (Carlisle, PA: U.S. Army War College, 1993).

The volume of IW literature is growing quickly. Besides this rapid growth, the duplication of materials among diverse venues (both print and electronic) makes it difficult to track the field. This set provides a compilation of materials established as authoritative sources and reference base for the student of Information Warfare:

- David Alberts, *The Unintended Consequences of Information Age Technologies*, Directorate ACTS (Washington, DC: NDU Press, April 1996).
- John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Foreword by Alvin and Heidi Toffler (Santa Monica, CA: RAND/National Defense Research Institute, 1997).
- John Arquilla and David Ronfeldt, "Cyber War Is Coming!" *Comparative Strategy* 12 (April-June 1993), 141-165. Available at http://www.stl.nps.navy.mil/c4i/cyberwar.html.
- "Operations," *U.S. Army Field Manual 100-5* (Washington, D.C.: 20 August 1982), Available at < http://www.psycom.net/iwar.1.html >

- *Report of the Defense Science Board Task Force on Information Warfare--Defense (IW-D),* Defense Science Board (Washington, DC: Office of the Secretary of Defense, November 1996).
- Reto Haeni, *An Introduction to Information Warfare* (Washington DC: School of Engineering and Applied Sciences, George Washington University, December 1995). Available via WWW at: http://www.seas.gwu.edu/student/reto/infowar/info-war.html
- Roger Molander, Andrew Riddle and Peter Wilson, *Strategic Information Warfare -- a New Face of War* (Santa Monica CA: RAND Corporation, 1995).
- Stuart Johnson and Martin Libicki, eds., *Dominant Battlespace Awareness* (Washington, DC: NDU Press,

1995).

- *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, US GAO/AIMD 96-84 (Washington, D.C.: General Accounting Office, May 1996).
- *The National Information Infrastructure Protection Act* (1995).
- Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunders Mouth Press, 1995).

DEYAN GOTCHEV: Born 1955. M.Sc. (1980, Physics of the Earth, Atmosphere, Space) from the Sofia University "St. Kliment Ohridski". Research Fellow (1989, Active Experiments) in the Space Research Institute of the Bulgarian Academy of Science. Author of over forty publications in solar- terrestrial physics, synergetics, non-linear dynamics, torsion fields, and fuzzy systems. Besides publications in the mentioned areas, he has authored a couple of papers on crisis management and other interdisciplinary topics. Address for correspondence: Space Research Institute-Bulgarian Academy of Science; Sofia 1000 P.O.Box 799, Bulgaria. E-mail: dejan@space.acad.bg.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Kaleidoscopic Approach to Security Shadows in the Age of Information

Deyan Gotchev

Keywords: Information warfare, asymmetric response, cyber-terrorism, information infrastructure vulnerability, psychological warfare.

Abstract: Information defies constraint by unique locus or finite production, i.e. space-related laws of functional spaces would not apply to "digital" systems. Information Warfare (IW) is impossible to be prosecuted in the established terms of national and transnational architectures. It is the next stage in evolution of attitudes toward authority. Security in the age of information warfare will be characterized by operations in the obscurant boundary region between real, often incomprehensible phenomena and dominating bluff. The opponents of future battlefields will become much more on a par. In an asymmetric strategic response the "victory" is based on a very small, or fuzzy differential of talent, performance, or luck.

Author:**Andrew Borden**
Title: **The Dialectics of Information - A Framework**
Year of issuance: **2000**
Issue: **Information & Security. Volume 4, 2000**
Hard copy: **ISSN 1311-1493**

THE DIALECTICS OF INFORMATION - A FRAMEWORK

Andrew BORDEN

Table Of Contents:

Introduction
The Shannon-Hartley Theorem
The Capacity of a Decision Making System
The Analog of the Shannon-Hartley Theorem for Decision Making Systems
Quantifying Mutual Information
The Dialectics of Information
Conclusion
References

Introduction

The dialectics of Information applies whenever there is a human conflict or competition in which information:

- Is a commodity that is not shared
- Is subject to attack

Three examples are:

- Military Command and control
- The game of bridge
- The banking industry

In the first example, attacks on the adversary’s information are commonplace and the need to protect friendly information is recognized.

In the second example as well, a good player will convey as much information to his partner as possible while concealing it from the opponents. Consistent with the rules of the game, providing misleading information is even allowed by playing an unusual card (false carding).

In the third example, protection of friendly information against attacks is recognized as critical to business success, but the attacks themselves are usually unethical, if not illegal. Exploitation of a competitors information is equally important, so data privacy is a critical element in the banking industry.

The purpose of this paper is to present a generic, domain-independent framework for the information dialectic and to show how the framework can be applied to any selected domain. The program for doing so is straightforward:

- Define the generic tasks relevant to the development of information
- Identify the generic types of attack that can be mounted against these tasks (Identify Attack measures)
- Show how the performance of the tasks can be protected against these Attack Measures (Identity Protect Measures)

This framework will be developed in the context of an analog to the Shannon-Hartley channel capacity theorem.

The Shannon-Hartley Theorem

The Shannon-Hartley Theorem is one of the most elegant mathematical results of the twentieth century. In the proof, signal and noise are represented as an infinite dimensional vector in Hilbert Space. The proof also uses a simple, but little known fact from geometry…that the mass of an n-dimensional sphere migrates to the surface when the number of dimensions increases. The proof of the theorem relates these ideas from physics and geometry to the very abstract mathematical characterization of Information. The theorem is as follows:

$$C = W * LOG_2 (1 + S/N) \qquad (1)$$

W is the bandwidth of a signal being transmitted over a noisy communications channel. S/N is the signal to noise ratio. C is the Channel Capacity, measured in bits per second. We are guaranteed that there exists a way to code information so that it can be transmitted at a rate arbitrarily close to the Channel Capacity over this noisy communications channel.[5]

Channel Capacity can be used as a unifying principle for Electronic Attack (EA) and Electronic

Protect (EP) Measures in Electronic Warfare (EW). Every EA measure except Exploitation is an attempt to reduce the bandwidth of an adversary signal and/or to reduce the Signal to Noise Ratio. Every (EP) Measure (except Protect measures against Exploitation) is an attempt to increase bandwidth and/or increase Signal to Noise Ratio. For example, communications frequency hopping as an EP measure uses a large total bandwidth to protect against Jamming, but a small instantaneous bandwidth to protect against interception and Exploitation. The large total bandwidth in this case makes it difficult for the jammer to set on the transmission frequency, thus preventing a reduction in Signal to Noise Ratio.

For another example, repeater or gate stealing EA techniques must achieve a certain reduction of Signal to Noise ratio within the bandwidth of the victim signal to be effective. The corresponding EP technique might utilize a combination of guards and filters to recognize and eliminate the unwanted jamming signal, thereby protecting the signal to noise ratio.

Against Exploitation, a very large bandwidth with low average power might be used. The low average power reduces the probability of intercept, but the energy over the large bandwidth can be summed to extract the information from the signal. Therefore, the transmitter compensates for the low signal to noise ratio with increased bandwidth to transmit information at a fast enough rate. The jammer can only achieve high signal to noise ratios over small portions of the bandwidth.

The use of the Shannon-Hartley channel capacity formula as a unifying principle in EW is a useful device when teaching the subject. It gives the students a number of logical pegs on which to hang their collective hats. It is only useful however, because the Shannon Hartley theorem has provided such an elegant and simple way of determining the Channel Capacity.

The Capacity of a Decision Making System

It is tempting to think of decision making in the presence of uncertainty as analogous to attempting to send information through a noisy-communications channel. When doing a decision making problem, we are attempting to classify an event or object as one of a number of recognizable events or objects. There is an initial amount of Entropy or uncertainty based on the *a priori* probability distribution. If we look at one attribute of the object being studied and compare it to the data base, we may be able to reduce the Entropy. The percent reduction in the entropy is the Signal to Noise ratio for this attribute. The number of bits by which the Entropy is reduced divided by the time it took to evaluate the attribute is the decision making channel capacity for this attribute (bits/second).

Presumably, we have used the most efficient Entropy reducer first. If it doesn’t solve the problem completely, we now have to evaluate the remaining entropy reducers (attributes) and use the one which is now most efficient. We continue recursively until the Entropy is reduced enough so that the probability of one event or classification exceeds the required confidence threshold. If we use all attributes and cannot reach the confidence threshold, the decision making system has failed for this object (event).

This process of designing an efficient decision making system can be summarized as follows:

- Compute the (information) Channel Capacities of all the available attributes, taking into account the current Entropy and the attribute values which are already known.
- Pick the available attribute with the best (information) Channel Capacity
- Measure this attribute
- Compare the result to the data base. (Note: This changes the (information) channel capacities of all the remaining attributes since they are not independent)
- If done, report
- If not done, go back to the first step

For example, experience tells us that Pulse Recurrence Interval is the most efficient uncertainty reducer when attempting to identify a radar. It will be used first, then the remaining best Entropy reducer, probably frequency, will be identified and used. This procedure is repeated until the confidence level is reached or until the process fails.

This procedure is analogous to using one noisy channel, re-evaluating, using another noisy channel, etc. Each branch in the decision tree leading to solutions uses a different sequence of attribute measurements. Unfortunately, there is no analog of the Shannon-Hartley theorem to give us an elegant determination of the overall Channel Capacity for this disorderly situation.

The Analog of the Shannon-Hartley Theorem for Decision Making Systems

In the place of the Shannon-Hartley Theorem, we use a result from the mathematics of information [4]:

$$I(\text{Situation} \mid \text{Observations}) = H(\text{Situation}) - H(\text{Situation} \mid \text{Observations}) \qquad (2)$$

H(Situation) is the initial amount of uncertainty (bits) in the problem to be solved. H(Situation | Observations) is the amount of uncertainty (bits) remaining after the decision making system has been used. Therefore, I(Situation | Observations), the Mutual Information of the decision making system in this situation, is the expected value of the amount of uncertainty that has been removed by the decision making system. (See Reference 4 for a complete discussion).

Formula 2 seems a most unsatisfactory substitute for the Shannon-Hartley theorem. (data) bandwidth and Signal to Noise ratio do not appear explicitly in the formula. With no elegant computational formula, it seems impossible, practically speaking, to use it for real problems. The solution to this dilemma is to substitute computing power for elegance.

Quantifying Mutual Information

Finding the optimal Decision-Making System (DMS) under the circumstances we have described is an uncommonly difficult type of problem called NP-Complete. By accepting a slightly sub-optimal, but demonstrably good, design method, we can develop a natural, formal method for building very efficient DMS's. The computations required are still formidable, but manageable if the problem isn't too large.

The computational difficulty is the down-side, but the corresponding advantage is that the computations enable the user to compute the (information) channel capacity as given in Formula 2. As when using the Shannon-Hartley formula, the designer specifies a confidence level and provides a data base and a capability to measure the values of a number of attributes. Presumably, each measurement has a cost in time. The noise (ambiguity) is inherent in the data base and is usually not under the control of the designer. For the attributes specified by the designer, the (information) Channel Capacity is a natural product of the design process. Response time and confidence level actually achieved are also available. The probably of a successful response and the conditional probability of a correct response are also provided.

The Mutual Information is a performance measurement very like the Shannon-Hartley channel capacity. It only has meaning however, if a standard, formal method is used to design the DMS. This method, and some experiments using it, were described in this journal.[1,2,3]

One of these experiments involved identifying a radar coming from a population of five radars. The Table contains the performance results for the best achievable DMS using the data base and measurement capabilities used in the problem.

Initial entropy (bits)	Final entropy (bits)	Entropy reduction (bits)	Mean time to classify (seconds)	(Information) Channel capacity (bits/second)
1.96	0.35	1.61	0.87	1.85

Based on the assumed *a priori* distribution of radars, the initial entropy is 1.96 bits. The conditional entropy (the final term in Formula 2) is 0.35 bits. Dividing the Entropy reduction by the mean time required gives the rate of entropy reduction in bits per second. This number means very little when taken out of context. However, a designer of Radar Classification algorithms would become very familiar with it and would have a pretty good idea of what (information) Channel Capacity would be good enough to meet operational requirements. If not good enough, the designer would attempt to improve it by increasing the (data) bandwidth (finding more parameters to measure and evaluate). Alternatively, the designer can state a requirement for higher quality data with less noise (ambiguity).

The Dialectics of Information

There are four tasks that must be performed on the information battlefield:

- Collect (data)
- Move (data)
- Store (data)
- Use (data) to perform situation assessment

The Collection task, for example, could be carried out by a search engine that looks for key words and retrieves text that might be relevant to the user's data requirements. Movement can be accomplished, by sending encrypted ASCII characters through a satellite link. Data can be Stored on paper in a filing cabinet or in compressed form on an optical disk.

If a standard method is used to design the situation assessment strategy, then we can give it a report card as shown above. Its performance will depend on the amount and quality of the data (the data bandwidth and the amount of noise). The data is vulnerable when it is being Collected, Moved and Stored. The Attack measures that can be taken against the data are the following:

- Degrade the data (delay or delete some data elements)
- Corrupt the data (add false data)
- Deny the data completely (usually by direct attack on the means of collecting, moving and storing)
- Exploit the data by listening, decoding and interpreting (usually when it is being moved)

An example of degradation against the Collection task would be the use of concealment. The use of dummies would be an example of Corruption against the Collection task. An example of Corruption against the Movement task would be intrusion and spoofing, that is transmitting false data that looks genuine. An example of Denial against the Storage task would be the introduction of computer viruses that damage operating systems, making the computer unusable for Situation Assessment purposes. The specific means for accomplishing Attack measures depend on the means being used to perform the information tasks

Exploitation is different from the other attack measures in that it does not affect the data in any way. It could be regarded as a part of the Collection task, rather than an Attack measure. As such, it would enhance (data) bandwidth and make adversary situation assessment more efficient.

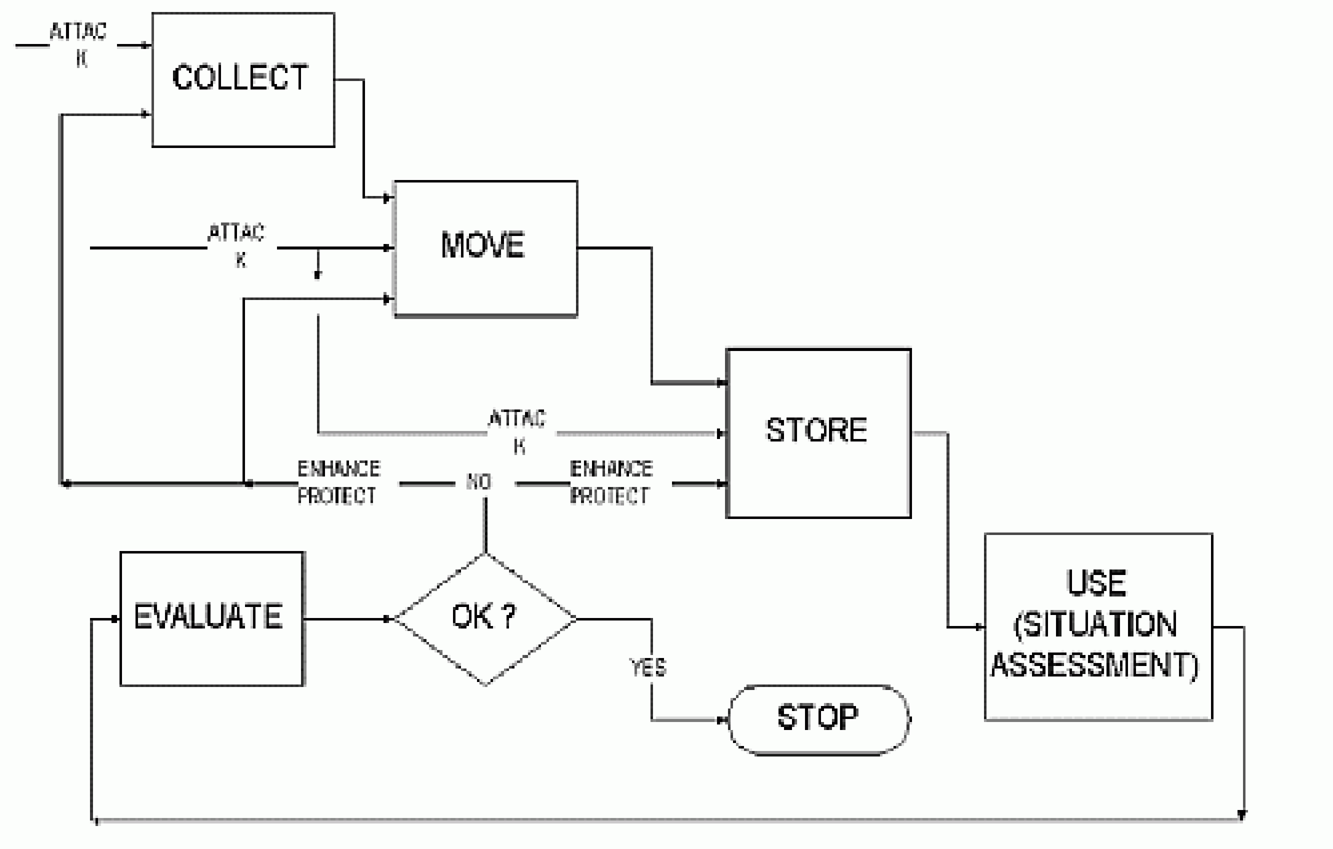

Figure 1. The Information Dialectic

The figure shows the framework for the information dialectic. The information tasks are shown: Collect, Move, Store and Use for Situation Assessment. Situation Assessment using the standard method of strategy design is evaluated for confidence and response time. This can only be done because the standard design method makes a large number of statistics available. If performance does not meet requirements, then the tasks of Collect, Move and Store must be enhanced. Either the (data) bandwidth must be increased by adding entirely new sources of data or the noise (ambiguity) must be minimized by protecting the three data tasks against attack.

The ability to measure the efficiency of Situation Assessment makes it possible to quantify Figures of Merit wherever the information dialectic applies. ..whether in war…in commerce or in contests of skill and ingenuity.

Conclusion

This domain independent framework for the dialectics of information is especially simple. It is only useful however, if the efficiency of the resulting Situation Assessment can be measured. The use of a standard design method for situation assessment strategies makes this evaluation possible.

References:

1. Andrew Borden, "The Design and Evaluation of Situation Assessment Strategies," *Information & Security: An*

International Journal 1, 1 (Summer 1998), 63 – 74.

2. Andrew Borden, "Human Intuition and Decision-Making Systems," *Information & Security: An International Journal* 1, 2 (Fall-Winter 1998), 67 – 72.
3. Linda Elliott and Andrew Borden, "Human Intuition and Decision-Making Systems (II)," *Information & Security: An International Journal* 2, 1 (Winter 1999), 50 – 54.
4. Pierre LaFrance, *Fundamental Concepts in Communications* (Prentice Hall International Editions, 1990).
5. Claude Shannon, "A Mathematical Theory of Communications", *Bell Systems Technical Journal* 27 (1948), 379 – 423, 623 – 656.

ANDREW BORDEN is a retired USAF officer with a long background in developing systems that make decisions, especially in military avionics. His last active duty assignment was as Deputy Chief of Staff for Intelligence, (then) Electronic Security Command. He has worked in industry, in academia and for NATO as Principal Scientist for Electronic Warfare, SHAPE Technical Centre (now the NATO C3 Agency). Mr. Borden is the Chief Scientist of DRH Consulting, San Antonio, Texas. He has advanced degrees in mathematics from Kansas State University and The Ohio State University. His latest research interests are in comparing human and machine-based decision making. Mr. Borden is member of the Editorial Board of *Information & Security*. Address for correspondence: DRH Consulting, 1210 Scenic Knoll, San Antonio, TX 78258; Fax: (210) 497 4581. E-mail: borden@wireweb.net.

BACK TO TOP

The Dialectics of Information – A Framework

Andrew Borden

Keywords: Electronic Warfare, Entropy, Information, Mutual Information, Shannon-HartleyTheorem, Situation Assessment.

Abstract: The Shannon-Hartley Theorem for the information-carrying capacity of a noisy communication channel is an elegant way to unify Attack and Protect concepts in Electronic Warfare (EW). Using this principle, all EW measures can be seen as attempts to increase (reduce) bandwidth or Signal to Noise Ratio. Shannon's Formula for Mutual Information is an extension of this principle to the Information Dialectic in which all Attack and Protect measures are attempts to increase (reduce) Information Bandwidth or Entropy (ambiguity). This characterization of Information Warfare is domain independent and very widely applicable.

Author:**Veselin Tselkov and Dragomir Pargov**
Title: **Information Assurance in C4I Sistems**
Year of issuance: **2000**
Issue: **Information & Security. Volume 4, 2000**
Hard copy: **ISSN 1311-1493**

INFORMATION ASSURANCE IN C4I SYSTEMS

Veselin TSELKOV and Dragomir PARGOV

Table Of Contents:

1. INTRODUCTION
2. A BROADER DEFINITION OF SECURITY
  Definition
  Key words
3. INFORMATION ASSURANCE
  COMSEC Components
  COMPUSEC Components
  Technical Security
  Physical security
  Protect, Detect, and React
4. SECURITY POLICY
  Discretionary Access Control (DAC)
  Object Reuse
  Labels
  Mandatory Access Control (MAC)
  Contents of the security policy
  Practical steps
5. A SYSTEM FOR INFORMATION SECURITY
  Basic functions
  Service functions
  Architectural Security Services
  Protection levels
6. A SET OF REQUIREMENTS
  Data Networks
  An example of Unclassified Enclave
References

1. INTRODUCTION

Information Assurance (IA) should be a key aspect of any C4I (Command, Control, Communications, Computers and Intelligence) architecture and system design. With that fact in mind, this paper develops a broader definition of security, information assurance architecture and a set of policy and implementation recommendations.

Why is security needed? The answer is simple—there is a threat out there and it is real and growing each and every day.

Given the severity of the threat, it is clear that unprotected communications and information systems are at risk. If they are not protected, a country may experience:

- exposure of classified information to unauthorized persons;
- destruction of critical data or, just as bad, loss of confidence in the correctness of the data;
- potential loss of control over military forces.

Finally, the performance of inadequately protected communications and information systems (CIS) can be degraded or reduced to zero at critical points in time by adversaries.

As mentioned earlier, the security threat to C4I systems is real and growing. Although all nations have their own classified estimations of the threats to their systems, here are a few quotes from unclassified sources:

- "More than 120 countries already have or are developing … computer attack capabilities." (US Defense Science Board)
- "It is estimated that the DoD is attacked about 250,000 times a year …" (Defense Information Systems Agency, US Department of Defense)
- "The CSI-FBI Computer Crime and Security Survey of 1996 states that $4.5 billion dollars was lost to businesses by compromises in information security. 42 % of all businesses report that they have experienced attacks." (Computer Security Institute, FBI)
- "Computer attacks have also become easier to carry out due to the proliferation of readily-available hacker information, tools, and techniques on the Internet." (US General Accounting Office)
- "… any marginally computer literate individual can use the Internet itself to quickly obtain basic information on the tools and techniques needed to become a computer hacker." (US General Accounting Office)

It is also important to realize that hacker skill levels vary from the computer novice to system experts with advanced technical degrees and years of experience in the information technology business.

Computer security protects your computer and everything associated with it - your building, your terminals and printers, your cables, and your disks and types. Most importantly, computer security protects the information you have stored in your system. For this reason computer security is often called information security.

2. A BROADER DEFINITION OF SECURITY

Definition

The popular conception of computer security is that its only goal is secrecy. Secrecy is a very important aspect of computer security, but it is not the whole story. There are three distinct aspects of computer security:

- confidentiality (secrecy);
- integrity;
- availability.

In some systems or application environments, one aspect of security may be more important than another. Your own assessment of what type of security your organization requires will influence your choice of the particular security techniques and products needed to meet those requirements.

Confidentiality

A secure computer system must not allow information to be disclosed to anyone who is not authorized to access it. In highly secure government system, secrecy ensures that users access only the information they are allowed, by the nature of their security clearances, to access.

Secrecy is of paramount importance in protecting national defense information and highly proprietary business information. In such environments, other aspects of security (e.g., integrity and availability), while important, may be less critical.

Integrity

A secure computer system must maintain the continuing integrity of the information stored in it. Accuracy or integrity means that the system must not corrupt the information or allow any unauthorized malicious or accidental changes to it.

In network communications, a related variant of accuracy, known as authenticity, provides a way to verify the origin of data by determining who entered or sent it, and by recording when it was sent and received.

Availability

A secure computer system must keep information available to its users. Availability means that the computer system's hardware and software keeps working efficiently and the system is able to recover quickly and completely if a disaster occurs.

In some ways, availability is baseline security need for everyone. If you cannot use your computer, you will not be able to tell whether your secrecy and accuracy goals are being met. Even users who abhor "security" agree that their computer systems have to keep working. Many of them do not realize that keeping systems running is also a type of security.

Key words

There are three key words that come up in discussion of computer security:

- vulnerability;
- threats;
- countermeasures.

Computer security is concerned with identifying vulnerabilities in a system and in protection against threats to that system.

Vulnerability

A vulnerability is a point where a system is susceptible to attack. Every computer system is vulnerable to attack. Security policies and products may reduce the likelihood that an attack will actually be able to penetrate your system's defences, or they may require an intruder to invest so much time and so many resources that it is just not worth it. However, there is no such thing as a completely secure system.

Threats

A threat is a possible danger to the system; the danger might be a person (a system cracker or a spy), a thing (a faulty piece of equipment), or an event (a fire or a flood) that might exploit a vulnerability of the system.

Countermeasures

Techniques for protecting your system are called countermeasures. There are many different types of countermeasures - methods of protecting computers and information, vulnerability's and threat's related.

3. INFORMATION ASSURANCE

Historically, the term Information Security was used to refer to the combination of computer security (COMPUSEC) and communications security (COMSEC). During the past several years, a new term has been developed to encompass a broader aspect of security concerns. This term is *Information Assurance* and, as shown on figure 1, covers not only the traditional areas of COMPUSEC and COMSEC but also includes protect, detect and react capabilities, as well as technical, personnel, physical and procedural security.

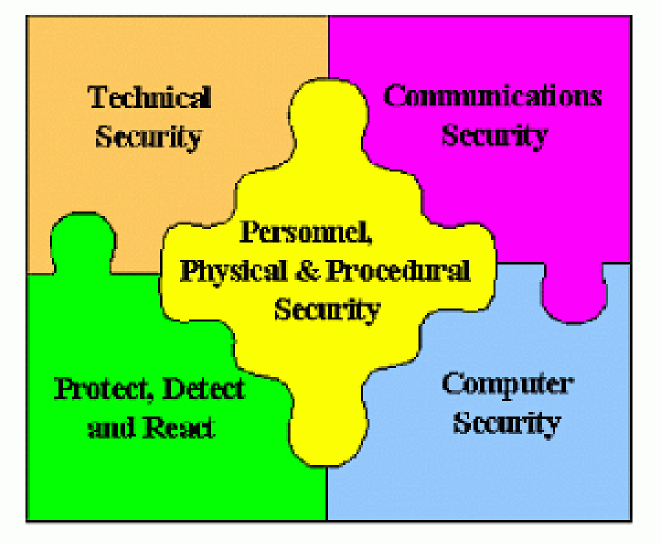
Technical Security
Communications Security
Personnel, Physical & Procedural Security
Protect, Detect and React
Computer Security

Figure 1: Information assurance

All of these disciplines are essential to an effective security posture in today's highly networked world. In summary, Information Assurance includes all of the information operations that protect and defend information and information systems by ensuring their availability, integrity, confidentiality and non-repudiation.

COMSEC Components

Communication security is based on the use of encryption (both symmetric and asymmetric) and associated security protocols and key management. The four basic types of encryption and some examples are link, net, bulk and end-to-end encryption.

Link Encryption

Link encryption is used to encrypt a single link and operates at the physical level of the OSI protocol stack. Encryption at this level generally encrypts all data including "fill" characters transmitted when no user data is available. There is essentially no information available to an adversary except for periodic resynchronizations. It prevents traffic flow analysis and denies cryptanalysts information about the structure of the plaintext. Protection against spoofing can also be provided by the use or error propagation techniques. Link encryption can be used between "red" switching facilities such as routers as well as on an end-to-end basis between users.

Net Encryption

Net encryption is a special case of link encryption that supports one-to-many secure communication on a half-duplex basis. Procedural techniques are used to determine who is transmitting. Technical tradeoffs involve synchronization techniques, key management and operational modes.

Bulk Encryption

Bulk encryption also functions at the physical layer of the OSI protocol stack and therefore shares many of the same characteristics of link encryption. The principal differences are that bulk encryption operates at higher data rates and usually on a TDM group.

End-to-End Encryption

End-to-end encryption (E3) is perhaps the most complex of the COMSEC approaches because it involves integrating security seamlessly into existing protocols. E3 solutions exist for circuit-switched and data networks. The latter include E3 at the session, and application layers.

Session layer E3 is similar to that for network level E3 but is associated with sessions not network layer packets. Similar security services, key management techniques and protocol features are used in products that implement SSL and TLSP. Both SSL and TLSP protocols support the negotiation of security features to be associated with each secure session. They also support mutual authentication, which is an important feature in distributed client server environments.

Application layer E3 includes capabilities such as S/HTTP, S/MIME and PGP. Secure Hyper Text Transport Protocol (S/HTTP) enables the creation of secure Webs while Secure Multiparty Internet Mail Extension (S/MIME) and Pretty Good Privacy (PGP) provide secure email capabilities. Each of these protocols supports confidentiality, integrity and strong identification and authentication.

File Encryption

File encryption can provide a degree of privacy in dedicated and system high environments but are not adequate by themselves for providing MLS capabilities on a workstation or server. An important characteristic of file encryption systems is their ability to provide an "escrow" capability. This enables an encrypted file to be recovered if the file user loses his key(s). Ideally this capability is enforced centrally and is transparent to the user. Access to the escrow key needs to be closely controlled to prevent potential abuse.

Security Management

Security management consists of a number of disciplines but the two key areas that need to be addressed are key management and the establishment of a public key infrastructure. The generation, distribution, activation, destruction, etc., of cryptographic key material is central to the effective use of COMSEC. The best approach is the use of electronic key management and black key distribution techniques. Many systems are being developed and many have already been fielded which use asymmetric cryptography for establishment of ad hoc secure communications. The enabling technology required to support this capability is a public key infrastructure (PKI) based on certificate authorities, certificate directories and standards and protocols necessary to exchange certificates and public keys.

COMPUSEC Components

In general, the COMSEC components just discussed protect data in transit. As mentioned earlier, another important aspect of security is protecting data on computer systems and within network components. Here the interest is in protecting the data from both authorized users and unauthorized users who gain access to the system. Computer security is the term used to refer to the security techniques embedded in computer systems that enable the user to trust those systems.

There are basically three levels of trust used in military systems today—dedicated system-high and multi-level security (MLS). Dedicated systems have the lowest level of trust and do not provide either discretionary or mandatory access controls between users of the system and the data residing on that system. Desktop systems and older servers with no access control over files are examples of dedicated systems. System-high systems provide discretionary access controls (DAC) between users of the system and the data residing on that system. Modern desktop systems and servers provide access control lists (ACLs) which determine who can have access to data files. Generally, the owner of the file decides who is authorized to get access and the system then enforces that decision. Both dedicated and system-high systems are based on the assumption that all users of the systems have a clearance equal to be higher than the most sensitive data on the system.

MLS systems provide mandatory access controls (MAC) in addition to DAC. An MLS system can have users who are not cleared for all of the data on the system (i.e., at least some users have a clearance level lower than the classification level of some of the data on the system). What MAC does is: (1) associate a clearance level with each user and a classification level with each file and (2) restrict user access only to those files for which he/she has an adequate clearance. In addition, MLS systems also enforce DAC. Thus, to get access to data a user must first pass the MAC test and then the owner of the data must have granted him access to that data.

Some examples of existing systems might make these concepts clearer. A simple DOS or WINDOWS-based PC typically grants access to all data on the system to any user of the system. In the case of WINDOWS NT, it can be configured to enforce DAC requirements thereby limiting access to data files to those granted access by the owner. WINDOWS NT also enables system administrators to limit network access based on identification and authentication. The WANG Guard is an example of a B3 trusted MLS platform which is based on the U.S. Orange book and suitable for acting as a connection between an UNCLASSIFIED environment and a SECRET environment. Trusted Solaris is an example of a general-purpose operating system that has been designed with MLS in mind.

Technical Security

In addition to the need for COMSEC, COMPUSEC and protect, detect and react components, there is a need to have a consistent approach on how to handle red-black and emanation protection. Typically, these requirements can often be met by using standard EMI and EMC standards coupled with zoning concepts to create threat free zones. In addition, it is important to prevent coupling between red and black components and wireless by providing adequate separation and/or shielding. Separation of red and black power is another critical aspect. Finally, fortuitous conductors should be avoided.

Physical security

Physical security is the protection of physical computer equipment from damage by natural disasters and intruders. Physical security methods include old-fashioned locks and keys, as well as more advanced technologies like smart cards and biometrics devices.

Protect, Detect, and React

The explosion of the Internet and the associated technology has produced an ever-expanding array of technology, which is finding its way into every aspect of the information technology domain. The World Wide Web paradigm is showing up in all aspects of military CIS and with it come all of the security weaknesses associated with these new technologies. Even when used in a private Intranet the weaknesses are still present, only the size of the user community is different. In the U.S., a concept called "protect, detect and react" is being used to counter the negative effects of what is otherwise a beneficial technological trend.

There are a variety of software tools, which implement this concept, and their capabilities include the following protection features:

- mapping networks to establish real connectivity
- assessing vulnerability of hosts and networks to known threats
- verifying proper configuration of components
- inspecting passwords to identify easily guessed passwords
- evaluating access control permissions
- In addition to protection tools there are detection and reaction products which typically provide the following capabilities:
- detection of unauthorized changes
- use of anti-virus tools
- detection and report of known attacks based on attack signatures
- termination of suspicious connections and access denial
- support for after-incident analysis

This is a rapidly changing and dynamic field and requires a concerted effort to implement in an effective manner. Remember that the hackers are constantly refining their tools and capabilities and consequently the tools of the defender have to evolve to meet that evolving threat.

4. SECURITY POLICY

A security policy is the set of rules and practices that regulate how an organization manages, protects, and distributes sensitive information. It is the framework in which the system provides trust. A security policy is typically stated in terms of subject and objects. A subject is something active in the system. Examples of subjects are users, processes, and programs. An object is something that a subject acts upon. Examples of objects are files, directories, devices, sockets, and windows. Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object. Security policy requirements are:

- Discretionary access control;
- Object reuse;
- Labels;
- Mandatory access control.

Discretionary Access Control (DAC)

DAC is a method of restricting access to files (and other system objects) based on the identity of users and/or groups to which they belong. The DAC requirement specifies that users should be able to protect their own files by indicating who can and who cannot access them (on a "need -to-know" basis) and by specifying the type of access allowed, e.g., read-only, read and modify, etc.

Object Reuse

Object reuse requirements protect files, memory, and other objects in a trusted system from being accidentally accessed by users who are not authorized to access them. Some obvious examples are:

- You store confidential data in the file, and eventually delete it. But suppose the system does not actually delete data from the physical disk, but simply rewrite the header of the file to indicate deletion;
- A user has left the company and later another user comes. The administrator assigns the new user the same ID like the ID of the left user. The new user may has access to certain information previously available to the user who left - information that he would not have been able to access if he followed normal system access rules.

Labels

Labels determine who can access what information in the trusted system. Labels and mandatory access control are separate security policy requirements, but they work together. Labels require that every subject (e.g., user, process) and storage objects (e.g., file, window, directory, and socket) have sensitivity labels associated with it. A user’s sensitivity label specifies level of trust, associated that user. A file’s sensitivity label specifies the level of trust that a user must have to be able access that files. Label integrity ensures that the sensitivity labels associated with subjects and objects are accurate representations of the security levels of these subjects and objects. A trusted system must be sure that when information is written by the system, that information continues to have protection mechanisms associated with it. Two important ways of securing exported information are to assign security levels to output devices, and to write sensitivity labels along with data.

Mandatory Access Control (MAC)

MAC puts all such access decisions under the control of the system. Systems providing MAC must assign sensitivity labels to all subjects and all objects in the system. Mandatory access controls use sensitivity labels to determine who can access what information in the system. Together, labeling and mandatory access control implement a multi-level security policy - a policy for handling multiple information classification at a number of different security levels within a single computer system.

Contents of the security policy

The security policy addresses the following topics:

- definition of accessible resources and services;
- access control;
- rules for local and remote identification and authentication ;
- use of cryptographic methods and devices for data protection and access control;
- audit;
- antiviral protection;
- security manuals (for administrators and users);
- education and certification.

Practical steps

The implementation of the security policy requires a number of practical steps related to:

- security administrator
- description of network's architecture;
- analysis of network's architecture (servers, workstations, software, users), users' access control rights to servers, services (applications and functions) and data;
- information technology interaction analyses;
- definition of security goals;
- risks analysis;
- making decisions for using methods, tools, devices and technologies;
- implementation end education.

5. A SYSTEM FOR INFORMATION SECURITY

Basic functions

The basic functions of the system are:

- identification and authentication;
- access control;
- firewalls;
- VPNs;
- remote access;
- cryptographic services;

- logs and audit;
- antivirus protection;
- emanation protection;
- traffic control;
- establish network scanning and vulnerability.

Service functions

The system supports the following service functions

- state control;
- detection and reaction to events, destroying security;
- test and selftest;
- logs.

Architectural Security Services

The development of security architectures and designs are often based on security services and the mechanisms, which provide those services. The generally accepted services and mechanisms are identified in Table 1.

Table 1. Security Services and Mechanisms

Service	Mechanism
Confidentiality	Encryption (link, bulk, E3) Access control (MAC/DAC)
Integrity	Hash and digital signature Access control (MAC/DAC)
Availability (Denial-of-Service)	Encryption (link, bulk, E3) Digital signature Access control (MAC/DAC)
Authentication	Encryption (digital signature)
Non-repudiation	Encryption (digital signature)

Confidentiality services ensure that data is not accessed, seen or otherwise available to unauthorized users whether it is stored on a workstation or server or is in transit over a network. Confidentiality requirements are enforced by using access control mechanisms on computers and by encrypting data while it is in transit over a network and sometimes while it is stored on disk. There are many types of encryption including link, bulk and end-to-end encryption (E3) which can be used and each is discussed in more detail later.

Integrity services ensure that data has not been altered or destroyed by an unauthorized action. Mechanisms used to protect the integrity of data include message hashing, encryption and access controls. Message hashing is a technique that creates a "checksum" based on a "one-way" function and attaches it to the data. This "one-way" function is often referred to as a "hash function." Any unauthorized change to the data while it is in transit or storage will be detected when a check is made by computing the "checksum" of the data as received and comparing it to the "checksum" already attached to the data. If they match, the data is considered correct. If they do not match, the data is considered corrupted. Digital signatures are a special encryption technique that will be discussed in more detail later but encryption, in general, can be used to support integrity requirements because it is essentially impossible for an adversary to modify data in a meaningful way while the data is encrypted. The data can be changed, but generally not without it being obvious to the users of that data. In the case of digital signatures, the encryption process does not encrypt the "text," but instead encrypts the message hash and other data designed to prevent replay and other types of attacks. Access controls limit access to data to authorized personnel making it impossible for unauthorized adversaries to modify the data.

Availability is focused on ensuring that a particular resource is accessible and useable upon demand by authorized personnel—i.e., that they are not denied access and use by an adversary. Again, encryption is used to prevent sophisticated attacks against networks and computer systems over communication links while access controls are used to prevent unauthorized personnel from shutting them down. These access controls also ensure that user personnel authorized access to systems and networks are prevented from accessing supervisory functions which would enable them to shut them down.

Authentication is how you prove you are who you say you are. In computer systems and networks, some mechanism is needed to ensure that the identification supplied is in fact the real identity of the individual. There are many techniques being used in modern identification and authentication systems but all of the strong ones depend on encryption and many depend on digital signatures.

Non-repudiation is a service that prevents entities involved in a communication exchange from denying having participated in that exchange. For example, non-repudiation can be used to prove that a certain user originated a message and that another user received that message. Again, digital signatures provide a strong technical solution for this requirement.

Protection levels

The system should be developed on the following levels:

- emanations protection;
- access control;
- communication;
- firewalls;
- servers and workstations protection;
- "end to end" protection;
- application protection;
- viruses prevention, detection and treatment;
- Audit and control.

6. A SET OF REQUIREMENTS

A set of requirements is as follows:

- Use trusted operation systems (such as Windows NT and Trusted Solaris);
- Use trusted DBMS (as Trusted ORACLE);
- Centralized administration, management and control;
- security administration in each LAN;

- Firewalls should be used to connect to external networks.
- Firewalls should also be used when connecting system-high classified LANs to a system-high WAN operating at the same security level.
- Develop and introduce an electronic key management system and Public Key Infrastructure (PKI);
- Implement Intrusion Detection Systems (IDS);
- Establish network scanning and vulnerability.

Data Networks

Data networks represent a much more complex security environment because of the complexity and openness of the workstations and servers that are typically interconnected by these networks. Today’s commercial computer systems and networks generally do not provide a level of trust adequate to permit interconnection of terminals operating at different classification levels on the same LAN or WAN. To overcome these limitations, the following security architectural recommendations should be followed:

- LANs should be operated at only one security level.
- Depending on the operational requirements, three separate LANs may be required. Typically, this would include LANs operating at the UNCLASSIFIED, SECRET and TOP-SECRET system high levels.
- The enclave concept described earlier should be used to protect each system high LAN.
- Military grade cryptography should be used to interconnect classified LANs over untrusted WANs or to connect them to system-high WANs.
- Firewalls should be used to connect UNCLASSIFIED LANs to external networks.
- Firewalls should also be used when connecting system-high classified LANs to a system-high WAN operating at the same security level.
- Community of interest security services within an enclave and between enclaves operating at the same security level can be provided by commercial security products. Such services include secure email, secure Web, etc.
- Red WANs should be operated at one system-high security level. Enclaves (e.g., LANs) operating at a different system-high classification level can be tunneled through a WAN based on the use of a military grade in-line network encryptor (INE).
- Interfaces between LANs or enclaves operating at different system high classification levels should only be interconnected with MLS Guards running appropriate trusted applications.
- Remote dial-up access to classified networks should be based on the use of military grade cryptography implemented at the physical layer of the OSI protocol stack. Strong identification and authentication should be implemented. Secure voice terminals with an appropriate data port would be one solution. Use of a secure laptop or mobile terminal is also feasible but connectivity to the classified network should still be based on physical layer encryption.

An example of Unclassified Enclave

Shown in 2 is an example of a typical unclassified enclave with a connection to the Internet or some other untrusted network. The simple LAN shown is notional and represents any local environment with a single security policy such as a campus environment or perhaps a MoD. Key security features include the following:

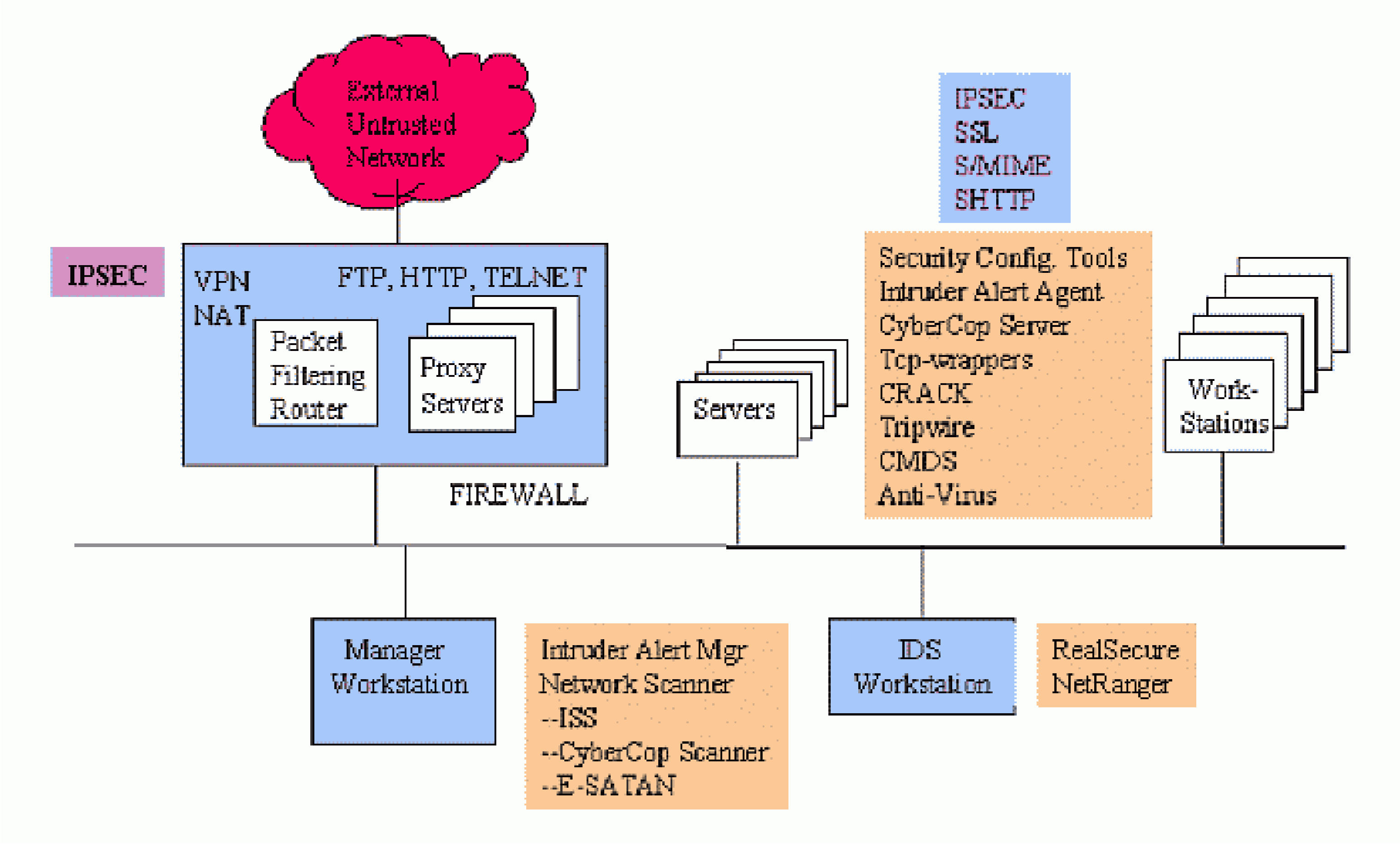

Figure 2: An Example of unclassified enclave

A firewall is used to control communication between the enclave and the external network(s) based on some established policy. It could include any combination of packet filtering, proxy applications, Virtual Private Network (VPN) and Network Address Translation (NAT). However, in today's high threat environment, the firewall alone is not really adequate to protect against all external threats and it provides no protection against trusted insiders.

An Intrusion Detection System (IDS) Workstation is usually hosted on its own platform to minimize its visibility to potential attackers. Its function is to monitor all LAN traffic for known attack signature and other suspicious behavior. When attacks are noted, an alarm can be sent locally and to a central facility and, in some cases, corrective action can be taken either unilaterally or in conjunction with a cooperating router or firewall. IDS data can also be used for post attack analysis.

A Security Manager provides a local facility to receive and react to data from security agents hosted on servers and workstations. It also provides a controlled environment for performing network scanning which tests all specified platforms for known security vulnerabilities.

Host-based tools are shown between the servers and workstations. These tools are resident on the platform to be protected and provide a variety of security services including virus protection, configuration verification, password checking, misuse detection, network access control and attack detection. Additional protection using end-to-end encryption such as IPSEC, SSL, S/MIME and SHTTP can be selectively supplied.

Example commercial products were given for each of these areas but there are many others available. One of the difficulties in pulling together a coherent approach is the selection of a common set of tools, which are used enterprise wide. This approach minimizes the complexity of the implementation and provides the basis for enforcing a common security policy.

References:

1. *Department of Defence Trusted Computer System Evaluation Criteria*, Department of Defence Standard DoD 5200.28-STD (Washington, DC: Library Number S225,711, 1985).
2. *Trusted Network Interpretation of the Trusted Computer Evaluation Criteria*, NCSC-TG-005, Version 1 (1987).
3. *Information Technology Security Evaluation Criteria* (1992).
4. Dragomir Pargov, Veselin Tselkov, Rusin Petrov and Iliya Kraytchev, "Security in Computer Systems," in *Information Aspects of Security and Development of Modern Societies*, Velizar Shalamanov and Todor Tagarev, editors (Sofia: AFSEA-Sofia, 11 - 13 September 1996), 93-98.
5. Veselin Tselkov, Dragomir Pargov and Rusin Petrov, "Criteria of Computer System Security Assessment and Evaluation," in *Information Aspects of Security and Development of Modern Societies*, Velizar Shalamanov and Todor Tagarev, editors (Sofia: AFCEA-Sofia, 11 - 13 September 1996), 99-103.
6. Veselin Tselkov and Dragomir Pargov, "Security of Information System on Internet," in Proceedings of the 1997 AFCEA-Sofia Seminar (Sofia: AFCEA-Sofia, 4 - 5 December 1997), 40-48.
7. Br. Schneir, *Applied Cryptology* (John Wiley, 1996).
8. RSA, Available at http://rsa.com.
9. Common Criteria for Information Technology Security Evaluation, version 2.1.

VESELIN TSELKOV: Born 1955. M.Sc. (1980, Mathematical Logic) from the Sofia University, Bulgaria. Ph.D. (1990, System programming, Network Information Management) from The Military Scientific and Research Institute. Associate Professor (1996, Informatics, Information Security). Currently Dr. Tsekov is Associate Professor in Defence Advanced Research Institute at the Military Academy "G.S.Rakovski". Main fields of interest are in the area of information assurance. Main topics of recent research: cryptography, software secure tools, security policy, intrusion detection systems. Address for correspondence: Defence Advanced Research Institute, "G.S.Rakovski" Defense Academy, 82 E. Georgiev Blvd., 1583 Sofia, Bulgaria. E-mail: vtselkov@md.government.bg and v.tselkov@nat.bg.

DRAGOMIR DRAGANOV PARGOV: Born August 15, 1949. Mr. Pargov received his BS in Electrical Engineering (1973) and M.Sc. degree in Mathematics and Computer Programming from the Technical University of Sofia. In 1997 he received his Ph.D. degree in Computer Sciences from the Technical University of Sofia. From 1979 to 1999 Dr. Pargov was assistant professor in the Military Scientific Institute in Sofia. Currently he is leading the Department of Information Security at ACT Ltd., Sofia. His main research interests and publications are in the field of computer security. Dr. Pargov may be contacted by phone: (++359 2) 373 522 or e-mail: D.Pargov@actsoft.bg.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Information Assurance in C4I Systems

Veselin Tselkov, Dragomir Pargov

Keywords: information assurance, security, security policy, cryptography, C4I systems, evaluation criteria, common criteria.

Abstract: This article presents a broader definition of security and examines the components of information assurance, as well as the main features of the information security policy, a set of requirements, and a system for information security. It reflects the authors' experience in development and implementation of information security systems in the Automated Information System of the Bulgarian armed forces, as well as their participation in the creation of the Strategy for Development of Information Society in Bulgaria. Some conclusions and recommendations from the 1999 U.S.-Bulgarian study of the C4 systems in the Bulgarian armed forces were also taken into account.

Author: **Eugene Nikolov**
Title: **Contemporary Trends in the Development of Information Security and Computer Virology**
Year of issuance: **2000**
Issue: **Information & Security. Volume 4, 2000**
Hard copy: **ISSN 1311-1493**

CONTEMPORARY TRENDS IN THE DEVELOPMENT OF INFORMATION SECURITY AND COMPUTER VIROLOGY

Eugene NICKOLOV

Table Of Contents:

1. Introduction
2. Information Security
2.1 Components
2.2 Relations
2.3 Function and Arguments
2.4 Procedures
3. Computer Virology
3.1 Working principles
3.2 The Investigation of computer viruses
3.3 Detection of computer viruses
3.4 Removal of computer viruses
Conclusion
References

1. Introduction

The information and its security were subject of special attention throughout the ages. All achievements in this area were highly appreciated and were finding immediate application. During the past years, the development of the contemporary society is correlated with the continuously growing information activity. The information accumulation and its movement through the Internet environment are the next challenge to not only to information security, but also to broader aspects of societal security. In these conditions the notion of *information security* becomes a basic instrument for evaluating the risks for an information unit. One of the main effects on the information security of a given information object stem from computer viruses and their derivatives. The science of *Computer Virology* emerges as a response to these challenges. It deals with analysis and synthesis of virus signatures used by the anti virus programs for detection, blocking and removal of the computer viruses. In the contemporary information society the computer virology turns into one of the most important agents for mastering of the "malicious thinking" and for guaranteeing the necessary information security.

2. Information Security

Let us consider the notion of information security as containing some components connected by specific relationships. The number of these components has to be a reasonable approximation to the exact image of the real phenomena. The number and the functional names of the components can be changed in the wanted direction if needed. The principle of the multiple decomposition can be applied in the analysis of each separate component, during which new components can appear or some of the existing can drop out. The relation between the components can be bound in specific mathematical relationships with functional character influenced by the changes in a number of given arguments. Lately, the information security function can be controlled by relevant parameters representing the projection of the separate components and their relative weight in the general pattern, when some assumptions and reasonable simplifications are made. Along with that, the information security can be interpreted as the possibility for a definite information unit with a definite composition and structure to be moved from the point A to the point B with guaranteed *constancy of the integrity* of the information unit and *constancy of the movement* of the source and receptor points. In this case, *constancy* means a lack of possibility for the "malicious thinking" to change the preliminary defined behavior.

2.1 Components

Data Security (S_{DATA}). In the gradation of the components this is the offset. The possibilities for the security evaluation on a data level are generalized in this component. This means an analysis of the possible critical points for the specific forms in which data emerge, exist and disappear, such as bit, byte, word, block, and package.

Computer Security ($S_{COMPUTER}$). The next component generalizes the possibilities for a security evaluation on a computer level. An analysis is performed here of the possible critical points for the separate modules as processor, memory, peripherals.

Communication Security ($S_{COMMUNICATION}$). In this component the possibilities for the security evaluation on a communication level are generalized. The analysis of the possible critical points includes the communication environment, as well as the processes of input/output, transformation, and compression.

Network Security ($S_{NETWORK}$). Here the possibilities for a security evaluation on a network level are generalized. The analysis of the possible critical points includes the modules network drive, network protocol, and network architecture.

Mobile Security (S_{MOBILE}). This component is a generalization of the possibilities for a security evaluation on an information object mobility level. The analysis of the possible critical points includes the object coordinates, access authorization, transfer by satellite.

Manipulations Security ($S_{MANIPULATIONS}$). This is a component in which the possibilities for a security evaluation are generalized on operator manipulations level. The analysis of the possible critical points includes manipulations on the objects key, mouse, pen, screen, etc., as well as the types of manipulations press, click, and touch.

Biometric security ($S_{BIOMETRIC}$). In this component the possibilities for a security evaluation on the operator's biological characteristics are generalized. The analysis of the possible critical points includes fingers, hands, palms, face, eyes, voice, scent, blood, and DNA.

Steganometric security ($S_{STEGANOMETRIC}$). The last component in this arrangement generalizes the possibilities for a security evaluation on the information object steganography level. The analysis of the possible critical points includes stegochannel, stegoobjects, and host signal.

2.2 Relations

The dynamics of the real processes require the formal definitions of the separate parts of a whole to be generalized by defining their relationships. A formal record of the above examinations for the information security components and their possible critical points, made by applying the multiple decompositions, is as follows:

$S_{DATA} = F\ (S_{bit}\ ,\ S_{byte}\ ,\ S_{word}\ ,\ S_{block}\ ,\ S_{package})$ (1.1)

$S_{COMPUTER} = F\ (S_{memory}\ ,\ S_{processor}\ ,\ S_{peripheral})$ (1.2)

$S_{COMMUNICATION} = F\ (S_{input/output}\ ,\ S_{transformation}\ ,\ S_{compression}\ ,\ S_{media})$ (1.3)

$S_{NETWORK} = F\ (S_{device}\ ,\ S_{protocol}\ ,\ S_{architecture})$ (1.4)

$S_{MOBILE} = F\ (S_{co\text{-}ordinates}\ ,\ S_{authorization}\ ,\ S_{satellite})$ (1.5)

$S_{MANIPULATIONS} = F\ (S_{key}\ ,\ S_{mouse}\ ,\ S_{pen}\ ,\ S_{screen}\ ,\ S_{press}\ ,\ S_{click}\ ,\ S_{touch})$ (1.6)

$S_{BIOMETRIC} = F\ (S_{fingers}\ ,\ S_{hands}\ ,\ S_{palms}\ ,\ S_{face}\ ,\ S_{eyes}\ ,\ S_{voice}\ ,\ S_{scent}\ ,\ S_{blood}\ ,\ S_{DNA})$ (1.7)

$S_{STEGANOMETRIC} = F\ (S_{stegochannel}\ ,\ S_{stegoobjects}\ ,\ S_{hostsignal})$ (1.8)

2.3 Function and Arguments

The formalization can be prolonged and transformed as follows:

$$
\begin{aligned}
S_{\text{INFORMATION}} = F\,(&\text{Data, Computer, Communication, Network,}\\
&\text{Mobile, Operator, Biometric, Stegometric}) \qquad (1.9)
\end{aligned}
$$

The general expression for the information security function and its arguments can be obtained by substitution:

$$
\begin{aligned}
S_{\text{INFORMATION}} = F\,[\,&(\underline{\text{bit, byte, word, block, package}}),\\
&(\underline{\text{memory, processor, peripheral}}),\\
&(\underline{\text{input/output, transformation, compression, media}}),\\
&(\underline{\text{device, protocol, architecture}}),\\
&(\underline{\text{co-ordinates, authorization, satellite}}),\\
&(\underline{\text{key, mouse, pen, screen, press, click, touch}}),\\
&(\underline{\text{fingers, hands, palms, face, eyes, voice, scent, blood, DNA}}),\\
&(\underline{\text{stegochannel, stegoobjects, host signal}})\,] \qquad (1.10)
\end{aligned}
$$

Depending on the kind and the depth of the investigations, the arguments can be defined as parameters with specific limits and relevant numeric values. In this way, a specific strategy for information security control can be realized along with guaranteeing and finding a reasonable balance among the requirements for security, speed, performance and price.

2.4 Procedures

The basic procedures for realizing the necessary information security level include *monitoring, blocking*, *removing*, *protection* and *verification*.

The procedures *monitoring*, *blocking* and *removing* have to be considered as a sequence of actions of the anti-virus programs on a single computer virus OR a single family computer viruses.

The procedure *protection* represents a functional unification of the above three procedures but on other objects. It should be considered as a sequence of actions of the anti-virus programs on some family of viruses OR all currently known families of viruses OR some family of virus derivatives OR all currently known families of virus derivatives.

The procedure *verification* contains two separate parts: ‘identification’ and ‘access’, which are very closely connected (this is the reason they are examined in a unified procedure). These parts in most cases accomplish an integrity check for specific information objects using control sums, which can be mathematical, steganometric and biometric.

The procedures discussed above represent a generalization of the contemporary views for information control in modern computer systems. They are the most important instruments of the information security, helping its control by relevant parameters, as well as the fast and effective evaluations of the multiple factors exerting influence on the operation of the separate workplace.

3. Computer Virology

3.1 Working principles

The first basic principle that computer viruses accede to is *reproduction.* The programs realizing the virus idea and its derivatives always accomplish the operation *self-reproduction*. At first, it was an ordinary copying with identical original and copy and this was making the work of the anti virus programs much easier. As a consequence, the virus writers very soon proceeded to a reproduction with a considerable difference between the copy and the original. Exceptional efforts are exerted to realize this idea and the achievements are considerable. Besides, nowadays the number of the generations is an astronomical figure. This makes the reproduction the hottest point in the rivalry between the viruses and the anti-virus programs. Secondary results of this perpetual competition are not always visible and widely known, but every new model of a computer or computer system, every new version of an operating system or application package contains the latest results of this competition.

Transportation is the second basic principle which computer viruses abide. It realizes the quantitative accumulation of the virus idea and its moving in space. Initially, the movement of the virus was limited to a single computer but later a suitable carrier (changeable carrier with enabled/disabled writing) was used. The network development provoked gradually the use of a communication type carrier. During the past few years the Internet became the most global and handy carrier of the virus idea and imposed the need for relevant and constantly updated virus filters. Main tools for realizing these filters are the Internet protocols. They are subjected to continuous improvements but, unfortunately, the number of security holes does not decrease. Another solution is the increase of the security level of each work place.

The malicious thinking is the third main characteristic of the computer viruses. It marks the limit between the scientific problems in the field of informatics and the computer viruses. Initially, the *reproduction* and the *transportation* existed only in the research laboratories and were used for scientific purposes. But starting with the early 80s—along with the development of the personal computers—the *malicious thinking* began also to use *reproduction* and *transportation*.

Depending on its goals, the malicious thinking could be divided into the following basic types:

Destruction. This is one of the first goals set and successfully realized by the malicious thinking. Main variants of destruction are: immediate, awaiting, single, and basic. Nowadays, a certain decrease of the virus' destructive action is observed, but its disappearance is highly unlikely.

Modification is the next goal of the malicious thinking. Everything is subject to modification - operation systems, application packages, local programs. The public and the personal information are modified in order to be attacked or to be made ready for future action. This trend, which is very dangerous, dominates malicious thinking in the Internet environment. The main cause is the contemporary infrastructure of the computer systems, which is not adjusted for a global access to their resources. This determines the serious lapses in the systems controlling the access and in the whole computer security. This is true to some extent even for the most modern Internet systems. Their designers are often not able to study them carefully in laboratory conditions. This is the reason security tests are performed in real conditions, which imply many risks. Unfortunately, this aspect is not secret for the malicious thinking.

Misappropriation. This goal is comparatively new and its propagation is limited. Until recently, information in its various forms was often appropriated, but money was rarely appropriated. However, the e-commerce development in Internet environment menaces to become a strong motivation for the development of the malicious thinking in this direction. The classical forms of attack are related to hooking of personal information and accomplishing of transactions causing damages. Unfortunately, despite the widely advertised multi-digit identifiers and passwords, the malicious thinking achieves remarkable success though nobody speaks about it - neither those who gain nor those who lose.

Good-natured thinking is the fourth fundamental principle to which computer viruses may accede. It is an alternative of the third one – the malicious thinking. Its use for the past few years has been constant and probably will remain unchanged in the future. Its main characteristic is the absence of planned losses of resources and information. Usually, it is manifested through various strange effects - sound, music, speech, inscription, image, multimedia, Internet activity, etc. They cam be categorized in the following basic types:

Joke - one of the first manifestations of the virus idea. Usually used by friends or acquaintances. Serious troubles are very rare and are caused by unconscious errors. The jokes are a herald of positive ideas and it may safely predicted that they will never disappear.

Advertising. This kind had very modest presence in the past but the exclusive possibilities for its development, especially in Internet environment, reserve a great future for it. However, if the reasonable proportion between usefulness and boredom is upset then, figuratively speaking, it crosses the line and may be classified as malicious thinking.

Experiment. This kind may be named "useful viruses" because they allow the investigation of complex systems that cannot be studied in a different way. If the experiments are made systematically by the appropriate organizations, they eliminate the risks and allow a reasonable management of the resources. But if experiments are made by curious programmers, they could also bring serious trouble.

3.2 The Investigation of computer viruses

The isolation of a working virus sample is the first step in virus investigation. In the past, computer virus designers did not take any precautions and every infected file provided such a sample. But later the viruses became encrypted and scattered in the file (files) body, which transformed the isolation in a highly qualified activity almost impossible for the common user.

The second step in the virus investigation is the program code *decomposition*. This is almost always non-trivial task. Very often the program code is repeatedly encrypted and compressed; non-standard identifiers, masks, and addressing are used; the virus writers rely on non-documented and badly known system functions, interruptions and procedures. Certain particularities of certain processor chips are used to a maximal extent. The implementation of a new virus idea is the most interesting for the anti-virus researchers. The family characteristics are unusable and the significance of every bit from the program code must be clarified. This process is one of the most difficult in the investigation.

The formal description of the program code is the next step aiming to prepare certain automated operations connected to the creation of a working model of the investigated computer virus. Most often the model is created on a matrix and vector basis and, sometimes, through the implementation of more complex mathematical instruments. The goal is to achieve object and class description in an appropriate hierarchy looking for some control of the events. But sometimes the examined sequence of actions cannot be realized, therefore one must rely on experience and intuition. Often the formal description implies complicated formulas calculating the needed coefficients. Sometimes it is impossible to use standard computing programs.

The computer virus *modeling* is an extension of the previous step. The basic problem is to verify all the known information and to create a working virus model. Now the researchers look for the process dynamics and the relevant narrow points of the created model's structure. Another important task is to create the so-called "temporal magnifier" allowing acceleration or delay of the local virus time. Thus, the full life cycle of a computer virus can be described and its future behavior can be forecasted. The factors, which are critical with regard to its reproduction and transportation schemes, are searched for in order to limit its spreading. The needed input data are loaded in the model and then a series of experiments are made during which preliminary planned statistical data are collected. Various modeling techniques are used, mainly analytical, simulative, or mixed. The choice is made generally according to the needed computing and non-computing processing and the needed experiments and statistics.

The decision-making is the step that requires good forecasting skills because the decision is made on the basis of a few virus samples, at best. It must be valid not only for the current generation of the investigated computer virus but also for the whole family. During the decision making process it is very important to take in consideration the program solutions that are realized already. The new solution must be incorporated in the existing ones without affecting the speed and the performance of the existing anti virus program. When principally new solutions are needed, long-term application and finalization of a separate programming module for the new class of computer viruses has to be created, bearing in mind the general performance and speed.

The program realization is the last step before getting the product ready for use. It is important here to choose such a programming language, or languages, that allow the creation of programs running simultaneously on various platforms, while taking into account the processor or the operating system. The correlation between the high-level languages and the assembler modules is also of a great significance, because the performance, the speed and the flexibility of the anti-virus program depend on it. All non-standard and specific operations of the anti-virus program, related to non-standard and specific functions and interruptions, are very often realized by the assembler modules. The screen interface also has a great importance for the final success of an anti-virus program. The expenditure needed to obtain a suitable solution is very often comparable with the rest of the expenses.

3.3 Detection of computer viruses

Signature analysis is one of the first methods applied for detection of computer viruses and their mutations. It consists of a continuous filtering of the information flows in certain spots of the computer configurations. The aim is to obtain a coincidence on an information unit level, most often byte, with the so-called virus signature. If such a coincidence occurs, this means that there is a virus code in the information flow. The creation of the virus signature of a separate virus or virus family is not a quickly-solvable problem. A non-repeating (unique), non-changing and the shortest possible sequence of hexadecimal or binary symbols must be found assuring a secure recognition of the viral code without false alarms. To find such a virus signature requires always some time, and this is seen as a serious disadvantage of this method. Another disadvantage is the consumption of system resources, which does not always go without penalty. A constant update of the virus signature base is needed, although, if Internet connection exists, this may be made automatically without disturbing the user.

The creation of self-mutating computer viruses is a serious challenge for this method, as each new reproduction requires some time for creating a new virus signature. Of course, sometimes it is possible to create a virus signature which is valid for all possible virus copies, but this requires an investigation of the full virus life cycle. Regardless of these disadvantages, the signature analysis is the most used method. It provides a reasonable balance between price, flexibility and applicability. It is easy for use, highly reliable, particularly if its application is combined with other methods and means. The future of this method is in the creation of means for shortened search. This means to replace, according to certain principles, few bytes from the virus signature with a unique byte. This byte is grouped along with other similar bytes to form a representative excerpt valid for a big group of virus signatures. The investigations in this direction show that, if the rates of increasing the performance of the processors and the other system resources decrease, this will immediately lead to the creation of new means for management of the virus signature base. It is necessary to obtain a unified standard virus signature base for all commercial realizations of anti virus programs. This would be an exceptional success for the computer security of the contemporary computer systems. The Internet, which is a manifestation of the idea of globalization and unification, brings closer the integration of the different bases.

Integrity check is the next basic method for detecting computer viruses. It is based on the use of the so called *control sums*. Special procedures are started in a virus-free environment to process all or some file objects and system points by special mathematical methods. As a result, hexadecimal sequences are obtained and they are constant if the chosen objects and points remain unchanged. This means that every virus attack or an attempt for accidental or deliberate change of an object or a point will change the control sums and therefore will be immediately detected. The application of this method requires calculation of the control sum every time when the system is started or the user gets access to a file object or point. This method provides high security but is time consuming and requires a lot of resources that can be used differently. Another disadvantage is the *post factum* reaction, which is inadmissible in some applications. For this reason, when possible, the object integrity is verified some time before the objects are used in real actions and, if it is necessary, backup copies can be found and started. Another possibility is to start a self-restoring procedure for the change localization and removal by mathematical means. The existing applications of this method include sophisticated encoding and decoding procedures. They are applied after the control sums calculation in order to preserve them from manipulation. In some procedures the control sum base, after being encoded several times with accidental component codes, is divided into several parts that are stored separately. These parts on the other hand change their locations continuously. The particularities of this method limit its application to systems with relatively constant composition and structure, because in a dynamic environment a number of serious problems arise. The integrity check can be integrated with the use of hardware security points using special integrated circuits with factory-made access control means. Such a protection offers almost ideal security but the prices are so high that very few real systems can afford it.

The combination of the integrity check with the signature analysis is a very good solution and can be often found in real systems.

Monitoring is the third method applied for detection of computer viruses and their derivatives. It requires creation of a relevant environment for monitoring the whole activity of a computer system. This includes:

Runtime evaluation of certain events and processes. Fully automated methods or an empirical human appraisal can be used. In the first case a database is created with standard runtimes, which are compared with the current values during the next starts and runs of the computer system. If a discrepancy bigger than a preliminary defined interval is detected, a warning message is generated. In the second case, the possible high skills and reflexes of the user can help the timely change detection in the computer system operation, but this method cannot be applied on a mass scale.

Evaluation of the non-standard screen interface reactions and behavior - automated methods with standard screens or other interface components also can be used for comparison, but the expenses are very high and their use is limited. It is easier to rely on the human factor but the requirements for high qualification are obligatory because the probability for false alarm is very high. Serious knowledge of the system and application resources is needed to obtain a high level of precision.

Evaluation of the input/output peripheral operations - the automated methods have the highest success in this case. Control sums including the run times for the relevant transactions are used relatively often. This is a good guarantee for the transactions' security and this solution has great prospects. The main problem is the accuracy of the measurements in the starting and ending points of the transaction, because thousandths and ten-thousandths of a second must be measured. In Internet the use of uniform time is necessary, but the possibilities for errors and false alarms are significant.

Restriction is the fourth method used in the computer virus detection. It uses two clearly defined areas of allowed and not allowed events and processes. Each frontier violation generates a warning message.

The permitted area represents a multitude of addresses, fields, operations, drives, etc., which are examined for reliability and possible regulations. The information flow movement (input/output points, routes, data volumes) is strongly regulated and the user is given a warning for each deviation. At present, these regulations can be applied only in relatively static systems, but the use of new algorithmic means for self-verification of the information flow content will decrease the importance of this kind of restrictions and increase the importance of the access and identification control for each object that is in contact with the information flow. The biometric user information combined with some cryptographic methods can assure a personal biometric tracing of events and processes and, thus, realize restrictions in the permitted area. Each contact for which biometric information does not exist will be thrown out of the permitted area.

The forbidden area usually is the multitude of addresses, fields, operations, drives, etc., for which the examination of the reliability and possible regulations is negative. They are risk points needing a strong protection. The requirement for the static character of the systems is strict because in dynamic systems the formulation of clear criteria is very difficult. The availability of some information for past behavior of the risk points is very important and requires the presence of automatic registration systems. The increased resource consumption is compensated by the possibility for analyzing the accumulation of incidents in the risk points.

3.4 Removal of computer viruses

The removal of the computer viruses and their derivatives from the attacked objects and information flows is a risky process. Despite of the precautions and the collected experience about 5 % of all virus attacks and incidents cause non-recoverable destruction. As a rule, they are a consequence of the malicious thinking, which has planned such a development of the virus attack. In this case the only possibility is to find uninfected objects and to copy them on the destructed objects. If system resources and objects are damaged, the system has to be re-installed. If data is damaged, then eventual backup copies have to be used.

If the computer virus removal is possible and necessary, it goes on in the following order:

Localization. This is the initial step when the location/s/ of the computer virus body has to be pointed out exactly. The existence of a mechanism connecting the separate virus parts and of control sums assuring the identification of these parts ought to be clarified. Viruses have to be localized in time too, because some of them exist in continuously closed locations, which open in a couple of ticks to allow an information exchange. This opening occurs if certain conditions are realized, and that is not always possible. If the localization is impossible, it is very important to obtain information about the causes and to modify the next phases. The presence of registering mechanisms is essential because they allow to track the history and the steps of the infection.

Identification is the next step in the computer virus removal. It has two modifications. The fast identification aims to point at a specific group, family or class of computer viruses emphasizing on the speed. The exact identification is a prolongation of the fast one and its goal is to identify exactly the virus and to specify if a mutation, a new variant or a dead virus body is found. This is not always possible but it is important to achieve an identification of the future variants if the virus makes use of a known working principle.

Removal is the third step in the computer virus removal. The virus body is deleted most often and the separate parts of the infected objects are jointed. It is very important to find out the exact boundaries of the virus to make possible the conglutination of the different parts. If the virus is in the beginning or in the end of a given object, the procedure is trivial, but nevertheless risky. If the virus body is located in specific system areas, for example the initial sectors of the hard disks, there are two possibilities. The first one is to find the original image of the object, which is often stored somewhere and to restore the object. The second one is to generate again this system object if sufficient information about it is kept. A special attention has to be paid to the group of viruses, which encrypt the whole content of some media, for example hard disks. In this case it is very important to decrypt the media before the virus removal. If this requirement is violated the data decryption after the virus removal may be impossible.

Deactivation is the next step in the virus removal. It represents a variety of the *cleaning* and is applied when the prognosis for the virus cleaning is negative, i.e., when the virus cleaning would destroy the object, whereas after the deactivation the object keeps on functioning normally in spite of the dead virus body in it. The basic task is to find the starting point of the virus and to write specific information on it. Thus, the virus cannot reproduce and transport itself anymore. This solution is not always possible but, if it is, the results are very good especially when the change of one byte kills the virus body and the system continues to work.

Verification of existent, known and accessible control sums related to the restored object is the next and often the last step in the computer virus removal. It has to provide a warranty for the restored object integrity and working capacity. If possible, a new control sum is generated and its coincidence with the database is verified.

Conclusion

Information security in the contemporary society becomes a global gauge of the risks during the rise, the existence and the disappearance of the information. It is subject to control by relevant parameters with a reasonable compromise among the requirements for security, speed, performance and price.

Computer virology is a dynamically developing contemporary branch of science, in which top achievements of mathematics, computer science, physics, chemistry, biology, genetics, etc., are combined. It is particularly important for guaranteeing the necessary information security in the contemporary society with its communication globalization and mobility.

References:

1. RISKS, Forum on Risks, http://catless.ncl.ac.uk/Risks
2. CERT, advisories, ftp://ftp.cert.org/pub/cert_advisories/
3. CIAC, Computer Incident Advisory Capability, http://www.ciac.org/
4. BUGTRAQ, forum, http://www.securityfocus.com/

EUGENE NICKOLOV is director of the National Laboratory of Computer Virology. Associate Professor at the Bulgarian Academy of Sciences. Holds a M.Sc. degree in Computer Science and a PhD degree (Optimizing Investigations on the Design of Computer Devices) from the Technical University of Sofia, Bulgaria. Member of a number of national and international unions and associations. Address: NLCV-BAS, Acad. G.Bontchev Str., Building 8, 1113 Sofia, tel.: (++359 2) 973 3398, E-mail: eugene@nlcv.bas.bg.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Contemporary Trends in the Development of Information Security and Computer Virology

Eugene Nickolov

Keywords: Information Security, Computer Virology, Modeling, Simulation, Dynamic Programming, Mobile Communications, Satellite Communications, Biometric, Steganometric.

Abstract: This article presents an analysis of the latest trends in information security and computer virology. The basic components of the information security are introduced, including *data security*, *computer security, communication security, network security, mobile security, manipulations security, biometric security,* and *steganometric security.* The main factors exerting influence on these components, as well as their relationships are shown. A formal record for the information security as a function of specific arguments is developed. The fundamental procedures of the information security are represented, including *Monitoring, Blocking, Removing, Protection* and *Verification*.

The analysis continues with the computer virology topic. In the beginning, the fundamental work principles of the computer viruses are examined: *Reproduction, Transportation, Malicious Thinking* and *Good-natured Thinking*. Then the main steps in the computer viruses investigation are analyzed: *Isolation, Decomposition, Formal Description, Modeling, Decision-making* and *Program Realization*. Next, methods for computer viruses detection are examined, such as *Signature analysis, Integrity Check*, *Monitoring* and *Restriction*. After that the basic steps during the computer viruses removal as *Localization, Identification, Removing, Deactivation* and *Verification* are shown.

In the conclusion, the role and the importance of the information security and the computer virology for the development of the contemporary society in conditions of growing communication mobility and globality are pointed out.

Author: **Metodi Popov**
Title: **Security Aspects of the Cellular Communications**
Year of issuance: **2000**
Issue: **Information & Security. Volume 4, 2000**
Hard copy: **ISSN 1311-1493**

SECURITY ASPECTS OF THE CELLULAR COMMUNICATIONS

Metodi POPOV

Table Of Contents:

Introduction
1. Basics of ciphering
2. Coding in cellular communications
3. Authentication procedure
4. The secrecy of voice and data
5. Secrecy of subscriber
6. Secrecy of the equipment
7. Secrecy of connections
8. Secrecy of signaling and control massages
Conclusion
References

Introduction

Important aspects of protection and security of the cellular radio systems and networks are discussed in this paper. It is shown that Public Land Mobile Networks (PLMN) need a higher level of protection than traditional telecommunication networks.

At an early stage in the development of the mobile radio systems and networks, it was apparent that the weakest part of the system was the radio path. To protect the system against unauthorized use of its resources and easy eavesdropping with radio equipment, it is necessary to perform two procedures concerning authentication of the users and their equipment and ciphering the user's information and data.

The cellular systems, being a type of a mobile radio system, have the ability to guarantee to its users the so called information and subscriber security: *secrecy* and *authentication.*

Th*e secrecy* is a mechanism that rules out the possibility to derive information from a communication channel.

The authentication of cellular service users is an approach that prevents the utilization or bringing in any changes in the telecommunication channel.

The encryption of information and signaling between Base Transceiver Station (BTS) and Mobile Station (MS) is a basic method of insuring the secrecy. At this stage digital cryptographic methods are also utilized to authenticate the messages.

Authentication of the messages by means of cryptographic methods is performed by bringing an identification code (IC) into the text. The identification code is a word or number with a fixed or variable length depending on the transmitted data. ICs are either well known to the sender and the receiver of the massage, or selected during the process of exchange. The receiver, after decrypting the message, through comparison makes sure that the received message has been transmitted by an authorized subscriber.

1. Basics of ciphering

A system of ciphering has to meet the following requirements [4,5,6]:

- the relation between the plain and the ciphering text has to be nonlinear;
- the ciphering parameters have to be changeable during the exchange.

The first requirement excludes the possibility to falsify the IC without knowing the identification key. The second one excludes the possibility of system malfunction caused by an unauthorized user trying extract a message from the system's memory and to profit by it.

The best approach to providing these requirements is to use the synchronous mode for signaling, which requires the system to posses a frame and symbol synchronization, which is undesirable for the better part of the cases. The more convenient way of meeting these requirements is to include symbols in the information sequence, which are correlated to the encryption data.

Now the encryption algorithms are divided into two groups [6]:

- classical algorithms;
- open key algorithms.

The first group algorithms use only one key for ciphering and deciphering, and the second one uses two keys: one for the transition from plain text to encryption text, and the other one for the transition from encryption to plain text. The main feature of this algorithm is that being familiar with only one of the keys does not allow you to find out the other one.

The open key algorithms are widely used in cellular systems. In these algorithms the key used for ciphering is the same for all the subscribers, and the other key used for decryption is secret. This feature is very useful for the limitation of the complexity of the protocol and the integration of the ciphering structure in cellular networks.

The open key ciphering algorithm is based on determining the, so called *one side function f*, which value y=f(x) from its definition area could easily be computed for any value of its argument x. To compute however the *inverse function* x=g(y)= g(f(x)) is practically impossible. In other words the one side function f(x) can be easily computed with the help of a computer in an acceptable short time range, but the time for the determination of the inverse function is unacceptably great in the modern conditions of development of the computer mathematics.

The first open key ciphering algorithm is called RSA (abbreviation of the first letter of its inventors' names **-** ***R****ivest*, ***S****hamir* and ***A****ldeman*). The algorithm is based on two functions E and D. The relation between these functions is given by the following equation [6]

$$D(E(*))=E(d(*))$$

One of them is used for the encryption of the messages, and the other for its decryption. By the way, the value of the function E (or D) does not allow to compute the function D or E easily, e.g. any subscriber of the system can compute the function E and guard in secret the function D. For example, for user of cellular services A there is an open key E_A and a secret key D_A.

Two subscribers A and B can use the RSA algorithm to send encryption messages. If subscriber A wants to send the message M to subscriber B, he can do it in three ways:

- to cipher the message M;
- to sign the message M;
- to cipher and sign the message M.

In the first case subscriber A converts the message M in message $C=E_B(m)$ using a secret key, then sends it to subscriber B. The later, after receiving the message C computes $D_A(C)=D_B(E_B(M))=M$.

In the second occasion subscriber A signs M by computing $F=D_A(M)$ and sends it to subscriber B (this is possible only if A knows the secret key D_A). B receives F and determines $E_A(F)=E_A(D_A(M))=M$. In this case, however, the secrecy is not guaranteed because each subscriber can do this operation by using the common key E_A.

In the third case A computes $F=D_A(M)$ and $C=E_B(F)=E_B(D_A(M))$. Then A sends C to B. B computes $D_B (C) = D_B(E_B(F)) = D_A(M)$ after receiving C. Then he computes $E_A(D_A(M))=M$.

The RSA algorithm provides an excellent protection of voce and data and is recommended for use in digital systems for mobile communications, including second generation cellular systems. In these systems the term "security" and "protection" means shutting out an unauthorized use of the system resources and ensuring secrecy of conversations between mobile users. In this aspect there are few approaches for achieving this protection:

- authentication;

- secrecy of transmitted voce and data;
- secrecy of subscriber;
- secrecy of equipment;
- secrecy of connections;
- secrecy of signals for command end control.

In the European standard for cellular communication GSM these approaches are fixed in Recommendations, which are given in table 1.[2,3]

Table 1

GSM 02.09	Secrecy aspects	Determines the features of secrecy used in GSM networks Recommends its use in mobile station and systems
GSM 03.20	Secrecy related with network functions	Determines the network functions, which are necessary for providing secrecy features, given in Rec. 02.09
GSM 03.21	Secrecy algorithms	Determines the cryptographic algorithms in communication system
GSM 02.17	User smart card (SIM)	Determines the main features of SIM

The following security related information is stored in the GSM hardware:

RAND - Random number, used for the authentication of a mobile subscriber;

SRES - Answer from a mobile station to the random number;

K_I - Individual user authentication key, which is used to compute SRES and the ciphering key;

K_C - Ciphering key, used for encryption/decryption of the messages and signals for command and control, transmitted over the radio channel;

A3 - Authentication algorithm, used to compute SRES;

A5 - Encryption/decryption algorithm;

A8 - Algorithm for the calculation of K_c;

CKSN - The Number of key sequences, which gives the real value of K_c. It is necessary to utilize different keys for transmitting and receiving;

TMSI - Temporary mobile subscriber international number;

IMSI - Identification mobile subscriber international number;

IMEI - International mobile equipment identity;

LAI - Location area identification number.

The distribution of this secrecy information in different elements of the cellular system is given in table 2.

Table 2

N	Network elementsand other hardware	Types of secrecy information
1.	Mobile station (MS)	A5
2.	Subscriber identity module (SIM)	A3, A8, IMSI, K_i, TMSI/LAI, K_c/CKSN, IMEI
3.	Authentication center (AUC)	A3, A8, IMSI/K_I
4.	Home location register (HLR)	Packet IMSI/RAMD/SRES/K_c
5.	Visitor Location register (VLR)	Packet IMSI/RND/SRES/K_c, Packet MSI/TMSI/LAI/K_c/CKSN
6.	Mobile switching center (MSC)	A5, triplet TMSI/IMSI/K_c
7.	Base station controller (BSC)	A5, triplet TMSI/IMSI/K_c

2. Coding in cellular communications

Generally speaking, the term *security* includes an error protection of information. To perform a procedure of RSA algorithm we need the messages to be divided into blocks with fixed length. Then every block is encoded in a CRC and a convolution code. Then the digital stream interleaves and is ciphered, as it is seen on figure 1. [7]

The speech coder reduces the data rate by compressing the 64 kbit/s input digital voice stream (m-law PCM) to create a 8 (in IS-54, IS-136 standard) or 13 kbit/s (in GSM standard) data stream. The IS-54 and the IS-136 standard accept a full-rate speech coder called *Vector Sum Excited Linear Prediction* (VSELP), which is replaced later from an ACELP (Algebraic Code Excited Linear Prediction) coder; the GSM standard and their derivative accept a full-rate speech coder called *Regular Pulse Excitation-Long-Term Prediction* (RELP or RPE-LTP). The incoming 64 kbit/s data are grouped into segments at a rate of 50 segments/s. Hence each segment contains 160 samples and represents a duration of 20 ms. Each segment is coded into 159 bits (in IS-54) or 260 bits (in GSM).[7]

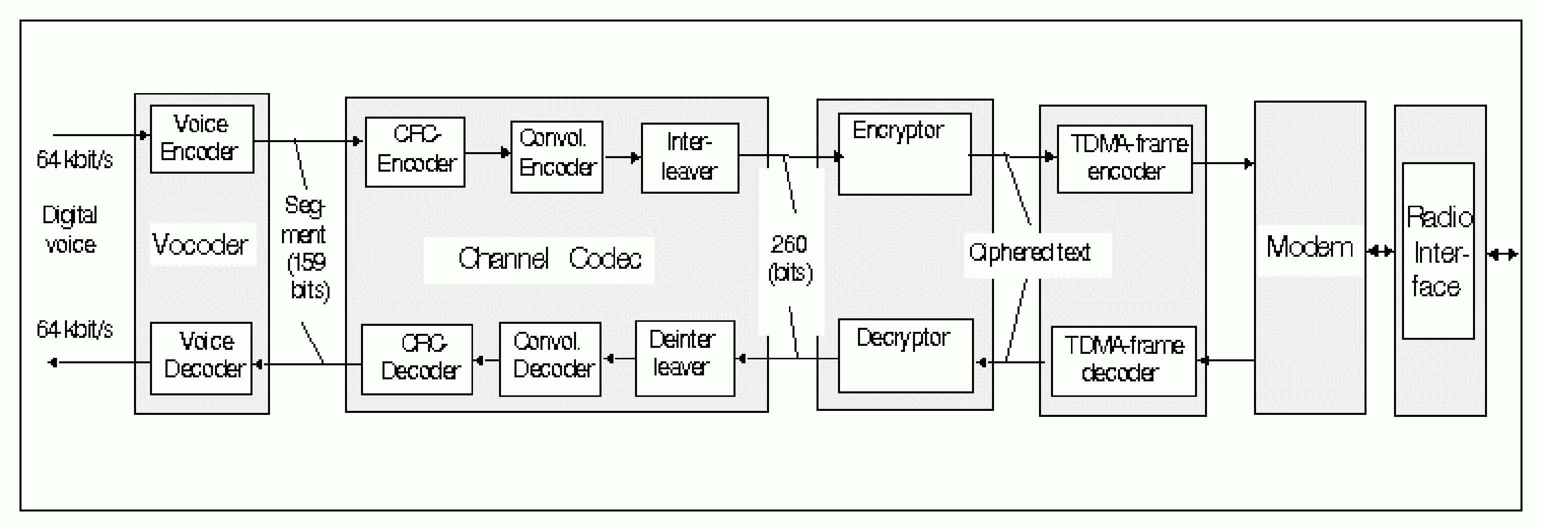

Figure 1: Basic scheme of coding and protection

Channel coder. The main function of the channel coder is to protect the data stream against the noise and fading that are inherent to a radio channel. The coder accomplishes this by adding extra or redundant bits. The greater the number of redundant bits, the higher the immunity to interference and the lower the bit-error rate. The tradeoff is an increased data rate.

The channel coder protects the data stream in five stages, represented on figure 2 [7]:

- Convolutional coding;
- Cyclic redundancy check (CRC) generation;
- Re-ordering and division;
- Interleaving;
- Burst generation.

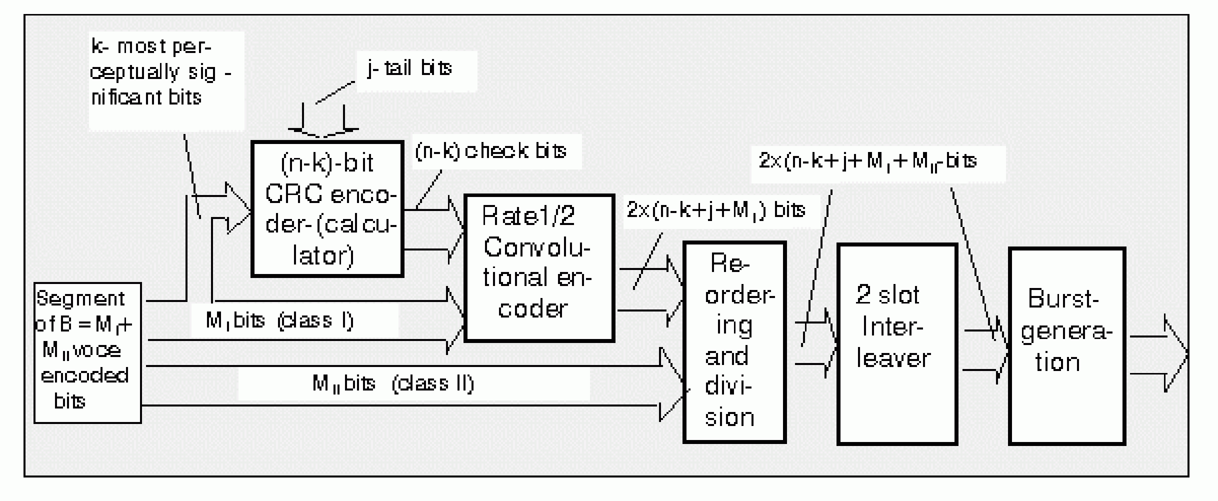
k- most per-ceptually sig -nificant bits
j- tail bits
(n-k)-bit CRC enco-der-(calcu-lator)
(n-k) check bits
Rate1/2 Convolu-tional en-coder
2x(n-k+j+M$_I$) bits
2x(n-k+j+M$_I$+M$_{II}$-bits
Re-order-ing and divi-sion
2 slot Inter-leaver
Burst-genera-tion
Segment of B = M$_I$+ M$_{II}$ voce encoded bits
M$_I$ bits (class I)
M$_{II}$ bits (class II)

Figure 2: Cannel coding scheme

The first two are mathematical operations, whereas the last two are heuristic approaches. The receiver performs an inverse operation to determine errors have occurred during propagation.

The output bit stream from voice encoder, consisting of segments with length, equal to B bits, is divided into two groups, consisting of M_I and M_{II} bits respectively. The bits of group M_I is called bits of class I. This bits is the most significant bits and it must be protected, against the nose and fading effects. In addition, k of these M_I bits are very important for decoding with high quality (these bits are called the most perceptually significant), and it must be CRC-encoded (usually it is used block (n, k) codes).

The M_I +(n-k)+j bits are then convolutional encoding in the 1/2 rate convolutional encoder. So the output segment will consist of 2 . (M_I +n-k +j) encoded bits. The last j bits fed into the convolutional encoder are tail bits of state 0 to force the encoder to also return to the zero state.

The remaining M_{II} bits, called class II bits are not protected. The encoding only significant bits (class I bits) reduces the bit rate in the system.

Convolutional coding provides error-correction capability by adding redundancy to the transmitted sequence. Convolutional encoding is implemented by linear feed forward shift registers. A convolutional coder is described by the rate at which data enters the coder and the rate at which data leaves the coder. For example, a rate 1/2 convolutional coder implies that for every 1 bit of data entering the coder, 2 bits leave the coder. The smaller the ratio, the greater the redundancy. This improves the error-protection capability.

GSM standard recommends that the bit of class 1 to be 182 and bits class II to be 78. IS-54 standard recommends that the bits of class I to be 77 and the bits of class 2 to be 82.

Cycle redundancy check (CRC) generation. Of the class 1 bits that are error-protected, it has been found that only 132 bits (in GSM) and 12 bits (In IS-54) are perceptually significant. Hence these bits are protected by using (n, k) CRC code .[7]

Re-ordering and division. After block and convolutional encoding the length of the segment is 2 . (M_I + n-k=j) bits. These bits are re-ordering first and then the segment is divided into eight frames [6] (figure 3-a).

Interleaving. In radio propagation, it has been found that the fading occurs at localized instances of time and space. As a result, interleaving spreads the information of the data stream across two frames, because it is unlikely that a clustered bit error would occur in successive frames. Finally, data propagated in burst.

To interleave the data from each frame is divided and spread across two transmitted slots using a MxN interleaving array. As a result, not all bits from a speech frame are lost by one bad slot (figure 3-b).

Burst generation. After the data has been compressed and error-protected, the bit stream is compressed (in time only) into a burst format. Burst timing offsets may be applied to facilitate dynamic time alignment (figure 3-c). After burst generation (division on packet) the packet interleaving is performed.

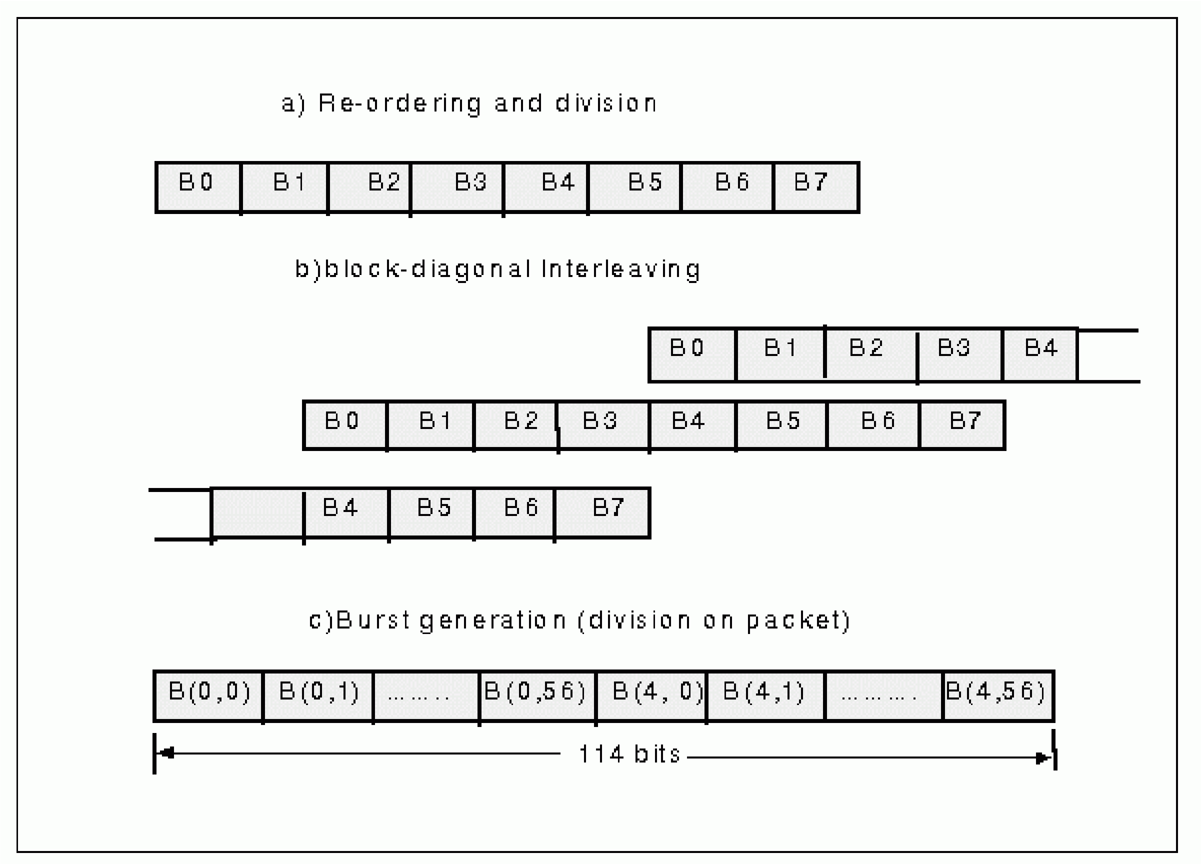

Figure 3: Re-ordering and interleaving coding information in GSM

The cannel coding of data and signals in the control cannel is performed by the same way. Table 3 shows the basic features of coding in three standards [7]:

Table 3

System/ coder	GSM	IS-54	IS-136
Type	RELP	VSELP	ACELP
Traffic channel			
Raw data rate	13 kbit/s	7,95 kbit/s	7,40 bit/s
Input bits distribution	Class Ia: 50 Class Ib: 132 Class II: 78	Class I: 77 Class II: 82	Class Ia: 48 Class Ib: 48 Class II: 52

Type of channel codes	1/2 rate convolution; K=5	1/2 rate convolution; K=6	1/2 rate convolution; K=5
CRC	3 bits on 50 bits or 1 bit per 16, 7 bits (53, 50)	7 bits on 77 bits or 1 bit per 11 bits (74, 77)	7 bits on 48 bits or 1 bit per 6,9 bits (55, 48)
Encoding data rate	22,8 kbit/s	13 kbit/s	13 kbit/s
Interleaving	Over 8 time slots	•ver 2 time slots	Over 2 time slots
Control channel			
Type of the channel codes	1/2 convolution K=5	1/4 convolution K=6	1/4 convolution K=6
CRC (block code)	40 bits on 184 (224, 184)	12 bits on 49 (61,49)	12 bits on 49 (61,49)

The length of the system cycle is chosen to be very long. For example, in the cellular system GSM this cycle is called hyperframe and its period is equal to 3 h 28 min 53 s and 760 ms. Such a long period is imposed for the purposes of ciphering. The hyperframe consists of superframes; superframe of multiframes; multiframe of TDMA frames. One hypreframe contents 2715647 TDMA frames. In cycle period every TDMA frame is numbered from 0 to N f_{max}. In RSA cryptographic algorithm the frame number is used as an input parameter.

The encryption/decryption process is discussed later in sections 4, 5, 6 and 7.

3. Authentication procedure

The purpose of the authentication is to protect the network against unauthorized use. It also enables the protection of the GSM Public Land Mobile Network (PLMN). Subscriber authentication is performed at each registration, at each call setup attempt (mobile originating or terminating), and before performing some supplementary services, such as activation or deactivation of the mobile station.

The frequency with which a particular PLMN applies the authentication procedure to its own subscribers is their responsibility. However, a PLMN shall apply the authentication procedure to visiting subscriber as often as this feature is applied to those subscribers in their home PLMN.

The procedure starts with the termination of the mobile *initialization* and *identification.*

Initialization.[1] Prior to establishing any communication links with other parties, the MS must first acquire synchronization with the GSM system. This process begins after the MS is turned on in a PLMN. The first step of the process is for the MS to search for and acquire a frequency control channel (FCCH) burst on some common control frequency cannel. The MS will scan all or part of 124 RF channels and obtain the average strength of each channel. During the scanning process, several readings of the RF level have to be taken so that the MS gets an accurate estimate of the channel power. Thus the scanning may take several seconds.

For each of the 124 channels, starting with the one of highest signal strength level, the MS searches for the Frequency Control Channel (FCCH). This is the first step of the process known as frequency synchronization. A diagram of the process is presented on figure 4. [1]

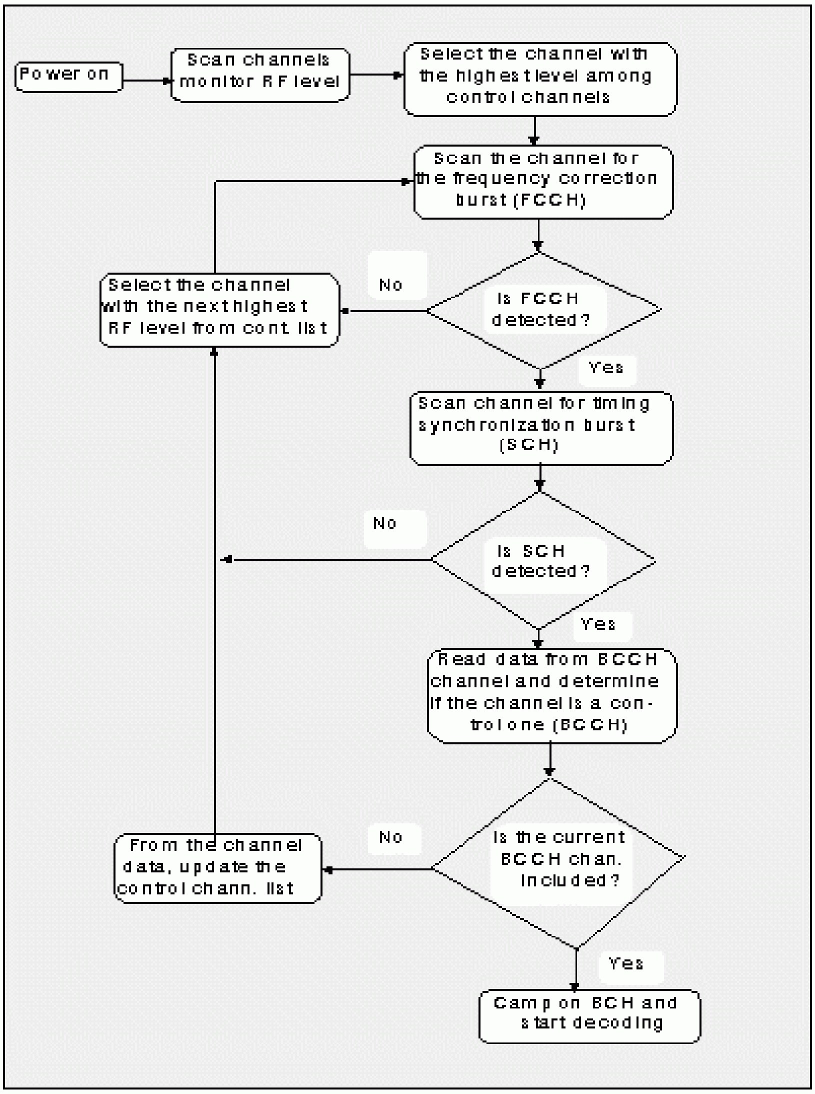
Power on
Scan channels monitor RF level
Select the channel with the highest level among control channels
Scan the channel for the frequency correction burst (FCCH)
Is FCCH detected?
No
Yes
Select the channel with the next highest RF level from cont. list
Scan channel for timing synchronization burst (SCH)
Is SCH detected?
No
Yes
Read data from BCCH channel and determine if the channel is a control one (BCCH)
Is the current BCCH chan. included?
No
Yes
From the channel data, update the control chann. list
Camp on BCH and start decoding

Figure 4: Initialization algorithm

For this purpose is used the frequency burst which is unique and easily recognizable. IF no frequency burst is detected, then the MS can go to a channel with the next highest signal strength level.

After the frequency correction burst is detected, the MS will try to synchronize with the time synchronization burst Synchronization Channel (SCH). The SCH always occurs in the next frame in the same time slot as the FCCH. This is eight burst periods later than the FCCH. SCH contains precise timing information on the time slot boundaries to permit refining the received slot timing. The SCH message also contains the current frame number to which the MS synchronize. This time synchronization is generally carried out in two steps: coarse and fine.

If synchronization does not occur, the process of frequency one with the next highest channel in the list may start. If the synchronization is successful, the MS will read the TDMA frame number and the Base Station (BS) identity code.

Assuming that the MS is in sync and decodes the information on a Broadcast Control Channel (BCCH). The BCCH information will contain such items as adjacent cell list. All BCCH transmissions are at standard power level, which permits the MS to compare received power from its own BTS as well as from adjoining BTS's. In case that the BCCH information is correctly decoded, the MS follows one of the two paths [1]:

- if the BCCH information includes the present BCCH channel, then the MS will simply stay on the channel;
- if the current channel is not in BCCH information list, or the received signal strength level is below the desired level, the MS will continue searching for the next control channel.

After the MS has successfully synchronized to a valid BCCH, the MS is now ready to register, receive paging, originate an outgoing call and doing identification and authentication.

Identification.[1] This procedure is used to identify the MS/SIM by its IMSI if the VLR does not recognize the TMSI sent by the MS. This lack of recognition can be a result of the mobile user's changing the MSC/VLR area from the last time he accessed the system or can be due to some other reason. If identification is required, the VLR sends a message, containing IMSI to the MSC. As a result of this message, MSC sends an Identity Request message to the MS. The ME responds by returning an Identity Response message containing its IMSI to the MSC. The MSC then sends the IMSI acknowledge to the VLR. If the IMSI is currently not in the VLR, then the VLR must get its file from the HLR identified in the IMSI. To du this, The VLR sends the HLR an Update Location message. Assuming that the IMSI is in fact registered in the HLR, the HLR responds with an Update Location Result message, followed by an Insert Subscriber Data message containing other pertinent data needed by the VLR. The VLR acknowledges the data transfer with an Insert Subscriber Data Result message to the HLR.

ALL this exchange of the messages is performed in accordance to RIL3-MM and MAP/D protocols.

Authentication.[1] GSM standard uses a sophisticated technique for authentication that consists of asking a question that only the right subscriber equipment (in this case the SIM-card) can answer. The core of this method is that a large number of such questions exist, and it is unlikely that the questions can be answered correctly by the wrong MS. The generic process of authentication is shown in figure 5.

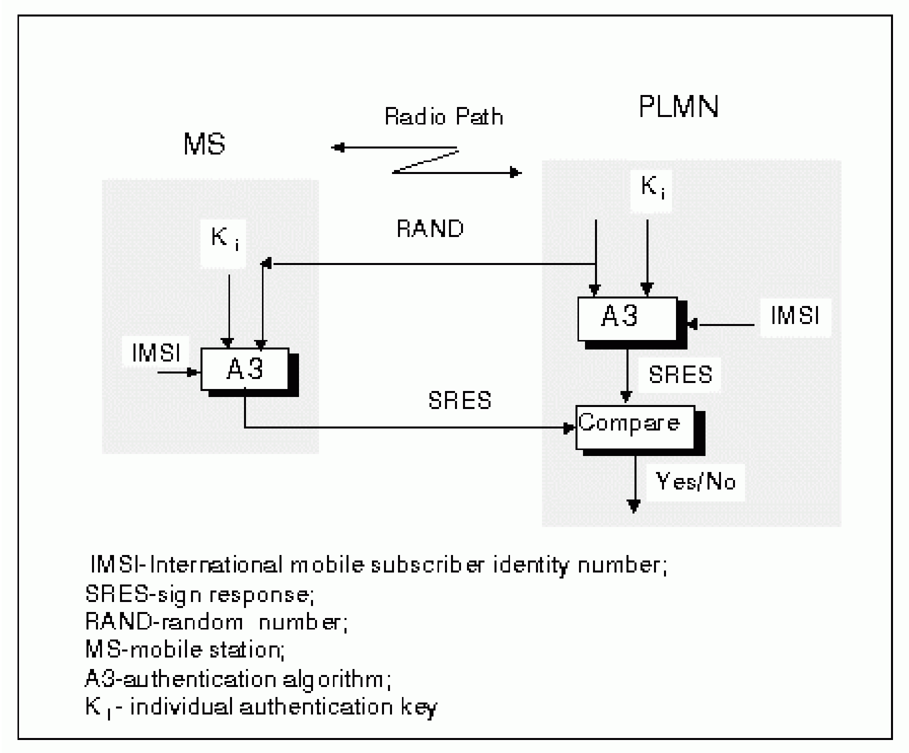

Figure 5: Authentication algorithm

The authentication algorithm A3 computes from a RAND, both at the MS and network (PLMN)

After the frequency correction burst is detected, the MS will try to synchronize with the time synchronization burst channel (SCH). The SCH always occurs in the next frame in the some time slot as the FCCH. This is and at Authentication Center (AuC). A signed response SRES, using an individual secret key K_i, attached to the mobile subscriber. The number RSND, whose value is drawn randomly between 0 and 2^{128}-1, is used to generate the response by the MS as well as by the fixed part of the network. It should be noted that the authentication process is carried out both at the MS and the network center MSC simultaneously. The Base Subsystems (BSS) remain transparent to this process.

It should also be noted that the MS only receives the random number over the radio path and in turn returns the SRES to the network. Thus an air interface mobile designation is not disclosed.

At the subscription time, the subscriber authentication key K_I is allocated to the subscriber together with its IMSI. The key K_I is stored in the AuC and used to generate a triplet (K_c, SRES, RAND) within the GSM system. As stated above, the same K_I is also stored at the MS in the SIM-card. In the AuC, The following steps are carried out in order to produce one triplet: a non predictable RAND is produced; RAND and K_I are used to calculate the SRES and ciphering key K_c using two different algorithms A3 and A8. This triplet is for each and every user and is then delivered to the network database HLR. This procedure is shown in figure 6.

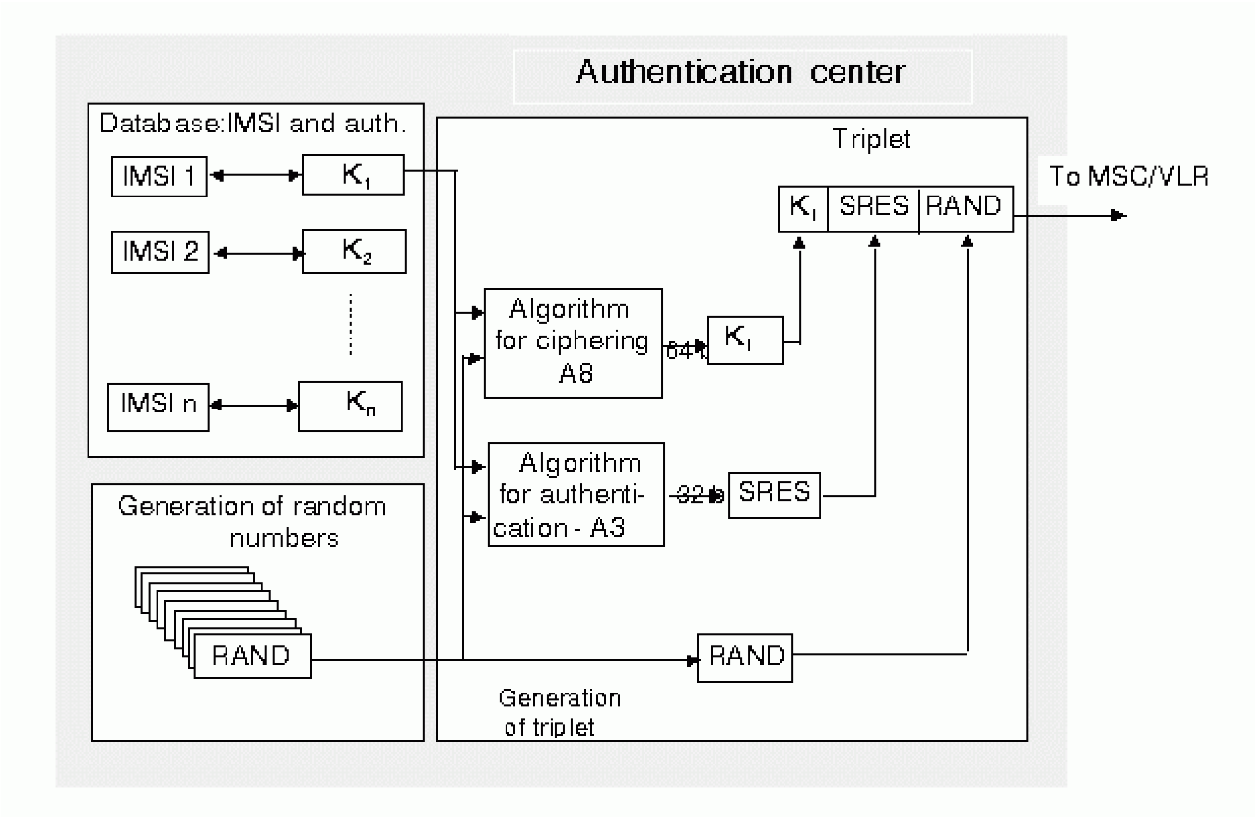

Figure 6: Generation of triplet (K_i, SRES, RAND)

The AuC begins the authentication and ciphering key generation procedure after receiving an identification of the subscriber from MSC/VLR. The AuC first queries the HLR for the subscriber's authentication key K_i. It then generates a 128 bits RAND for use as a challenge, to be sent to the MS for verification of the MS' authenticity. RAND is also used by the AuC, with K_I in the algorithm A3 for authentication, to calculate the expected correct SRES from the MS. RAND and K_I are also used in the AuC to calculate the cipher key K_c with algorithm A8. The SRES is a 32-bit number, and K_c is a 64-bit number.

The HLR transmits the value of RAND, SRES and K_c to the MSC/VLR (see figure 7 [1]) for interaction with the MS.

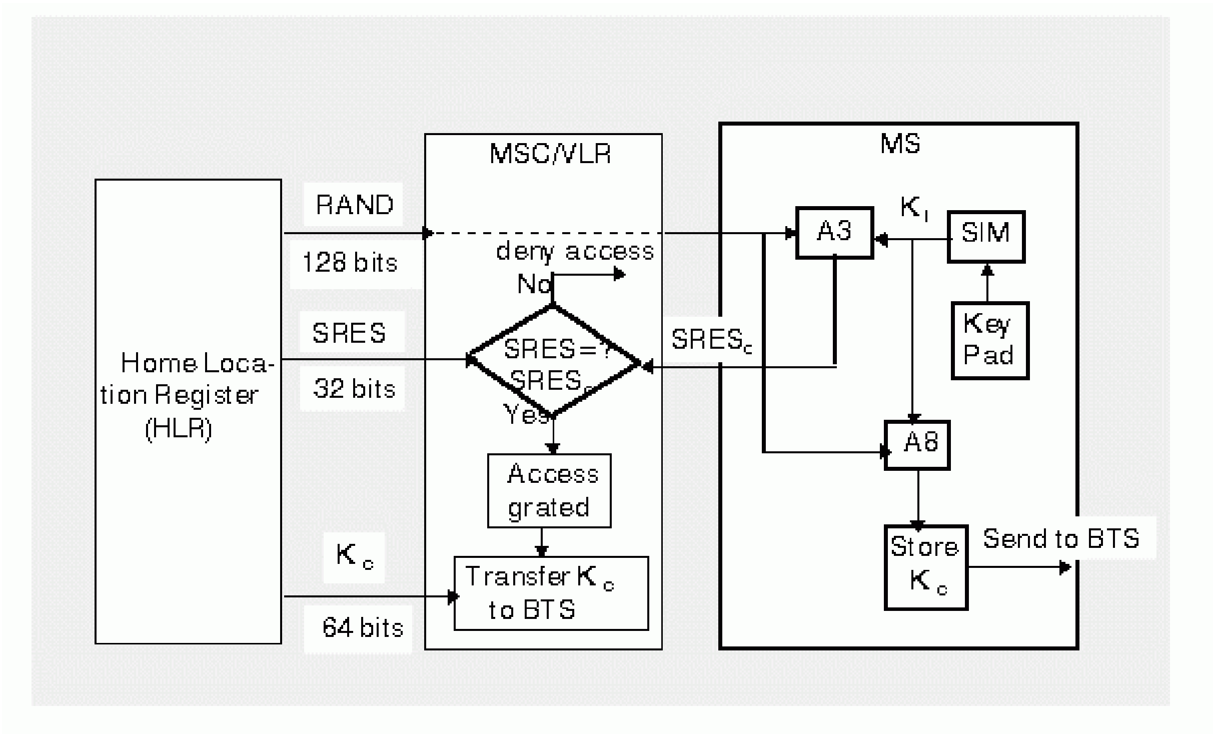

Figure 7: Full authentication process in GSM system

Algorithms A3 and A8 are not fully standardized by GSM and may be specified at the direction of PLMN operators. To protect the secrecy of the user, the authentication key is not sent to the MSC/VLR.

Based on the discretion of the PLMN operator, the authentication key can be of any format and length. The MSC/VLR forward the value of the RAND to the MS, which also has the correct K_I and algorithm A3 stored in its SIM card. The SIM then uses RAND and K_c in these algorithms to calculate the authentication $SRES_c$ and cipher key. The MS sends the calculated $SRES_c$ back to MSC/VLR, which compares it with the value signet response received from the HLR/AuC. If the $SRES_c$ and SRES agree, the subscriber access to the system is granted, and the cipher key K_c is transferred to the BTS for use in encrypting and decrypting messages to and from the MS. If the computed signed response at the MS and the signed response disagree, the subscriber access to the system is denied.

In summary, the VLR initiates authentication toward the MS and checks the authentication result.

4. The secrecy of voice and data

The secrecy of data and voice on the radio path is obtained by its encryption. It is well known that cellular systems of second and third generation use digital transmission and hence it brings an excellent level of protection by using digital cryptographic methods.

The ciphering algorithm is synchronized with the TDMA clock and adds very little complexity to the MS. The cipher key is obtained as a side product of the authentication procedure and differs from call to call. The GSM is designed so that a single encryption algorithm is used for protection of all transmitted data in dedicated mode, whether it is user information (speech or data), user-related signaling (messages carrying the called phone numbers) or even system-related signaling (the messages carrying radio measurement result to prepare handover)

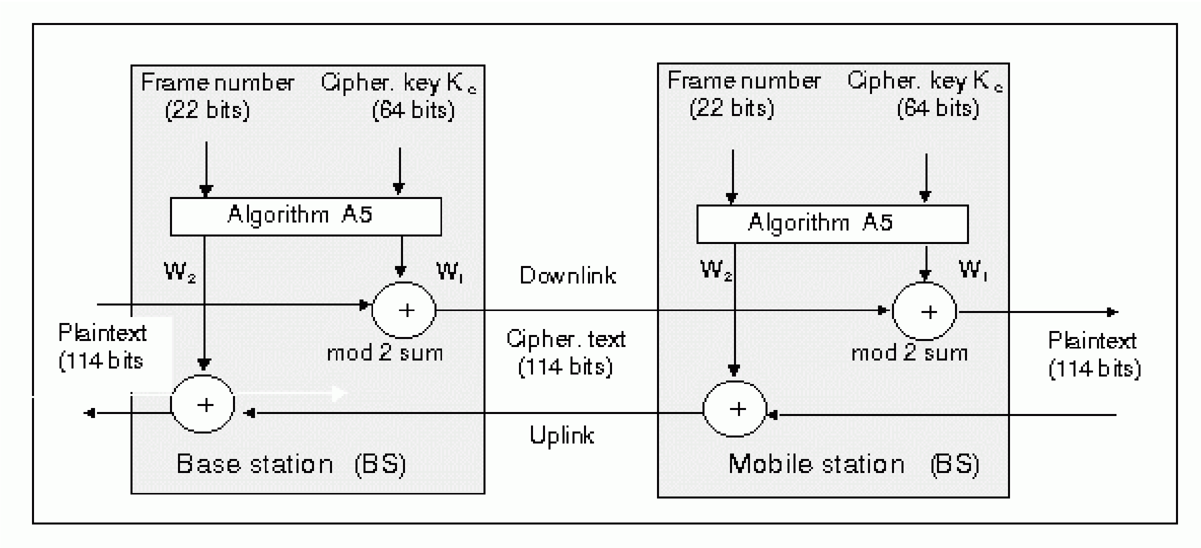

Figure 8: Data flow encryption/decryption process

Data flow on the radio path is obtained by a bit-per-bit binary addition of the user data flow and ciphering bit-stream generated by the GSM algorithm A5 using a ciphering key K_c. This exact process of encryption/decryption at the MS and at the base station is shown in figure 8. [1]

Code words W_1 and W_2 for downlinks and uplinks are changed at every frame. When modulo 2 is added with plain text, W_1 outputs ciphered text. On other side, the ciphered text, when modulo 2 is added with W_2 , outputs the plain text. The ciphering/deciphering function is placed on the transmission chain between the interleave and the modem (refer to figure 1). Since A3 and A8 are always running together, these two are implemented as a single algorithm in most cases. The algorithm A5 is standardized in the whole of GSM.

The encryption/decryption procedure starts by CMC (ciphering mode command), transmitted from MSC/VLR to MS via BSS.

5. Secrecy of subscriber

For excluding a determination (identification) subscriber by the interception of messages, sent on the radio link, any subscriber is assigned "temporary identity card" TMSI, which real only within the Location Area (LA). In other LA he is assigned new TMSI. If subscriber is not yet assigned temporary number (for instance, under first including the rolling stations), identification is conducted the attach (or detach) the international identification number (IMSI). After the completion of the procedure of authentication and beginning of ciphering mode, TMSI will be sent to the •S only in the scrambled type. This TMSI will be used under all following accesses to the system. If •S moves over to the new area of location, its TMSI must be sent together with identification area numbers (LAI), in which TMSI was assigned to the subscriber.

6. Secrecy of the equipment

The aspects of secrecy of the equipment are realized by means of equipment identification. The complete equipment identification process is shown in figure 9.

The administrative use of the International Mobile Equipment Identity (IMEI) enables the operator to check the mobile equipment identity at call setup**.** The purpose of this feature is to make sure that no stolen or unauthorized mobile equipment is used in the system.

The equipment identification procedure consists of the MSC/VLR's requesting the IMEI from the MS and sending it to a standalone entity called Equipment Identification Register (EIR).

On reception of the IMEI at the AuC, the EIR makes use of three possible defined lists [1,4,5]:

- *A white list* containing all numbered series of all equipment identities that have been allocated in the different participating GSM countries;
- *A black list* containing all equipment identities that are barred. This listing may be a result of information on stolen equipment;
- *A gray list* containing faulty or unapproved mobile equipment. This equipment is under observation but not barred for service.

Although the GSM specification recommends using the equipment identity at each and every call, the frequency of identification really lies with the individual operators. The system operator can make decisions in this regard.

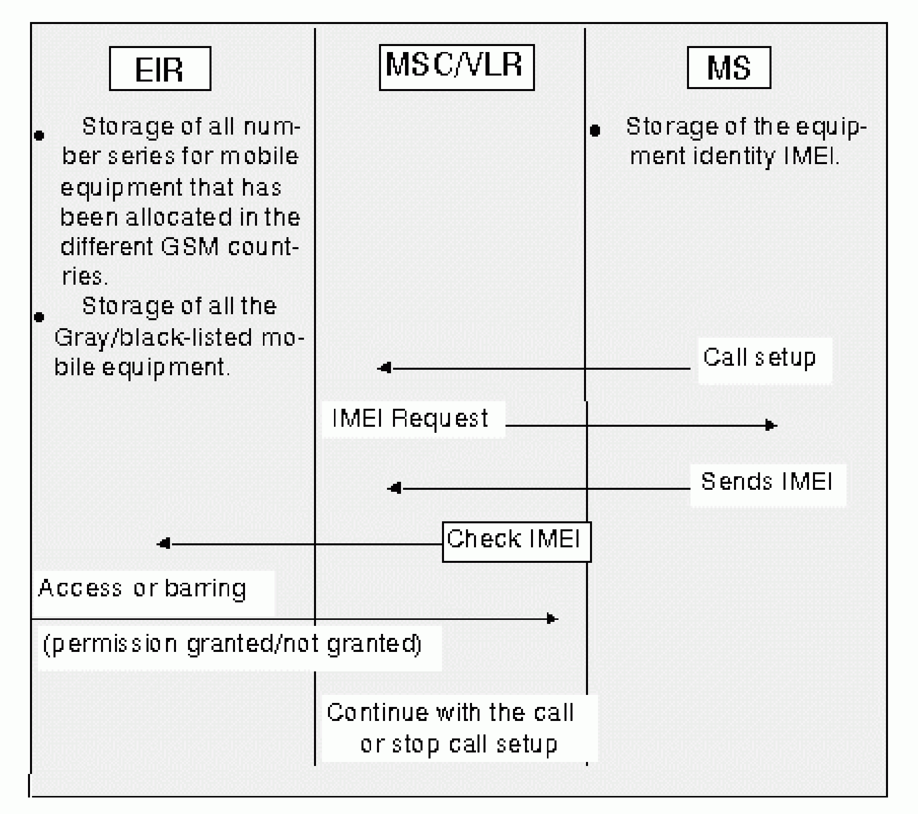
EIR
MSC/VLR
MS
Storage of all number series for mobile equipment that has been allocated in the different GSM countries.
Storage of all the Gray/black-listed mobile equipment.
Storage of the equipment identity IMEI.
Call setup
IMEI Request
Sends IMEI
Check IMEI
Access or barring
(permission granted/not granted)
Continue with the call or stop call setup

Figure 9: Equipment identification process

The equipment identification process starts with the MSC/VLR's requesting MS for its IMEI. In response, The MS sends its identity that, if positively checked by the equipment identity register (EIR), allows the MS to proceed further with the call. The MS is not allowed to continue with the call if the equipment identity does not match the stored value of the identity in the register.

As shown on figure 9, an IMEI request is initiated by the MSC/VLR combination as a result of MS's requesting a call setup. Upon receiving the IMEI request, The MS sends the equipment identification to the MSC/VLR, which is subsequently checked against the stored values in the EIR.

7. Secrecy of connections

When performing a procedure of adjustment of location on the control channel is realized exchange between MS and BTS service messages, containing the temporary subscriber number TMSI. In this case in the radio link it is necessary to ensure secrecy of renaming TMSI and its attribute to the concrete subscriber.

Let’s consider, the ensured secrecy in the procedure adjustment of the location, if the subscriber conducts a communication link and at the same time goes from one area of location in the another.

In this case the mobile station has already registered in the Visitor Location Register (VLR) with the temporary number TMSI, corresponding to the former area of location. When entering in the new area of location a procedure of recognition is realized, which is held at hold, scrambled in the radio link TMSI, sent with the name of location area identity (LAI) simultaneously. LAI gives information to the MSC/ VLR and allows to require a former area of location on the status of subscriber and its file, having excluded exchange by these service messages on control channel. In this way the messages transmitted on the communication channel is send as a scrambled information text, with the interruption of messages in the handover process, on 100-150 ms.

The procedure of adjustment of location, including features of secrecy is shown in figure 10. [6]

8. Secrecy of signaling and control massages

The confidentiality feature of physical connections (physical radio channels) means that the user information and signaling exchanged between the BTS and the MS are not made available or disclosed to unauthorized individuals, entities or processes. The purpose of this feature is to ensure the privacy of the user information (voice and non voice) as well as the user related signaling elements. All speech and data are ciphered, and all associated signaling information is protected.

Privacy protection during the exchange between network’s elements, is realized by means of Authentication Center (AuC). AuC is a main object, and is in charge of all safety aspects. This center can be a separate object or part of some equipment, for instance, in HLR. How to control AuC decides, who will be entrusted access to the network. GSM Interface with AuC is not determined.

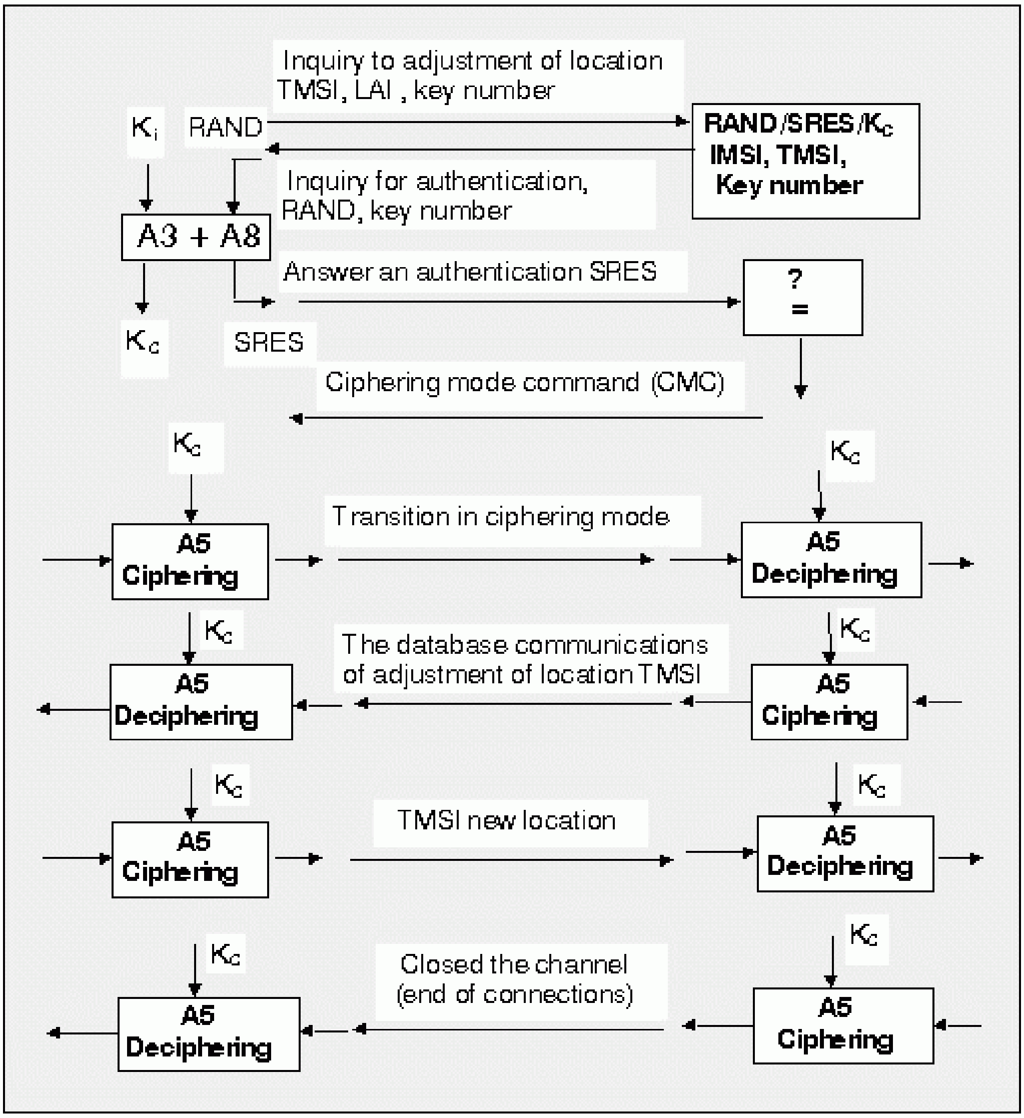

Figure 10: Procedure of adjustment of location

AuC deals with the following:

- generation of the individual authentication keys K_i of the users and its corresponding IMSI;
- generation of a triplet RAND/SRES/K_C for each IMSI and decryption this triplet for HLR at needed.

If MS moves over to the new area of location with new VLR, the later one will get secret information on this MS. This can be provided in two ways:

- MS conducts a procedure of identification on its IMSI. For the purpose, VLR requires from HLR the triplet RAND/SRES/$K_{C,}$ belonging this IMSI;
- MS conducts an authentication procedure using an old temporary number TMSI with LAI name. The new VLR requires old VLR for sending IMSI and staying groups from RAND/SRES/K_C, belonging this TMSI/LAI.

If a mobile subscriber stays on for a longer period in VLR, then after certain amount of accesses with authentication, VLR from considerations of secrecy will require new triplet RAND/SRES/K_C from HLR.

All these procedures are determined in recommendations GSM 09.02.

Checking an authentication is executed in VLR. VLR sends RAND on MSC and takes SRES corresponding responses. After positive authentication TMSI is placed with IMSI. TMSI and used encryption key K_C are sent in MSC. These procedures are also determined in recommendations GSM 09.02.

The issues of security of information on the radio link were described in section 4. Further details may be found in recommendations GSM 09.08.

Conclusion

Important aspects of security and protection of information of cellular communications (channel coding, authentication, encryption of user data and signaling information and the positive mobile equipment identification), before providing the user with service have been fully explored. The radio path information is protected due to channel coding and ciphering. The authentication procedure ensures that the network is accessed only by legitimate subscribers. Equipment ID ensures that the MS is using the correct brand of transceivers. All these features provide the secrecy of subscribers, equipment, user’s data and signaling information and different connections.

References:

1. Asha Mehrotra and Leonard Golding, "Mobility and Security Management in the GSM System and Some Proposed Future Improvement," *Proceedings of the IEEE* 86, 7 (July 1998).
2. European Telecommunication Standard Institute/Global System for mobility, ETSI/GSM specification vol.3.20, Section 3 (January 1993).
3. European Telecommunication Standard Institute/Global System for mobility, ETSI/GSM specification vol.2.17, Section 3 (January 1993).
4. V. Michel, "The Security Features in the GSM System," in *Proceedings of the 6-th World Telecommunications Forum* (Geneva: October 1991).
5. P.Vander Arend, "Security Aspects and the Implementation in the GSM System," in *DCRC Conference Proceedings* (Hagen, Gernmany: October1988).
6. U.A. Gromakov, *Standards and Systems of Mobile Communications* (Moscow: EkoTrandz, 1998) - in Russian.
7. Metodi Popov, *Coding in the Cellular Communications* (Sofia: ProCon, 2000) - in Bulgarian.

METODI KOSTADINOV POPOV is born in 1941. He holds a M.Sc. degree in Radio and Telecommunications from the "G.S. Rakovsky" Defense Academy (1980) and Ph.D. degree in communication networks and systems from the "G.S. Rakovsky" Defense Academy. Since 1982 Dr. Popov is Associated Professor at the Radioelectronics Department of the "Vassil Levsky" Army Academy in Veliko Tirnovo. Author of ten books and over 80 papers devoted to the problems of communications signals, systems and devices. Main research interests are in the area of cellular communications. Member of IEEE and BSUAE. Address for correspondence: Radioelectronics Department, "Vassil Levsky" Army Academy, Veliko Tirnovo, Bulgaria. E-mail: Kalbanov@usa.net.

BACK TO TOP

e-mail: infosec@mbox.digsys.bg

Security Aspects of the Cellular Communications

Metodi Popov

Keywords: security, secrecy, authentication, coding, cellular communications, GSM

Abstract: This article describes the basic principles and approaches used in cellular communications to guarantee protection of voice and data massages, connections, network and system equipment. It is well known that Public Land Mobile Networks (PLMN) needs a higher level of protection than traditional telecommunication networks. The second generation cellular systems as a kind of mobile digital radio systems allow to guarantee the so called information and subscriber security to their users discussed in the paper as *secrecy* and *authentication.* In the second generation cellular systems the terms "security" and "protection" (based on the GSM-standard) mean preventing unauthorized use of the system resources and ensuring secrecy of conversations (based on RSA-algorithm) between mobile users. In this aspect, the author describes the following approach to protection and security: *authentication; secrecy of transmitted voice and data; secrecy of subscriber; secrecy of equipment; secrecy of connections; and secrecy of signals for command and control.* Because in wider sense the term *security* includes also error protection of information, various standards for coding in cellular systems are described and compared.

Author:**Veselin Tselkov**
Title: **Cryptographic Software Solution for Information Protection in a Corporate Intranet**
Year of issuance: **2000**
Issue: **Information & Security. Volume 4, 2000**
Hard copy: **ISSN 1311-1493**

CRYPTOGRAPHIC SOFTWARE SOLUTION FOR INFORMATION PROTECTION IN A CORPORATE INTRANET

Veselin TSELKOV

Table Of Contents:

1. INTRODUCTION
2. BASIC CSSW SERVICES
3. ARCHITECTURE OF CSSW
    Descriptions
4. ORGANIZATIONAL STRUCTURES
    Administration and Control Center
    Key Distribution and Management Center (KDMS)
    Security Administrators
5. CSSW DESCRIPTION
References

1. INTRODUCTION

The development of the Internet as the world’s biggest network lays the foundation of the Information Society. The number of corporate systems based on the Internet technologies is gradually increasing. This leads to a rise in the threats and attacks to corporate Intranets. As a consequence, the security problems become imminent and have potentially greater impact.

The architecture of a corporate Intranet consists of nodes (local networks from workstations, servers, and communications devices) and internode communications.[3]

A number of technologies have been developed to protect these communications:

- firewalls
- virtual private networks (VPNs)

- traffic management;
- network management and audit;
- applications management and audit;
- intrusion detection systems;
- identification and authentication;
- encryption.

Cryptographic algorithms and mechanisms (symmetrical and asymmetrical) are the basis of almost all defensive technologies. However, for a significant part of commercially distributed products and technologies there are either government restrictions on the use of cryptographic mechanisms (for example, there are restrictions to the length of the keys in the United States) or necessity to receive special licenses allowing their purchase.[5,6]

Corporations dealing with top secret data have specific requrements towards their own cryptographic systems. The CSSW is a solution for cryptographic software to protect the information in a corporate Intranet.

2. BASIC CSSW SERVICES

CSSW is a Windows based software system for cryptographic protection. CSSW uses symmetrical and asymmetrical algorithms and provides the following services [1,2,7]:

- identification and authentication of users;
- identification and authentication of applications;
- cryptographic protection on file and block data levels;
- digital signature;
- access control to cryptographic functions;
- logs;
- cryptographic application program interface (CAPI).

3. ARCHITECTURE OF CSSW

CSSW consists of the following modules (figure 1):

- Crypto Machine (CM);
- Crypto Application Program Interface (CAPI);
- Local Crypto Server (LCS);

- Global Crypto Server (GCS);
- Security Administration and Control Center (SACC);
- Crypto Keys Distribution and Management Center (CKDMC);
- Security Applications.

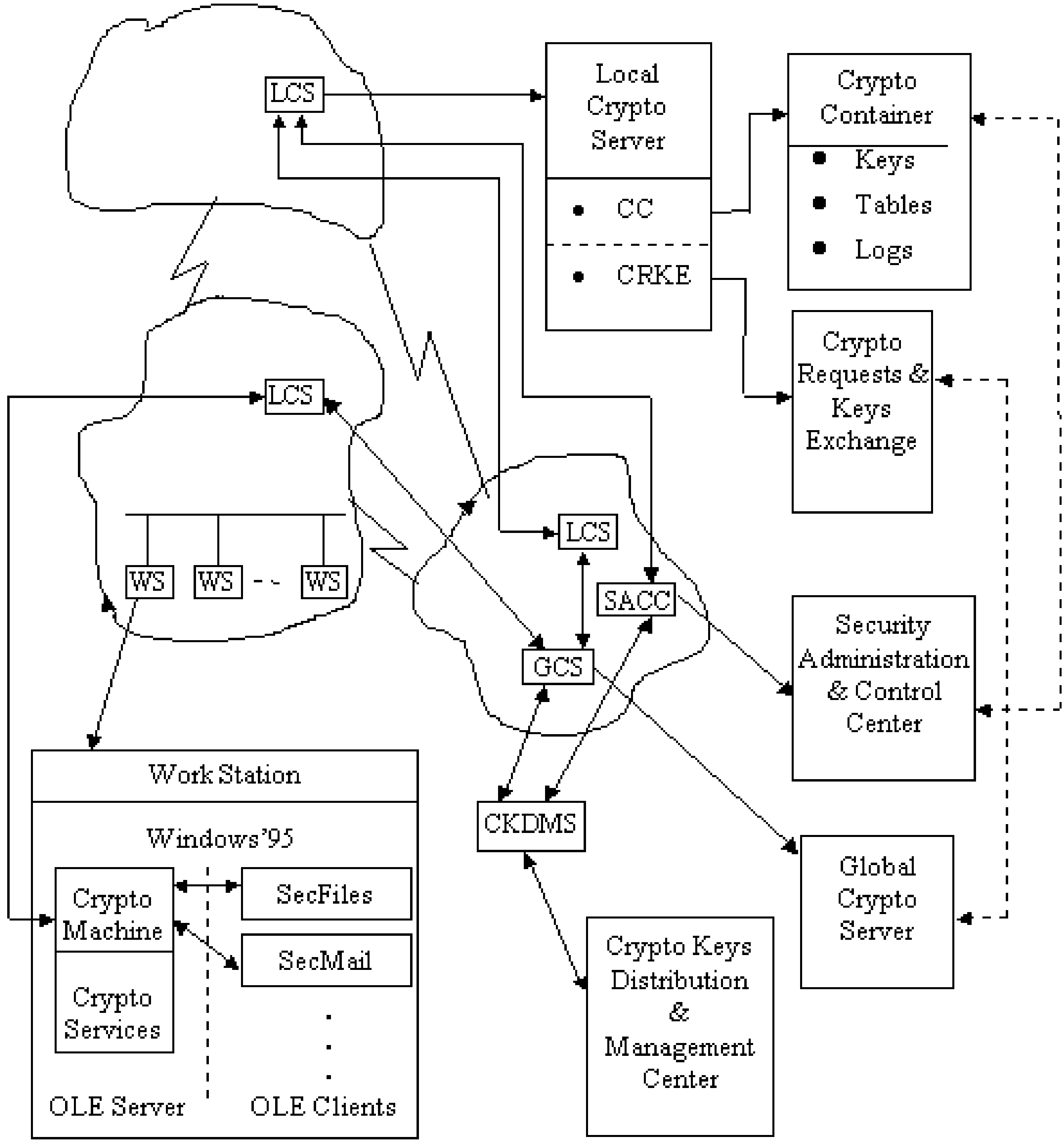

Figure 1: Architecture of CSSW

Descriptions

Crypto Machine

The Crypto Machine is a system process, working on all workstations and servers. It is an OLE Automation Server providing access control and CAPI.

Crypto Application Program Interface

Crypto Application Program Interface is included in Crypto Machine. It provides a set of cryptographic functions to user applications, which must be developed as an OLE Automation Client.

Local Crypto Server

There is a Local Crypto Server in every node. LCS consists of:

- Crypto Container (CC). CC is a storage for cryptographic keys, system tables end logs of all users in its node;
- Crypto Requests and Keys Exchange (CRKE). CRKE realizes interactions in processes of key requests and exchange.

Global Crypto Server

The module Global Crypto Server executes requests for cryptographic keys and manages their distribution. It is only one for the whole corporate Intranet and controls all Local Crypto Servers.

Security Administration and Control Center

The module Security Administration and Control Center administers and controls the executed tasks with the CSSW system. Connected with all LCS, SACC summarizes and analyzes the information of all the logs.

Crypto Keys Distribution and Management Center

Crypto Keys Distribution and Management Center generates, distributes and manages keys and passwords. It is connected with GCS.

Security Applications

CSSW is an open system for designing and developing information security applications. Some of its typical applications are disk, directory, file, e-mail, clipboard, or data base protection. Based on Microsoft standards, all applications of CSSW can be integrated with Microsoft products, i.e., MS Office.

4. ORGANIZATIONAL STRUCTURES

CSSW supposes implementation of organizational structure including

- Administration and Control Center (ACC);
- Key Distribution and Management Center (KDMC);
- Security administrators (SA).

Administration and Control Center

SACC works in the ACC. SACC executes:

- definition of users, resources, and access rights;
- definition of schemes for information interactions;
- correspondence with the Key Distribution and Management Center;
- control of the state of CSSW;
- detection and reaction to destructive events;
- control of logs and audit.

Key Distribution and Management Center (KDMS)

KDMC generates keys and passwords according to the definitions by SACC.

Security Administrators

SA supports LCS (GCS) in the node by:

- defining users, resources, and access rights in the node;
- defining schemes for information interactions;
- configuring LCS;
- supporting cryptographic tools;
- installing and administrating both user's and LCS's software;
- communicating with ACC;
- detecting and reacting to destructive events;
- controlling logs and auditing.

5. CSSW DESCRIPTION

CSSW description includes description of nodes, workstations (users), applications, and groups of keys for each application. For each workstation the description covers the applications, which will use the cryptographic functions of the Crypto Machine module and the accessible (to this application) groups of keys.

The main nodes are described through Node.Name and Node.Id.

Main workstations are described through WS.Name and WS.Id.

The main application descriptions are Appl.Name and Appl.Id.

The main group descriptions are Group.Name and Group.Id.

Each workstation needs:

- a list of security applications working on this workstation;
- a list of available groups of keys for each security application.

System files

The system files for each workstation or server are:

- CryptoMachine.GFG - configuration file for the Crypto Machine;
- SysTbl - system table;
- ApplTbl - application table, containing a list of security applications working on this workstation;
- For each security application there is a ApplGrTbl - group table, containing a list of available groups of keys for each security application.

CSSW tools

Depending on its use, CSSW tools are separated as follows:

- software tools for a workstation;
- software tools for a security administrator;
- software tools for the Key Distribution and Management Center;
- software tools for the Administration and Control Center.

Software tools for a workstation

The software tools for a workstation include:

- Crypto Machine;
- Security Applications.

Data exchange between Crypto Machine and security application is based on the standard Windows interface - Object Linked and Embedded (OLE). The Crypto Machine is an OLE Automation Server and security applications are OLE Automation Clients.

A password is required to start the Crypto Machine. If the password is incorrect, the system function ShutDown will be executed.

A user, who does not know the password still may use the workstation without access to any cryptographic functions and encrypted data.

Each application, which uses the Crypto Machine, is identified and authenticated. If this is done successfully, the application receives a list of available groups of keys and continues to work normally.

Every Crypto Machine writes the executed tasks in a log file. The record of the log file contains:

- workstation's IP address;
- application name;
- date and time;
- cryptographic service;
- key;
- error code.

The log files can be accessed from the Administration and Control Center or the security administrator.

Software tools for a Security Administrator

The software tools for a security administrator include:

- LCSConfig - for configuration of LCS;
- LCSActual - to support keys and passwords;
- LCSInstall and CMInstall - to install software on the LCS and workstations;
- LCSConfig and CMConfig - to configure software on the LCS and workstations;

- CSSWView - to audit the use of Crypto Machines.

Software tools for KDMC

Software tools for Key Distribution and Management Center include:

- a tool for definition of the architecture;
- a tool for definition of security applications and groups of keys;
- a tool for definition of relations between workstations, applications, and groups;
- a tool for generation, distribution, and management of keys and passwords;
- a tool for audit and control.

Software tools for Administration and Control Center

Software tools for Administration and Control Center include:

- a tool for administration;
- a tool for audit and control.

There are two modes of work:

- reporting all records in the logs;
- filtered reporting.

The CSSW, described in this article, was designed on DELPHI, v.3 –5, [4] and based on DBMS ORACLE. It was applied in projects of the Institute for Advanced Defense Research of the "G.S. Rakovski" Defense Academy in Sofia, Bulgaria.

References:

1. Veselin Tselkov, *et.al.*, "A software security tools for information protection in PCs – "CS_SECURE_TOOLS," in *Proceedings of the First National Conferences "INFORMATIC'94"* (Sofia, Bulgaria: SAI, 1994), 235-240.
2. Dragomir Pargov, Veselin Tselkov, Rusin Petrov and Iliya Kraytchev, "Security in Computer Systems," in *Information Aspects of Security and Development of Modern Societies*, Velizar Shalamanov and Todor Tagarev, editors (Sofia: AFSEA-Sofia, 11 - 13 September 1996), 93-98.
3. Veselin Tselkov and Dragomir Pargov, "Security of Information System on Internet," in *Proceedings of 1997 AFCEA-Sofia Seminar* (Sofia: 4-5 December 1997), 40-48.
4. M. Cantu, *Mastering Delphi 5* (Sofia: Softpress, 2000).

5. Br. Schneir, *Applied Cryptology* (John Wiley, 1996).

6. *RSA*, Available at http://rsa.com.

7. Deborah Russell and G.T. Gangemi, *Computer Security Basics* (O'Reily & Associates, 1991).

VESELIN TSELKOV: Born 1955. M.Sc. (1980, Mathematical Logic) from the Sofia University, Bulgaria. Ph.D. (1990, System programming, Network Information Management) from The Military Scientific and Research Institute. Associate Professor (1996, Informatics, Information Security). Currently Dr. Tsekov is Associate Professor in Defence Advanced Research Institute at the Military Academy "G.S.Rakovski". Main fields of interest are in the area of information assurance. Main topics of recent research: cryptography, software secure tools, security policy, intrusion detection systems. Address for correspondence: Defence Advanced Research Institute, "G.S.Rakovski" Defense Academy, 82 E. Georgiev Blvd., 1583 Sofia, Bulgaria. E-mail: vtselkov@md.government.bg and v.tselkov@nat.bg.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Cryptographic Software Solution for Information Protection in a Corporate Intranet

Veselin Tselkov

Keywords: cryptography, information security, cryptographic software

Abstract: This paper presents an original approach to the implementation of cryptographic software in a system for information protection in a corporate Intranet. It describes the architecture, the functional features, and the components of the system. The specific software solution was designed during a projects performed by the Institute for Advanced Defense Research at the "G.S. Rakovski" Defense Academy in Sofia, Bulgaria. The system is based on DBMS ORACLE. DELPHI was used in its design.

Author:**Atanas Nachev**
Title: **Electromagnetic Radiation and the Computer Data Security Problem**
Year of issuance: **2000**
Issue: **Information & Security. Volume 4, 2000**
Hard copy: **ISSN 1311-1493**

ELECTROMAGNETIC RADIATION AND THE COMPUTER SYSTEMS DATA SECURITY PROBLEM

Atanas NACHEV

Table Of Contents:

The Problem
Methods for Providing Effective Security
References

The Problem

This problem stems from two basic facts. The first is connected with the physics of the processes taking place in digital electronic equipment. The second is due to the way of representing, processing, and transferring the information. The presence of current pulses in power buses due to the impulse character of the functioning of the digital integrated circuits, the existence of inductive and capacity parasite connections, which cause the emergence of high frequency current, and the impulse character of the currents in connecting cables and interface chains all cause the emergence of parasite electromagnetic emissions, which are transmitted as electromagnetic waves. At the same time, in the cables of the power supply alternating currents are induced in such a way that the power supply circuitry becomes a source of secondary wide band emission.

The problem of the electromagnetic emission of computer systems is mainly a problem of peripheral units, the electronic screens of monitors and printers. The modules of the videotract of the monitor are one of the main reasons for the parasite electromagnetic emissions. The field, created by them, contains the whole information about the formed images. This is specified by the principle of image formation on the monitor’s screen. It is known that the video signal modulates the current of the electronic ray in accordance to the law for the received image. In that way the video signal turns to digital signal, the logical units create light dots on the luminophor of the screen. Results of studies of electromagnetic emissions of different monitors, carried out with the help of selective sensors and spectrum analyzers, show the level and the spectral characteristics of the generated electromagnetic field which depend on the type of the visualized information and the quantity of the visualized signs. The level of the narrow bands does not depend on the filling up of the screen but the system of synchronization and the frequency of the repetition of the light dots that specify it. The video amplifier is a powerful source of wide band electromagnetic emission. Practically all interface conductors can be observed as transmission antennas of electromagnetic waves. Their structure contains the whole information of the transferred data. The spectral characteristics of the field are directly dependent on the structure of the impulse consequence, transmitted along the conductors, and the energetic parameters of the field are specified by both the size and the form of the corresponding conductors and the size and the frequency of the currents. The generated electromagnetic field when computer systems operate has wide spectrum and random character of the density of the frequency and the levels of the spectrum. The frequency spectrum is too wide; it can take a band varying from several MHz to 1000 MHz and even more.[4] We should stress that each microcomputer system has a specific electromagnetic emission (features of the spectrum and its power). Placing several computers in a room with limited proportions does not lead to interference of the electromagnetic field and thus corrupting the information because of the reasons mentioned above. In the spectrum of electromagnetic emissions frequencies equal to and multiple to the clock frequency are also present.

The definition of the frequency range of the electromagnetic field containing the information of the processed data is often quite important in terms of choosing the appropriate methods and means of protection. The means for visualizing and for providing data input should be treated as major information sources in the context of the discussed problem.

Methods for Providing Effective Security

The following methods for providing effective security of the information against remote unsanctioned access through limiting the influence of electromagnetic emissions are considered feasible:

- Use of computer systems with appropriate design that provides low levels of electromagnetic energy emission. These are the means that normally belong to the so-called TEMPEST protection;
- Adequately screening the premises where the computers are placed and used;
- Use of devices for active protection [4] which generate and emit masking electromagnetic fields with corresponding characteristic.

The use of computer systems with low levels of electromagnetic emissions is perfect solution to the problem, but it involves considerable financial expenditures. Nowadays such installations can be found at the market. The major drawback of these security systems is their higher cost compared to the cost of conventional computers. For this reason there are not many producers of such systems.

The wide usage of screened premises is inexpedient because of financial, ergonomic and other reasons.

The use of appliances for *active security* [4] is promising and economically suitable. Its application is possible if the following requirements are met:

- generating and emitting electromagnetic field which secures effective masking of electromagnetic emissions transmitted by computer systems;
- emission of masking electromagnetic field with a capacity that does not "pollute" the radio frequency spectrum, i.e. the conditions of electromagnetic compatibility with other radio electromagnetic appliances are not disturbed;
- the presence of effective means for constant control over the parameters of the masking electromagnetic field, i.e. control over the presence of the necessary protective effect;
- limiting the possibilities of using computer systems when the necessary level of security is not reached;
- clear signaling when the conditions for protection are disturbed.

To limit the influence of electromagnetic emissions when the active security approach is implemented we can choose between:

- supplying each computer system with emitters of masking electromagnetic field;
- constructing systems for protecting premises and buildings equipped with computer systems.

Experiments are under way for using compensation of the electromagnetic emissions by creating a mirror-image field of the electromagnetic field generated by computer systems.[4] It is not consider possible to use this method widely.

Furthermore, protection systems can be constructed as systems for:

- independent (autonomous) protection;
- protection of premises using devices for blocking;
- protection of premises and buildings using devices for blocking and exercising central control over the security.

The autonomous protection is realized by installing security devices in the premises, which function independently without any relation to the operation of the computer systems. Administering effective control over the masking field and the generation of signal when the conditions of effective protection are violated is a must.

When blocking devices are used, the emitters of the masking field are integrated in the computer systems. When the masking effect is disturbed or when it disturbs the functioning of the system, data processing becomes impossible. It is obvious that the blocking should be done without any loss of information or violating the systems’ software. Another modification of this method is the use of reserve security means which are switched on automatically when a flaw appears in the corresponding emitters of the masking electromagnetic field. Its use is suitable for protecting premises where servers are placed and switching them off is objectionable.

Protecting premises by using locking devices and centrally controlled security devices is suitable for large buildings where top secret data is processed. The merit of the system is that it allows operative interference when there is a problem concerning the working capacity of the elements forming its structure.

Pseudo-white noise, modulated or not by noise signal impulse jamming can be used either separately or in combination with methods for protecting information through limiting the electromagnetic emissions in computer systems and their masking (active security). According to the way of generating the sequence of the impulses, both modulated and not modulated, we can have:

- impulse jamming with a constant amplitude and frequency of consequence;
- modulated and not modulated impulse jamming with a random amplitude and frequency of consequence;

It is possible also to imitate images on the screen or imitate other useful information signals.

The emission of active quasi-constant bordering jamming in the whole frequency range of the electromagnetic impulse emission from computer systems is one of the effective methods for information security. A disadvantage of this method is the need for creating a set of higher harmonics of the masking electromagnetic field over these from the electromagnetic emissions. There are some difficulties concerning the requirements of even overlapping of the frequency range from several MHz to 1GHz and more. In some cases this leads to difficulties in accomplishing the terms for effective masking of the electromagnetic emissions regarding the requirements for electromagnetic compatibility. For generating of bordering not modulated impulse jamming the use of fluctuation processes arising in semiconductors at certain conditions,[4, 5] as well as processes of excitation of constant signals in noise generators with distributed fluctuating systems, are recommended.

During the operation of computer systems high frequency electrical currents are generated in the power grid, which create conditions for remote access to the processed data. These are the reasons why protection should be provided for securing the power supply; also electromagnetic emissions should be subsided.

In conclusion, we should say that electromagnetic emissions from computer systems are subject to unsanctioned access to the processed data and therefore represent real danger. That is why the removing of the influence of electromagnetic emissions is an important element of the data securing system.

References:

1. Dragomir Pargov, Veselin Tselkov, Rusin Petrov and Iliya Kraytchev, "Security in Computer Systems," in

Information Aspects of Security and Development of Modern Societies, Velizar Shalamanov and Todor Tagarev, editors (Sofia: AFSEA-Sofia, 11 - 13 September 1996), 93-98.

2. Veselin Tselkov, "The challenges of 21th century for security of the information society," in *Proceedings of the 1999 AFCEA-Sofia Seminar* (Sofia: AFCEA-Sofia, November 25-26, 1999), 35-40.
3. *Systems for protecting digital equipment against remote access*, USA Patent No W090/00840.
4. *Computer security device*, European Patent No 0240328.
5. *Method and apparatus for preventing external detection of signal information*, USA Patent No W090/09067.

ATANAS NACHEV is an Associate professor at the "G.S. Rakovski" Defense Academy in Sofia, Bulgaria. Since January 2000 he is Head of "C4I systems" Section of the Institute for Advanced Defence Research. Prior to this appointment, Dr. Nachev served as Head of Communications and Information Systems Section of the Military Research Institute of the General Staff of the Bulgarian Armed Forces. He holds a M.Sc. (1979) and Ph.D. (1985) degrees in Computer Science.

BACK TO TOP

Information & Security. An International Journal
e-mail: infosec@mbox.digsys.bg

Electromagnetic Radiation and the Computer Systems Data Security Problem

Atanas Nachev

Keywords: information security, information assurance, electromagnetic emission.

Abstract: One set of problems in the area of information security is caused by electromagnetic emissions. This paper covers related risks and threats and describes a basis for solutions for information assurance. Presented are also original methods for solving the problem of electromagnetic emission.

INFORMATION WARFARE AND SECURITY

by Dorothy E. Denning

Addison-Wesley, December 1998, ISBN: 0201433036, 544 pages

In recent years, information warfare has captured the attention of government officials, information security specialists, and curious onlookers. The term is used to cover a broad spectrum of activity but especially a scenario wherein information terrorists, using not much more than a keyboard and mouse, hack into a computer and cause planes to crash, unprecedented power blackouts to occur, or food supplies to be poisoned. The terrorists might tamper with computers that support banking and finance, perhaps causing stock markets to crash or economies to collapse. None of these disasters has occurred, but the concern is that they, and others like them, could happen, given the ease with which teenagers have been able to romp through computers with impunity--even those operated by the U.S. Department of Defense.

This book may serve as introduction to information warfare. It is about operations that target or exploit information media in order to win some objective over an adversary. It covers a wide range of activity, including computer break-ins and sabotage, espionage and intelligence operations, telecommunications eavesdropping and fraud, perception management, and electronic warfare. The book is about teenagers who use the Internet as a giant playground for hacking, competitors who steal trade secrets, law enforcement agencies who use information warfare to fight crime and terrorism, and military officers who bring information warfare to the battleground. It is about information-based threats to nations, to business, and to individuals--and countermeasures to these threats. It spans several areas, including crime, terrorism, national security, individual rights, and information security.

The objectives of the book are fourfold. The first is to present a comprehensive and coherent treatment of offensive and defensive information warfare in terms of actors, targets, methods, technologies, outcomes, policies, and laws. Information warfare can target or exploit any type of information medium--physical environments, print and storage media, broadcast media, telecommunications, and computers and computer networks. All of these are treated within the book, albeit with a somewhat greater emphasis on computer media. The second objective is to present a theory of information warfare that explains and integrates operations involving this diverse collection of actors and media within a single framework. The theory is centered on the value of information resources and on "win-lose" operations that affect that value. The third is to separate fact from fiction. The book attempts to present an accurate picture of the threat, emphasizing actual incidents and statistics over speculation about what could happen. Speculation is not ignored, however, as it is essential for anticipating the future and preparing for possible attacks. A fourth objective is to describe information warfare technologies and their limitations, particularly the limits of defensive technologies. There is no silver bullet against information warfare attacks.

The book provides a reasonably comprehensive treatment of the methods and technologies of information warfare. It may be useful for making informed judgments about potential threats and defenses. The book is intended for a broad audience, from the student and layperson interested in learning more about the domain and what can be done to protect information assets, to the policy maker who wishes to understand the nature of the threat and the technologies and issues, to the information security specialist who desires extensive knowledge about all types of attacks and countermeasures in order to protect organizational assets. It was also written for an international audience. Although the focus is on activity within the United States, activity outside the United States is included.

The book is divided into three parts. Part I introduces the concepts and principles of information warfare. There are three chapters. Chapter 1, Gulf War--Infowar, begins with examples of information warfare taken from the time of the Persian Gulf War and the continuing conflict with Iraq. It summarizes the principles of information warfare and discusses trends in technology and information warfare. Chapter 2, A Theory of Information Warfare, presents a model of information warfare in terms of four main elements: information resources, players, offensive operations, and defensive operations. It relates information warfare to information security and information assurance. Chapter 3, Playgrounds to Battlegrounds, situates information warfare within four domains of human activity: play, crime, individual rights, and national security. It summarizes some of the activity in each of the areas.

Part II covers offensive information warfare operations. It is organized around media and methodologies and gives numerous examples of incidents in each category. There are eight chapters. Chapter 4, Open Sources, is about media that are generally available to everyone, including Internet Web sites. It covers open source and competitive intelligence, invasions of privacy, and acts of piracy that infringe on copyrights and trademarks. Chapter 5, Psyops and Perception Management, is about operations that exploit information media, particularly broadcast media and the Internet, in order to influence perceptions and actions. Chapter 6, Inside the Fence, is about operations against an organization's resources by insiders and others who get inside access. It covers traitors and moles, business relationships, visits and requests, insider fraud, embezzlement and sabotage, and physical break-ins. Chapter 7, Seizing the Signals, is about operations that intercept communications and use sensors to collect information from the physical environment. Telecommunications fraud and physical and electronic attacks that disrupt or disable communications are also covered. Chapter 8, Computer Break-Ins and Hacking, is about computer intrusions and remote attacks over networks. It describes how intruders get access and what they do when they get it. Chapter 9, Masquerade, is about imposters who hide behind a facade. It covers identity theft, forgeries, and Trojan horses. Finally, Chapter 10, Cyberplagues, is about computer viruses and worms.

Part III covers defensive information warfare, including strengths and limitations of particular methods. It has five chapters. Chapter 11, Secret Codes and Hideaways, is about methods that conceal secrets, including cryptography (encryption), steganography, anonymity, and locks and keys. Chapter 12, How to Tell a Fake, is about methods of determining whether information is trustworthy and genuine. It covers biometrics, passwords, integrity checksums, digital signatures, watermarking, and badges and cards. Chapter 13, Monitors and Gatekeepers, is about monitors that control access to information resources, filter information, and detect intrusions into information systems or misuse of resources. Chapter 14, In a Risky World, is about what organizations can do to deal with risk. It includes vulnerability monitoring and assessment, building and operating secure systems, risk management, and incident handling. Finally, Chapter 15, Defending the Nation, is about the role of the government in defensive information warfare. Three areas are covered: generally accepted system security principles, protecting critical infrastructure.

About the author:

Dorothy E. Denning is Professor of Computer Science at Georgetown University. She is the author of a classic book in the field, *Cryptography and Data Security*, a coeditor (with Peter J. Denning) of a more recent work, *Internet Besieged: Countering Cyberspace Scofflaws*, and the author of 100 papers on computer security. Her book provides a comprehensive and coherent treatment of offensive and defensive information warfare, identifying the key actors, targets, methods, technologies, outcomes, policies, and laws. Whatever your interest or role in the emerging field of information warfare, this book will give you the background you need to make informed judgments about potential threats and our defenses against them.

INFORMATION SECURITY ARCHITECTURE:

AN INTEGRATED APPROACH TO SECURITY IN THE ORGANIZATION

by Jan Killmeyer Tudor

CRC Pr., September 2000, Hardcover - 424 pages, ISBN: 0849399882

In a comprehensive treatment of information security the author describes the five key components of Information Security Architecture: organization/infrastructure, policy and procedure security baseline of system components, security awareness and training, and compliance.

The first chapter defines information security in terms of integrity, confidentiality, and availability, describes client-server environments and states issues in the development of strategic IT plans. Chapter 2 examines diverse issues of organizations such as information/resource ownership, roles of security officers, teams and committees, and human resources management issues. The next chapter is devoted to policies, standards and procedures. It covers policies on organizational security, confidentiality agreements, e-mail and Internet, security standards and procedures manuals.

Chapter 4 describes the baseline for security assessments, examining access control and program change management, LAN/WAN, operating systems and applications. It lists typical security issues in a sample baselining workplan. The next two chapters examine training and compliance issues. Chapter 7 looks at disaster recovery planning and seeks balances between security capability and cost, and between system performance and security. Chapter 8 presents main technological issues: encryption, firewalls, proxy servers, one-time passwords, and remote access servers. In the final chapter Tudor outlines the steps necessary to establish an integrated and effective security program.

The book contains a useful glossary and is accompanied by a CD with forms and worksheets to assist the reader in developing and implementing his or her own plan for information security in the organization.

INFORMATION SECURITY MANAGEMENT HANDBOOK

by Micki Krause and Harold F. Tipton, Editors

Fourth Edition, October 1999, 728 pages

CRC Press - Auerbach Publications. ISBN: 0849398290

Completely revised and updated, the new edition reveals the precise nuts and bolts of exactly how to secure systems against all intruders and security threats, no matter where they come from. It provides dozens of case studies and analyses showing exactly how to protect systems and data using the latest tools. It is also one of the most important references used to prepare for the Certified Information System Security Professionals examination. It will give the IT professional an appreciative look at security, computer crimes, and legal aspects of performing technical investigative duties.

The book's thirty-three articles are organized in ten domains as follows:

- Access Control Systems and Methodology;
- Telecommunications and Network Security (secured connections to external networks, internet firewalls, internet security, extranet access control issues, firewall management, network layer security, transport layer security, application layer security protocols for networks, security of communication protocols and services);
- Security Management Practices (security awareness program, enterprise security architecture, risk analysis and assessment, protecting high tech business secrets, information security management in the healthcare industry);
- Applications and Systems Development Security, i.e., security models for object oriented databases;
- Cryptography (fundamentals of cryptography and encryption, principles and applications of cryptographic key management, implementing kerberos in distributed systems, PKI);
- Security Architecture and Models (microcomputer and LAN security)
- Operations Security, Threats;
- Business Continuity Planning and Disaster Recovery Planning;
- Law, Investigations and Ethics;

- Physical Security.

CODING IN CELLULAR COMMUNICATIONS

by Metodi Popov

ProCon, Sofia, 2000, 348 pages, ISBN 954-90121-6-6, Edition in Bulgarian

Book Series: On the Way to Information Society

The ever increasing use of cellular communications in Bulgarian society, business and everyday life put on the specialists' agenda the task to master the fundamentals, modern principles and approaches to building and operating this type of communications systems. That is why ProCon Ltd. published the monograph "Coding in Cellular Communications" by Metodi Popov at the end of this year. The book is devoted to information coding in second generation cellular systems and is a logical consequence of two previous books by the same author - "Cellular Communications" and "Systems and Networks for Personal Communications" provided by the same publisher in 1996 and 1998 respectively.

The book contains an introduction, six chapters and appendixes. The features of cellular communications systems, considered by the author as smart communications systems, are outlined in the first chapter. The main system elements, interrelationships, encoding/decoding and modulation processes in the most common model of a smart digital communications system are described.

The second and the third chapters are devoted to encoding/decoding voice sources with instantaneous (scalar) and vector (model) quantization. There are plenty of books about the scalar quantization encoders, while books on vector quantization encoders are still rather rare. The well known and fundamental result of the Rate Distortion Theory stipulates that better performance can be achieved by quantizing vectors instead scalars, even if the continuous amplitude source has no memory. Additionally, if the signal samples are statistically dependent, that dependency can be exploited by jointly quantizing block of samples or parameters for achieving better efficiency compared with the one achieved by scalar quantization. That is why various approaches for constructing LPC-vocoders in many cellular standards are described and analyzed in this book. I believe the comparative analysis will be of interest to many communications specialists.

The forth chapter is devoted to channel encoding (decoding) of digital information. Digital information from the voice encoder's output has very low redundancy. The main function of the channel encoder is to protect the data stream against the noise and fading which are inherent in radio channels. In cellular communications the data stream is protected in five stages: convolutional coding; cycle redundancy check (CRC) generation; reordering and division; interleaving and burst generation. That is why channel with no own memory transforms into independent error channel, including both interleaver and de-interleaver. The trade-off is an increased data rate.

In order to reduce CRC bits, adding into the digital information stream, the latter is divided in two classes. The bits of class I are the most significant bits and they must be protected against noise and fading effects (convolutional codes are usually used in this case). In addition, *k* of these bits are very important for high quality decoding (these bits are called the most perceptually significant), and they must be CRC-encoded The block (n, k) codes are usually used in this case. The class II bits are not protected. Encoding only significant bits—class I bits—reduces the bit rate in the system. Practical issues of the implementation of second-generation cellular system channel encoders (decoders), i.e., in terms of effectiveness, are analyzed and compared in the fifth chapter.

The approaches of cellular systems channel coding improve system's performance by expanding the bandwidth of the transmitted signal by an amount equal to the reciprocal of the code rate. The resulting coding gain is achieved at a cost of doubling the bandwidth of the transmitted signal and, of course, at the additional cost in the implementation complexity of the receiver. In other words, channel coding is an effective method for trading bandwidth and implementation complexity for transmitter power. Therefore, as a rule this method applies to digital communications systems that are designed in the power-limited region.

The cellular systems are characterized with strongly limited power in the up link and, in this aspect, the same approach of channel coding is described as currently satisfying. But the consequent instantaneous increase of frequency deficit when the system signal power is assigned calls for implementing means of effective transmission. This is facilitated from the fact of instantaneous power adaptive adjusting, emitted from mobile user having limited power. This is possible when coding and modulation are treated as an integrated process, combining trellis-codes and multilevel phase modulations, such as ASK, PSK, DPSK or QAM. In this case a performance gain can be achieved without expanding the signal bandwidth.

The problems of the coded modulation are discussed in chapter six. The widely used in core cellular network subsystems V-modems (V.32, V.33 and V.34) are also described in this chapter. The structure of the cellular system IS-54 mobile station is given in one of the appendixes as an example of implementing ideas, principles and methods of coding and decoding, described in this book.

I reckon that the monograph "Coding in Cellular Systems" will appeal not only to radio and telecommunications engineers, but will be a useful reading for students, postgraduates and doctoral students who are working in the field of communications networks and systems. The long teaching experience of the author is a guarantee for that.

Georgi Todorov

NETWORK SECURITY FUNDAMENTALS

By Peter Norton and Mike Stockman

SAMS, 2000. ISBN: 0-672-31691-9.

his book is designed to give network administrators of any level an overview of the issues and practices involved in keeping a computer network safe from any source, whether outside or inside the network. This area has been important since the first computers started talking to each other, but interest in this area has grown in recent years as more computers have networking cards and software built in, and as the cost of the networking infrastructure (cabling, hub, routers, and so on) has plummeted.

An even stronger driving force behind the interest in networking security has been connectivity to the Internet, which is not only more available than ever, but is also becoming faster and more accessible. "Always On" is a big marketing point for cable modems and digital subscriber lines, but the same connection that allows the access to the Internet at will also allows others to enter your network by the same path. This book shows how to restrict access so that you have as much control as possible over who can see and change your systems and data.

The news has been full of reasons why you need to stay informed on networking security. Crackers are constantly inventing new ways to enter your network through bugs in your servers, flaws in Web browsers, misconfigured access privileges, weak passwords, trojan horse programs, and numerous other methods. Even worse is that newly discovered security holes are soon picked up by "script kiddies," or people who don't have the skill or intelligence to discover these flaws themselves but who seem to have unlimited time on their hands to exploit the flaws once others make them known.

There is no perfectly secure server, router, network operating system, or any other networking component. There is no such thing as uncrackable network, except for one that isn't connected at all. The most powerful element you have working for you are *preparation* and *information*. This book can help you get started on both, so you can prepare your network against most intrusion and set your systems up to notify if an attack does occur. It can also help you with information about how attacks work and where to go to find the latest updates on flaws and fixes, and what to replace with more secure alternatives.

Your allies in this fight to secure your information and systems are the security analysts, the government and educational security forces such as CERT and GIAC, and the developers of security products you can add to your network for protection, such as firewalls, routers, and intrusion detection systems. These allies are mentioned throughout this book, as well as listed in an appendix.

This book also describes how to win the cooperation of your primary allies in the fight against network crackers: your users. Through the education of your users, you can prevent social-engineering attacks (where the users are tricked into providing illicit access to your network), password-cracking attacks (where too simple passwords provide a hole into your network), and other attacks from inside and outside of your network. Without the education and cooperation of your users, none of the solutions in this book will keep you safe for long.

Finally, this book describes ways in which you can provide, rather than restrict, access to your network, but in a safe way that supports your users while protecting your resources.

About the authors:

Computer software entrepreneur and writer Peter Norton established his technical expertise and accessible style from the earliest days of PC. His Norton Utilities was the first product of its kind, giving early computer owners control over their hardware and protection against myriad problems. His flagship titles, *Peter Norton's DOS Guide* and *Peter Norton's Inside the PC* (SAMS Publishing) have provided the same insight and education to computer users worldwide for nearly two decades. Peter Norton's former column in *PC Week* was among the highest regarded in that magazine's history. His expanding series of computer books continues to bring superior education to users, always in Peter's trademark style, which is never condescending nor pedantic. From their earliest days, changing the "black box" into a "glass box," Peter's books, like his software, remain among the most powerful tools available to beginners and experienced users, alike.

Mike Stockman has been writing documentation and training users in the United States and Europe for more than 12 years. He has written about networking products for Windows 3.x, 95, and NT, as well as numerous other projects for Windows, MacOS, Solaris, and other operating systems.

LAN TIMES GUIDE TO SECURITY AND DATA INTEGRITY

by Marc Farley, Tom Stearns and Jeffrey Hsu

Mc Graw-Hill, 1996. ISBN: 0-7-882166-6.

he old Chinese proverb, "May you live in interesting times," applies as much today as it ever has, especially in the word of computer networking. The rapid growth of the Internet in the last 18 months has left many networking professionals wondering what will come next. Foremost among their concerns are questions about data protection. While many people view the Internet enthusiastically as the next great computing renaissance, many of the people who responsibly manage networks that attach to the Internet fear the unknown risks to their data. But the Internet is not the only cause for alarm. Indeed, most of the changes on networks today are internally generated. Companies are increasingly dependent on their LANs to support important business functions, resulting in an increase in LAN-resident data and a healthy concern over its safety. As the amount of data grows administrators have to look for new technologies and techniques that provide the protection they need.

This book is intended to help LAN administrators understand the issues and technology of data protection in this changing world. It uses a multidisciplinary approach to give the reader a broad perspective. Therefore, a wide range of topics are presented, including backup and recovery, archiving, hierarchical storage management (HSM), redundant systems, system security, user security management and policies, authentication, encryption, viruses, and disaster recovery planning.

The first two chapters are intended to familiarize readers with the status of network data protection today, including an examination of the threats that could cause data to be lost or stolen. Chapter 3 is an in-depth analysis of LAN backup, the foundation of any data protection scheme. It includes a discussion of the problems that cause backup systems to fail and the various technologies that can be employed to solve the problems. The fourth chapter looks at ways to manage data growth more effectively through archiving and HSM techniques. In Chapter 5, several ways are examined to implement redundancy to protect LAN systems and data.

Chapter 6 switches the focus to database systems, particularly the problems of backing up database systems on LANs. The issues of database protection are continued in the next chapter, which discusses the issues of security problems associated with database systems.

The topic of security on LANs is continued in Chapter 8 through 11. General system security, network security, advanced technologies for authentication and encryption on networks, viruses and virus protection are described in detail. The last two chapters of the book deal with future considerations. Chapter 12 looks at disaster recovery planning, and how the reader might best prepare to avoid the business-ruining calamity that could happen someday. Finally, chapter 13 examines developing trends in computing technology today and attempts to predict where some potentially dangerous exposures lie for data in the future.

About the authors:

Marc Farley has a wealth of experience helping end users select and implement backup and recovery systems for their LANs. He also worked with storage experts throughout the computer industry, assisting them in the development and delivery of LAN backup and recovery solutions to their customers. Tom Stearns is a computer consultant specializing in Xbase work. He is also the co-author of *Visual* FoxPro *Programming Basics*. Jennifer Hsu is an experience author, consultant, and journalist specializing in the area of computers and scientific technologies. He has over a decade of teaching and training experience and is currently a Professor of Information Systems at Montclair State University.

NETWORK INTRUSION DETECTION:

AN ANALYST’S HANDBOOK

By Stephen Northcutt, Judy Novak and Donald McLachlan

SAMS, 2000, Second Edition. ISBN: 0-7357-1008-2.

he need for intrusion detection analysis continues to grow. This book is training aid and reference for intrusion detection analysis. It is based on the authors’ experience in training and certification of intrusion analysts and the formal training curriculum, developed over the years. The second edition adds material that will help the reader to learn intrusion detection and to prepare for certification. For those who are willing to put the effort to become truly skilled at intrusion detection, it not only provides the knowledge, but also the structure for an accelerated learning curve.

The handbook is written by three authors with diverse experience. Stephen Northcutt is author of several books including *Incident Handling Step by Step* and *Intrusion Detection-Shadow Style*, as well as contributing editor for *Securing NT Step by Step* published by the SANS Institute. He was the original author of the Shadow intrusion detection system and leader of the Department of Defense's Shadow Intrusion Detection Team before accepting the position of Chief for Information Warfare at the Ballistic Missile Defense Organization. He serves as the lead incident handler for the Global Incident Analysis Center and Director of Training and Certification for the SANS Institute. Judy Novak is senior security analyst at the Johns Hopkins University Applied Physics Laboratory. She is involved in information assurance and research and development for the APL enterprise network. She worked for three years on the Army Research Labs Computer and Incident Response Team. Donald McLachlan' main strength is in systems and network programming in C on Unix and various real time operating systems. This strength is coupled with experience in designing and implementing link layer protocols for HF network data communications systems, as well as with long experience with computer system security.

COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION

Historically each nation and multi-national organization established its own set of computer security evaluation criteria. Examples included the UK, Canadian, U.S. and European Union security evaluation criteria. Although these evaluation criteria were similar in scope and adequate for their own unique environments, they were, in fact, different in detail. These differences resulted in developers of trusted products having to subject their products to separate evaluations by each nation or multi-national organization. There was no mutual recognition of evaluations among the nations and this quickly became an impediment to the development of trusted products because it fragmented the market into too many pieces thereby reducing the economic incentive for the developers—it became too costly and took too long to get approval of trusted products. Realizing this problem would only worsen over time, the nations agreed in the spring of 1993 to develop a set of Common Criteria, which would replace the ITSEC, CTCPEC, TCSEC, FC and others. The nations indicated above have signed up to participate in the development and subsequent use of the Common Criteria. A great deal of progress has been made since 1993 and the first and second versions of the CC were released in January 1996 and January 1998 respectively. The Common Criteria and related efforts now form a common basis for developing and evaluating trusted products in the U.S., Canada, the European Union, NATO and other nations. It is already facilitating the mutual recognition of evaluations and thereby broadening the availability of trusted products for all participants.

The Common Criteria (CC) provide a framework for the development of protection profiles, which are the mechanism used to specify the user's security requirements in an implementation independent manner. Based on the protection profile developers can then develop a security target that is a detailed statement of the security features that they will provide to meet the protection profile. The security target is usually specific for each implementation and includes the assurance requirements that the developer intends to meet. The CC also provides a set of predefined assurance packages, referred to as Evaluation Assurance Levels (EALs), which are based to some extent on existing evaluation criteria—e.g., the Trusted Computer Security Evaluation Criteria (TCSEC). International Mutual Recognition Agreements for EALs 1 through 3 have already been agreed between the US, CA, and the UK. Development of Protection Profiles is underway and several already exist for C2 and B1 systems and firewalls. Security Targets have also been submitted by developers for firewalls, routers and some applications.

TCSEC

Trusted Computer System Evaluation Criteria (TCSEC), known as Orange Book, are published in august 1983 by National Computer Security Centre (NCSC), a part of National Security Agency (NSA). They define the basic classes and trusted computer system evaluation criteria.

The Orange Book defines four broad hierarchical divisions of security protection. In increasing order of trust, they are:

- D - minimal security;

- C - discretionary protection;
- B - mandatory protection;
- A - verified protection.

Each division consists of one or more numbered classes, with higher numbers indicating a greater degree of security.

Although many of the concepts and mechanisms described in the Orange Book are applicable to network environment, the Orange Book doesn’t define what’s needed to make a network secure. Concerns about the security of data transmitted over communications networks led to the development of standard criteria for evaluating the level of trust that can be placed in a computer network. In an effort to extend the TCSEC evaluation classes to trusted network system and components, NCSC published the Trusted Network Interpretation of the Trusted Computer Evaluation Criteria (TNI, the Red Book) in 1987. Like The Orange Book , the Red Book describes broad security principles. Because network evaluation is still so ill defined when viewed from perspective of actual system in complex network environment, the Red Book requirements are likely to be revised in the near future.

ITSEC

Information Technology Security Evaluation Criteria (ITSEC, published by the Federal Republic of Germany in 1992), defines a standard that’s under development for international security. The ITSEC, which have become known as "Europe’s White Book" defines classes of functionality and assurance levels.

COMMON CRITERIA

ISO (the International Organization for Standardization) and the IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of international standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote. International Standard ISO/IEC 15408 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information Technology, in collaboration with the Common Criteria Implementation Board, a joint entity composed of members of the Common Criteria Project Sponsoring Organizations. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organizations as Common Criteria for Information Technology Security Evaluation, version 2.0.

The seven governmental organizations collectively called “the Common Criteria Project Sponsoring

Organizations" are:

- Communications Security Establishment, Canada
- Service Central de la Sécurité des Systèmes d'Information, France
- Bundesamt für Sicherheit in der Informationstechnik, Germany
- Netherlands National Communications Security Agency, The Netherlands
- Communications-Electronics Security Group, United Kingdom
- National Institute of Standards and Technology, United States
- National Security Agency, United States

The version 2.1 of the Common Criteria for Information Technology Security Evaluation (CC 2.1) is a revision that aligns it with International Standard ISO/IEC 15408:1999. In addition, the document has been formatted to facilitate its use. Security specifications written using this document, and IT products/systems shown to be compliant with such specifications, are considered to be ISO/IEC 15408:1999 compliant. CC 2.0 was issued in May, 1998. Subsequently, a Mutual Recognition Arrangement was established to use the CC as the basis of mutual recognition of evaluation results performed by the signatory organisations. ISO/IEC JTC 1 adopted CC 2.0 with minor, mostly editorial modifications in June, 1999.

CC version 2.1 consists of the following parts:

- Part 1: Introduction and general model;
- Part 2: Security functional requirements;
- Part 3: Security assurance requirements.

The Common Criteria project - Sponsoring organizations:

GERMANY:

Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Information Security Agency (GISA)
Abteilung V
Postfach 20 03 63
D-53133 Bonn
Germany
Tel: +49.228.9582.300, Fax: +49.228.9582.427
E-mail: cc@bsi.de
WWW: http://www.bsi.bund.de/cc

NETHERLANDS:

Netherlands National Communications Security Agency
P.O. Box 20061
NL 2500 EB The Hague
The Netherlands
Tel: +31.70.3485637, Fax: +31.70.3486503
E-mail: criteria@nlncsa.minbuza.nl
WWW: http://www.tno.nl/instit/fel/refs/cc.html

UNITED KINGDOM:

Communications-Electronics Security Group
Compusec Evaluation Methodology
P.O. Box 144
Cheltenham GL52 5UE
United Kingdom
Tel: +44.1242.221.491 ext. 5257, Fax: +44.1242.252.291
E-mail: criteria@cesg.gov.uk
WWW: http://www.cesg.gov.uk/cchtml
FTP: ftp://ftp.cesg.gov.uk/pub

UNITED STATES - NIST:

National Institute of Standards and Technology
Computer Security Division
820 Diamond, MS: NN426
Gaithersburg, Maryland 20899
USA
Tel: +1.301.975.2934, Fax: +1.301.948.0279
E-mail: criteria@nist.gov
WWW: http://csrc.nist.gov/cc

UNITED STATES - NSA:

National Security Agency
Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 20755-6740
USA
Tel: +1.410.859.4458, Fax: +1.410.684.7512
E-mail: common_criteria@radium.ncsc.mil
WWW: http://www.radium.ncsc.mil/tpep/

Organizations

Hewlett Packard – www.hp.com

Hiverworld (Enterprise network security) – www.hiverworld.com

Internet Security System – www.iss.com

NetSecure Software – www.netsecuresoftware.com

Network-1 Security Solutions, Inc – www.network-1.com

ODS networks – www.ods.com

Surf CONTROL – www.surfCONTROL.com

TRIPWIRE Security Systems, Inc. – www.tripwiresecurity.com

White Papers

www.sans.org/tools.htm

Some consolidated information security vulnerabilities

http://cve.mitre.org

www.iss.net

http://seclab.cs.ucdavis.edu

www.cs.purdue.edu/coast/projects/vdb.html

www.rootshell.com

Public domain security tools

ftp://ciac.llni.gov/pub/ciac/sectools/unix/

ftp://coast.cs.purdue.edu/pub/tools/

ftp://ftp.cert.org/pub/tools/

ftp://ftp.porcupine.org/pub/security/index.html

ftp://ftp.funet.fi/pub/unix/security

Incident response centers

www.auscert.org.au/

www.cert.org/

www.ciac.llnl.gov/

www.assist.mil

www.fedcirc.gov

www.first.org

www.cert.dfn.de/eng/dfncert/

www.nasairc.nasa.gov/incidents.html

www.fbi.gov/nipc/index.htm

www.fbi.gov/contact/fo/fo.htm

www.cert.dfn.de/eng/csir/europe/certs.htm

Good security web sites

www.cerias.purdue.edu/coast

www.telstra.com.au/info/security.htm

www.nsi.org/compsec.htm

www.securityportal.com/

www.tne.nl/instit/fo/intern/wkinfsec.htm www.java.sun.com/security/

www.ntbugtrag.com/

www.boran.com/security/

www.icsa.net/

www.IOpht.com/

ftp.porcupine.org/pub/security/index.htm

Government security web sites

www.itpolicy.gsa.gov/

www.cit.nih.gov/security.html

www.nswc.navy.mil/ISSEC

www.ncsl.nis.gov/

Underground security web sites

www.pharck.com/

www.2600.com/

Some good security books

www.amazon.com/

www.clbooks.com/

www.barnesandnoble.com/

Books

- Actually Useful Internet Security Techniques by Larry J. Hughes Jr.
- Applied Cryptography: Protocols, Algorithms and Source Code in C by Bruce Schneier

- Building Internet Firewalls by Brent Chapman & Elizabeth D. Zwicky
- Cisco IOS Network Security by Cisco Systems
- Designing Network Security by Mike Kaeo
- Firewalls and Internet Security by Bill Cheswick & Steve Bellovin
- Halting the Hacker: A Practical Guide To Computer Security by Dorothy E. Denning
- Internet Security for Buisness by Gene Shultz, et al
- Instruction Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response by Edward G. Amoroso
- Instruction Detection: Network Security Beyond the Firewall by Terry Escamilla
- Securing Java: Getting down to buisness with mobile code by Gary McGraw and Ed Felten
- Linux Security by John S. Flowers
- NT 4 Security by Michel Moncur, Charles Perkins and Matthew Strebe
- Network Intrusion Detection by Simson Garfinkel
- Practical UNIX and Internet Security, 2nd Edition by Simson Garfinkel & Gene Spafford
- The NCSA Guide to Enterprise Security: Protecting Information Assets by Michel E. Kabay
- Virtual Private Networks, 2nd Edition by Charlie Scott, Paul Wolfe, et al
- Web Security Sourcebook by Avi Rubin, Dan Geer, and Marcus Ranum
- Web Security & Commerce by Simson Garfinkel with Gene Spafford

Some good security mailing lists

Send your subscription to the email address listed for each group, usualy with a "subscribe listname" in the body of the message.

- Best Security List (bos) best-of-security-request@cyber.com.au
- Bugtraq Full Disclosure List listserv@securityfocus.com
- CERT Advisories cert-advisory-request@cert.org
- CIAC Advisories (ciac bulletin) Majordomo@rumpole.llnl.gov
- COAST Security Archive coast-request@cs.purdue.edu
- Firewalls Digest (firewall-digest) majordomo@lists.gnac.net
- Firewall Wizards (firewall-wizards) majordomo@nfr.net

- FreeBSD Security issues majordomo@freebsd.org
- Intrusion Detection Systems (ids) majordomo@uow.edu.au
- Linux Security Issues linux-security-reguest@RedHat.com
- Legal Aspects of Computer Crime (lacc) majordomo@suburbia.net
- NT Bugtraq listserv@listserv.ntbugtraq.com
- The RISKS Forum (risks) risks-request@csl.sri.com
- WWW Security (ww-security-new) majordomo@nsmx.rutgers.edu
- The Virus Lists (virus-l & virus) LISTSERV@lehigh.edu
- The SANS Digest subject: "subscribe." info@sans.org
- The SANS NewsBites subject: "NewsBites Subscription" digest@sans.org
- The SANS NT Digest subject: "NT Digest." info@sans.org

STARTING POINTS FOR ANTIVIRUS SOFTWARE

A list of Antivirus Software is:

- Symantec - www.symantec.com (Norton AntiVirus 2000);
- Command Software System - www.commandcom.com (Command AntiVirus 4.57);
- F_Secure www.f-secure.com – (F-Secure Anti-Virus 5);
- Computer Associates www.antivirus.cai.com – (InoculateIT 4.5 Personal Edition);
- McAfee – www.mcafee.com – (McAfee VirusScan 4.04);
- Norman Data Defense – www.norman.com – (Norman Virus Control 4.72);
- Panda Software – www.pandasoftware.com – (Panda Antivirus Platinium);
- Trend Micro – www.antivirus.com – (PC-cillin 6).

NOTES ON INTERNET SECURITY

(by the SANS Institute)

he SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they learn and find solutions for the challenges they face. SANS was founded in 1989. The core of the Institute includes security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire SANS community. During 2000 and 2001, this core will grow rapidly as the Global Incident Analysis Center (GIAC) and the GIAC Certification programs develop mentors who will help new security practitioners master the basics.

The SANS community creates four types of products

- System and security alerts and news updates
- Special research projects and publications
- In-depth education
- Certification

Many SANS resources, such as news digests and research summaries and award-winning papers and security alerts are free to all who ask. Income from printed publications funds university-based research programs. The Global Incident Analysis Center and special research projects are funded by income from SANS educational programs.

Contact addresses:

SANS Institute
5401 Westbard Ave. Suite 1501
Bethesda, MD 20816

Email for information: sans@sans.org
Email for research programs: sansro@sans.org
Email for vendor programs: exhibits@sans.org
Email for certification programs: giactc@sans.org
Conference Registration phone: +1 720 851 2220
Conference Registration FAX: +1 720 851 2221
Office phone: +1 301 951 0102
Office Fax: +1 301 951 0140

The ten most critical Internet security threats (by SANS Institute Roadmap, 3rd edition, Summer of 2000)

1. BIND weaknesses: nxt, qinv and in.named allow immediate root compromise.
2. Vulnerable CGI programs and application extentions (e.g., ColdFusion) installed on web servers.

3. Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd (CalendarManager), and rpc.statd that allow immediate root compromise.
4. RDC security hole in the Microsoft Internet Information Server (IIS).
5. Sendmail buffer overflow weaknesses, pipe attacks and MIMEbo, allow immediate root compromise.
6. sadmind and mountd.
7. Global file sharing and inappropriate information sharing via NetBIOS and Windows NT ports 135>139 (445 in Windows2000), or UNIX NFS exports on port 2049, or Macintosh Web sharing or AppleShare/IP on ports 80, 427, and 548.
8. User Ids, espacially root/administrator with no passwords or weak passwords.
9. IMAP and POP buffer overflow vulnerabilities or incorrect configuration.
10. Default SNMP community strings set to ‘public’ and ‘private’.

The Ten Worst Security Mistakes Information Technology People Make (by SANS Institute Roadmap, 3rd edition, summer 2000)

1. Connecting systems to the Internet before hardening them (removing unnecessary service and patching necessary ones).
2. Connecting test systems to the Internet with default accounts/passwords.
3. Failing to update systems when security vulnerabilities are found and patches or upgrades are available.
4. Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI (public key infrastructures).
5. Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated.
6. Failing to maintain and test backups.
7. Running unnecessary services, especially ftpd, telnetd, finger, rpc, mail, rservices.
8. Implementing firewalls with rules that allow malicious or dangerous traffic-incoming or outgoing.
9. Failing to implement or update virus detection software.
10. Failing to educate users on what to look for and what to do when they see a potential security problem.

ACRONYMS

AC	Access Control
ACL	Access Control List
BSI	Bundesamt für Sicherheit in der Informationstechnik
C4I	Command, Control, Communication, Computing and Intelligence
CAPI	Cryptographic Application Program Interface
CC	Common Criteria
CESG	Communications-Electronics Security Group
CIS	Communication and Information Systems
COMPUSEC	Computer Security
COMSEC	Communications Security
DAC	Discretionary Access Controls
DMS	Decision-Making System
DSB	Defense Science Board
E3	End-to-End Encryption (E3)
EA	Electronic Attack
EAL	Evaluation Assurance Levels
ElP	Electronic Protection
EmP	Emanations Protection
EW	Electronic Warfare
FW	Firewall;
GIAC	Global Incident Analysis Center
GISA	German Information Security Agency

I&A	Identification and Authentication;
IA	Information Assurance
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
INE	In-line Network Encryption
IS	Information Security.
ISO	International Organization for Standardization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria (Europe’s White Book)
IW	Information Warfare
JTC	Joint Technical Committee
KDMC	Keys Distribution and Management Center
LAN	Local Area Network
MAC	Mandatory Access Control.
MLS	Multi-Level Security
NAT	Network Address Translation
NCSC	National Computer Security Centre
NNCSA	Netherlands National Communications Security Agency
NSA	National Security Agency
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
RA	Remote Access
S/HTTP	Secure Hyper Text Transport Protocol
S/MIME	Secure Multiparty Internet Mail Extension

SSL	Secure Socket Lear
TCSEC	Trusted Computer Security Evaluation Criteria (Orange Book)
TNI	Trusted Network Interpretation of the Trusted Computer Evaluation Criteria (Red Book)
VPN	Virtual Private Network
WAN	World Area Network

INFORMATION SECURITY IN THE 21st CENTURY: GLOBAL CONVERGENCE

Swedish-Bulgarian Government IT Security Conference

Swedish-Bulgarian Government IT Security Conference was held from 18 to 24 September 1999 in the Council of Ministers' Hotel in Bansko, Bulgaria--in the foothills of the Pirin Mountain. Main objective of the conference was to establish and strengthen the scientific contacts and collaboration among Swedish and Bulgarian scientists, researchers, and industry representatives.

The International Organizing Committee was co-chaired by Arne Jernelov from the FRN - Swedish Council for Planning and Coordination of Research, and Eugene Nickolov from the National Laboratory of Computer Virology - Bulgarian Academy of Sciences (NLCV-BAS).

The conference was hosted by the National Laboratory of Computer Virology.

Over fifty Bulgarian and Swedish scientists and users participated in the conference, and thirty-two reviewed papers were presented at eight plenary sessions. Two additional sessions for discussions and the concluding session were focused on scientific and policy management issues related to the basic problems of information security.

The topics covered were compliant with European Union's Fifth Framework Program:

- Information Technology and Science;
- Communication science and Human-Computer Interaction;
- Network Technology, Network Security;
- Software Engineering, Middleware, Groupware;
- Data protection, Storage Technology, Cryptography;
- Electronic Commerce, Payment and Signature;
- Security Systems;
- Identification Systems.

Additionally, representatives of governmental institutions of both countries decided of initiate joint activities in the field of IT security, which without any doubt will contribute to the solution of some of the major problems in this area.

NATIONAL LABORATORY OF COMPUTER VIROLOGY

BULGARIAN ACADEMY OF SCIENCES

Organizational status: The National Laboratory of Computer Virology at the Bulgarian Academy of Sciences is unique scientific organization in Bulgaria, specialized in the domain of computer virology and information security.

Subject of research: Computer virology as an independent scientific branch is founded on the achievements of several fundamental scientific branches such as mathematics, computer science, physics, chemistry, and, lately, biology of cell bodies and genetics of microorganisms. The devising of computer viruses is a creative human activity. It has originated almost simultaneously with the creation of the first computer program. And as it often occurs with the human achievements, this idea found its "negative" realization in the information destruction in the millions of computers all over the world. Companies worldwide, each having a judgment on the computer world, make considerable investments in the competition *viruses vs. anti-viruses*, because the outcome of this competition will define to a great extent the future of the computer systems. In particular, this was a typical activity for the past few years when the idea of the biological behavior of the computer viruses and genetically borrowed mechanisms for propagation became a reality and when the self-encoding and self-mutating algorithms of the computer viruses followed closely the model of biological cells and organisms.

Main research areas: Computer Security; Communications Security; Data Security.

Priorities:

- Investigation and classification of new viruses;
- Methods and means for discovery of computer viruses;
- Methods and means for removing computer viruses;
- Methods and means for data recovery;
- Approbation of methods and means listed above;
- Studies in the domain of encryption standards;
- Investigations in the field of the systems for access control;
- Investigations in the domain of client-server applications.

Investigation methods:

- Evaluation of the influence of operational environments - definitions and parameters;
- Evaluation of a given class of computer viruses - definitions and parameters;

- Creation of analytical models - simplification and verification;
- Optimization processes - function, parameters and experiments;
- Creation of simulation models - simplification and verification;
- Analysis of achievements, conclusions, recommendations, corrections;
- Algorithmic solutions for a given class of virus signatures;
- Program realizations for a given class of virus signatures;
- Creation of programs included in the product NLAB;
- Monthly versions for the updating of NLAB.

Main achievements: Compact programs are created for certain platforms, identify more than 50 000 virus signatures and remove the viruses. Effective protections of the type "monitor" and "checker" are created, assuring minimal loss of resources.

Subject of the research of the departments of NLCV:

1. *Department of Computer Security:* Methods and means for discovering and removing computer viruses in computers and computer systems with various operational systems and platforms.

2. *Department of Communications Security:* Methods and means for network protection from computer viruses in computers and computer systems with various operational systems and platforms.

International collaboration: The Laboratory plays an active role in the initiatives and the projects of ACM (Association for Computer Machinery), CARO (Computer Anti-virus Researcher's Organization), EICAR (European Institute for Computer Anti-virus Research), IEEE/CS (IEEE's Computer Society), ISSA (Information Systems Security Association). An active part is also taken in electronic conferences on anti virus topics in the following networks: INet, InterNet, JANet, OMNet, UUNet, VIRNet etc. The Laboratory is a member of the worldwide union of the developers of anti-virus software – Anti-Virus Products Developers. Through the International Federation of Information Processing (IFIP) personal contacts are made and official correspondence exchanged with different technical committees and work groups, for example: IFIP/TC11/WC11.1 Security Management, IFIP/TC11/WG11.3 Database Security, IFIP/TC/WC11.5 System Integrity and Control, IFIP/TC11/WC11.8 Computer Security Education. Leading young specialists from NLCV undertake business trips, specialization courses and work in the USA, Canada, Belgium, Japan, Sweden, Denmark, Iceland and other countries.

Education and training: NLCV takes an active part in the training of highly qualified scientists, researchers and staff. In the past years, few dozens of graduation papers were prepared in the Laboratory and submitted successfully in fulfillment of graduation requirements. A series of post-graduate works by external orders were carried out. Few submissions of Ph.D. dissertations are forthcoming. Specialists from the Laboratory lecture and carry on practical sessions on Computer Virology, Computer Security, Communications Security, Data Protection, Computer Network and Systems and Operating Systems in the Sofia University "St. Climent Ohridksi", the Technical University of Sofia, the University for National and World Economy in Sofia, the New Bulgarian University, Burgas, and the Free University. Courses on "Methods and Means for Computer Protection" are organized together with staff from the Parliament, the Presidency, the Ministry of Defense, the Ministry of Finance, the Ministry of Foreign Affairs, the Ministry of Internal Affairs, the Ministry of Transportation and Communications, the National Electric Company and other governmental organizations, as well as for private companies.

RESEARCH AND DEMONSTRATION CENTRE

of the Institute for Advanced Defence Research

During the year 2000 a team of IT researchers form the Institute for Advanced Defence Research designed and launched Research and Demonstration Centre (RDC). Main areas of activity of RDC are as follows:

- Installation, investigation and evaluation of hi-tech achievements in the area of information and communications technologies for the needs of the Ministry of Defence and the national security of the Republic of Bulgaria;
- Demonstration of technical and system capabilities;
- Design of pilot projects and evaluation of the technological propositions for C4I system development;
- Education and training.

The tests and expert investigation of the technical solution of the different programmes of the MoD will be completed in accordance with a new model of the life cycle of C4I systems for the Bulgarian armed forces.

The Research and Demonstration Centre will be one of the points of formal contacts between research and teaching staff of the Bulgarian armed forces and the most developed world leaders in area of communications and information technologies.

RDC has the following structure:

- research-demonstration hall with investigation area and site for presentations, press-conferences and lectures;
- Internet laboratory;

- Net–technology and information security laboratory;
- Electronic systems and means laboratory;
- Spectral measurement laboratory;
- Area for business contacts.