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.

I&S