INFORMATION ASSURANCE IN C4I SYSTEMS

Veselin TSELKOV and Dragomir PARGOV

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.

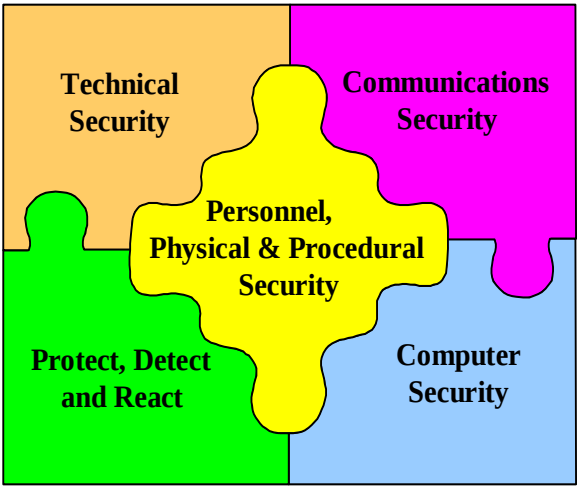

Figure 1: Information assurance

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:

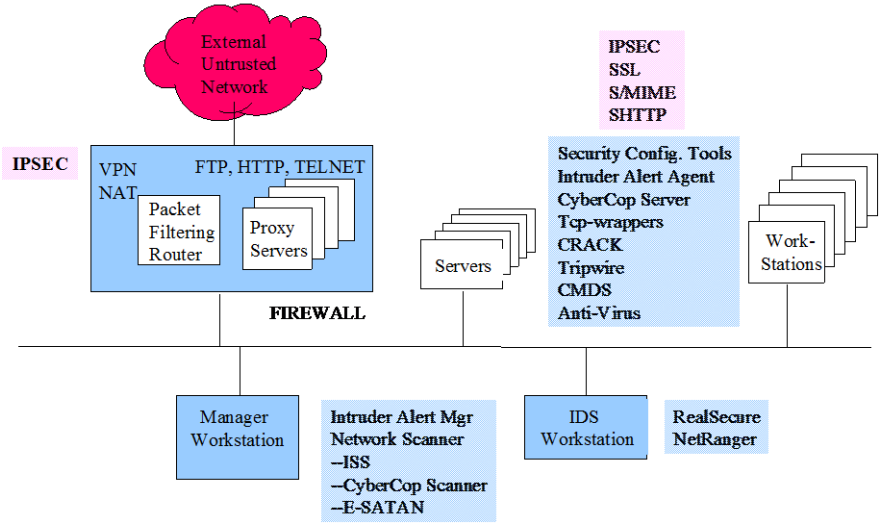

Figure 2: An Example of unclassified enclave

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.