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.

Information warfare is a â€œholistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations.â€ The 2010 Military Doctrine of the Russian Federation says that these measures are implemented â€œto achieve political objectives without the utilization of military force.â€ In contrast to Soviet propagandaâ€”which the regime went to great lengths to proclaim as the truthâ€”modern Russian information warfare does not prioritize this, modern information warfare seeks to plant seeds of doubt and distrust; to confuse, distract, polarize and demo