"Security of Computer Systems and Networks" Book Preview

Article *in* Computer Science and Information Systems · June 2007

Source: DBLP

CITATIONS
2

READS
9,772

4 authors:

Dragan Pleskonjic
IGT (formerly GTECH)
92 PUBLICATIONS **83** CITATIONS
SEE PROFILE

Nemanja Maček
Visoka Škola elektrotehnike i računarstva strukovnih studija u Beogradu
65 PUBLICATIONS **195** CITATIONS
SEE PROFILE

Borislav Djordjevic
University of Belgrade
79 PUBLICATIONS **132** CITATIONS
SEE PROFILE

Marko Caric
Visoka Škola elektrotehnike i računarstva strukovnih studija u Beogradu
28 PUBLICATIONS **35** CITATIONS
SEE PROFILE

UDC 004.6

"Security of Computer Systems and Networks" Book Preview

Dragan Pleskonjić[1], Nemanja Maček[2], Borislav Đorđević[3], Marko Carić[2]

1 Finsoft Ltd,16-18 Hatton Garden, London EC1N 8AT, UK
Kosovska 51, 11000 Belgrade, Serbia
dragan.pleskonjic@finsoft.com, dragan@conwex.org
2 Advanced School of Electrical Engineering (VETŠ)
Vojvode Stepe 283, 11000 Belgrade, Serbia
nmacek@vets.edu.yu, stonerhate@gmail.com, carmar@vets.edu.yu
3 "Mihajlo Pupin" Institute
Volgina 15, 11000 Belgrade, Serbia
bora@impcomputers.com

Abstract. This paper presents preview of the new book titled "Security of Computer Systems and Networks" (original in Serbian language "Sigurnost računarskih sistema i mreža") – textbook for University lectures, but also a book that covers majority of important areas concerning current state of security. The book is the result of lecturing experience, research in this area, and also practical experience that authors have in many fields, including but not limited to architecture and design of security products and software, network projects, consultancy, analysis of issues and problems and providing solutions to them. It is not just a textbook for students, as it is suitable for all IT professionals and also for company management including IT as well as general management for companies, organizations and government agencies that base their vital infrastructure on computer and mobile technology. It is suitable for decision makers and for people who want to get almost complete overview of the computer and network security as it is now. In some areas of computer security, such as intrusion prevention and detection systems, e-commerce, and proper network and operating system security administration, this book goes one step further, presenting some novelties in the field and suggesting new solutions for actual problems.

1. Introduction

Computer systems and networks security is an issue that has been around us all for a long period of time. Security has initially been governments' and military problem for quite some time – let's just say – long enough. Then it has become a problem that numerous financial institutions have faced with (banks, insurance companies, investing funds). Now, with Internet and mobile technology being heavily used in business and everyday life, almost anyone

who uses a computer and Internet cuts the deal with security in one way or another. For example, an individual that just wants to shop something on e-Bay heavily relies on security issues. Although this is as a very simple example which appears so easy to solve, it actually covers many aspects of computer security and requires a lot of math, sweat, hard work and proper planning.

Students at colleges and universities, IT professionals, software architects, developers, network and security administrators and many others are required to be quite familiar with security, privacy, protection and similar topics and issues.

This is also important area for senior company management and decision makers as security in different area, including protecting vital infrastructure is “sine qua non” for today’s companies and organizations.

2. Motivation, Goals and Who Should Read this Book

This book is based on lectures that are presented to students on “Computer Networks Security” in many years and on different schools and universities. It also covers experience gained through practical work in the field. This includes architecture and design of computer networks, complex software projects and information systems, network security administration as well as research done in particular areas of computer systems and information security.

This book serves the protectors – the persons who are willing to give their best shot to protect their assets 24/7. Note that hackers have all the time in the world to wait, and yes, they will catch you while you take a nap and get what they want – be it the money, the data or revenge. It reveals the threats, the attacks and dangers you will be exposed to on the Internet, as well as the methods, techniques, tools, procedures and products that can help you to establish a bit more secure network or computer system. The book is suitable for both beginners, medium and high level users, programmers, administrators, designers and other professionals that interoperate with security in one way or another. It is a textbook both for students that attend this course on their colleges and for management of companies that rely on computer systems and networks. It explains both the theory and the practice – one step at a time without taking detours to details we found unnecessary. This book will not teach you how to break into someone's network, or decrypt your neighbor's e-mail, but it will teach you how to make your network more secure and protect your e-mail's confidentiality and integrity.

3. Book Scope and Content

The first problem that authors have faced with is how to present this material to readers, having in mind that many areas are closely linked and overlapped,

and also having in mind necessary preconditions and knowledge required for active following and understanding of subjects that we are talking about. We identified that knowledge of mathematics, computer architectures, operating systems, computer networks and communications (including good knowledge of standard protocols and protocol stacks), data models and structures, databases, programming (especially system level programming, C, C++, C# and Java languages), and Internet is necessary. Also, many particular areas from above list and some additional are recommended knowledge to successfully follow book content

In this situation, we took decision to briefly cover some areas at the beginning of book chapters and to remind readers before going into depth of security elaboration.

Another challenge was that this book, even highly technical has to deal with some areas that are not technical. Security is not just math and technology. It depends a lot on psychological and social aspects (simply said – on people and their weaknesses), organizational, management, social sciences, legal and economic issues and also on organizations and policies. These makes book truly multidisciplinary and requires wider knowledge of many different areas.

3.1. Chapters and appendices

Book contains 16 chapters and 5 appendices arranged in a manner we find suitable for students, beginners, but also advanced users, system administrators, software developers and IT and company management.

Chapter 1: Threats, attacks, security and methods of protection. This chapter covers the basics of computer system and network security: security attacks and threats, mechanisms and services, security as an evolving process and the C.I.A. (confidentiality-integrity-availability) triad. This chapter also covers threat modeling, risk equation, security strategies (like layers of protection) and two basic security models (secured channel and gatekeeper/ACL based model) and deals with the information classification. This chapter is introduction to almost anything you will find in latter chapters. For example, it is a normal path for a reader to understand what modification attack is first and then to read more on session hijacks as well as it is necessary to understand what secure channel is if you are about to read more on cryptographic protocols.

Chapter 2: Security architectures and models. This chapter covers some basics regarding security architectures – abstraction, information hiding, protection rings, security labels, modes of operation and distributed architectures, as well as architecture vulnerabilities (covert channel, lack of perimeter checking, maintenance hook vulnerability and TOC/TOU attack), and recovery procedures. Aside from that, this chapter deals with the evaluation criteria (TCSEC and ITSEC), accreditation, and certification

(DITSCAP and NIACAP). At the beginning of the second part of this chapter we have tried to resolve the problem which is common for many authors and publishers: we've tried to explain the difference between terms Safety and Security. The second part of the chapter requires some basic knowledge of formal theories as it deals with the different information security models – access control models (Bell-LaPadula, access matrix and take-grant model), integrity models (Biba and Clark-Wilson) and information flow models (non-interference model and composition theories).

Chapter 3: Cryptography. Although there are many different ways to improve security, cryptography still has a major role in the world of information protection. Therefore, this chapter is dedicated to a short review of useful cryptographic accomplishments. At the beginning of the chapter, we've managed to put up together a subset of mathematical facts and theorems which are necessary for a reader to understand the processes of encryption, signing and calculating hash. Like many other books on cryptography, this book also contains a short history of encryption, a process which has, thanks to cryptoanalysis, been forced to advance from simple origins to very complex algorithms. This book covers most modern symmetric (DES, AES, IDEA and all AES finalists) and public key encryption algorithms (RSA and ElGammal), stream ciphers (RC4 for example), hash functions (MD5 and SHA), pseudorandom number generators, as well as digital signatures, certificates and public key infrastructure. At the end of this chapter, we've given some pointers to readers that wish to use cryptography in their business or everyday life, as many software products provide a user with ability to use complex algorithms with the aid of a simple interface, without a need to know details of algorithms and the way that they are implemented.

Chapter 4: Cryptographic and authentication protocols. This chapter is a rather easy reading, but also a logical successor to 120 pages of cryptographic algorithms and problems (which readers that lack knowledge of maths usually try to avoid). Therefore, cryptography by itself is removed as much as it was possible from this chapter, leaving only some basics and protocols. We can call it “Security protocols”. To simplify this, this chapter is suitable both for ones that are familiar with computer networks and for those who are familiar with cryptography but do not know how to set up their IP address. This chapter covers two crucial forms of security protocols: cryptographic protocols (SSL and IPSec working in transport and tunneling mode with both AH and ESP protocols as well as IKE key-exchange protocol explained in a rather simple way) and authentication protocols (Kerberos and RADIUS). However, due to publisher's scope limitation, installation, configuration and administration of software that implements these protocols is not described and analyzed in this chapter as it requires deep knowledge of Linux operating system's networking services.

Chapter 5: Firewalls. Unlike written in the book Firewalls 24/7, we've really tried to simplify firewalling to its very basics. We've managed to basically

cover all aspects of firewalling in theory and practice: packet filtering, NAT and proxies. This chapter will teach a reader how to install a firewall on a $100 computer using any Linux distribution that comes with a Netfilter and iptables (for packet filtering and NAT) and Squid (for proxy). Port scanning is also explained and reader is introduced to how it really works through a couple of examples based on Nmap. Windows workstation users will find some useful information on freeware firewalls for Windows workstation computers and network administrators are introduced in a very simple way to packet filtering with Cisco routers. You will not find ISA or any other commercial enterprise firewall solutions reviewed here – please, feel free to use Linux with iptables and squid in order to achieve higher goals and have smaller expenses.

Chapter 6: Intrusion detection and prevention systems. Firewalls and cryptographic tunnels will protect your network from outsiders. But you still have a problem with semi-outsiders and insiders including their mutual collaboration. And with the hackers that will exploit any known vulnerability in your security configuration. So what shall you do? You set up an intrusion detection/prevention system (IDS/IPS) that sends alerts on suspicious activities that are invisible to firewalls. This chapter covers these systems – their basics and classification according to different criteria (what and where they do their job and how they detect intrusions) and the theory behind them (true/false positives/negatives, sensitivity, specificity, accuracy, ROC and predictive values). Snort is briefly explained (its structure and configuration) as an open-source solution and the de-facto IDS standard. Aside from Snort, Fortego All-Seeing Eye is also briefly described as a very strict after-the fact Windows IDS that requires some initial training. This chapter introduces a new IDS system for wireless networks (WIDS) that has been developed by one of authors. The use of artificial intelligence in IDS/IPS systems is briefly discussed in this chapter and is, in parts, a novelty of authors.

Chapter 7: Malicious software. This chapter deals with software that knows no strict and precise definitions – malicious software (malware). Malware can be defined as any code that is written with intent to cause damage to computer (be it networked or not), or to make it hard or impossible for users to use that computer or to compromise data confidentiality. There are various forms of malware – some require carriers, others do not; some of them do replicate; others do not. This chapter covers almost any type of malware – worms, viruses, logic bombs, trojans, spyware and adware (the last one being usually nothing more than a user molester). Each type is defined and briefly elaborated. Readers are also introduced to specific malware (like MyDoom and Sasser worms) that have managed to cause major damage at their best and to free ways (free software and precaution that should be considered) to protect their assets from malware. A special part of this chapter is dedicated to rootkits – a stealth threat that makes an attacker invisible and gives him the root privileges over a target computer. UNIX and Windows rootkits are

classified and analyzed in this chapter as well as the famous example of unfair usage of rootkits it an edgy legal DRM matter.

Chapter 8: E-commerce and Internet security. E-business is becoming a common form of business these days as it reduces costs and introduces new ways to starting, development and growth of business. But, the fact that the Internet is the e-business infrastructure of Internet introduces several new security risks and possibilities that the attackers can exploit. The criminal goes there where the money already is – in this case, to the Internet, where you can find it at its worst form. This chapter deals with the e-business security; we hope that it will inform readers of security risks that are related to e-commerce and to adequate protection methods and mechanisms. Aside from that, this chapter covers other aspects of Internet security – phishing, pharming, spam, VoIP and P2P network security.

Chapter 9: Wireless and mobile networks security. The growth of wireless and mobile networks reminds us on growth of Internet in mid 90's. Simple implementation of devices, flexibility, reduced costs and a choice of different devices (wireless network cards and access points) from different vendors are several factors that support the growth. Due to their advantages, wireless networks are commonly used in many institutions, companies or other private or public organizations. Aside from that, there is also a trend of setting up hot spots on places where many people pass by – these hot spots will let anyone who uses a supported communication device to connect to the Internet. On the other hand, the use of wireless networks is usually followed by many problems regarding security and privacy. At its lowest layer – just check out how the antenna spreads the signal throughout the air. Can you really be so certain that no unauthorized users will catch that signal – can you precisely define the wireless network perimeter? No. This chapter deals with all of security problems related to wireless and mobile networks – Wireless LAN security (WEP, 802.1x, EAP, WPA, and 802.11i, for example), GSM security and Bluetooth security. Major algorithms, standards, protocols, security procedures and testing tools are briefly described in a matter we find suitable for most readers.

Chapter 10: Operating system security. Everything runs on a certain form of operating system. Running a perfectly safe application or service on an insecure operating system may give a fake sense of security but actually equals to disaster. Therefore, an administrator must make a host operating system as much secure as possible. This chapter is divided in three parts. The first part deals with the fundamental concepts of operating system security and protection (protection domains, access matrices, operating system security mechanisms, etc.). The second part deals with the Linux security (file system access control, user accounts, sudo, networking, sandboxing with chroot jail, syslog, etc.), but most of the principles and techniques discussed here can be used with any UNIX based operating system. The third part discusses basics of Microsoft's Windows security (user

accounts, group policies, NTFS permissions, auditing, etc.) This chapter is suitable for almost everyone – ranging from a home user who wants to hide files from his little sister or parent who want to protect his kids, to a network administrator who wants to protect his shared resources and understand what has been written to log files.

Chapter 11: Database security. When we talk about information security, we think about secure transfer and secure storage of data. When we talk about secure storage, we mostly think of secured file systems (described in chapter 3) and databases. This chapter deals with the various aspects of database security. Chapter begins with basic database security administration – permissions, roles, views and stored procedures. Despite the fact that database should normally reside behind the Web server and in private network (not in the DMZ), it's logical position in the network and firewall protection doesn't make it prone to malicious activities, like a well known SQL injection. We've used MS SQL Server to demonstrate that improperly protected database can be easily manipulated by an attacker that is familiar with SQL injection attacks.

Chapter 12: Secure programming. Software development is a process that gives birth to many useful applications but also to numerous security flaws and vulnerabilities. Although some authors might agree that this chapter should reside somewhere on the beginning of the book, we have found that it fits right here – not all computer users are programmers; and if they even are familiar with programming, a chance that they will have access to closed source software is very small. Therefore, we have decided to deal with the computer and network administration and engineering problems first, and with the designer's and programmer's issues later. This chapter deals with the fundamentals of secure programming – that is a writing a code and having security in mind. It covers the buffer overflow problem in C and C++ (a problem that can be exploited to inject malicious code into another application or service), the most important aspects of secure programming in Java and methods of software products protection (registration keys, keyfiles, authorization and dongles). This chapter also covers the advantages of managed code and the new Security Development (SDL) lifecycle from Microsoft.

Chapter 13: Network monitoring. Reliability and availability of computer systems and networks has become a critical aspect of many production sites these days and one of security goals, as well. Due to that, several protocols and complete sets of tools for network monitoring and management have been developed. This chapter covers basics of network monitoring and management, without detouring into unnecessary details. SNMP protocol is briefly described, as well as the Nagios network monitoring system. No detailed instructions for this tool installation have been given, as we consider that readers that deal with network monitoring are usually familiar with software installation and administration on Linux systems.

Chapter 14: Organizational, physical, legal and social aspects. Unlike other chapters, this one is focused on the topics that most "geeks" will definitely try to avoid. Those topics are based on management, sociology, psychology, organization, and law. Although many might disagree, this is equally important domain as cryptography and firewalling and, as such, should not be avoided. This chapter covers the basics of previously mentioned aspects – organizational, ethical and legal aspects in brief. Aside from that, biometrics and steganography are also briefly described. This chapter talks about intellectual property, authors' rights and software piracy and different approaches to these problems. Social aspect of security problems are also topic covered in this chapter.

Chapter 15: Business continuity and disaster recovery planning. If the computer network is used as infrastructural basis of business information systems, you do not have any guaranties that everything will work perfectly and strictly according to plan. That means that you should be aware of the fact that incidents do happen and therefore you must prepare a plan to recover your business from occurring incidents. Incidents are not just minor security violations (like unauthorized access) which can easily be fixed, but also some fundamental dangers that can lead to cancellation of business. The business cancellation will last according to the quality of your business continuity and disaster recovery plans, which this chapter deals with. Unlike other domains of protection which are based upon reducing risk and setting up protection mechanisms, this domain handles with the fact that the worst thing has already happened. Business continuity planning deals with the planning and infrastructure which is necessary to provide normal business activities once that incident occur. Unlike that, disaster recovery planning domain deals with the procedures necessary for successful business recovery with the minimum negative consequences for your organization. Aside from that, this chapter covers the basics of archiving and backup (which safeguards your data) and computer forensics (which can help you find the guilty ones and prosecute them in the court of law).

Chapter 16: Ethical hacking and penetration testing. Once all protection mechanisms, tools and procedures have been successfully deployed, implemented, installed and configured, complete security configuration must be tested. Different methods of network penetration testing have been developed and have proven to be reliable and effective. Unfortunately, hackers are not predictive at all as they constantly develop new methods and techniques to achieve their goals. Aside from that, attackers have more time and they can usually choose time and means (tools and techniques) to perform a successful attack. Therefore, company management came up with a trick: to hire a person that is familiar with hacking to test their network against weaknesses, penetration and different type of attacks. These persons – white hat hackers or ethical hackers – have in depth knowledge of what hackers do but are men of trust and are in line with ethical aspects of

computing. This chapter covers penetration testing and ethical hacking in brief – what is it, how it's being done as well as the corresponding legal and ethical aspects.

Also, book has five interesting appendices:

Appendix A: Security standards and certifications. Covers the most important security standards (ISO 17799, ISO 27001, NIST standards like DES and AES, Common Criteria and Internet standards) and certification programs (CISSP, CHECK, CESG, GIAC, CCSP, INFOSEC).

Appendix B: Free security tools, open source software and other security resources. This appendix briefly describes a subset of open-source and free security related software, mostly for Windows operating systems, as Linux distributions already contain this as integral part. Aside from that, reader can find other free security-related resources (web pages, books, blogs, etc.)

Appendix C: Cryptographic tables. Contains cryptographic tables that are related to algorithms discussed in chapter 3 (for example, DES S-boxes).

Appendix D: Source code. Java sources that are solutions to cryptographic problems presented and, in parts, solved, at the end of chapter 3.

Appendix E: BIOS passwords recovery. This appendix explains a couple of standard methods for BIOS password recovery.

4. Presumptions and Limitations

This book does not pretend to be kind of book which covers all existing areas in security space. Security, privacy, access control, cryptography and many other areas are fast growing and changing landscape. It is probably impossible to cover all of these areas in details with one book, unless it has 3-5000 pages, which is making it heavy to carry around. Authors' intention was to make a comprehensive overview of all areas of security, go into depth with most important ones and directs readers to additional resources and further readings.

It is easy to recognize that, in moment you publish something, there is a risk that information might be obsolete. Although authors did their best to keep this book up to date with current status of security problems, issues but also products and solutions, no one can guarantee that something will not be obsolete and that some facts or solutions will not change within next couple of years, or maybe even months (see 5.1). However, we have to mention that some fundamental principles and guidelines are timeless and do to change as the time passes by. This book will teach students to look around, analyze, think, and come up with solutions on their own. Book gives the knowledge

and the information, yet of much greater importance is that it teaches students about procedures, ways and possibilities to solve actual problems and to look into the future and continuously develop themselves in the field of computer security.

5. Current State of the Security Area and Discussion

The current state of security is much worse than the average user believes. A black hat hacker (which can accordingly to RSA labs are classified into “hired guns” category) is making several thousands of dollars every day and is never being caught. Unlike them, many security professionals who are in charge of infrastructure protection usually know less about the current state of hacking than the average system administrator. And the worst thing is that the tools and procedures used for protection today have been used to hack several years ago.

Let's explain this in brief. Millions of users are using proprietary operating systems to run critical applications and store confidential information without installing patches and service packs. Different bots own millions of computers at any moment of time; malware is not only about showing ads – real malware don't want you to know about it as it wants your confidential data. Numerous people have their confidential information stolen due to their choice not to use mandatory encryption (which, outside of the government, is usually NOT mandatory).

There are no silver bullets in security – actually, there is no single product you can buy that will solve all your security problems protect you against all computer threats (although many vendors say there is). There is no single product that will protect you against 100 percent of the threats that it claims it will prevent (although vendors say it will).

The one thing that anyone interested in security must understand is the following: security is not a solution, nor a product; it's an evolving process (as illustrated in 5.1), resulting in a constant encounter within good and the bad guys. Unless this fact is fully accepted by ones who are in charge of security processes than the hackers will definitely have a prosperous future. We are not trying to scare anyone; we're just trying to submit a message that security requires constant learning, upgrading, research, testing and creativity.

5.1. Breaking the SHA and NIST new hash function contest

Within next four years, the U.S. government will cease to use SHA-1 for digital signatures. The reason for this is that associate professor Wang Xiaoyun of Beijing's Tsinghua University and Shandong University of Technology, and her associates, have already cracked SHA-1. Wang also cracked MD5, the hash algorithm most commonly used before SHA-1 became popular. Previous attacks on MD5 required over a million years of

supercomputer time, but Wang and her research team obtained results using ordinary personal computers. In addition to the U.S. government, well-known companies like Microsoft, Sun and many others have also announced that they will no longer be using SHA-1.

National Institute of Standards and Technology (NIST) is having a competition for a new cryptographic hash function. NIST did a good job managing the AES process (competition for Advanced Encryption Standard). They are obviously going to do in similar way with hash functions. You'll find Announcement for the Development of New Hash Algorithm for the Revision of Federal Information Processing Standard (FIPS) 180–2, Secure Hash Standard here. During 2005 and 2006, NIST sponsored two workshops to discuss the requirements for a new hash function, and eventually announced a competition to choose a replacement for SHA-1.

Submissions will be due in fall 2008, and a single standard is scheduled to be chosen by the end of 2011. This is a reasonable schedule. Designing a secure hash function seems harder than designing a secure encryption algorithm, although we don't know whether this is inherently true of the mathematics or simply a result of our imperfect knowledge. Producing a new secure hash standard is going to take a while. Luckily, we have an interim solution in SHA-256. This is big chance to create something really big and important in security area. Bruce Schneier told that his Twofish team is going to reconstitute and get to work on an Advanced Hash Standard submission.

6. Novelties and Comparison to Other Books

Unlike many others, we've did our best to write a comprehensive and systematic book. We haven't detoured into unnecessary details, but have managed to touch depth with most important areas (for example, anyone who deals with security must be familiar with firewalls – therefore, firewalling is heavily discussed and explained with a state of an art firewall, which is also free). On the other hand, not every security officer will deal with biometrics – therefore, biometric mechanisms are only briefly described.

We're also aware of the fact that most of computer users hate maths (logarithms in finite fields, or large number factorization, for example) and we've did our best to keep chapter 3 free of maths as much as it was possible and make it easily readable to anyone. Many books that deal with cryptography rely heavily on math knowledge.

One more thing that we're particularly proud of is our effort to make readers aware of security oriented open source software. Like we've written in chapter 14, there are two types of systems: open and closed ones. If you use open source software, which means that you can analyze and inspect the code of security mechanisms (in this case, the application or service) and practically be sure that it will do what it is designed to do and nothing more. That means that you can check it for existence of trapdoors and backdoors, and in the end be sure that it will not send any data to manufacturer's servers (it is really not

important what it sends, it is important if it sends the data without your permission – this is how your privacy gets violated). If you use closed source software, the only thing that can help are patches and service packs, but you will not have a guarantee of the data leek (except manufacturer's promise). Therefore, we've done our best to encourage readers to at least give a try and test the open source (or at least, freeware) security solutions.

Aside from that, the authors are very proud of two novelties that are briefly described in this book, as some of the authors have worked on them.

6.1. Intrusion detection and prevention systems

Chapter 6 includes some of novelties in the area of intrusion detection and prevention systems (IDS/IPS). Based on author's work and papers published in this area, this book covers in more depth state of the art of these systems. It includes definition of criteria for design, implementation, and evaluation of IDS/IPS systems, and new approach in usage of artificial intelligence in intrusion detection and prevention. This includes elaboration of expert systems, fuzzy logic and neural networks. Also, it defines WIDS – wireless intrusion detection systems and WIPS – Wireless Intrusion Prevention System with multilevel and multidimensional approach. WIDS/WIPS consists of Agent, Sensor, Server and Management and reporting tools. Intention is to create automated, self-learning and autonomous system that can improve protection and security of system or network in real time and independently of new threats and attack methods. As this is current research topic, book includes some of already published research presented on security conferences.

6.2. eNovčanik (eng. eWallet)

Chapter 8 includes description of the new Internet based payment service. In Serbian language name eNovčanik means eWallet and this service is brand new on local market. It also can be used as payment service which avoids usage of credit cards everywhere. One of book authors is cofounder and coarchitect of eNovčanik, together with group of people that have been working on that project. This service is chosen as it employs number of security and protection mechanism which can serve as base for learning of e-commerce security mechanism. This includes security protocols, cryptography, anti-phishing and anti-fraud mechanisms and techniques. Also, it includes improved mechanisms of authetication, age verification and usage of principles described in other chapters in this book. eNovčanik has been chosen as way to explain many of security mechanism coupled together in one service that intentend to be used by many clients and customers. Example of eNovčanik is also used as way and possibility to explain end-to-end solution for e-commerce in new markets and in situation when credit card

fraud increases what caused that kind of service to be more expensive for merchants and also clients.

6.3. Other

Number of other interesting and some rather new and recent developments are covered in various parts of this book. We will briefly mention here some of them. Appendix 3 holds source code of number of encryption algortithms as well as **cryptoanalysis** code for some of them. This appendix is closely related to chapter 3 which is dedicated to cryptography. Description of new **Payment Card Industry Data Security Standard (PCI DSS)** is also included as part of chapter 8 which is related to e-commerce and Internet security. This book includes brief description of newly introduced **Security Development Lyfecycle (SDL)** process by Microsoft in chapter 12 that deals with secure programming.

7. Achieved Results and Conclusions

We certainly do hope that this book will make a difference – maybe not a big one, but at least it will make students, engineers, administrators, programmers and other computer users aware of the complexity that security as an evolving process has. To simplify that – we hope that this book will make people aware of security problems discussed in 5. We have really tried not to push readers with maths in cryptography; instead, we've tried to tell our readers that it is important part of their computer software and to show them how they can use it for free. We've also tried to teach our readers that money does not necessarily buys a good security mechanisms – a good firewall can be set up with $100 computer running Linux and iptables, as we've described in chapter 5 of this book. This is a comprehensive manual that serves the protectors, not a hacker's handbook; if you are looking for malicious recourses, we suggest you to try somewhere else. At the end of this paper, we must say once again that this is the first systematic computer security book in Serbian language.

Here are all the **book details**:

- **Title:** Sigurnost računarskih sistema i mreža
- **Authors:** Dragan Pleskonjić, Nemanja Maček, Borislav Đorđević, Marko Carić
- **Publisher:** Mikro knjiga, Beograd, Srbija
- **Year of publication:** 2007
- **ISBN:** 978-86-7555-305-2

- **Format:** 16,8 x 23,5cm, pages: 752

Book preview on publishers Web site:
- http://www.mk.co.yu/pub/store/prikaz.php?KOD=SRSM

Detailed book contents on authors' Web site can be found at:
- http://www.conwex.info/draganp/books_SRSiM.html
- http://www.nmacek.co.nr/SR-books-srsim.html

References

1. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: "Sigurnost računarskih sistema i mreža", Mikro knjiga, Beograd, 2007., ISBN 978-86-7555-305-2
2. B. Schneier, „Applied Cryptography", Second Edition, John Wiley & Sons, Inc, 1996.
3. D. Stinson, „Cryptography – Theory and Practice", CRC Press, Boca Raton, Florida, 1995.
4. D. Pleskonjić, „A Development Environment for Generating System for Universal Network Connecting", IEEE Technical Applications conference NORTHCON 96, Seattle, Washington, USA, November 1996.
5. D. Pleskonjić, „Wireless Intrusion Detection Systems (WIDS)", 19th Annual Computer Security Applications Conference, Las Vegas, Nevada, USA, December 8-12, 2003.
6. B. Đorđević, D. Pleskonjić, N. Maček, „Operativni sistemi: UNIX i Linux", Viša elektrotehnička škola, Beograd, 2004.
7. B. Đorđević, D. Pleskonjić, N. Maček, „Operativni sistemi: teorija, praksa i rešeni zadaci", Mikro knjiga, 2005.
8. D. Pleskonjić, V. Milutinović, N. Maček, B. Đorđević, M. Carić, „Psychological profile of network intruder", IPSI 2006, Amalfi, Italy, March 23-26, 2006.
9. D. Pleskonjić, „Protecting wireless computer networks by using intrusion detection agents", IPSI 2005, Venice, Italy, November 10-13, 2005.
10. N. Maček, Borislav Đorđević, Slobodan Obradović, Dragan Pleskonjić, „Kriptografski zaštićeni Linux sistemi datoteka", INFOTEH JAHORINA 2007, 27-30. mart 2007.
11. D. Pleskonjic, S. Omerovic, S. Tomazic, "Network Systems Intrusion: Concept, Detection, Decision, and Prevention", IPSI BgD Transactions on Internet Research, January 2007, Volume 3, Number 1, ISSN 1820-4503

Dragan Pleskonjić is Chief Executive Officer (CEO) at BEG Finsoft (Belgrade branch of Finsoft Ltd, London, UK based company) and also Security Architect. He is also professor of Computer Networks Security and Operating Systems. He has Master of Science (in Serbian: Magistar) in Computer Science in area of Security and Cryptography from the University of Zagreb, Faculty of Electrical Engineering and Computing and is a Ph.D. candidate at the University of Belgrade, area of wireless networks security. He is one of the founders of "eNovcanik a.d." Internet payment service. He used to lead software development in Belgrade division of Los Angeles headquartered company Empower LLC. He has been a project leader and software development manager for PCTEL, Inc. (NASDAQ: PCTI, USA based company), i.e. its wireless network software division in Belgrade. Prior to acquiring by PCTEL, he was research and development manager of Chicago based startup cyberPIXIE, Inc. wireless solutions company. He specializes in security for wireless networks and systems and has a US Patent Pending in this area. He spent several years as the head of the networks and communications department at Belgrade technical Lola Institute. He has held leading positions in a number of industry projects, as well as in research and development projects, mostly in the area of computer networks, security, and programming for network security. He is the author of over twenty papers at conferences and seminars, including IEEE and ACM events, and several books and other teaching materials. He is a member of ACM society and ACM SIGSAC (Special Interest Group on Security, Audit and Control), and also a member of IEEE and IEEE Computer Society.

Nemanja Maček is an assistant at the Department of Computer Science at the Advanced School of Electrical Engineering, Belgrade, since 2003. He received his degrees in Computer Science from the Advanced School of Electrical Engineering in 2003, and in Information Technologies from the University of Novi Sad in 2005. Currently, he is working on his Ph.D. thesis in management at the University of Belgrade. His major research interests regarding security of computer systems and networks are related to storage encryption, social engineering (information hijacking with spyware and heavy advertising) and digital forensics. He also fights against software patents and stands for development and use of open-source operating systems and software. He is the author of a number of books in operating systems, computer networks and security, as well as of several papers for magazines and conferences, covering topics like journaling filesystem performance and computer security.

Borislav S. Đorđević was born in Serbia and received BSEE, MS and Ph.D. degrees from the University of Belgrade. He is a professor of Computer Science at the University of Belgrade and a member of UNIX/Linux research team of the Institute Mihailo Pupin. His teaching and research activities are in the areas of disk systems, storage systems and operating systems. He joined Institute Mihailo Pupin – Computers division as an research assistant, working on disk drivers for PC platforms. Later, he joined UNIX development

division in the Institute Mihailo Pupin, working on UNIX disk optimization project, tuning UNIX for large databases, data protection and connecting UNIX with other operating systems. He is the author of books in operating systems, as well as of over 20 refereed papers.

Marko Carić is an assistant at the Department of New Computer Technologies at the Advanced School of Electrical Engineering, Belgrade, since 2002. He received his degree in Maths (Statistics and probability theories) from the University of Belgrade in 2002. Currently he is working on his master's degree in computer science at the University of Belgrade. His major research interests are cryptography, operating systems and network security.