IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4189

Network Security Software Skills

Göran Pulkkis and Kaj Grahn
Arcada Polytechnic, Metänpojankuja, Finland, Tel: +358-9-525321, Fax: +358-9-525322, {goran.pulkkis, kaj.grahn}@arcada.fi

ABSTRACT

This paper is a topical overview of network security software and related skills needed by present network security professionals. Covered topics are antivirus protection software, firewall software, cryptographic software standards like IPSec and TLS/SSL, cryptographic software like VPN, SET, secure e-mail, secure network management, and smart card applications as well as security administration software like intrusion detectors, port scanners, password crackers and management of network security software. Tools and API's for security software development are presented. University and polytechnic level network security education is surveyed and the need for inclusion of network security software development skills in such education is pointed out.

INTRODUCTION

The steadily growing international computer network user community needs an expanding staff of well educated network security professionals to guarantee the reliability of the global IT infrastructure of computer nodes in wired and wireless networks. Network security tools are usually software tools. Network security professionals should know these tools, how to use and develop them, and what kind of network security they can provide.

ANTIVIRUS PROTECTION SOFTWARE

The ideal antivirus approach is prevention. Since 100% virus prevention is difficult to achieve, virus types must be identified and such viruses for which prevention fails must be removed /1/. Four generations of antivirus software are described in /2/. Examples of recent advanced antivirus techniques are generic decryption technology (**GD**) for efficient detection of polymorphic viruses /3/, which must decrypt themselves to activate, and the comprehensive approach called **Digital Immune System**, proposed by IBM in 1997. Both these antivirus approaches are described in /1/.

FIREWALL SOFTWARE

The software and/or hardware of most TPC/IP routers support basic user defined IP packet filtering rules. A packet filtering firewall can also be a stand-alone device on a network link. For example, a PC/Linux computer can be used as an IP packet filtering router between two network connections (see for example Chapter 9 in /11/). Another stand-alone firewall device is the Cisco Secure PIX 500 Firewall /12/ with IP packet traffic controlled by a stateful connection oriented algorithm (Adaptive Security Algorithm) and user authentication/authorization based on an efficient Cut-Through Proxy functionality. For some routers advanced firewall functionality is available as add-on software. An example is the Cisco IOS Firewall add-on module /13/ to Cisco Internetwork Operating System for data traffic filtering on the network, transport, and application layers. A typical application level gateway is a protocol oriented proxy server - for example a PC/Linux computer with two network connections executing proxy software - on a network link, for example a http proxy, a smtp proxy, a ftp proxy, etc. Firewall software can also protect individual computers connected to a public TCP/IP network /14/.

CRYPTOGRAPHIC SOFTWARE APPLICATIONS

Classification

Cryptographic network security software implements either secure network level data communication or secure application level data communication. Standards for TCP/IP networks proposed by IETF /15/ are available for both cases. Many cryptographic software applications use certificates of the PKI (WG pkix in /15/) on Internet. PKI client software like ID2 Personal /16/ is a necessary component of such applications. Protection of sensitive cryptographic data and operations is usually implemented as smart card applications /4/.

Software for Secure Network Level Data Communication

Most software for secure network level data communication in TCP/IP networks is based on the IPSec standard (WG ipsec in /15/). Optionally encrypted payloads of new IP packets (IPSec packets) are transmitted over the network. IPSec packets are routed until they reach an IPSec node, where the packet payloads are - encrypted payloads are first decrypted - unpacked to traditional IP packets. Two computers can implement end-to-end security through the same TCP/IP network with properly installed and configured IPSec software in both computers. A widely used IPSec application is VPN software for providing secure LAN functionality for geographically distributed LAN segments and computers interconnected by a public TCP/IP network /5/.

Software for Secure Application Level Data Communication

Secure application level communication software in TCP/IP networks is based on the TLS standard (WG tls in /15/) derived from v3.0 of the SSL protocol introduced by Netscape Communications as a basis of a secure http protocol, https. The TLS/SSL protocol requires an established client-server TCP connection between two communicating computers and uses the socket interface for data communication. After the establishment of a TCP connection both computers execute the SSL Handshake Protocol in order to agree on the cryptographic algorithms and keys for the actual data communication. In this context X.509 certificates may be used for client/server authentication. For the actual data communication the SSL Record Protocol is used. Sending side protocol steps are shown in Fig. 1. Received data packets are decrypted, data integrity is MAC-checked, checked data is decompressed if necessary, and finally data fragments are re-assembled to application data.

With TLS/SSL, secure version of other application level TCP/IP protocols (pop3s, imaps, smtps, nntps, and ldaps) than http have been implemented and made available to the Internet community.

Reading mail from a remote mailbox using pop3s or imaps protects mailbox passwords and the contents of fetched e-mail messages against attacks based on eavesdropping on network traffic.

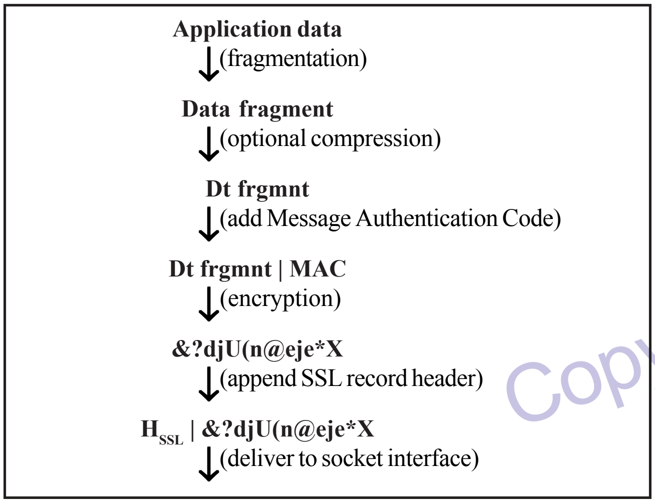
Full e-mail security requires e-mail client program extensions for signing and/or encrypting outgoing e-mail messages as well as for decrypting and/or signature checking incoming e-mail messages. The most widely used e-mail client security extensions are PGP and S/MIME /1/. Neither PGP nor S/MIME is based on TLS/SSL, but X.509 certificates and the PKI on Internet (WG pkix in /15/) are used for authentication both in TLS/SSL and in S/MIME. PGP certificates are created when PGP users sign and attach own trust levels to public keys of other PGP users.

The SSH protocol is an application level protocol introduced for secure remote login in TCP/IP networks /6/, /17/. Presently SSH is a de-facto Internet security standard (WG secsh in /15/). In SSHv3 also

This paper appears in *Issues and Trends of Information Technology Management in Contemporary Organizations,* the proceedings of the Information Resources Management Association International Conference. Copyright © 2002, Idea Group Inc.

Copyright Idea Group Inc.
Copyright Idea Group Inc.
Copyright Idea Group Inc.
Copyright Idea Group Inc.

Figure 1: Sending side SSL record protocol steps



PKI certificate and smart card based user authentication are supported /18/.

SET /19/ is an open encryption and security specification designed to protect credit card transactions on Internet. A core transaction is a **purchase transaction**, which consists of **order information (OI)** encrypted by the public key **KpubM** of the merchant, and **payment information (PI)** encrypted by the public key **KPubB** of the bank (credit card issuer). All encrypted information is signed (a dual signature) with the private key **KPrivC** of the cardholder. The “cryptographic logic” of a purchase transaction is shown in Fig. 2. **X.509**$_C$ is a certificate for the public key of the cardholder. Some transaction details have been streamlined on purpose in order to show more clearly how security and privacy are ensured. A compact description of SET is found in /1/.

Figure 2: “Cryptographic logic” of a purchase transaction in SET

cardholder ——> $Sig_{KPrivC}(E_{KPubM}(OI) | E_{KPubB}(PI)) | X.509_C$ ——> merchant
gw(bank) <——— $Sig_{KPrivC}(E_{KPubM}(OI) | E_{KPubB}(PI)) | X.509_C$ <—— merchant
gw(bank) ————> info about payment authorization ————> merchant

The SET protocol can only be used to secure payment transactions with credit card in TCP/IP networks. Other steps in electronic commerce (orders, confirmations, deliveries, etc.) are not supported. SEMPER /20/ is a EU project for standardization of the security architecture of value chains in e-commerce. An overview of electronic payment systems is published in /7/.

Network management and monitoring software for TCP/IP networks is usually based on the Simple Network Management Protocol (SNMP), an application level protocol. The first versions of SNMP lacked security features. In SNMPv3 (WG snmpv3 in /15/), secure authentication and encryption are incorporated in the specifications for SNMP managers and secure access control is included in the specifications for SNMP agents. Details of the security features in SNMPv3 are found in /1/.

Smart Card Applications

The computationally secure randomness applied to key creation in public key cryptography may cause security problems, if these keys are used in network connected computers. Intruders may identify keys as random areas in the main memory, since code and data are usually structured. Therefore should a private key be stored on a smart card together with the code of the cryptographic operations using it. Then all cryptographic operations using the key are executed on the card. Once installed a private key should never leave a smart card. The use of keys on a smart card is protected by pin codes or biometrically by digital fingerprint comparison and/or by digital voice recognition. A numerical keypad dedicated to the smart card is necessary for pin code security.

The characteristics of present smart cards are defined by several ISO 7816 standards /21/. Smart cards exchange byte sequences - called APDU’s in ISO 7816 - with smart card readers. The file structure of many current smart card operating systems is based on the pkcs#15 standard /22/.

Smart card applications call functions of some Application Programming Interface, when information and operations coded on smart cards are needed. Examples of such API’s are implementations of the pkcs#11 standard /22/ and Microsoft CryptoAPI /23/. Moreover, API’s for smart card applications need interface software to smart card reader drivers. Usually such interface software is an implementation of the PC/SC Specifications in /24/. A smart card application example is the Finnish Electronic Identity Card (FINEID card) /25/.

SECURITY ADMINISTRATION SOFTWARE

Security administration software includes **intrusion detection**, **management software** for security software and **vulnerability checking**.

An Intrusion Detection System (IDS) /1/ monitors traffic in a network and/or user behavior in a host computer to identify possible intruders and/or anomalous behavior and/or misuse.

Network security software in host computers and in other network nodes like routers, configurable switches is often controlled by management software. An example is the distributed IDS described in /8/. Management software is also available for multiple installations of Cisco Secure PIX Firewalls /12/. The Digital Immune System described in /1/ as well as security software developed and delivered by F-Secure /26/ are also centrally managed and updated.

A major vulnerability of password protection is insufficient password quality. Passwords can be too short or easily guessed or cracked. A potential intruder could run a password cracker on the encrypted passwords stored in a computer. A system administrator should often do the same, disable user accounts with bad passwords, and urge users to use only good passwords. A freeware password cracker, L0phtCrack, can be downloaded from /27/.

Intrusion into a computer in a TCP/IP network occurs through open ports. Intrusion prevention thus requires administration based on regular vulnerability scans for open ports. The vulnerability scan procedure is described in /9/. In /10/ is described how the three-step “handshake” to establish a TCP connection can be manipulated in intrusion attempts. A freeware port scanner, Nmap, can be downloaded from /28/. Information on available commercial port scanners is available at /29/.

SECURITY SOFTWARE DEVELOPMENT

Antivirus protection programming skills require studies of self-modifying code programmed in assembler, in high level programming languages, and in scripting languages as well as of virus sensitive vulnerabilities in common operating system environments.

Firewall software programming skills are based on skills in software implementations of the TCP/IP protocol stack. Programming exercises and projects to design software of the IP, TCP, UDP and application level protocols should therefore be included in advanced network security education.

For development of network applications with built-in application level security the open source toolkit OpenSSL is available /30/. OpenSSL can be installed on UNIX, Windows, and Mchintosh comput-

Copyright Idea Group Inc.

ers as a library of C functions available to a C compiler. Also commercial development tools for SSL-protected network applications are available. RSA Security and Certicom offer software developer kits based on C and Java /31/, /32/.

VPN software is implemented as add-on or integrated software controlled by operating systems of workstations, servers, and routers /33/, /34/, /35/. Development skills for VPN software and other IPSec applications require a deep knowledge especially in IKE - the encryption key management protocol in IPSec. Education of IPSec specialists should include installation, configuration, and test use of VPN software as well as source code studies of VPN implementations combined with programming exercises in which new features and/or modifications are introduced into the examined VPN software. Arcada Polytechnic has in cooperation with the LM Ericsson IPSec Competence Center implemented a multimedia IPSec tutorial, in which the characteristics of IPSec and especially IKE are illustrated with audio supported text presentations, pictures and animations.

RSAEuro is an open source cryptographic toolkit providing various preprogrammed functions in C. RSAEuro can be downloaded for example from ftp.funet.fi /36/.

In smart card application development usually some development kit for smart card programming is used. Microsoft offers a Smart Card Toolkit based on the use of visual programming tools /37/.

NETWORK SECURITY SOFTWARE SKILLS IN HIGHER EDUCATION

Education of computer scientists and IT professionals in universities and polytechnics includes as a rule courses in computer and network security /38/. Several universities also offer MSc programs in information security /39/-/44/. Usually these courses and programs cover information security administration, antivirus protection, firewall techniques, intrusion prevention and detection, theory and applications of cryptography, and information security standards. Computer scientist and IT professionals educated by these courses and programs should have knowledge as well as skills about installation, configuration, use, and user support of present network security software. However, university and polytechnic level network security education seldom covers network security software development skills like programming TLS/SSL applications, IPSec applications, SET applications, PKI applications, authentication solutions, applications with digital signatures, antivirus protection software, firewall software and smart card programming. Education of IT professionals in Arcada Polytechnic includes an undergraduate course on Computer and Network Security and specialization courses on IPSec Applications and TLS/SSL Programming.

CONCLUSIONS

Network security skill management along with educational aspects is a demanding field. University and polytechnic level education for network security software skills should include:

- installation, configuration, and test use of all categories of available network security software solutions and products,
- source code inspection exercises of open source network security software solutions,
- programming exercises and projects with TLS/SSL application development environments, cryptographic toolkits like RSAEuro, IPSec applications, SSH applications, PKI applications, and smart card applications.

More emphasis should be put on network security software development skills in present upper level network security education, especially in postgraduate educational programs focusing on information security. Also student participation in related research should be supported.

REFERENCES

/1/ Stallings, W. *NETWORK SECURITY ESSENTIALS Applications and Standards.*USA: Prentice-Hall, 2000.

/2/ Stephenson, P. “Preventive Medicine.” *LAN Magazine*, November 1993.

/3/ Nachenberg, C., Computer Virus-Antivirus Coevolution.” *Comm. ACM,* Jan. 1997.

/4/ Rankl, W. and Effing, W. *Smart Card Handbook e2.* UK: Wiley, 2000, ISBN 0471988758.

/5/ Doraswamy, N. and Harkin, D. *IPSec The New Security Standard for the Internet, Intranets, and Virtual Private Networks.* USA: Prentice-Hall, 1999.

/6/ Ylönen, T. “SSH - Secure Login Connections over the Internet.” *Proc. Sixth USENIX Security Symposium,* San Jose, California, USA, July 1996.

/7/ Oppiger, R. *Security Technologies for the Word Wide Web.* USA: Artech House, 2000.

/8/ Heberlein, L., Mukherjee, B., and Levitt, K. “Internetwork Security Monitor: An Intrusion-Detection System for Large-Scale Networks.” *Proc. 15th National Computer Security Conference,* Oct. 1992.

/9/ Conry-Murray, A. “Vulnerability Assessment Tools.” *Network Magazine,* April 2001.

/10/ Scambray, J., McClure, S., and Kurtz, G. *Hacking Exposed e2.* USA: Osborne/McGraw-Hill, 2001.

/11/ Linux Network Administrators Guide. http://www.linux.se/doc/nag2 (3.6.2001).

/12/ Cisco PIX 500 Firewalls. http://www.cisco.com/warp/public/cc/pd/fw (3.6.2001).

/13/ Cisco IOS Firewall. http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft (3.6.2001).

/14/ Zone Labs, Inc. http://www.zonelabs.com (3.6.2001).

/15/ Active IETF Working Groups. http://www.ietf.org/html.charters/wg-dir.html (7.1.2002).

/16/ ID2 Personal Web page. http://www.id2tech.com/products/2d.html (25.9.2001).

/17/ SSH Secure Shell Features. http://www.ssh.com/products/ssh/features.html (27.5.2001).

/18/ SSH Secure Shell Support Page. http://www.ssh.com/support/ssh/index.cfm (25.9.2001).

/19/ The official web site of SET. http://www.setco.org (3.6.2001).

/20/ SEMPER Secure Electronic Marketplace for Europe. http://www.semper.org (27.5.2001).

/21/ Portal of International Organization for Standardization ISO. http://www.iso.org (6.1.2002)

/22/ Public-Key Cryptography Standards. http://www.rsasecurity.com/rsalabs/pkcs (7.1.2002)

/23/ The Crypto API and Cryptographic Service Providers. http://msdn.microsoft.com/library/en-us/dnw98bk/html/thecryptoapicryptographicserviceproviders.asp (6.1.2002)

/24/ PC/SC Workgroup Portal. http://www.pcscworkgroup.com (6.1.2002)

/25/ Web page of the Finnish Electronic ID Card. http://www.fineid.fi (27.5.2001).

/26/ F-Secure Enterprise Solutions. http://www.f-secure.com/products (12.6.2001).

/27/ @stake Research Labs. http://www.atstake.com/research/lc3/download.html (25.9.2001).

/28/ Web Page of Nmap Network Security Scanner. http://www.insecure.org/ (25.9.2001).

/29/ Securityportal at Atomictangerine Site. http://www.securityportal.com/ (25.9.2001).

/30/ The OpenSSL Project. http://www.openssl.org/ (15.9.2001).

/31/ RSA BSAFE. http://www.rsasecurity.com/products/bsafe/ (13.6.2001).

Copyright Idea Group Inc.

Copyright Idea Group Inc.

Copyright Idea Group Inc.

Copyright Idea Group Inc.

/32/ SSL Plus Products. http://www.certicom.com/products/ssl_plus_prod.html (25.9.2001).

/33/ Protecting Data in Transit - VPN+. http://www.f-secure.fi/products/vpnplus (16.6.2001).

/34/ Cisco Systems VPN Solutions. http://www.cisco.com/warp/public/75/solutions/network/vpn.shtml (16.6.2001).

/35/ Linux FreeS/WAN. http://www.freeswan.org (16.6.2001).

/36/ FUNET ftp server. ftp://ftp.funet.fi/pub/crypt/cryptography/libs (12.6.2001).

/37/ Windows for Smart Cards Toolkit for Visual Basic 6.0. http://www.microsoft.com/windowsce/smart card/start/datasheet.asp (6.2.2002)

/38/ List of crypto and security courses. http://avirubin.com/courses.html (5.1.2002).

/39/ EMU Information Security Program. Eastern Michigan University, http://www.emich.edu/public/bted/default.htm (5.1.2001).

/40/ InfoSec Masters program with a Concentration in Information Security. James Madison University, http://www.infosec.jmu.edu (5.1.2002)

/41/ Faculty of Information Technology – Courses, Master of Information Technology. Queenslands University of Technology, http://www.qut.edu.au/pubs/hbk_current/courses/IT50.html (5.1.2002)

/42/ MSc Information Security and Computer Crime. University of Glamorgan, Courses of School of Computing, http://babylon1.isd.glam.ac.uk/Prospectus/view.php3?ID=849&sfrom=easy&dosommat=school (5.1.2002)

/43/ The MSc programmes. Royal Holloway College, University of London. http://www.isg.rhul.ac.uk/msc/msc_home.shtml (7.1.2002)

/44/ MSc Information Technology Security. University of Westminster, http://www.wmin.ac.uk/item_new.asp?ID=3888&wp=pg (5.1.2002)

Copyright Idea Group Inc.
Copyright Idea Group Inc.
Copyright Idea Group Inc.
Copyright Idea Group Inc.

0 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/proceeding-paper/network-security-software-skills/31762

Related Content

Fog Caching and a Trace-Based Analysis of its Offload Effect
Marat Zhanikeev (2017). *International Journal of Information Technologies and Systems Approach (pp. 50-68).*
www.irma-international.org/article/fog-caching-and-a-trace-based-analysis-of-its-offload-effect/178223

Optimization of Cogging Torque Based on the Improved Bat Algorithm
Wenbo Baiand Huajun Ran (2023). *International Journal of Information Technologies and Systems Approach (pp. 1-19).*
www.irma-international.org/article/optimization-of-cogging-torque-based-on-the-improved-bat-algorithm/323442

Representing Meta-Artifacts
(2012). *Design-Type Research in Information Systems: Findings and Practices (pp. 115-134).*
www.irma-international.org/chapter/representing-meta-artifacts/63108

Information Systems, Software Engineering, and Systems Thinking: Challenges and Opportunities
Doncho Petkov, Denis Edgar-Nevill, Raymond Madachyand Rory O'Connor (2008). *International Journal of Information Technologies and Systems Approach (pp. 62-78).*
www.irma-international.org/article/information-systems-software-engineering-systems/2534

Mediated Embodiment in New Communication Technologies
Laura Aymerich-Franch (2018). *Encyclopedia of Information Science and Technology, Fourth Edition (pp. 4234-4244).*
www.irma-international.org/chapter/mediated-embodiment-in-new-communication-technologies/184130