Institut für Verwaltungs- und Wirtschaftsinformatik
der Universität Koblenz

Literaturhinweise

zur Vorlesung

Grundlagen der IT-Sicherheit

Bachelorstudiengänge im Fachbereich Informatik

Prof. Dr. Rüdiger Grimm <grimm@uni-koblenz.de>

Version 29.10.2009

Themenplan (1.9.2009)

V1 Was kann passieren / Angriffe
V2a Vertrauen (ggü. WS0809 gekürzt)
V2b Internet (ggü. WS0809 neu)
V3 Krypto-Einführung
V4 Kryptoanwendungen
V5 Symmetrische Kryptoalgorithmen
V6 Asymmetrische Kryptoalgorithmen
V7 Signaturen
V8 PKI
V9 XML-Security / SOA-Security
V10 IPSec, SSL, SMIME
V11 Authentifizierungsprotokolle
V12 Malware
V_add1 Zahlentheorie
V_add2 Komplexitätstheorie
V_add3 Fair Exchange

Zu V1: Was kann passieren / Angriffe

Eckert, Claudia (2009): IT-Sicherheit. Konzepte, Verfahren, Protokolle. Studienausgabe. Oldenbourg Verlag, München, 2009.

Schneier, Bruce (2003): Beyond Fear: Thinking Sensibly about Security in an Uncertain World. Copernicus Books, 2003.

Schneier, Bruce (2000): Secrets and Lies. John Wiley & Sons, 2000.

Schneier, Bruce (1996): Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd Ed. Wiley & Sons, Chichester 1996, 758 p.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2008): IT-Grundschutzhandbuch – Standardsicherheitsmaßnahmen. 10. Ergänzungslieferung Oktober 2008. http://www.bsi.de/gshb/deutsch/ oder als Loseblattsammlung in 3 Ordnern mit jährlich 2 Er-

gänzungslieferungen, ISBN 3-88784-915-9.

BSI (2009): Computer-Viren – Definition und Wirkungsweise. BSI-Kurzinformationen. http:www.bsi.bund.de, dort unter „Publikationen, Buchstabe C“, z. Zt. bei https://www.bsi.bund.de/cln_155/ContentBSI/Publikationen/Faltblaetter/F19Kurzviren.html [25.8.2009]

Harris, Evan (2003): The Next Step in the Spam Control War: Greylisting. Revised: 2003-08-21. http://projects.puremagic.com/greylisting/whitepaper.html [29.10.2009]

Karsten Fernkorn & Sören Siebert GbR, Berlin (2009): eRecht24, bes. IT-Sicherheit. http://www.e-recht24.de/it-sicherheit.html [25.8.2009]

Projekt REMO (1992): Amann, Esther; und Atzmüller, Hugo (1992): IT-Sicherheit - was ist das? In: Datenschutz und Datensicherung (heute heißt die Zeitschrift: "Datenschutz und Datensicherheit") 6/92. Vieweg Verlag, Wiesbaden, Juni 1992, S. 286-292. s. besonders Definition auf S. 287.

Universität Koblenz, Fachbereich 4, Demonstrationsseite Achtung Angriff, http://www.achtung-angriff.de/ [29.10.2009]

Zu V2a: Vertrauen

Grimm, R.: Vertrauen im Internet – Wie sicher soll E-Commerce sein? In: G. Müller, M. Reichenbach (Hrsg.): Sicherheitskonzepte für das Internet. Springer, Reihe Xpert.press, Heidelberg 2001, S. 57-86.
s. auch http://www.tu-ilmenau.de/ifmk Forschung Diskussionsbeiträge Nr. 01

Trust-Center:

ITU: X.509 (1988/2005): Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. Approved in 2005-08. http://www.itu.int/rec/T-REC-X.509 [1.9.2009]

In Eckert, Claudia (2007): IT-Sicherheit. Konzepte, Verfahren, Protokolle. Studienausgabe. Oldenbourg Verlag, München, 2007, Abschnitt 9.1 „Zertifizierung“.

Tauschek, Philip: Trust-Service-Infrastrukturen. Technische und strategische Aspekte des Trustcenter-Geschäfts. Dissertation Universität Regensburg 2001. Physica-Verlag Heidelberg 2002.

Überblick DFN-PKI. http://http://www.pki.dfn.de/ [1.9.2009]

Käuferschutz bei eBay/PayPal: http://pages.ebay.de/paypal/kaeuferschutz.html [1.9.2009]

Download-Service über (ClickandBuy Payment) www.clickandbuy.com [1.9.2009]

Online-Treuhandservice: https://www.escrow.com/solutions/escrow/process.asp [1.9.2009]

Anhang, andere Vertrauensmodelle:

Baier, Annette: Vertrauen und seine Grenzen. In: Martin Hartmann, Claus Offe (hrg.): Vertrauen – Die Grundlage des sozialen Zusammenhalts. Campus, Frankfurt/M., 2001, pp. 37-84. (Original: Trust and Antitrust. In: Ethics, 96, 1986, pp. 231-260.)

Herbert H. Clark, Eve V. Clark: Psychology and Language. Harcourt Brace Jovanovich, New York 1977.

Erikson, E.: Childhood and society. New York, Norton 1950.

Herbert P. Grice: Logik und Konversation. In: G. Meggle (Hrsg.): Handlung, Kommunikation, Bedeutung. Frankfurt/M., 1979, 243-265. (Original: Logic and Conversation. In: P. Cole, J. Morgan (Ed.): Syntax and Semantics. Vol. 3. Seminar Press, New York, 1975, pp. 41-58.

Grimm, R.: Digitale Kommunikation. Oldenbourg Verlag, München 2005, Kap. 5.

Niklas Luhmann: Vertrautheit, Zuversicht, Vertrauen: Probleme und Alternativen. In: Martin Hartmann, Claus Offe (Hrsg.): Vertrauen – Die Grundlage des sozialen Zusammenhalts. Campus, Frankfurt/M., 2001, pp. 143-160.
(Original: N. Luhmann: Familiarity, Confidence, Trust. In: Diego Gambetta (Ed.): Trust – Making and Breaking Cooperative Relations. Basil Blackwell, Oxford 1988, pp. 94-107.)

Dieter E. Zimmer: So kommt der Mensch zur Sprache. Haffmanns Taschenbuch 1016, Zürich 1986.

Zu V2b: Internet und Internet-Routing

Internet-Aufbau und Geschichte:

Grimm, Rüdiger: Digitale Kommunikation. Oldenbourg Verlag, München, 2005, Kap. 7.

Tanenbaum, Andrew S.: Computer Networks. Prentice Hall. 3rd Edition, Upper Saddle, NJ, 2003. Deutsche Ausgabe: Computernetzwerke. Pearson Studium, 2003, 949 S.

Steigner, Christoph: Vorlesungsunterlagen zu „Rechnernetze“, Fachbereich 4:Informatik der Universität Koblenz/Landau.

TCP/IP und ARP:

Tanenbaum, Computer Networks.

Comer, Internetworking with TCP/IP.

RFC1180: A TCP/IP Tutorial. Socolofsky & Kale. ftp://ftp.isi.edu/in-notes/rfc1180.txt.

Stevens, TCP/IP Illustrated, Vol.1+2.

RFC 791: Internet Protocol. J. Postel. Sep-01-1981. (Obsoletes RFC0760)

RFC 793: Transmission Control Protocol. J.Postel, September 1981.

RFC 2001: TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms. W. Stevens. January 1997.

RFC 2481: A Proposal to add Explicit Congestion Notification (ECN) to IP. K. Ramakrishnan und S. Floyd. January 1999.

CIDR:

RFC 1517: Applicability Statement for the Implementation of CIDR. RFC 1518: An Architecture for IP Address Allocation with CIDR. RFC 1519: CIDR, An Address Assignment and Aggregation Strategy. RFC 1520: Exchanging Routing Information Across Provider Boundaries in the CIDR Environment.

1999 Pacific Bell Internet Services: Classless Inter-Domain Routing (CIDR) Overview. http://public.pacbell.net/dedicated/cidr.html [4.4.2009]

Ralph Becker: IP Address Subnetting Tutorial. Updated January 25, 2007. Copyright © 1996-2007 by Ralph Becker <ralphb at whoever.com> http://www.ralphb.net/IPSubnet/index.html

[4.4.2009]

Heiko Holtkamp <heiko at rvs.uni-bielefeld.de>: Einführung in TCP/IP. Bes. Kap. 3. AG Rechnernetze und Verteilte Systeme, Technische Fakultät, Universität Bielefeld. 18.6.1997, zuletzt geändert 14.2.2002. White Paper, 59 Seiten. http://www.rvs.uni-bielefeld.de/~heiko/tcpip/ [4.4.4009]

Zu V3: Einführung in die Kryptographie

Schneier, Bruce (1996): Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd Ed. Wiley & Sons, Chichester 1996, 758 p.

Eckert, Claudia (2005): IT-Sicherheit. Konzepte, Verfahren, Protokolle. Studienausgabe. Oldenbourg Verlag, München, 2005, 412 Seiten.

Klaus Schmeh (2001): Safer Net: Kryptographie im Internet und Intranet. dpunkt Verlag, Heidelberg, 2. Auflage 2001, 562 Seiten.

Zu V4: Anwendungen der Kryptographie

E-Schlüssel:

ekey biometric systems GmbH - Produktübersicht: http://www.ekey.at/products/products.asp [11.11.2007]

Autoschlüssel : http://de.wikipedia.org/wiki/Funkschl%C3%BCssel [11.11.2007]

Wolfgang Rankl, Wofgang Effing (2002): Handbuch der Chipkarten. Aufbau - Funktionsweise - Einsatz von Smart Cards. Hanser Fachbuchverlag, 2002.

GSM:

B. Walke: Mobilfunknetze und Ihre Protokolle. Band 1, Teubner Verlag, 2000

Bundesamt für Sicherheit in der Informationstechnik: GSM-Mobilfunk – Gefährdungen und Sicherheitsmaßnahmen / Referat III. Bonn, 2003.
http://www.bsi.de/literat/doc/gsm/index.htm [11.11.2006]

PayTV:

Ralf-Philipp Weinmann and Kai Wirt. Analysis of the dvb common scrambling algorithm. In Proceedings of the 8th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security (CMS 2004). Springer LNCS.

Ulrich Reimers. DVB, The Family of International Standards for Digital Video Broadcasting. Springer, 2nd Ed., 2004.

WLAN:

Detken, Kai-Oliver (2006): WLAN-Sicherheit von WEP bis CCMP, in DACH Security 2006, Syssec, 2006, 187-201

The Cable Guy – Mai 2005, Überblick zu Wi-Fi Protected Access 2 (WPA2) Veröffentlicht: 06. Mai 2005, http://www.microsoft.com/germany/technet/datenbank/articles/600761.mspx [11.11.2007]

The Cable Guy – November 2004, Datenverschlüsselung und -integrität mit WPA, Veröffentlicht: 01. Nov 2004, http://www.microsoft.com/germany/technet/datenbank/articles

/600513.mspx, Stand: [11.11.2007]

Rech, Jörg (2006): Wireless LANs – 802.11-WLAN-Technologie und praktische Umsetzung im Detail, Heise-Verlag, Hannover, 2006.

Zu V5 und V6: Kryptographische Verfahrene

Cryptool von: www.cryptool.de [26.6.2007]. Download, installieren, probieren!

V5: Symmetrische Verfahren

Hash-Funktionen, 1-Time-Pad, DES, IDEA:

Schneier, Bruce: Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd Ed. Wiley & Sons, Chichester 1996, 758 p.

AES / Rijndal:

National Institute of Standards and Technology (NIST): FIPS-197, Federal Information Processing Standards Publication 197. Announcing the ADVANCED ENCRYPTION STANDARD (AES). November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [24.11.2005]

Dining Cryptographers:

Chaum, David: Security without Identification: Transaction Systems to make Big Brother obsolete. In: Communications of the ACM, Vol. 28, No. 10, 1030-1044, Oct 1985. Übersetzt ins Deutsche als "Sicherheit ohne Identifizierung", in: Informatik Spektrum 1987, No.10, 262-277. *Dieser Artikel enthält das sog. „Dining Cryptographers Problem“*.

Zum Selbst-Ausprobieren:

Das Cryptool unter www.cryptool.de [27.11.2005]

V6: Asymmetrische Verfahren Diffie-Hellman, Verschlüsselung und Signatur, El-Gamal, DSS, RSA, Zero Knowledge, Remailer

Überblicksliteratur:

wie in V3, z.B. Schneier (1996), Eckert (2005), Schmeh (2001).

RSA Laboratories: PKCS #1-10, Public Key Cryptography Standards, Nov 1, 1993. http://www.rsasecurity.com/.

David Kahn:The Codebreakers: The Story of Secret Writing. MacMillan, New York 1967.

Originalliteratur:

W. Diffie, M.E. Hellman: New Directions in Cryptography. IEEE Transactions on Information Theory. Vol.IT-22, 644-654, 1976.

R. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Com ACM, Vol 21 No 2, 120-126, Feb 1978.

T. ElGamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on IT, Vol.IT-31, 469-472, 1985.

A: Fiat; A. Shamir: How to Prove Yourself…“. Crypto’86, Springer LNCS 263, 1987.

U. Feige, A. Fiat, A. Shamir: Zero Knowledge Proofs of Identity. Journal of Cryptology, Vol.1, No.1, 77-94, 1988.

Lance Cottrell <loki@obscura.com>, (keine Zeitangabe, ca. 2000): Mixmaster & Remailer Attacks. Original from http://www.obscura.com/~loki/remailer/remailer-essay.html [27.11.2006 not found].
Dagegen die Deutsche Übersetzung, Lutz Donnerhacke (2005): Mixmaster- & Remailer-Angriffe. Download von http://www.iks-jena.de/mitarb/lutz/anon/remailer-essay.html [27.11.2006]

Zu V7: Digitale Signaturen und Angreifermodelle

BSI-Literatur zur Digitalen Signatur, http://www.bsi.bund.de/esig/index.htm

C. Eckert (2005): IT-Sicherheit. Konzepte, Verfahren, Protokolle. Studienausgabe. Oldenbourg Verlag, München, 2005, 412 Seiten.

R. Grimm (2000): E-Commerce-Sicherheit, Kryptografie und Digitale Signatur. Ein Beitrag zum 3. Freiburger Wirtschaftssymposium “Wissens Wert”, Oktober 1999/April 2000. http://www.uni-koblenz.de/~grimm/texte/dsig-freiburg.pdf

B. Esslinger et al. (2003): CrypTool Skript –Mathematik und Kryptographie. Skript zu CrypTool,
download von http://www.cryptool.de/ (last update V. 1.3.04, 17-07-2003, 161 Seiten, deutsch ca. 1 MB).

Empfehlung, PGP selbst auszuprobieren, download z.B. von ftp://ftp.cert.dfn.de/pub/pgp

A. Pfitzmann, M. Köhntopp (2001): Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In: H. Federrath (Ed.): Designing Privacy Enhancing Technologies; Proc. Workshop on Design Issues in Anonymity and Unobservability; LNCS 2009; 2001; 1-9.

Fam. Quisquater and Fam. Guillou (1989): How to Explain Zero-Knowledge Protocols to Your Children. Advances in Cryptology - CRYPTO‘89. Springer Lecture Notes in Computer Science 435 (1990), 628-631.

David Chaum (1982): Blind signatures for untraceable payments. Advances in Cryptology: Proc. Crypto’82, Plenum Press, 1983, 199-203.

Zu V8: Public-Key Infrastrukturen

Zimmermann, Philip et al.: “Documentation” of The International PGP Home Page, http://www.pgpi.org, e.g. PGP User’s Guide, the original of PGP 2.6.2i, Phil Zimmerman, 11 October 1994, www.pgpi.org/doc/guide/2.6.3i/. And: PGP 7.0 User's Guide in English, Sep 2000, Jan 2001, www.pgpi.org/doc/guide/7.0/en/ [27-11-2006]

Garfinkel, S.: PGP: Pretty Good Privacy. A Guide for PGP Users. O'Reilly &Associates, Inc., Sebastopol, CA, January 1995.

J. Callas, L. Donnerhacke, H. Finney, R. Thayer: OpenPGP Message Format. Internet Standard Request for Comments RFC 2440, November 1998, 65 pages.
http://www.ietf.org/rfc/rfc2440.txt [27.11.2006]

B. Ramsdell, Editor: S/MIME Editor: S/MIME Version 3 Message Specification. Internet Standard Request for Comments RFC 2633, June 1999, 32 pages.

http://www.ietf.org/rfc/rfc2633.txt [27.11.2006]

ITU: X.509 (1988/2005): Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. Approved in 2005-08. http://www.itu.int/rec/T-REC-X.509 [2-9-2009]

(Historisch interessant, aber überholt: Internet IETF: Privacy Enhancement for Internet Electronic Mail. Part I-IV ("PEM"). RFC 1421-1424, Feb 93.)

Noch zu V8 PKI, besonders zum Signaturgesetz:

Stefan Kelm: Signaturgesetz quo vadis? In: DFN-Mitteilungen 58 3/2002, S. 17-120.

Johann Bizer: Elektronische Signaturen im Rechtsverkehr. In: Kröger, Gimmy (Hrsg.): Handbuch zum Internet-Recht. 2. Aufl., Springer, Heidelberg usw. 2002. (1026 Seiten) S. 39-94.

A. Roßnagel: Das neue Recht elektronischer Signaturen. Neufassung des Signaturgesetzes und Änderungen des BGB und der ZPO. In: Neue Juristische Wochenschrift (NJW) 25/2001, 54. Jg., 18.6.2001.

Richtlinie der Europäischen Gemeinschaft zur elektronischen Signatur. z.B. auf Englisch:

"Directive 1999/93/EC on a community framework for electronic signatures", 13.12.1999. http://www.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf [27-11-2006]

Deutsches Gesetz zur Elektronischen Signatur SigG, in “Informations- und Kommunikationsdienste-Gesetz (IuKDG)”, Beschluß des Deutschen Bundestages vom 13. Juni 1997, und Neufassung des Gesetzes SigG vom Mai 2001: http://www.iukdg.de [27-11-2006]

BSI-Literatur zur Digitalen Signatur, http://www.bsi.bund.de/esig/index.htm [16-01-2006]

Vor allem auch: Projekt SPHINX, PKI für sichere E-Mail: http://www.bsi.bund.de/aufgaben/projekte/sphinx/index.htm [27-11-2006]

Empfehlung, PGP selbst auszuprobieren, download z.B. von ftp://ftp.cert.dfn.de/pub/pgp [16-01-2006]

Zu empfehlen: Studium des X.509-Zertifikats unter (1.) Browser/Security, und (2.) im CrypTool zum Ausprobieren kryptographischer Verfahren (darunter Zertifikate) am PC, CrypTool 1.4, download executable file von http://www.cryptool.de/ (last update, 28-07-2006).

Zu V9: XML Security

Background:

Tim Bray et al: Extensible Markup Language (XML) 1.0. W3C Recommendation, 10 Feb 1998, http://www.w3.org/TR/REC-xml [2.2.2006]

Ed Simon, Paul Madsen, Carlisle Adams: An Introduction to XML Digital Signatures. August 2001. http://www.xml.com/pub/a/2001/08/08/xmldsig.html [2.2.2006]

Murdoch Mactaggart (IBMDev@TextBiz.com): Enabling XML security. An introduction to XML encryption and XML signature. http://www-106.ibm.com/developerworks/xml/library/s-xmlsec.html/index.html [no more available!]

Blake Dournaee: XML Security. RSA Press, McGraw-Hill, New York etc, 2002, 379 pages.

XML Signaturen:

W3C (Eastlake, Reagle, Solo): XML-Signature Syntax and Processing. W3C Recommendation 12 Feb 2002. http://www.w3.org/TR/xmldsig-core/ [2.2.2006]

IETF (Eastlake, Reagle, Solo): XML-Signature Syntax and Processing. RFC 3275. March 2002. http://www.ietf.org/rfc/rfc3275.txt [2.2.2006]

XML Encryption:

W3C (Eastlake, Reagle): XML Encryption Syntax and Processing. W3C Recommendation 10 Dec 2002. http://www.w3.org/TR/xmlenc-core/ [2.2.2006]

XML Key Management:

W3C (Ford et al.): XML Key Management Specifications (XKMS). W3C Note 30 March 2001. http://www.w3.org/TR/xkms/ [2.2.2006]

XML Privacy Policies:

W3C, Platform for Internet Content Selection (PICS). PICS Technical Specifications, Completed Specifications for PICS-1.1, Service Descriptions (Oct 1996), insb. „PICS Signed Labels (DSig)“ und „PICS Statement of Principles“. www.w3.org/PICS/; [2.2.2006]

W3C (Cranor et al.): The Platform for Privacy Preferences 1.0 (P3P1.0) Specification; W3C Recommendation 16 April 2002. http://www.w3.org/TR/P3P/ [2.2.2006]

SOA / Web-Services:

Dostal,Wolfgang ; Jeckle, Mario ;Melzer, Ingo ; Ziegler, Barbara: Service-orientierte Architekturen mit Web-Services. Konzepte – Standards – Praxis. Elsevier, Spektrum Akademischer Verlag, 2005.

Staab, Steffen; Grimm, Rüdiger; Bizer, Johann; u.v.a. (2007): Technikanalyse und Risk Management für Service-orientierte Architekturen in virtuellen Organisationen. BMBF-Studie, veröffentlicht vom Bundesministerium für Bildung und Forschung, Sep 2007.

XML Pay:

VeriSign: XML Pay – XML Trust Services. White Paper. Nov 2000. (5 pages)

VeriSign: XML Pay 1.0 Core Specification. 20 Nov 2000. (65 pages)

*XML E-Commerc*e:

Different Approaches, e.g. BMEcat, xCBL, cXML, ICE, RosettaNet, ebXML. See: 13. Esswein, Werner; Zumpe, Sabine: Realisierung des Datenaustauschs im elektronischen Handel. Informatik Spektrum 25/4, August 2002, Springer, Berlin, Heidelberg, 251-261.

Homebanking:

SIZ, VR-Banken (2004): Der Banking Kernel HBCI, Stand 29.4.2004, http://www.hbci-kernel.de/fints.htm [5.9.2006].

FinTS Version 4.0 (2004), http://www.hbci-zka.de/ [5.9.2006]: Financial Transaction Services; Weiterentwicklung des 1996 erstmals vom ZKA (Zentraler Kreditausschuss) veröffentlichten Online-Banking Standards. Highlights: http://www.hbci-zka.de/spec/fints_v4_0.htm [5.9.2006].

Zu V10: IPSec, SSL, S/MIME

Public Key Cryptographic Standards (PKCS):

RSA Laboratories: PKCS #1-15, Public Key Cryptography Standards.
E.g. at http://de.wikipedia.org/wiki/PKCS [11.11.2007]

J. Jonsson and B. Kaliski jr., RSA Laboratories: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Feb 2003.
http://tools.ietf.org/html/rfc3447/ [11.11.2007]

IPSec and IPv6:

RFC 1825: Security Architecture for the Internet Protocol (IPSec). R. Atkinson, August 1995.

RFC 1826: IP Authentication Header (AH). R. Atkinson, August 1995.

RFC 1827: Encapsulating Security Payload (ESP). R. Atkinson, August 1995.

RFC 1883: Internet Protocol, Version 6 (IPv6). S. Deering, R. Hinden, Dec 1995.

Download from http://www.rfc-editor.org/, http://www.rfc-editor.org/rfc.html, http://www.rfc-editor.org/rfcsearch.html

SSL/TLS:

Freier, Alan; Karlton, Philip; Kocher, Paul: The SSL Protocol, (Secure Socket Layer), Version 3.0. Internet Draft, 18 Nov 1996, 63 pages, draft-freier-ssl-version3-02.txt. Deleted from Internet-drafts server. Now included in Transport Layer Security (TLS) standardization efforts of the IETF, http://www.ietf.org/html.charters/tls-charter.html [11.11.2007].

Dierks, Tim; Riscorla, Eric (2006): The Transport Layer Security (TLS) Protocol, Version 1.1. Internet Official Protocol Standard (STD 1) RFC 4346 (obsoletes RFC 2246, June 2003). April 2006, 87 pages. http://www.ietf.org/html.charters/tls-charter.html [11.11.2007]

Blake-Wilson, S.; et al.: Transport Layer Security (TLS) Extensions. Internet Standard RFC 3546. Updates (but does not replace) RFC 2246, June 2003, 29 pages.

Esslinger, Bernhard; Müller, Maik: Secure Sockets Layer (SSL) Protokoll – Sichere Internetkommunikation mittels SSL und Sicherheits-Proxy. DuD 12/1997, 691-697.

Hirsch, Frederick J.: Introducing SSL and Certificats Using SSLeay. In Web Security – A Matter of Trust (World Wide Web Journal). O’Reilly. Sebastopol, 1997, 141-173.

Mühl, Judith: IPSec und SSL. Unveröffentlichte Seminararbeit, TU Darmstadt. Juni 1998, 16 Seiten. Erhältlich von R. Grimm als PDF-File <SSL-IPSEC_Seminararbeit.pdf>. (Nur für IPSec teilw. gut)

Baum-Waidner, Birgit; Herfert, Michael: Transport Layer Security (TLS). In: Untersuchung Sicherheitsverfahren für E-Commerce, TeleTrusT AG 4 „Open E-Commerce Security“, 23.2.1999, 11 Seiten. Erhältlich von R. Grimm als PDF-File <SSL_herfert_tls.pdf>. (Sehr guter Text)

S/MIME:

N. Borenstein, N. Freed: MIME (Multipurpose Internet Mail Extensions), Part 1: Mechanisms for Specifying and Describing the Format of Internet Message Bodies. Network Working Group, RFC 1521, September 1993, 70 pages.

B. Ramsdell, Editor: S/MIME Editor: S/MIME Version 3 Message Specification. Internet Standard Request for Comments RFC 2633, June 1999, 32 pages.

RFC 2630: CMS: Cryptographic Message Syntax. R. Housley, Spyrus, June 1999.
Earlier version: RFC 2315: PKCS #7: Cryptographic Message Syntax. Version 1.5. B. Kaliski, RSA Labs, March 1998.

R. Grimm: Sicherheit für offene Kommunikationsnetze. In: Günter Müller, Andreas Pfitzmann (Ed.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison Wesley, Bonn, Reading (MA) 1997 (Informationssicherheit), 105-132.

Zu V11: Authentifizierungsprotokolle

Überblick:

Fries, Otfried; Fritsch, Andreas; Kessler, Volker; Klein, Birgit (Herausg.): Sicherheitsmechanismen. R. Oldenbourg Verlag, München 1993.

Schneier, Bruce: Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd Ed. Wiley & Sons, Chichester 1996, 758 p.

Klaus Schmeh: Safer Net: Kryptographie im Internet und Intranet. dpunkt Verlag, Heidelberg, 2. Auflage 2001, 562 Seiten.

Needham-Schroeder (konventionell) und Kerberos:

Needham, R.M.; Schroeder, M.D: Using Encryption for Authentication in Large Networks. In: Comm. ACM 21 No.12, 1978, 993-999.

Steiner, J.G.; Neumann, C.; Schiller, J.I.: Kerberos: An Authentication Service for Open Network Systems. USENIX Winter Conference, Dallas Texas, 9-12 Feb 1988. Proceedings pp. 191-202. (Project Athena, MIT, Boston MA).

Needham-Schroeder (asymmetrisch):

Needham, R.M., Schroeder, M.D: Authentication Revisited. In: Operating Systems Review 21 No.1, 1987, 7.

Burrows, Abadi, Needham: A Logic of Authentication. Digital System Research Center, CA, 1989.

X.509:

ISO/IEC 9594-8, ITU X.509 (1988/92): Information technology – Open Systems Interconnection – The Directory – Authentication Framework. 1988/1993(E).

Anson, C.; Mitchell, C.: Security Defects in CCITT Recommendation X.509 – The Directory Authentication Framework. In: Computer Comm. Review 20 No.2, 1990.

Müller, M.; Plattner, B.: Security Capabilities of X.509: Evaluation and Constructive Criticism. In: Proceedings of the IFIP TC6/WG6.5 International Conference on Message Handling Systems and Application Layer Communication Protocols, Zürich, 3.-5. Oktober 1990, pp. W1.1-16.

Zu V12: Malware (Viren, Würmer usw.)

Bonroy, Frederic: Malware infiltration using camouflage techniques. Diplomarbeit Universität Koblenz, Mai 2007.

Eckert, Claudia: IT-Sicherheit, Konzepte - Verfahren - Protokolle. München, Oldenbourg Verlag, 2006.

Peter Sczor: The Art of Computer Virus Research and Defense. SymantecPress, 2005.

Vesselin Bontchev: Dissertation über Viren. Universität Hamburg, 1998.

BSI: Informationen zu Computer-Viren. Bd. 2 der Schriftenreihe zu IT-Sicherheit, 2. erw. Auflage, April 1997. http://www.bsi.bund.de/av/virbro/index.htm (11.11.2007)

D. Russel et al.: Computer Security Basics. O'Reilly, Sebastopol CA, 1991.

P.J. Denning (ed.): Computers Under Attack – Intruders, Worms and Viruses. ACM Press, New York, 1990.

W. Gleißner et al.: Manipulation in Rechnern und Netzen. Addison-Wesley, Bonn etc. 1989.

F. Cohen: Computer Viruses, Theory and Experiments. Computers & Security, 6, 22-35, 1985.

Weitere Weblinks zu „Malware“:

http://www.bsi.bund.de/av/index.htm (Aktuelles über Computer.Viren)

http://www.computerhistory.org/timeline/?category=net

http://www.research.ibm.com/antivirus/timeline.htm

http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport

http://www.bsi.bund.de/av/virbro/

http://www.ec-net.de/EC-Net/Navigation/netz-informationssicherheit.html

http://www.wildlist.org/

http://www.people.frisk-software.com/~bontchev/papers/naming.html

http://secwatch.org/

http://www.lavasoft.de/

http://www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.mspx

http://sourceforge.net/projects/rkhunter/

Zu V_add1: Kryptographie: Elementare Zahlentheorie

Viele einführende Lehrbücher in die elementare Zahlentheorie, darunter zum Beispiel

Scholz, B.; und Schoeneberg, A.: Einführung in die Zahlentheorie. Sammlung Göschen de Gruyter, wiederholte Auflage, z.B. 5. Auflage Berlin, New York 1973, 128 S.

M.O. Rabin: Digital Signatures and Public-Key Functions as Intractable as Factorization. MIT Lab. of Computer Science, Technical Report, MIT/LCS/TR-212, Jan 1979.

M.O. Rabin: Probabilistic Algorithm for Testing Primality. Journal of Number Theory, Vol.12, No.1, 128-138, Feb 1980.

Knuth, Donald E.: The Art of Computer Programming. Vol. 2: Seminumerical Algorithms. 2nd Ed. Adison Wesley, Reading MA (USA) 1981. 688 S.

Bressoud, David M.: Factorization and Primality Testing. Springer, New York (USA) 1989. 237 S.

Cormen, Th. H.; Leiserson, C. E.; Rivest, R.; und Stein, C.: Algorithmen – Eine Einführung. Oldenbourg Verlag München, Wien, 2004, 1188 Seiten. Darin besonders: Kap. 31, Zahlentheoretische Algorithmen, S. 851 ff. Originale Ausgabe „Introduction to Algorithms“, MIT Press and McGraw-Hill Book Company, 2001.

Grimm: Online-Texte zum ggT und zum Chinesischem Restklassensatz.

Zu V_add2: Kryptographie: Komplexitätstheorie

Gary, Michael R., and Johnson, David S.: Computers and Intractability – A Guide to the Theory of NP-Completeness. W.H. Freeman and Company, New York (USA) 1979. Copyright 1979 Bell Telephone Labs Inc. ISBN 0-7167-1044-7. 340 S.

Cormen, Th. H.; Leiserson, C. E.; Rivest, R.; und Stein, C.: Algorithmen – Eine Einführung. Oldenbourg Verlag München, Wien, 2004, 1188 Seiten. Darin besonders: Kap. 34, NP-Vollständigkeit, S. 969 ff. Originale Ausgabe „Introduction to Algorithms“, MIT Press and McGraw-Hill Book Company, 2001.

Schöning, Uwe: Theoretische Informatik - kurzgefaßt. Spektrum Akademischer Verlag, 2. Auflage Heidelberg 1995. 188 S.

Zu V_add3: Fair Exchange / CEM

Pagnia, Vogt, Gärtner: Fair Exchange. The Computer Journal, 2001.

Asokan, N.: Fairness in Electronic Commerce. PhD Thesis, University of Waterloo, May 1998.

Bahreman, A.; Tygar, D.J.: Certified Electronic Mail. Proceedings of the Internet Society Symposium on Network and Distributed System Security, 3-19, San Diego, Cal., Feb 3-4, 1994.

Grimm, R.: A Model of Security in Open Telecooperation. In: IFIP Transactions C-7. Elsevier Science Publishers B.V. (North-Holland), 1992, pp. 425-440.