1 Bücher

[Ecke 04, GORP 04, GaSp 96, ZCC 00, Hone 02, Grim 01, BoKa 01, Stal 98, TrWa 02, Schn 96, Baue 00, Denn 99, Oaks 98, Stei 98, Kahn 96]

Im folgenden wird vertiefende Literatur zu den einzelnen Abschnitten der Vorlesung angegeben:

2 Einleitung

2.1 Internet Wurm versus Slammer Wurm

[EiRo 89, MPSS 03, Slam 03]

3 Grundlagen

3.0.1 OSI Security Architecture

[X.800, X.802, X.803, X.810, X.811, X.812, X.813, X.814, X.815]

4 Security Engineering

4.1 DoS und DDoS

[CERT 99, Ditt 99a, Ditt 99b, Ditt 99c, Ditt 00, Chan 02]

4.2 SPAM

[EU 03]

4.3 Mobile Code

[CERT 00, SecArch1.2, Gong 98a, GMPS 97, Gong 97, GoSc 98]

4.3.1 Java Sicherheitsarchitektur

[SecArch1.2, Gong 98a, GMPS 97, Gong 97, GoSc 98]

4.4 Buffer Overflow

[Smit 97]

4.5 Twenty Most Vulnerabilities

[SANS]

5 Kryptologie

5.0.1 Steganographie

[FFWW 99, WePf 00, Prov 01, PrHo 02]

5.1 DES

[FIPS 46-2]

5.2 AES

[FIPS 197]

5.3 RSA

[Koch 96, Kali 96, Silv 01]

5.4 Krptographische Hash-Funktionen

[Rive 92, Touc 95]

6 Sicherheitsmaßnahmen

6.1 One-Time-Password Verfahren

[Hall 95, HMNS 98]

6.2 Biometrie

[PPJ 01, JHPB 97, KaJa 96, KaJa 96, MaMa 02, Mats 02, PPK 03]

6.3 Kerberos

[KoNe 93]

Literatur

[Baue 00] Bauer, F.L.: *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*, Band 3. Springer, Berlin, 2000.

[BoKa 01] Bosworth, S. und M.E. Kabay (Herausgeber): *Computer Security Handbook*. Wiley, New York, fourth Auflage, 2002.

[CERT 00] CERT Coordination Center: *Results of the Security in ActiveX Workshop*. Technischer Bericht, CERT CC, Pittsburgh, PA, USA, Dezember 2000, `http://www.cert.org/reports/activeX_report.pdf` .

[CERT 99] CERT Coordination Center: *Results of the Distributed-Systems Intruder Tools Workshop* . Technischer Bericht, CERT/CC, November 1999, `http://www.cert.org/reports/dsit_workshop-final.html` .

[Chan 02] Chang, R. K. C.: *Defending against Flooding-Based Distributed Denial–of–Service Attacks: A Tutorial*. IEEE Communications, 40(10):42–51, Oktober 2002.

[Denn 99] Denning, D. E.: *Information Warfare and Security*. Addison–Wesley, Reading, 1999.

[Ditt 00] Dittrich, D.: *The "mstream" distributed denial of service attack tool.* Technischer Bericht, University of Washington, 2000, `http://staff.washington.edu/dittrich/misc/mstream.analysis.txt` .

[Ditt 99a] Dittrich, D.: *The DoS Project's "trinoo" distributed denial of service attack tool.* Technischer Bericht, University of Washington, 1999, `http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt` .

[Ditt 99b] Dittrich, D.: *The "Tribe Flood Network" distributed denial of service attack tool.* Technischer Bericht, University of Washington, 1999, `http://staff.washington.edu/dittrich/misc/tfn.analysis.txt` .

[Ditt 99c] Dittrich, D.: *The "stacheldraht" distributed denial of service attack tool.* Technischer Bericht, University of Washington, 1999, `http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt` .

[Ecke 04] Eckert, C.: *IT–Sicherheit: Konzepte — Verfahren — Protokolle.* Oldenbourg, München, 3 Auflage, 2004.

[EiRo 89] Eichin, M. W. und J. A. Rochlis: *With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988.* In: *Proceedings of the 1989 IEEE Computer Society Symposium on Security and Privacy*, Oakland, Ohio, 1989. , `http://www.thok.org/intranet/resume/mwe97.html` .

[EU 03] EU Kommission: *Unerbetene E–Mails: Kommission diskutiert Spam–Bekämpfung mit Vertretern aus Wirtschaft und Verwaltung sowie Verbraucherverbänden.* Presseerklärung, Oktober 2003, `http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm` .

[FFWW 99] Federrath, H., E. Franz, A. Westfeld und G. Wicke: *Steganographie zur vertraulichen Kommunikation.* IT-Sicherheit, (3):10–13, 1999, `http://os.inf.tu-dresden.de/~westfeld/publikationen` .

[FIPS 197] National Institute of Standards and Technology (NIST): *Advanced Encryption Standard (AES).* Federal Information Processing Standards 197, U.S. Department of Commerce, Gaithersburg, November 2001, `http://csrc.nist.gov/encryption/aes/` .

[FIPS 46-2] National Institute of Standards and Technology (NIST): *Data Encryption Standard (DES).* Federal Information Processing Standards 46-2, U.S. Department of Commerce, Gaithersburg, Dezember 1993, `http://www.itl.nist.gov/fipspubs/fip46-2.htm` .

[GaSp 96] Garfinkel, Simson und Gene Spafford: *Practical Unix and Internet Security.* O'Reilly & Associates, 2 Auflage, 1996.

[GMPS 97] Gong, L., M. Mueller, H. Prafullchandra und R. Schemers: *Going Beyond the Sandbox: An Overview of the New Security Architecture in the Java(TM) Development Kit 1.2.* In: *Proceedings of the USENIX Symposium on Internet Technologies and Systems*, Monterey, California, USA, Dezember 1997. USENIX, `http://java.sun.com/security/usenix-jdk12security.ps` .

[Gong 97] Gong, Li: *Surviveable Mobile Code is Hard to Build.* In: *Foundations for Secure Mobile Code Workshop*, 1997, `http://www.cs.nps.navy.mil/research/languages/statements/` .

[Gong 98a] Gong, L.: *Secure Java Class Loading*. IEEE Internet Computing, 2(6):56–61, November 1998.

[GORP 04] Gerloni, H., B. Oberhaitzinger, H. Reiser und J. Plate: *Praxisbuch Sicherheit für Linux–Server und -Netze*. Hanser, Mai 2004, `http://www.nm.ifi.lmu.de/~sicherheitsbuch` . ISBN 3–446–22626–5, 430 p.

[GoSc 98] Gong, Li und Roland Schemers: *Signing, Sealing, and Guarding Java Objects*. Nummer 1419 in *LNCS*, Seiten 206–216, Berlin, Heidelberg, 1998. Springer, `http://link.springer.de/link/service/series/0558/bibs/1419/14190206.htm` .

[Grim 01] Grimes, R. A.: *Malicious Mobile Code — Virus Protection for Windows*. O'Reilly, 2001.

[Hall 95] Haller, N.: *RFC 1760: The S/KEY One-Time Password System*. RFC, IETF, Februar 1995, `ftp://ftp.isi.edu/in-notes/rfc1760.txt` .

[HMNS 98] Haller, N., C. Metz, P. Nesser und M. Straw: *RFC 2289: A One-Time Password System*. RFC, IETF, Februar 1998, `ftp://ftp.isi.edu/in-notes/rfc2289.txt` .

[Hone 02] The Honeynet Projekt (Herausgeber): *Known your Enemy – Revealing the Security Tools, Tactics, and Motives of the Blackhat Community*. Addision Wesley, 2002.

[JHPB 97] Jain, A., L. Hong, S. Pankanti, und R. Bolle: *An Identity Authentication System using Fingerprints*. Proceedings of the IEEE, 85(9):1365–1388, 1997.

[Kahn 96] Kahn, D.: *The Codebreakers: The Story of Secret Writing*. Scribner, 1996.

[KaJa 96] Karu, K. und A. Jain: *Fingerprint Classification*. Pattern Recognition, 29(3):389–404, 1996.

[Kali 96] Kaliski, B.: *Timing Attacks on Cryptosystems*. RSA Bulletin 2, RSA Laboratories, Januar 1996, `http://www.rsasecurity.com/rsalabs/bulletins/index.html` .

[Koch 96] Kocher, P. C.: *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*. In: Koblitz, N. (Herausgeber): *Advances in Cryptology - CRYPTO '96*, Band 1109 der Reihe *Lecture Notes in Computer Science (LNCS)*, Seiten 104–113. August, Springer, August 1996, `http://www.cryptography.com/resources/papers/crypto1996.html` .

[KoNe 93] Kohl, J. und C. Neuman: *RFC 1510: The Kerberos Network Authentication Service (V5)*. RFC, IETF, September 1993, `ftp://ftp.isi.edu/in-notes/rfc1510.txt` .

[MaMa 02] Matsumoto, T. und H. Matsumoto: *Impact of artificial "gummyfingers on fingerprint systems*. In: Renesse, R. L. van (Herausgeber): *Optical Security and Counterfeit Deterrence Techniques IV*, Nummer 4677 in *Proceedings of SPIE*, Januar 2002.

[Mats 02] Matsumotu, T.: *Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies — A Case Study for User Identification —*. Presentation, ITU-T Workshop on Security, Seoul, 2002, `http://www.itu.int/itudoc/itu-t/workshop/security/present/` .

[MPSS 03] Moore, D., V. Paxson, S. Savage, C. Shannon, S. Staniford und N. Weaver: *Inside the Slammer Worm*. IEEE Security & Privacy, 1(4), 2003, `http://www.computer.org/security/v1n4/j4wea.htm` .

[Oaks 98] Oaks, Scott: *Java Security*. The Java Series. O'Reilly, 1998.

[PPJ 01] Pankanti, S., S. Prabhakar und A. Jain: *On the Individuality of Fingerprints*. In: *Proceedings Computer Vision and Pattern Recognition (CVPR)*, Hawaii, Dec. 11-13 2001. .

[PPK 03] Prabhakar, S., S. Pankanti und A. K. Jain: *Biometric Recognition: Security and Privacy Concerns*. IEEE Security and Privacy, 1(2):33–42, März 2003.

[PrHo 02] Provos, N. und P. Honeyman: *Detecting Steganographic Content on the Internet*. In: *Network and Distributed System Security Symposium (ISOC NDSS 02)*, San Diego, CA, 2002. , `http://www.citi.umich.edu/u/provos/cv.html#papers` .

[Prov 01] Provos, Niels: *Defending Against Statistical Steganalysis*. In: *10th USENIX Security Symposium*, Washington, DC, 2001. , `http://www.citi.umich.edu/u/provos/cv.html#papers` .

[Rive 92] Rivest, R.: *RFC 1321: The MD5 Message-Digest Algorithm*. RFC, IETF, April 1992, `ftp://ftp.isi.edu/in-notes/rfc1321.txt` .

[SANS] SANS (SysAdmin, Audit, Network, Security) Institute: *The Twenty Most Critical Internet Security Vulnerabilities*, `http://www.sans.org/top20/` .

[Schn 96] Schneier, Bruce: *Applied Cryptography*. Wiley & Sons, Second Auflage, 1996.

[SecArch1.2] Gong, Li: *Java 2 Platform Security Architecture*. Technischer Bericht Version 1.2, Sun Microsystems, Inc., Palo Alto, CA, 2001, `http://java.sun.com/j2se/1.4/docs/guide/security/spec/security-spec.doc.html` .

[Silv 01] Silverman, R. D.: *A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths*. RSA Bulletin 13, RSA Laboratories, November 2001, `http://www.rsasecurity.com/rsalabs/bulletins/index.html` .

[Slam 03] Cooperative Association for Internet Data Analysis (CAIDA): *The Spread of the Sapphire/Slammer Worm*. `http://www.caida.org/outreach/papers/2003/sapphire/`, 2003, `http://www.caida.org/outreach/papers/2003/sapphire/` .

[Smit 97] Smith, N.: *Stack Smashing Vulnerabilities in the UNIX Operating System*. Technischer Bericht, Southern Connecticut State University, 1997, `http://destroy.net/machines/security/nate-buffer.ps` .

[Stal 98] Stallings, W.: *Cryptography and Network Security — Principles and Practice*. Prentice Hall, 1998.

[Stei 98] Stein, L. D.: *Web Security: A Step–by–Step Reference Guide*. Addison–Wesley, 1998.

[Touc 95] Touch, J.: *RFC 1810: Report on MD5 Performance*. RFC, IETF, Juni 1995, `ftp://ftp.isi.edu/in-notes/rfc1810.txt` .

[TrWa 02] Trappe, W. und L. C. Washington: *Introduction to Cryptography with Coding Theory*. Prentice Hall, 2002.

[WePf 00] Westfeld, A. und A. Pfitzmann: *Attacks on Steganographic Systems*. In: Pfitzmann, A. (Herausgeber): *Information Hiding. Third International Workshop, IH'99*, Nummer 1768 in *LNCS*, Seiten 61–76. Springer, 2000, `http://os.inf.tu-dresden.de/~westfeld/publikationen` .

[X.800] ITU: *X.800 — Data Communication Networks; Open Systems Interconnection (OSI); Security Structure and Application — Security Architecture for Open Systems Interconnection for CCITT Applications*. Recommendation, International Telecommunication Union, Geneva, 1991.

[X.802] ITU: *X.802 — Data Networks and Open System Communications Security — Information Technology — Lower Layer Security Model*. ITU–T Recommendation, International Telecommunication Union, Geneva, 1995. also published as ISO/IEC International Standard 13594.

[X.803] ITU: *X.803 — Data Networks and Open System Communications Security — Information Technology — Upper Layer Security Model*. ITU–T Recommendation, International Telecommunication Union, Geneva, 1995.

[X.810] ITU: *X.810 — Data Networks and Open System Communications Security — Information Technology — Open Systems Interconnection — Security Frameworks for Opens Systems: Overview*. ITU–T Recommendation, International Telecommunication Union, Geneva, 1996. also published as ISO/IEC International Standard 10181-1.

[X.811] ITU: *X.811 — Data Networks and Open System Communications Security — Information Technology — Open Systems Interconnection — Security Frameworks for Opens Systems: Authentication Framework*. ITU–T Recommendation, International Telecommunication Union, Geneva, 1995. also published as ISO/IEC International Standard 10181-2.

[X.812] ITU: *X.812 — Data Networks and Open System Communications Security — Information Technology — Open Systems Interconnection — Security Frameworks for Opens Systems: Access Control Framework*. ITU–T Recommendation, International Telecommunication Union, Geneva, 1995. also published as ISO/IEC International Standard 10181-3.

[X.813] ITU: *X.813 — Data Networks and Open System Communications Security — Information Technology — Open Systems Interconnection — Security Frameworks for Opens Systems: Non–repudiation Framework*. ITU–T Recommendation, International Telecommunication Union, Geneva, 1996. also published as ISO/IEC International Standard 10181-4.

[X.814] ITU: *X.814 — Data Networks and Open System Communications Security — Information Technology — Open Systems Interconnection — Security Frameworks for Opens Systems: Confidentiality Framework*. ITU–T Recommendation, International Telecommunication Union, Geneva, 1995. also published as ISO/IEC International Standard 10181-5.

[X.815] ITU: *X.815 — Data Networks and Open System Communications Security — Information Technology — Open Systems Interconnection — Security Frameworks for Opens Systems: Integrity Frameworks*. ITU–T Recommendation, International Telecommunication Union, Geneva, 1995. also published as ISO/IEC International Standard 10181-6.

[ZCC 00] Zwicky, E. D., S. Cooper und D. B. Chapman: *Building Internet Firewalls*. O'Reilly, 2 Auflage, 2000.