

indications as to how to proceed on to the next step as well as the grade until that point. The project can be attempted in three ways: 1. Without seeking any sort of help 2. Using some provided hints 3. Using exact directions The IRC includes the files needed for this project: 1. Web Security project 2. Web Hacking exercises (XSS and Script-attacks) covering client-side and server-side vulnerability exploitations, respectively 3. Documentation for installation and use for the above 4. A PowerPoint file describing Web hacking. This file is crucial to understanding how to use the exercises since it clearly explains the operation using screen shots. This project was designed and implemented by Professor Sreekanth Malladi of Dakota State University.

**B.3 Programming Projects** The programming project is a useful pedagogical tool. There are several attractive features of stand-alone programming projects that are not part of an existing security facility. 1. The instructor can choose from a wide variety of cryptography and network security concepts to assign projects. 2. The projects can be programmed by the students on any available computer and in any appropriate language; they are platform and language independent. 3. The instructor need not download, install, and configure any particular infrastructure for stand-alone projects.

**440 Appendix B / Projects for Teaching Network Security** There is also flexibility in the size of projects. Larger projects give students more sense of achievement, but students with less ability or fewer organizational skills can be left behind. Larger projects usually elicit more overall effort from the best students. Smaller projects can have a higher concepts-to-code ratio, and because more of them can be assigned, the opportunity exists to address a variety of different areas. Again, as with research projects, the students should first submit a proposal. The student handout should include the same elements listed in Section B.1. The IRC includes a set of twelve possible programming projects. The following individuals have supplied the research and programming projects suggested in the instructor's manual: Henning Schulzrinne of Columbia University; Cetin Kaya Koc of Oregon State University; and David M. Balenson of Trusted Information Systems and George Washington University.

**B.4 Laboratory Exercises** Professor Sanjay Rao and Ruben Torres of Purdue University have prepared a set of laboratory exercises that are part of the IRC. These are implementation projects designed to be programmed on Linux but could be adapted for any Unix environment. These laboratory exercises provide realistic experience in implementing security functions and applications.

**B.5 Practical Security Assessments** Examining the current infrastructure and practices of an existing organization is one of the best ways of developing skills in assessing its security posture. The IRC contains a list of such activities. Students, working either individually or in small groups, select a suitable small-to-medium-sized organization. They then interview some key personnel in that organization in order to conduct a suitable selection of security risk assessment and review tasks as it relates to the organization's IT infrastructure and practices. As a result, they can then recommend suitable changes, which can improve the organization's IT security. These activities help students develop an appreciation of current security practices and the skills needed to review these and recommend changes. Lawrie Brown of the Australian Defence Force Academy developed these projects.

**B.6 Firewall Projects** The implementation of network firewalls can be a difficult concept for students to grasp initially. The IRC includes a Network Firewall Visualization tool to convey and teach network security and firewall configuration. This tool is intended to teach and reinforce key concepts including the use and purpose of a perimeter firewall, the use of separated subnets, the purposes behind packet filtering, and the shortcomings of a simple packet filter firewall.

**B.9 / Reading/Report Assignments** **441** The IRC includes a .jar file that is fully portable and a

series of exercises. The tool and exercises were developed at U.S. Air Force Academy. B.7 Case Studies Teaching with case studies engages students in active learning. The IRC includes case studies in the following areas: ■■ Disaster recovery ■■ Firewalls ■■ Incidence response ■■ Physical security ■■ Risk ■■ Security policy ■■ Virtualization Each case study includes learning objectives, case description, and a series of case discussion questions. Each case study is based on real-world situations and includes papers or reports describing the case. The case studies were developed at North Carolina A&T State University. B.8 Writing Assignments Writing assignments can have a powerful multiplier effect in the learning process in a technical discipline such as cryptography and network security. Adherents of the Writing Across the Curriculum (WAC) movement (<http://wac.colostate.edu/>) report substantial benefits of writing assignments in facilitating learning. Writing assignments lead to more detailed and complete thinking about a particular topic. In addition, writing assignments help to overcome the tendency of students to pursue a subject with a minimum of personal engagement—just learning facts and problemsolving techniques without obtaining a deep understanding of the subject matter. The IRC contains a number of suggested writing assignments, organized by chapter. Instructors may ultimately find that this is an important part of their approach to teaching the material. I would greatly appreciate any feedback on this area and any suggestions for additional writing assignments. B.9 Reading/Report Assignments Another excellent way to reinforce concepts from the course and to give students research experience is to assign papers from the literature to be read and analyzed. The IRC includes a suggested list of papers, one or two per chapter, to be assigned. A PDF copy of each of the papers is available at <https://app.box.com/netsec6e>. The IRC also includes a suggested assignment wording.

442 References

Abbreviations

ACM Association for Computing Machinery

IBM International Business Machines Corporation

IEEE Institute of Electrical and Electronics Engineers

NIST National Institute of Standards and Technology

ALVA90 Alvare, A. "How Crackers Crack Passwords or What Passwords to Avoid." Proceedings, UNIX Security Workshop II, August 1990.

ANDE80 Anderson, J. Computer Security Threat Monitoring and Surveillance. Fort Washington, PA: James P. Anderson Co., April 1980.

ANDE95 Anderson, D., et al. Detecting Unusual Program Behavior Using the Statistical Component of the Next-generation Intrusion Detection Expert System (NIDES). Technical Report SRI-CSL-95-06, SRI Computer Science Laboratory, May 1995. [www.csl.sri.com/programs/intrusion](http://www.csl.sri.com/programs/intrusion).

ANTE06 Ante, S., and Grow, B. "Meet the Hackers." Business Week, May 29, 2006.

AROR12 Arora, M. "How Secure is AES against Brute-Force Attack?" EE Times, May 7, 2012.

AXEL00 Axelsson, S. "The Base-Rate Fallacy and the Difficulty of Intrusion Detection." ACM Transactions and Information and System Security, August 2000.

AYCO06 Aycock, J. Computer Viruses and Malware. New York: Springer, 2006.

BALA98 Balasubramanian, J., et al. "An Architecture for Intrusion Detection Using Autonomous Agents." Proceedings, 14th Annual Computer Security Applications Conference, 1998.

BARD12 Bardou, R., et al. "Efficient Padding Oracle Attacks on Cryptographic Hardware," INRIA, Rapport de recherche RR-7944, Apr. 2012. <http://hal.inria.fr/hal-00691958>.

BASU12 Basu, A. Intel AES-NI Performance Testing over Full Disk Encryption. Intel Corp. May 2012.

BAUE88 Bauer, D., and Koblenz, M. "NIDX—An Expert System for Real-Time Network Intrusion Detection." Proceedings, Computer Networking Symposium, April 1988.

BELL90 Bellare, S., and Merritt, M. "Limitations of the Kerberos Authentication System." Computer Communications Review, October 1990.

BELL94a Bellare, M., and Rogaway, P. "Optimal Asymmetric Encryption—How to Encrypt with RSA." Proceedings, Eurocrypt '94, 1994.

BELL94b Bellare, S., and Cheswick, W.

"Network Firewalls." IEEE Communications Magazine, September 1994. BELL96a Bellare, M.; Canetti, R.; and Krawczyk, H. "Keying Hash Functions for Message Authentication." Proceedings, CRYPTO '96, August 1996; published by Springer-Verlag. An expanded version is available at <http://www-cse.ucsd.edu/users/mihir>. BELL96b Bellare, M.; Canetti, R.; and Krawczyk, H. "The HMAC Construction." CryptoBytes, Spring 1996. BINS10 Binsalleeh, H., et al. "On the Analysis of the Zeus Botnet Crimeware Toolkit." Proceedings of the 8th Annual International Conference on Privacy, Security and Trust, IEEE, September 2010. BLEI98 Bleichenbacher, D. "Chosen Ciphertext Attacks against Protocols Based on the RSA Encryption Standard PKCS #1," CRYPTO '98, 1998. BLOO70 Bloom, B. "Space/time Trade-offs in Hash Coding with Allowable Errors." Communications of the ACM, July 1970. BRYA88 Bryant, W. Designing an Authentication System: A Dialogue in Four Scenes. Project Athena document, February 1988. Available at <http://web.mit.edu/kerberos/www/dialogue.html>. References 443 CERT01 CERT Coordination Center. "Denial of Service Attacks." June 2001. [http://www.cert.org/tech\\_tips/denial\\_of\\_service.html](http://www.cert.org/tech_tips/denial_of_service.html). CHAN02 Chang, R. "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial." IEEE Communications Magazine, October 2002. CHEN04 Chen, S., and Tang, T. "Slowing Down Internet Worms," Proceedings of the 24th International Conference on Distributed Computing Systems, 2004. CHEN11 Chen, T., and Abu-Nimeh, S. "Lessons from Stuxnet." IEEE Computer, 44(4), pp. 91–93, April 2011. CHIN05 Chinchani, R., and Berg, E. "A Fast Static Analysis Approach to Detect Exploit Code Inside Network Flows." Recent Advances in Intrusion Detection, 8th International Symposium, 2005. CHOI08 Choi, M., et al. "Wireless Network Security: Vulnerabilities, Threats and Countermeasures." International Journal of Multimedia and Ubiquitous Engineering, July 2008. COMP06 Computer Associates International. The Business Value of Identity Federation. White Paper, January 2006. CONR02 Conry-Murray, A. "Behavior-Blocking Stops Unknown Malicious Code." Network Magazine, June 2002. COST05 Costa, M., et al. "Vigilante: End-to-End Containment of Internet Worms." ACM Symposium on Operating Systems Principles, 2005. CSA10 Cloud Security Alliance. Top Threats to Cloud Computing V1.0. CSA Report, March 2010. CSA11a Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. CSA Report, 2011. CSA11b Cloud Security Alliance. Security as a Service (SecaaS). CSA Report, 2011. DAMI03 Damiani, E., et al. "Balancing Confidentiality and Efficiency in Untrusted Relational Databases." Proceedings, Tenth ACM Conference on Computer and Communications Security, 2003. DAMI05 Damiani, E., et al. "Key Management for Multi-User Encrypted Databases." Proceedings, 2005 ACM Workshop on Storage Security and Survivability, 2005. DAVI89 Davies, D., and Price, W. Security for Computer Networks. New York: Wiley, 1989. DAWS96 Dawson, E., and Nielsen, L. "Automated Cryptoanalysis of XOR Plaintext Strings." Cryptologia, April 1996. DENN87 Denning, D. "An Intrusion-Detection Model." IEEE Transactions on Software Engineering, February 1987. DIFF76 Diffie, W., and Hellman, M. "Multiuser Cryptographic Techniques." IEEE Transactions on Information Theory, November 1976. DIFF79 Diffie, W., and Hellman, M. "Privacy and Authentication: An Introduction to Cryptography." Proceedings of the IEEE, March 1979. DIMI07 Dimitriadis, C. "Analyzing the Security of Internet Banking Authentication Mechanisms." Information Systems Control Journal, Vol. 3, 2007. EFF98 Electronic Frontier Foundation. Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design. Sebastopol, CA: O'Reilly, 1998. ENIS09 European Network and Information Security Agency. Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA Report, November 2009. FEIS73 Feistel, H. "Cryptography and Computer

Privacy.” *Scientific American*, May 1973. FLUH00 Fluhrer, S., and McGrew, D. “Statistical Analysis of the Alleged RC4 Key Stream Generator.” *Proceedings, Fast Software Encryption 2000*, 2000. FLUH01 Fluhrer, S.; Mantin, I.; and Shamir, A. “Weakness in the Key Scheduling Algorithm of RC4.” *Proceedings, Workshop in Selected Areas of Cryptography*, 2001. FORD95 Ford, W. “Advances in Public-Key Certificate Standards.” *ACM SIGSAC Review*, July 1995. 444 References FOSS10 Fossi, M., et al. “Symantec Report on Attack Kits and Malicious Websites.” Symantec, 2010. FRAN07 Frankel, S., et al. *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*. NIST Special Publication 800-97, February 2007. GARD77 Gardner, M. “A New Kind of Cipher That Would Take Millions of Years to Break.” *Scientific American*, August 1977. GOLD10 Gold, S. “Social Engineering Today: Psychology, Strategies and Tricks.” *Network Security*, November 2010. GOOD11 Goodin, D. “Hackers Break SSL Encryption Used by Millions of Sites.” *The Register*, September 19, 2011. GOOD12a Goodin, D. “Why Passwords Have Never Been Weaker—and Crackers Have Never Been Stronger.” *Ars Technica*, August 20, 2012. GOOD12b Goodin, D. “Crack in Internet's Foundation of Trust Allows HTTPS Session Hijacking.” *Ars Technica*, September 13, 2012. GRAN04 Grance, T.; Kent, K.; and Kim, B. *Computer Security Incident Handling Guide*. NIST Special Publication 800-61, January 2004. HACI02 Hacigumus, H., et al. “Executing SQL over Encrypted Data in the Database-Service Provider Model.” *Proceedings, 2002 ACM SIGMOD International Conference on Management of Data*, 2002. HEBE92 Heberlein, L.; Mukherjee, B.; and Levitt, K. “Internetwork Security Monitor: An Intrusion-Detection System for Large-Scale Networks.” *Proceedings, 15th National Computer Security Conference*, October 1992. HILT06 Hiltgen, A.; Kramp, T.; and Wiegold, T. “Secure Internet Banking Authentication.” *IEEE Security and Privacy*, Vol. 4, No. 2, 2006. HONE05 The HoneyNet Project. “Knowing Your Enemy: Tracking Botnets.” *HoneyNet White Paper*, March 2005. <http://honeynet.org/papers/bots>. HOWA03 Howard, M.; Pincus, J.; and Wing, J. “Measuring Relative Attack Surfaces.” *Proceedings, Workshop on Advanced Developments in Software and Systems Security*, 2003. HUIT98 Huitema, C. *IPv6: The New Internet Protocol*. Upper Saddle River, NJ: Prentice Hall, 1998. IANS90 I’Anson, C., and Mitchell, C. “Security Defects in CCITT Recommendation X.509 – The Directory Authentication Framework.” *Computer Communications Review*, April 1990. ILGU95 Ilgun, K.; Kemmerer, R.; and Porras, P. “State Transition Analysis: A Rule-Based Intrusion Detection Approach.” *IEEE Transaction on Software Engineering*, March 1995. JANS11 Jansen, W., and Grance, T. *Guidelines on Security and Privacy in Public Cloud Computing*. NIST Special Publication 800-144, January 2011. JAVI91 Javitz, H., and Valdes, A. “The SRI IDES Statistical Anomaly Detector.” *Proceedings, 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, May 1991. JHI07 Jhi, Y., and Liu, P. “PWC: A Proactive Worm Containment Solution for Enterprise Networks.” *Third International Conference on Security and Privacy in Communications Networks*, 2007. JUEN85 Jueneman, R.; Matyas, S.; and Meyer, C. “Message Authentication.” *IEEE Communications Magazine*, September 1988. JUNG04 Jung, J., et al. “Fast Portscan Detection Using Sequential Hypothesis Testing.” *Proceedings, IEEE Symposium on Security and Privacy*, 2004. KLEI90 Klein, D. “Foiling the Cracker: A Survey of, and Improvements to, Password Security.” *Proceedings, UNIX Security Workshop II*, August 1990. KNUD98 Knudsen, L., et al. “Analysis Method for Alleged RC4.” *Proceedings, ASIACRYPT ’98*, 1998. KOBL92 Koblas, D., and Koblas, M. “SOCKS.” *Proceedings, UNIX Security Symposium III*, September 1992. References 445 KOHL89 Kohl, J. “The Use of Encryption in Kerberos for Network Authentication.” *Proceedings, Crypto ’89*, 1989; published by Springer-Verlag. KOHL94 Kohl, J.; Neuman, B.; and Ts’o, T. “The Evolution of the Kerberos Authentication Service.”

In Brazier, F., and Johansen, D. eds., *Distributed Open Systems*. Los Alamitos, CA: IEEE Computer Society Press, 1994. Available at <http://web.mit.edu/kerberos/www/papers.html>. KUMA97 Kumar, I. *Cryptology*. Laguna Hills, CA: Aegean Park Press, 1997. KUMA11 Kumar, M. "The Hacker's Choice Releases SSL DOS Tool." *The Hacker News*, October 24, 2011. <http://thehackernews.com/2011/10/hackers-choice-releases-ssl-ddos-tool.html#>. LATT09 Lattin, B. "Upgrade to Suite B Security Algorithms." *Network World*, June 1, 2009. LEUT94 Leutwyler, K. "Superhack." *Scientific American*, July 1994. LINN06 Linn, J. "Identity Management." In Bidgoli, H., ed., *Handbook of Information Security*. New York: Wiley, 2006. LIPM00 Lipmaa, H.; Rogaway, P.; and Wagner, D. "CTR Mode Encryption." NIST First Modes of Operation Workshop, October 2000. <http://csrc.nist.gov/encryption/modes>. MA10 Ma, D., and Tsudik, G. "Security and Privacy in Emerging Wireless Networks." *IEEE Wireless Communications*, October 2010. MANA11 Manadhata, P., and Wing, J. "An Attack Surface Metric." *IEEE Transactions on Software Engineering*, Vol. 37, No. 3, 2011. MAND13 Mandiant "APT1: Exposing One of China's Cyber Espionage Units," 2013. <http://intelreport.mandiant.com>. MAUW05 Mauw, S., and Oostdijk, M. "Foundations of Attack Trees." *International Conference on Information Security and Cryptology*, 2005. MEYE13 Meyer, C.; Schwenk, J.; and Gortz, H. "Lessons Learned from Previous SSL/TLS Attacks A Brief Chronology of Attacks and Weaknesses." *Cryptology ePrint Archive*, 2013. <http://eprint.iacr.org/2013/>. MILL88 Miller, S.; Neuman, B.; Schiller, J.; and Saltzer, J. "Kerberos Authentication and Authorization System." Section E.2.1, *Project Athena Technical Plan*, M.I.T. Project Athena, Cambridge, MA, 27 October 1988. MIRK04 Mirkovic, J., and Relher, P. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms." *ACM SIGCOMM Computer Communications Review*, April 2004. MITC90 Mitchell, C.; Walker, M.; and Rush, D. "CCITT/ISO Standards for Secure Message Handling." *IEEE Journal on Selected Areas in Communications*, May 1989. MOOR01 Moore, A.; Ellison, R.; and Linger, R. "Attack Modeling for Information Security and Survivability." *Carnegie-Mellon University Technical Note CMU/SEI-2001-TN-001*, March 2001. MORR79 Morris, R., and Thompson, K. "Password Security: A Case History." *Communications of the ACM*, November 1979. NACH02 Nachenberg, C. "Behavior Blocking: The Next Step in Anti-Virus Protection." *White Paper*, SecurityFocus.com, March 2002. NCAE13 National Centers of Academic Excellence in Information Assurance/Cyber Defense. *NCAE IA/CD Knowledge Units*. June 2013. NEUM99 Neumann, P., and Porras, P. "Experience with EMERALD to Date." *Proceedings, 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, April 1999. NEWS05 Newsome, J.; Karp, B.; and Song, D. "Polygraph: Automatically Generating Signatures for Polymorphic Worms." *IEEE Symposium on Security and Privacy*, 2005. NIST95 National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. Special Publication 800-12. October 1995. OECH03 Oechslin, P. "Making a Faster Cryptanalytic Time-Memory Trade-Off." *Proceedings, Crypto 03*, 2003. 446 References ORMA03 Orman, H. "The Morris Worm: A Fifteen-Year Perspective." *IEEE Security and Privacy*, September/October 2003. PARZ06 Parziale, L., et al. *TCP/IP Tutorial and Technical Overview*, 2006. [ibm.com/redbooks](http://ibm.com/redbooks). PELT07 Peltier, J. "Identity Management." *SC Magazine*, February 2007. PERR03 Perrine, T. "The End of Crypt () Passwords . . . Please?" ;login:, December 2003. POIN02 Pointcheval, D. "How to Encrypt Properly with RSA." *CryptoBytes*, Winter/Spring 2002. <http://www.rsasecurity.com/rsalabs>. PORR92 Porras, P. *STAT: A State Transition Analysis Tool for Intrusion Detection*. Master's Thesis, University of California at Santa Barbara, July 1992. PROV99 Provos, N., and Mazieres, D. "A Future-Adaptable Password Scheme." *Proceedings of the 1999 USENIX Annual Technical Conference*, 1999. RADC04 Radcliff, D.

"What Are They Thinking?" Network World, March 1, 2004. RIVE78 Rivest, R.; Shamir, A.; and Adleman, L. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." Communications of the ACM, February 1978. ROBS95a Robshaw, M. Stream Ciphers. RSA Laboratories Technical Report TR-701, July 1995. ROBS95b Robshaw, M. Block Ciphers. RSA Laboratories Technical Report TR-601, August 1995. ROS06 Ros, S. "Boosting the SOA with XML Networking." The Internet Protocol Journal, December 2006. [cisco.com/ipj](http://cisco.com/ipj). SALT75 Saltzer, J., and Schroeder, M. "The Protection of Information in Computer Systems." Proceedings of the IEEE, September 1975. SCHN99 Schneier, B. "Attack Trees: Modeling Security Threats." Dr. Dobbs's Journal, December 1999. SEAG08 Seagate Technology. 128-Bit Versus 256-Bit AES Encryption. Seagate Technology Paper, 2008. SIDI05 Sidiroglou, S., and Keromytis, A. "Countering Network Worms Through Automatic Patch Generation." IEEE Security and Privacy, November-December 2005. SING99 Singh, S. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books, 1999. SNAP91 Snapp, S., et al. "A System for Distributed Intrusion Detection." Proceedings, COMPCON Spring '91, 1991. SPAF92a Spafford, E. "Observing Reusable Password Choices." Proceedings, UNIX Security Symposium III, September 1992. SPAF92b Spafford, E. "OPUS: Preventing Weak Password Choices." Computers and Security, No. 3, 1992. SPAF00 Spafford, E., and Zamboni, D. "Intrusion Detection Using Autonomous Agents." Computer Networks, October 2000. STAL15 Stallings, W., and Brown, L. Computer Security. Upper Saddle River, NJ: Pearson, 2015. STAL16 Stallings, W. Cryptography and Network Security: Principles and Practice, Seventh Edition. Upper Saddle River, NJ: Pearson, 2016. STAL16b STEI88 Steiner, J.; Neuman, C.; and Schiller, J. "Kerberos: An Authentication Service for Open Networked Systems." Proceedings of the Winter 1988 USENIX Conference, February 1988. STEP93 Stephenson, P. "Preventive Medicine." LAN Magazine, November 1993. STEV11 Stevens, D. "Malicious PDF Documents Explained," IEEE Security & Privacy, January/ February 2011. SYMA13 Symantec, "Internet Security Threat Report, Vol. 18." April 2013. TSUD92 Tsudik, G. "Message Authentication with One-Way Hash Functions." Proceedings, INFOCOM '92, May 1992. VACC89 Vaccaro, H., and Liepins, G. "Detection of Anomalous Computer Session Activity." Proceedings of the IEEE Symposium on Research in Security and Privacy, May 1989. References 447 VANO94 van Oorschot, P., and Wiener, M. "Parallel Collision Search with Application to Hash Functions and Discrete Logarithms." Proceedings, Second ACM Conference on Computer and Communications Security, 1994. VIGN02 Vigna, G.; Cassell, B.; and Fayram, D. "An Intrusion Detection System for Aglets." Proceedings of the International Conference on Mobile Agents, October 2002. WAGN00 Wagner, D., and Goldberg, I. "Proofs of Security for the UNIX Password Hashing Algorithm." Proceedings, ASIACRYPT '00, 2000. WANG05 Wang, X.; Yin, Y.; and Yu, H. "Finding Collisions in the Full SHA-1." Proceedings, Crypto '05, 2005; published by Springer-Verlag. WEAV03 Weaver, N., et al. "A Taxonomy of Computer Worms." The First ACM Workshop on Rapid Malcode (WORM), 2003. WOOD10 Wood, T., et al. "Disaster Recovery as a Cloud Service Economic Benefits & Deployment Challenges." Proceedings, USENIX HotCloud '10, 2010. XU10 Xu, L. Securing the Enterprise with Intel AES-NI. Intel White Paper, September 2010. ZOU05 Zou, C., et al. "The Monitoring and Early Detection of Internet Worms." IEEE/ACM Transactions on Networking, October 2005. 448 Page 20: Definition From An Introduction to Computer Security: The NIST Handbook by Barbara Guttman and Edward A. Roback, U.S. Department of Commerce, 1995. Page 20–21: Three Objectives in Terms of Requirements and the Definition From Standards for Security Categorization of Federal Information and Information Systems. Published by U.S.

Department of Commerce, © 2004. Page 21–22: From Standards for Security Categorization of Federal Information and Information Systems, U.S. Department of Commerce, 2004. Page 28: From Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications. Copyright © International Telecommunication Union. Used by permission of International Telecommunication Union. Page 29: Two specific authentication From Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications. Used by permission of International Telecommunication Union. Page 31: From Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications. Copyright © International Telecommunication Union. Used by permission of International Telecommunication Union. Page 32: From Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications. Copyright © International Telecommunication Union. Used by permission of International Telecommunication Union. Page 32: From 2013 National Centers of Academic Excellence in Information Assurance Designees Announced, National Security Agency, 2013. Page 51: Feistel, H. “Cryptography and Computer Privacy.” Scientific American, Vol 228, No 5 pp 15–23 May 1973. Page 64: From Cryptology: System Identification and KeyClustering by I. J. Kumar. Published by Aegean Park Press, © 1997. Page 72–73: Comments to NIST concerning AES Modes of Operations: CTR-Mode Encryption, National Institute of Standards and Technology (NIST), National Institute of Standards and Technology, 2000. Page 80: From Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer, 02e by D. W. Davies and W. L. Price. Published by Wiley, © 1989. Page 82: From “Message Authentication with One-Way Hash Functions” by Gene Tsudik from ACM SIGCOMM Computer Communication Review, Volume: 22, Issue: 05, pp: 29–38. Published by ACM, Inc., © 1992. Page 91: Lists From HMAC: Keyed-Hashing for Message Authentication by H. Krawczyk, M. Bellare and R. Canetti. Published by Internet Engineering Task Force, © 1997. Page 134: X.509 Hierarchy: A Hypothetical Example from Series X: Data Networks, Open System Communications And Security X.509 -International Standard Iso/lec 9594-8. Used by permission of International Telecommunication Union. Page 143: From The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology by Peter Mell and Timothy Grance, U.S. Department of Commerce, 2011. Page 165: From The EAP-TLS Authentication Protocol by D. Simon, B. Aboba, R. Hurst. Published by Internet Engineering Task Force, © 2008. Page 174: From NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology by Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf. Published by U.S. Department of Commerce, © 2011. Page 179: Table 01 Security and Privacy Issues and Recommendations from Guidelines on Security and Privacy in Public Cloud Computing by Wayne Jansen and Timothy Grance, U.S. Department of Commerce, 2011. Page 180–181: From “Executing SQL Over Encrypted Data in the Database-Service-Provider Model” by Hakan Hacigümüs, Bala Iyer, Chen Li and Sharad Mehrotra from A Proceeding SIGMOD ‘02 Proceedings of the 2002 ACM SIGMOD International Conference on Management of Data, pp: 216–227. Published by ACM Inc., © 2002. Page 182: From SecaaS: Defined Categories of Service 2011. Published by Cloud Security Alliance, © 2011. Page 182: Following SecaaS Categories of Service from SecaaS: Defined Categories of Service 2011. Published by Cloud Security Alliance, © 2011. Page 243: From Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i: Recommendations of the National Institute of Standards and Technology by Sheila Frankel, Bernard Eydt, Les Owens and Karen

Scarfone, U.S. Department of Commerce, 2007. Page 244: From Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i: Recommendations of the National Institute of Standards and Technology by Sheila Frankel, Bernard Eydt, Les Owens and Karen Scarfone. U.S. Department of Commerce, 2007. Page 245: From Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i: Recommendations of the National Institute of Standards and Technology by Sheila Frankel, Bernard Eydt, Les Owens and Karen Scarfone, U.S. Department of Commerce, 2007. Page 259–260: From TCP/IP Tutorial and Technical Overview by Lydia Parziale, David T. Britt, Chuck Davis, Jason Forrester, Wei Liu, Carolyn Matthews and Nicolas Rosselot. Published by IBM Corporation, © 2006. Page 262–263: Excerpt from Multipurpose Internet Mail Extensions (MIME) Part Two by Ned Freed and Nathaniel S Borenstein. Published by Internet Engineering Task Force, © 1996. Page 264–265: From Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples by Ned Freed and Nathaniel S Borenstein. Published by Internet Engineering Task Force, © 1996. Page 266: From DRAFT NIST Special Publication 800-177: Trustworthy Email by SRamaswamy Chandramouli, Simson Garfinkel, Stephen Nightingale and Scott Rose, U.S. Department of Commerce, 2015. Page 267: From DRAFT NIST Special Publication 800-177: Trustworthy Email by SRamaswamy Chandramouli, Simson Garfinkel, Stephen Nightingale and Scott Rose, U.S. Department of Commerce, 2015. Page 273: From Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification by B. Ramsdell and S. Turner. Published by Internet Engineering Task Force, © 2010. Page 283: From Resource Records for the DNS Security Extensions by R. Arends, R. Austein, M. Larson, D. Massey and S. Rose. Published by Internet Engineering Task Force, © 2005. CreDItS CREDITS 449 Page 306: From IPv6: The New Internet Protocol by Christian Huitema. Published by Pearson, © 1998. Page 306: The Document From IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap by S. Frankel and S. Krishnan. Published by Internet Engineering Task Force, © 2011. Page 307: From Security Architecture for the Internet Protocol by S. Kent and K. Seo. Published by Network Working Group, © 2005. Page 326: From IPv6: The New Internet Protocol by Christian Huitema. Published by Pearson, © 1998. Page 334: From Cryptographic Suites for Ipsec by P. Hoffman. Published by Network Working Group, © 2005. Page 338: NIST Special Publication 800-83 Revision 1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops, U.S. Department of Commerce. Page 348: Most of Which are Still Seen in Active Use from Internet Security Threat Report 2013, Volume 18. Published by Symantec Corporation, © 2013. Page 356: From Know your Enemy: Tracking Botnets by Paul Bacher, Thorsten Holz , Markus Kötter and Georg Wicherski. Published by The HoneyNet Project, © 2005. Page 362: LAN Magazine. Page 365–366: Security and Privacy in Communications Networks and the Workshops, IEEE. Page 371: IEEE Communications Magazine. Page 377: From Computer Security Incident Handling Guide by Karen Kent and Brian Kim, National Institute of Standards and Technology, 2004. Page 380: De Alvare, A. “How Crackers Crack Passwords or What Passwords to Avoid.” Proceedings, UNIX Security Workshop II, August 1980; US Department of Commerce. Page 382: Technical Report : STAT -- A State Transition Analysis Tool For Intrusion Detection, ACM. Page 385: From “An Intrusion-Detection Model” by Dorothy E. Denning in IEEE Transactions on Software Engineering, Volume: 13, Issue: 02, pp: 222–232. Published by IEEE, © 1987. Page 393: From Intrusion Detection Message Exchange Requirements by M. Wood and M. Erlinger. Published by Network Working Group, © 2007. Page 394: From The Intrusion Detection Message Exchange Format (IDMEF) by H. Debar, D. Curry and B. Feinstein. Published by Network Working Group, © 2007. Page



**394: From The Intrusion Detection Exchange Protocol (IDXP) by B. Feinstein and G. Matthews. Published by Network Working Group, © 2007. Page 397: From Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute of Standards and Technology by Karen Scarfone and Paul Hoffman, U.S. Department of Commerce, 2009. Page 402–403: Adapted from on Spafford, Eugene. “Observing Reusable Password Choices.” Proceedings, UNIX Security Symposium III. September 1992. Accessed at <http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1969&context=cstech>. Page 417: Lists of Following Weaknesses of Packet Filter Firewalls from Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute of Standards and Technology by Karen Scarfone and Paul Hoffman. Published by U.S. Department of Commerce, © 2009. Page 419: From SOCKS Protocol Version 5 by M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas and L. Jones. Published by Network Working Group, © 1996. 450 InDeX A Access, 30, 41 control, 29, 401–402 threats, 41 Accessibility, 223 Access point (AP), IEEE 802.11, 233 Access policy, 412–413 Access requestor (AR), 161 supplicants, 161 Accidental association, 224 Account or service hijacking, 178 Active attacks, security, 25–27 Add Round Key AES, 57 algorithm, 56–59 Data Encryption Algorithm (DEA), 52 Data Encryption Standard (DES), 52–55 decryption, defined, 47, 97 Diffie–Hellman key exchange, 104–107 Digital Signature Algorithm (DSA), 108 elliptic curve cryptography (ECC), 109 encryption, 47, 96 mix columns, 59 public-key cryptography, 96–100 RSA public-key encryption, 101–103 state array, 56 structure, 56 subkey generation, 52 substitution bytes, 56 symmetric block encryption, 52–59 triple Data Encryption Standard (3DES), 54–55 Ad hoc networks, 224 Advanced Encryption Standard (AES), 52, 55–59 Advanced persistent threats (APTs), 341–342 AES. See Advanced Encryption Standard (AES) Algorithms, 46, 52–59, 62–63, 100–109, 273–274, 316 cryptographic, 273–274 ESP, 316 HMAC, 91–93 S/MIME, 273–274 Anti-replay service, ESP, 316–317 Application-level gateway, 419 Application proxy, 419 Architecture, 24–25 open systems interconnection (OSI), 24–25 Attack(s), 25–27. See also Cryptanalysis; Security attacks; Threats active, 27 chosen plaintext, 49 ciphertext only, 48 denial-of-service (DoS), 30 insider, 379 intruder, 377 kits, 340 known plaintext, 49 man-in-the-middle, 107–108 messages, types of for, 49 passive, 25 password, 135–136 security, 25–27 source routing, 417 sources, 340–341 tiny fragment, 417–418 Attacking IRC chat networks, 357 Attack surfaces, 36–37 Attack trees, 37–39 Audit records detection-specific, 383 field action, 383 exception-condition, 383 object, 383 resource-usage, 383 subject, 383 time-stamp, 383–384 native, 383 Authentication, 29, 79–84, 164, 189, 192–193, 215. See also Message authentication; Message authentication codes (MAC) applications, 119–155 client/server exchange, 137 data origin, 29, 32 dialogues, 125–132 forwarding, 135 IEEE 802.11i phase, 237–240 IKE key determination, 327–328 Internet Protocol (IP), 323 interrealm, 135 Kerberos, 124–137 key exchange client and server, SSL, 200–201 message, 78–112 methods, 164 peer entity, 29 pretty good privacy (PGP), 279–280 public-key infrastructure (PKI), 146–149 remote user, 120–122 server (AS), 125, 166 service exchange, 136 X.509 service, 139 Authority key identifier, 145 B Backdoor (trapdoor), 359 Barcode readers, 224 Barrier security, 230 Base-rate fallacy, 388–389 Basic service set (BSS), IEEE 802.11, 233–234 Bastion host, 421 Bcrypt, 400. See also Hash functions Behavior-blocking software, 363 Block ciphers, 50, 52, 63–65 cipher block chaining (CBC) mode, 68–70 cipher feedback (CFB) mode, 70–71 InDeX 451 Circuit-level gateway, 419–420 Circuit-level proxy, 419 Clandestine user, intruders, 377 Clear signing, S/MIME, 277 Client/server authentication exchange, 137 Client-side vulnerabilities, 352–353 drive-by-download, 352–353 Cloud auditor, 175 Cloud-based applications, 226 Cloud broker, 175 service aggregation, 176 service arbitrage, 176 service intermediation, 176 Cloud carrier, 175**

Cloud computing abuse and nefarious use of, 177 control functions and classes, 185 deployment models community cloud, 173 hybrid cloud, 173–175 private cloud, 173 public cloud, 173 elements, 171–174 measured service, 172 on-demand self-service, 172 rapid elasticity, 172 reference architecture, 174–176 resource pooling, 172–173 service models, 173 Infrastructure as a service (IaaS), 173 Platform as a service (PaaS), 173 Software as a service (SaaS), 173 Cloud consumer, 175 Cloud provider, 175 Cloud security risks and countermeasures abuse/nefarious use of cloud computing, 177 account or service hijacking, 178 data loss or leakage, 178 insecure interfaces and APIs, 177 malicious insiders, 177 shared technology issues, 177–178 unknown risk profile, 178 as a service business continuity and disaster recovery, 184 data loss prevention (DLP), 183–184 elements, 184 e-mail security, 184 encryption, 184 identity and access management (IAM), 183 intrusion management, 184 network security, 184–185 security as a service (SecaaS), 182 security assessments, 184 security information and event management (SIEM), 184 web security, 184 Codebook, 68 defined, 68 electronic (ECB), 68 Code, message authentication (MAC), 211–212 defined, 48 design of, 50 electronic codebook (ECB), 68 modes of operation, 68 plaintext processing, cryptography, 48 Bloom filter, 404–406 Bogus reconfiguration commands. See Network injection Boot sector infector, 346 Bots, uses of, 356–357 attacking IRC chat networks, 357 DDoS attacks, 356 installing advertisement add-ons and BHOs, 357 keylogging, 356 manipulating online polls/games, 357 sniffing traffic, 356 spamming, 356 spreading new malware, 356 Bring-your-own-device (BYOD) policy, 228 Broad network access, 171–172 Browser helper objects (BHOs), 357 Business continuity and disaster recovery, 184 C Canonical form, MIME and S/MIME, 264 Certificates, 140–144, 148, 200–201, 278 certification authority (CA), 140, 147, 276, 278 client types, 208 enhanced security services, 278–279 extensions, 141 forward, 143 issuer, 140, 141, 146 key information, 141 path constraints, 146 period of validity, 141 policy information, 145 policy mappings, 146 public-key, 138–139 reverse, 143 revocation list (CRL), 144, 278 revocation of, 144 serial number, 141 signature, 141 signature algorithm identifier, 141 S/MIME, 278 subject, 141 unique identifiers, 141 user's, obtaining, 142–144, 278 version, 140–141 X.509, 139–146 Certificates-only message, S/MIME, 278 Certificate usage field, 285 Certification authority (CA), 138, 147 key distribution, 138 public-key infrastructure (PKI), 146–149 X.509 certificates, 139–146 Change Cipher Spec Protocol, 191, 194–195, 201 Channels, 215–216, 223 Cipher block chaining (CBC) mode, 68–70 Cipher feedback (CFB) mode, 70–71 Cipher suites, TLS, 207 Ciphertext, 48, 97 452 InDeX D Data confidentiality, 28, 29 integrity, 30 origin authentication, 29 Data Encryption Standard (DES), 52–55 algorithm, description of, 53 strength of, 53–54 triple (3DES), 54–55 Data loss prevention (DLP), 178, 183–184 Data protection, cloud computing attributes, 181 encryption scheme, 181 multi-instance model, 180 multi-tenant model, 180 NIST guidelines on security and privacy, 178–180 primary key, 181 relation, 181 tuples, 181 Decryption algorithm, 47, 97 Demilitarized zone (DMZ) networks, 423–425 Denial-of-service (DoS) attack, 30 constructing attack network, 370–371 hit list, 371 local subnet, 371 random, 371 topological, 371 countermeasures, 371–372 detection and filtering, 371 prevention and preemption, 371 source traceback and identification, 371 defined, 225 direct, 369 flooding-based, 370 internal resource, 368 reflector, 369 De-perimeterization, 227 Detection-specific audit records, 383 Device security, 228–230 Diffie–Hellman key exchange, 104–105, 200, 202, 224 algorithm, 105–106 anonymous, 200 ephemeral, 200 fixed, 199 introduction to, 104–105 man-in-the-middle attack, 107 protocols, 107–108 Digital Signature Algorithm (DSA), 108, 109 Digital signatures, 108–112 generation and verification, 110–111 RSA, algorithm, 111–112 Digital Signature Standard (DSS), 108 Discovery phase, IEEE 802.11i, 240–242 Distributed firewall,

426–427 configuration, 427–428 Distributed intrusion detection central manager module, 390–391 host agent module, 390 LAN monitor agent module, 390 Distribution system (DS), IEEE 802.11, 233 Communications channel (CC), 38 Community cloud, 173 Complete mediation, 33 Components, IDES, 394–395 Compression S/MIME, 272–273 SSL, 192 Computer-generated passwords, 403 Computer security, defined, 20 Confidentiality, 20–22, 45–73, 241, 271, 316, 320. See also Encryption data, 20, 28, 29 Encryption data, 249 Internet Protocol (IP), 322 pretty good privacy (PGP), 279–280 traffic flow (TFC), 316 Connection Protocol, SSH, 209, 215–219 Connection, TLS, 192 Controls access, 413–414 Cookie exchange, 327 Countermeasures distributed intelligence gathering approaches, 366–367 host-based behavior-blocking software, 363 host-based scanners, 362–364 first-generation scanner, 362 fourth-generation scanner, 363 second-generation scanner, 362–363 third-generation scanner, 363 malware countermeasure approaches detection, 361 generality, 361 global and local coverage, 361 identification, 361 minimal denial-of-service costs, 361 removal, 361 resiliency, 361 timeliness, 361 transparency, 361 perimeter scanning approaches, 364–365 egress monitors, 365 ingress monitors, 364–365 rootkit countermeasures, 364 spyware detection and removal, 364 worm countermeasures filter-based worm containment, 365 payload-classification-based, 365 rate halting, 366 rate limiting, 366 signature-based worm scan filtering, 365 TRW scan detection, 366 Credential service provider (CSP), 121–122 CRL issuer, PKI, 148 Cross-certification, PKI, 148 Cryptanalysis, 48–50 Cryptographic computations, 202–203 Cryptography, 48, 99–100. See also Public-key cryptography algorithms, 105–106 classification of systems, 48 cryptosystems, applications for, 99–100 encryption structure, 97–99 public-key, 96–109 requirements for, 100 InDeX 453 cryptanalysis, 48–50 cryptography, 48 Data Encryption Standard (DES), 52–55 decryption algorithms, 97 digital signatures, 108 double, 135 end-to-end, 123 Feistel cipher structure, 50–52 introduction to, 46 key distribution, 123–124, 137–139 message authentication and, 78–112 National Institute of Standards and Technology (NIST), 42, 52, 87, 108 plaintext, 48–50, 97 propagating cipher block chaining (PCBC), 135 public-key, 96–109 RSA algorithm, 101–103 stream cipher, 48, 63–65, 70 symmetric, 46–52 symmetric block algorithms, 52–59 system dependence, 134 triple Data Encryption Standard (3DES), 54–55 End entity, PKI, 147 End-to-end encryption, 123 EnvelopedData, S/MIME, 275–276 Exchange format, Intrusion detection, 393–395 Exchanges, 136–137. See also Key exchange authentication service, 136 client/server authentication, 137 Kerberos, 134–136 ticket-granting service, 136–137 Extended service set (ESS), IEEE 802.11, 234 Extensible Authentication Protocol (EAP), 164 authentication methods, 164–165 EAP-GPSK (EAP Generalized Pre-Shared Key), 165 EAP-IKEv2, 165 EAP-TLS (EAP Transport Layer Security), 165 EAP-TTLS (EAP Tunneled TLS), 165 exchanges, 165–168 authentication server, 166 EAP authenticator, 166 EAP passthrough mode, 166 EAP peer, 166 RADIUS, 166 layered context, 164 messages code, 166 data, 167 flow in pass-through mode, 167 identifier, 166 length, 166 Extensible Markup Language (XML), 394 External business requirements, 227 F Fail-safe default, 33–34 Feistel cipher structure, 50–52 File infector, 346 File sharing, 348 Filter-based worm containment, 365 DNS-based Authentication of Named Entities (DANE), 266–267, 284–286 for SMTP, 286 TLSA record, 284–285 DNS Security Extensions (DNSSEC), 266, 280–284 domain name system, 280–282 protocol, 282–284 Domain-based Message Authentication, Reporting, and Conformance (DMARC), 267–268 functional flow, 298 on receiver side, 296–298 reports, 299 on sender side, 296 DomainKeys Identified Mail (DKIM), 289–295 E-mail threats, 290–291 functional flow, 292–295 strategy, 291–292 Double bastion inline, 424, 428 Double bastion T, 428 Double encryption, 135 Dynamic Host Configuration Protocol (DHCP), 164 E EAP-GPSK (EAP

Generalized Pre-Shared Key), 165 EAP-IKEv2, 165 EAP-TLS (EAP Transport Layer Security), 165 EAP-TTLS (EAP Tunneled TLS), 165 Eavesdropping. See Man-in-the middle attacks Economy of mechanism, 33 Electronic codebook (ECB), 68 Electronic data interchange (EDI), 145 Electronic mail security, 253–299 DomainKeys Identified Mail (DKIM), 289–295 instant messenger facility, 348 pretty good privacy (PGP), 279–280 Secure/Multipurpose Internet Mail Extension (S/ MIME), 268–279 Electronic monitoring, 397 Electronic user authentication means of, 122 NIST model for, 121–122 Elliptic curve cryptography (ECC), 109 Elliptic curve digital signature algorithm (ECDSA), 109 E-mail formats, 258–266 E-mail security, 184 E-mail threats, 266–268 Encapsulating security payload (ESP), 314–321 algorithms, 316 anti-replay service, 316–317 format, 314–316 padding, 316 transport mode, 317–320 tunnel mode, 320–321 Encapsulation, 35 Encryption, 45–73, 81–82, 99–100, 104, 109, 137, 184, 225. See also Block ciphers; Public-key cryptography; Stream ciphers Advanced Encryption Standard (AES), 52, 55–59 algorithms, 46, 52–59, 62–63, 100–109 block ciphers, 50, 52, 63–65 ciphertext, 97 454 InDeX I Identifier (ID), 395, 396, 398 Identity and access management (IAM), 183 Identity theft (MAC spoofing), 224 IEEE 802.11i LAN, 236–250 authentication phase, 239, 242–243 characteristics of, 236–237 connection termination, 240 discovery phase, 239–241 key management phase, 241, 244–246 phases of operation, 237–240 protected data transfer phase, 239, 248–249 pseudorandom function (PRF), 249–250 Robust Security Network (RSN), 237 IEEE 802.11 LAN, 230–236 association-related services, 235 message distribution, 235 network components, 233–234 protocol architecture, 231–233 IEEE 802.1X port-based network access control, 163, 168–170 EAP-Key, 170 EAP-Logoff, 170 EAPOL-EAP, 170 EAPOL-Start, 170 packet body, 170 length, 170 packet type, 170 protocol version, 170 terminology related to IEEE 802.1X, 170 802.1X access control, 170 Independent basic service set (IBSS), IEEE 802.11, 233 Information access threats, 41 security, 18 Infrastructure as a service (IaaS), 173 Initialization, 192 PKI, 148 Insecure interfaces and APIs, 177 International Telecommunication Union (ITU), 24 Internet Architecture Board (IAB), 303 Internet banking server (IBS), 38 Internet Engineering Task Force (IETF) standards from, 42 Internet key exchange (IKE), 325–333 cookies, 327 header and payload formats, 329–333 IKEv5 message exchange, 328–329 key determination protocol, 326–329 Internet mail architecture, 254–258 e-mail components, 254–256 e-mail Protocols, 256–258 Internet Protocol (IP), 134, 303–309. See also Internet Protocol security (IPsec) authentication plus confidentiality, 322–323 combining security associations (SA), 322–325 cryptographic suites, 333–335 dependence, 134 encapsulating security payload (ESP), 314–321 Internet key exchange (IKE), 325–333 security (IPsec), 309–314 Firewall, 164, 410–428 basing, 420–423 bastion host, 421 host-based, 421–422 personal, 422–423 characteristics and access policy, 412–413 application protocol, 413 IP address and protocol values, 412 network activity, 413 user identity, 413 location and configurations, 423–428 distributed, 426–427 DMZ networks, 423–425 summary of, 427–428 virtual private networks, 425–426 need for, 411–412 types of, 414–420 application-level gateway, 419 circuit-level gateway, 419–420 packet filtering, 414–418 stateful inspection, 418–419 Forward certificate, 143 Fourth-generation scanner, 363 Fragmentation, SSL, 192 G GPS capability on mobile devices, 228 Group master key (PMK), IEEE 802.11i, 246–247 H Hackers, 377–378 Handheld PDAs, 224 Handshake Protocol, 165, 197–199 Hashed passwords, 397–399 Hash functions, 82–91, 399–400 HMAC, 91–93 one-way, 82–84 requirements, 84–85 secure, 84–85 Secure Hash Algorithm (SHA), 87 SHA-1 secure functions, 87–91 simple, 85–86 strong collision resistance, 84 weak collision resistance, 84 Heartbeat Protocol, 204–205 HMAC, 91–93 algorithm, 92–93 design objectives, 91–92 Honey pots, 391–393 Host audit record (HAR), 390–391 Host-based firewalls, 421–422 Host-

based scanners, 362–363 Host keys, SSH, 209–214 Host-resident firewall, 427 HTTPS, 188, 207–208 Human attack surface, 36–37 Hybrid cloud, 173 InDeX 455 K Kerberos, 124–137 authentication dialogues, 125–133 forwarding, 135 server (AS), 125 service exchange, 136 client/server authentication exchange, 137 differences between versions 4 and 5, 134–136 double encryption, 135 encryption system dependence, 134 environmental shortcomings, 134–135 Internet protocol dependence, 134 interrealm authentication, 135 introduction to, 124 message byte ordering, 134 nonce, 136 options, 136 password attacks, 135–136 principal, 134 propagating cipher block chaining (PCBC) encryption, 135 realms, 133–134, 136 session keys, 135 technical deficiencies of, 135 ticket-granting server (TGS), 126–127 ticket-granting service exchange, 136–137 ticket lifetime, 134–135 times, 136 version 4, 125–133 version 5, 134–137 Key distribution, 126, 140–142, 242, 247–248. See also Exchanges; Private keys; Public keys center (KDC), 123 certificate authority (CA), 138 hierarchy, 246 IEEE 802.11i management phase, 241, 246–249 permanent key, 123 pretty good privacy (PGP), 279–280 private key, 270 public-key certificates, 138 public-key distribution of secret keys, 138–139 session key, 123 wireless network security, 244–248 Keyed hash function. See Message authentication codes (MAC) Key exchange, 104–108, 199–200, 212, 325–333 certificate messages for, 200–201 client authentication and, 201 Diffie–Hellman, 104–108, 199 Internet, 325–333 Internet (IKE) key determination protocol, 326–329 protocols, 107 RSA, 199 server authentication and, 200–201 SSH Transport Layer Protocol, 210–211 Key generation, 203, 213–214, 278 AP, 239 S/MIME, 278 Keylogger, 358 Keylogging, 356 security association database (SAD), 309–311 security policy database (SPD), 309, 311–312 traffic processing, 312–314 Internet Protocol security (IPsec), 303–314 documents, 306–307 packets, 312–314 policy, 309–312 routing, 306 transport mode, 308 tunnel mode, 308–309 Internet security, 253–299 defined, 19 electronic mail, 253–299 Internet protocol (IP), 164, 303–309 Transport Layer Security (TLS), 165, 190–207 transport-level, 187–219 Internet Security Association and Key Management Protocol (ISAKMP), 325 Internet service provider (ISP), 411 Internet standards Internet Architecture Board (IAB), 42 Internet Engineering Task Force (IETF), 42 RFCs, 42 Intruder behavior patterns criminals, 378 hackers, 377–378 insider attacks, 379 Intruders, 375–406 behavior patterns, 377–379 intrusion detection audit records, 383–384 base-rate fallacy, 388–389 distributed, 389–393 exchange format, 393–396 rule-based, 386–388 statistical anomaly detection, 384–386 intrusion techniques, 379–381 password management bloom filter, 404–406 hashed passwords, use of, 397–400 selection strategies, 403–404 user choices, 400–403 vulnerability of, 396–397 Intrusion Detection Exchange Protocol (IDXP), 394 Intrusion Detection Message Exchange Format (IDMEF), 393 Intrusion Detection System (IDES), 386 audit records, 383–384 base-rate fallacy, 388–389 distributed, 389–393 exchange format, 393–396 functional components, 394–395 rule-based, 386–388 statistical anomaly detection, 384–386 Intrusion management, 184 Intrusion techniques access control, 379–381 one-way function, 379 IP address spoofing, 417. See also Packet filtering firewall IPsec protocols, 425 Isolation, 35. See also Security design principles ITU-T Recommendation X.800, 24, 25, 27, 29–32 456 InDeX approaches to, 79–84 code (MAC), 81–82, 93–95 digital signatures, 109–112 encryption, and, 80–81 hash functions, 82–91 introduction to, 79 key distribution, 137–139 one-way hash functions, 82–84 public-key cryptography, 96–109 secure hash functions, 84–91 technique, 95–96 TLS, 190, 192–194 Message authentication codes (MAC), 114, 193, 211 Message authentication key distribution, 137–139 Message Handling Service (MHS), 254 Messages, 26, 27, 30, 45–73, 79–84, 136, 277–278, 331–332. See also Encryption; Public-key cryptography attacks on, types of, 49 authentication, 78–112 byte ordering, 134 confidentiality, 45–73 modification of, 30 pretty good privacy (PGP),

279–280 release of contents, 25 Secure/Multipurpose Internet Mail Extension (S/MIME), 268–279 SSH exchange, 214–215 Message User Agents (MUA), 254, 255 Metamorphic virus, 346 Misfeasor, intruders, 377 Mix columns, AES, 57 Mobile code, 352 Mobile device security, 226–230 cloud-based applications, 226 de-perimeterization, 227 elements, 229 external business requirements, 227 growing use of new devices, 226 strategy barrier security, 230 device security, 228–229 traffic security, 230 VPNs, 230 threats applications by unknown parties, 228 interaction with systems, 228 location services, 228 physical security controls, 227 untrusted mobile devices, 227 untrusted networks, 228 Mobility, 223 Model for network security, 39–42 Modification of messages, 27, 30 Modularity, 35 Morris worm, 350–351 Multipartite virus, 346 Multipurpose Internet Mail Extensions (MIME), 259–266 canonical form, 264 content types, 261–263 transfer encodings, 263–266 Mutation engine, 346 Key management. See Key distribution Key pair recovery, PKI, 148 Key pair update, PKI, 148 Keystream, defined, 64 L Layering, 35. See also Security design principles Least astonishment, 36 Least common mechanism, 34 Least privilege, 34 Limitations, firewall, 413 Link encryption, 123 Local area networks (LANs), 411, 425 Logical link control (LLC) layer, IEEE 816, 233 Logic bomb, 356 M MAC protocol data unit (MPDU), IEEE 816, 232–233, 235, 241–242 Macro viruses, 346–347 MAC service data unit (MSDU), IEEE 816, 232–234 Mail (DKIM), 289–295 e-mail threats, 290–291 functional flow, 292–295 Internet mail architecture, 254–258 strategy, 291–292 Mail Submission Agent (MSA), 255–256 Malicious association, 224 Malicious insiders, 177 Malicious software or malware attack kits, 340 attack sources, 340–341 classification of, 339–340 terminology, 339 types, 338–341 Malware countermeasure approaches detection, 361–362 generality, 361 global and local coverage, 361 identification, 361 minimal denial-of-service costs, 361 removal, 361 resiliency, 361 timeliness, 361 transparency, 361 Man-in-the-middle attack, 107–108, 199, 224 Manipulating online polls/games, 357 Markov process, 386. See also Statistical anomaly detection Masquerade, 27 Masquerader, intruders, 376 Master secret creation, 202 Master session key (MSK), IEEE 802.11i, 246 Measured service, 172 Media access control (MAC) layer, IEEE 816, 232–233 Media gateway, 162 Memory sticks, 227 Message authentication, 78–112 InDeX 457 P Packet exchange, SSH, 210–213 Packet filtering firewall, 414–418 Packets, IPsec, 312–314 Padding, 194, 315 Pairwise master key (PMK), IEEE 802.11i, 246–247 Pairwise transient key (PTK), IEEE 802.11i, 246–247 Passive attacks, security, 25–27 Password attacks, Kerberos, 135–136 Password cracking approaches, 400 Password management, Intruders bloom filter, 404–406 hashed passwords, use of, 397–400 selection strategies, 403–404 user choices, 400–403 vulnerability of, 396–397 Payload(s), 338 attack agent remote control facility, 357 uses of bots (see Bots, uses of) Zombie, 356 classification-based worm containment, 365 information theft credential theft, 358, 359 identity theft, 359 keylogger, 358 phishing and identity theft, 358–359 reconnaissance and espionage, 359 spyware, 358 stealthing backdoor (trapdoor), 359 rootkit, 359–360 system corruption, 355–356 logic bomb, 356 ransomware, 355 real-world damage, 355–356 Stuxnet worm, 356 Peer entity authentication, 29 Peer-to-peer networks, 224 Permanent key, defined, 123 Personal firewall, 422–423 Personal network Bluetooth devices, 224 Phishing and identity theft phishing attack, 358 spear-phishing attack, 358 Physical layer, IEEE 816, 231 Physical security controls, lack of, 227–228 Plaintext, 48–50, 97 chosen, attack, 49 defined, 48 known, attack, 48–49 public-key encryption, 96 Platform as a service (PaaS), 173 Policy server, 161 Polymorphic virus, 346 Port forwarding, SSH, 217–219 Pre-shared key (PSK), IEEE 802.11i, 246 Pretty good privacy (PGP), 279–280 Private cloud, 173 N National Institute of Standards and Technology (NIST), 42, 52, 87, 108 Native audit records, 383 Network access control (NAC) access requestor (AR), 161 supplicants,

161 context, 162 enforcement methods DHCP management, 164 firewall, 164 IEEE 802.1X, 163 VLANs, 163 NAS media gateway, 162 policy server, 161 RAS, 162 policy server, 161 Network access server (NAS), 162 Network activity, 413 Network attack surface, 36 Network injection, 225 Network security, 17–42, 119–155, 184–185, 222–250 applications, 138 authentication, 119–155 computer security, 18 defined, 18 HTTPS, 188, 207–208 information security, 18 International Telecommunication Union (ITU), 24 Internet Engineering Task Force (IETF), 42 internet security, 19 Internet standards, 42 introduction to, 17–42 mechanisms, 21–24, 32 model for, 39–42 open systems interconnection (OSI) architecture, 24–25 Secure Shell (SSH), 208–219 Secure Sockets Layer (SSL), 190–191 services, 25, 29–32 threats, 43, 177 transport-level, 187–219 violations of, 3 wireless, 222–250 X.800 standard recommendations, 24, 27–28, 31–32 Nonce, 95, 328, 332 Kerberos, 136 Nonrepudiation, 28, 30 Nontraditional networks, 224 O Oakley Key Determination Protocol, 325 On-demand self-service, 172 One-way function, 379. See also Intrusion techniques authentication, 82–84 hash functions, 82–84 Open design, 34 Open systems interconnection (OSI), 24–25 Options, Kerberos, 136 458 InDeX certification authority (CA), 147 CRL issuer, 148 end entity, 147 key pairs, 148 model, 146–149 PKIX management functions, 148 PKIX management protocols, 149 registration authority (RA), 147–148 repository, 148 Public keys, 97, 99, 140, 145 authority key identifier, 145 certificates, 138–139, 145 cryptography, 97, 99 defined, 99 distribution, 137–138 revoking, 146 secret keys, distribution of using, 138–139 subject key identifier, 145 usage, X.509 authentication service, 147 Q Quick Response (QR) code, 228 Quoted-printable transfer encoding, 264 R Ransomware, 355 Rapid elasticity, 172 Rate halting, 366 Rate limiting, 366 RC4 algorithm, 65–67 generation, 66 initialization of S, 65–66 logic, 66 strength of, 66–67 Reactive password checking strategy, 403 Realm, 124–137 concept of, 134 Kerberos version 4, 125–134 Kerberos version 5, 134–137 Real-world damage, 355–356 Reconnaissance and espionage, 359 credential theft, 359 identity theft, 359 Record Protocol, 191–194 Registration authority (RA), PKI, 147–148 Release of message contents, 25 Relying party (RP), 122 Remote access server (RAS), 162 Remote Authentication Dial-In User Service (RADIUS), 166 Remote execution capability, 368 Remote file access or transfer capability, 348 Remote login capability, 348 Replay, 27 Replay attacks, 126 Repository, PKI, 138 Request for Comment (RFC) standards, 25, 259, 290–291 RFC 4686, e-mail threats, 290–291 RFC 5322, S/MIME, 268–269 security recommendations, 24 Private keys, 145–146, 270–271, 279 pretty good privacy (PGP), 279–280 public-key cryptography and, 99–100 usage, X.509 authentication service, 145 Proactive password checker, 403–404 Propagating cipher block chaining (PCBC) encryption, 135 Propagation infected content macro viruses, 346–347 nature of viruses, 342–345 scripting viruses, 346–347 viruses classification, 345–346 mobile code, 352 Morris worm, 350–351 remote execution capability, 348 remote file access or transfer capability, 348 remote login capability, 348 social engineering spam (unsolicited bulk) e-mail, 353–354 Trojan horses, 354–355 state of worm technology, 351–352 target discovery, 348–349 vulnerability exploit client-side vulnerabilities, 352–353 drive-by-downloads, 352 electronic mail or instant messenger facility, 348 file sharing, 348 worm propagation model, 349–350 Protected data transfer phase, IEEE 802.11i, 239, 248–249 Protocol Diffie–Hellman, 104–105 key exchange, 104–105 PKIX management, 148–149 Pseudorandom function (PRF), 62, 203–204, 249–250 IEEE 802.11i, 249–250 IKEv2, 334–335 TLS, 203–204 Psychological acceptability, 34 Public cloud, 173 Public-key cryptography, 96–109 algorithms, 96–109 applications for, 99–100 ciphertext, 97 cryptography, 96–109 decryption algorithm, 97 Diffie–Hellman key exchange, 104–107 Digital Signature Standard (DSS), 108 elliptic curve (ECC), 109 encryption algorithm, 105–107 encryption structure,

97–99 plaintext, 97 private keys, 97, 99 public keys, 97, 99 requirements for, 100 RSA public-key encryption, 101–104 secret keys, 99 Public-key encryption, 96–109 algorithm, 46 digital signatures, 108 structure, 96–109 Public-key infrastructure (PKI), 146–149 InDeX 459 Security as a service (SecaaS), 182 Security assessments, 184 Security association database (SAD), 310–311 Security association (SA), IP, 309–310, 322–325 Security attacks, 25–27 active, 27 defined, 25 denial of service, 27 masquerade, 27 modification of messages, 27, 30 passive, 25–27 release of message contents, 25 replay, 27 traffic analysis, 26 Security design principles, 32–36 Security information and event management (SIEM), 184 Security mechanisms, 23–24, 31–32 services and, relationship of, 32 X.800 recommendations, 31 Security policy, 395 Security policy database (SPD), 311–312 Security policy violation, 39 Security services access control, 29 authentication, 29 availability, 30 data confidentiality, 29 data integrity, 28, 30 defined, 25, 30 nonrepudiation, 30 Sender policy framework (SPF), 267, 286–289 mechanism modifiers, 288 operation, 289 on receiver side, 288–289 on sender side, 288 Separation of privilege, 34 Sequence number, 137 Service models, 173 Service request, SSH, 213 Service set identifier (SSID) broadcasting, 225 Service threats, defined, 41 Session keys, 60, 123, 135 defined, 60, 123 Kerberos, 135 Shared technology issues, 177–178 Shift rows, AES, 56 Signal-hiding techniques, 225 Signature detection, 382. See Rule-based detection SignedData, S/MIME, 276–277 Simple Mail Transfer Protocol (SMTP), 415–416, 418 Single bastion inline, 424, 428 Single bastion T, 428 Small office/home office (SOHO) applications., 428 Smartphones, 227 SMTP, 415–416, 418 SOCKS, components, 420 Software as a service (SaaS), 173 Software attack surface, 36 Source routing attacks, 417 SSL/TLS attacks, 205–207 Stanford Research Institute (SRI), 386 Resource pooling, 172–173 Resources, 223 Response, IDES, 395 Reverse certificate, 143 Revocation, 144, 148 certificates, X.509 authentication service, 143 request, PKI, 148 Rivest-Shamir-Adleman (RSA) algorithm, 199–202 Rootkit countermeasures, 364 external mode, 360 kernel mode, 360 memory based, 360 persistent, 360 user mode, 360 virtual machine based, 360 Round Add Round Key, 57 AES encryption, 59 function, Feistel cipher, 50–52 Routing, IPsec, 306 RSA, 101–104 public-key encryption, 101–104 RSA probabilistic signature scheme (RSA-PSS), 111 Rule-based anomaly detection, 386 Rule-based detection, 382 Rule-based intrusion detection, 386–388 Rule-based penetration identification, 387–388 S Salt value, 397. See also Hashed passwords Screening router, 428 Scripting viruses, 346–347 Second-generation scanner, 362 Secret keys, 46, 99, 138–139 encryption using, 46 key management, 138–139 public-key cryptography, 99, 138–139 public-key distribution of, 138–139 Secure Hash Algorithm (SHA), 87 Secure hash functions. See Hash functions Secure/Multipurpose Internet Mail Extension (S/MIME), 268–279 certificate processing, 278–279 clear signing, 277 cryptographic algorithms, 273–274 messages, 274–278 Multipurpose Internet Mail Extensions (MIME), 259–266 Secure Shell (SSH), 208–219 channels, 216 Connection Protocol, 209 host keys, 209–210 key exchange and generation, 213–214 message exchange, 214–215 packet exchange, 210–213 port forwarding, 217–219 Transport Layer Protocol, 209–213 User Authentication Protocol, 209, 214 Secure Sockets Layer (SSL), 190 Securing wireless transmissions, 225–226 460 InDeX Threshold random walk (TRW) scan detection, 366 Ticket-granting server (TGS), 126 Ticket-granting service exchange, 136–137 Ticket lifetime, 134–135 Time series model, 386 Times, Kerberos, 136 Timestamp authentication, 127, 137 Tiny fragment attacks, 417–418 Traffic analysis, 26 Traffic flow confidentiality (TFC), 316 Traffic processing, IP, 312–314 Traffic security, 230 Transport Layer Protocol, SSH, 209–213 Transport Layer Security (TLS), 65, 91, 165, 190–207 alert protocol, 191 cipher spec, 194–197 cryptographic computations, 202–204 handshake



protocol, 197–202 message authentication code (MAC), 211–212 padding, 194 pseudorandom function (PRF), 203–204 record protocol, 192–194 Transport-level security, 187–219 HTTPS, 188, 207–208 Secure Shell (SSH), 188, 207–208 Socket Layer (SSL), 190 Transport Layer Security (TLS), 190–207 Web considerations, 188–190 Transport mode, IP, 308–309, 317–320 Triple Data Encryption Standard (3DES), 54–55 Trojan horses, 354–355 Tunnel mode, IP, 308–309, 320–321 U UNIX implementations, 399–400 Unknown risk profile, 178 User credential compromise, 39 User credential guessing, 39 User identity, 413 User terminal and user (UT/U), 38 V Virtual local area networks (VLANs), 163 Virtual private network (VPN), 230, 425–426 Viruses concealment strategy encrypted virus, 346 metamorphic virus, 346 mutation engine, 346 polymorphic virus, 346 stealth virus, 346 nature of dormant phase, 343 execution phase, 343 infection mechanism, 343 payload, 343 propagation phase, 343 triggering phase, 343 trigger, logic bomb, 343 State array, AES, 56 Stateful inspection firewalls, 418–419 Statistical anomaly detection, 382 profile-based, 384 counter, 385 gauge, 385 interval timer, 385 mean and standard deviation, 385–386 resource utilization, 385 threshold analysis, 384 Stealth virus, 346 Stream ciphers, 63–67 defined, 48 design considerations, 64 keystream, 64 plaintext processing, cryptography, 48 RC4 algorithm, 65–67 structure of, 63–65 Stuxnet worm, 355, 359 Subject field, 144, 147 Subkey, Kerberos, 137 Substitution bytes, AES, 56 Symmetric encryption, 46–52 block cipher, design of, 50 block size, 50 ciphertext, 47 computationally secure, 49 cryptanalysis, 48–50 cryptography, 48 decryption algorithm, 47 encryption algorithm, 46 Feistel cipher structure, 50–52 key size, 51 plaintext, 46, 48–49 principles of, 46–52 requirements of, 47 round function, 50 rounds, number of, 50 secret key, 46 subkey generation algorithm, 52 T Tablets, 227 Target discovery hit list, 371 random, 371 scanning or fingerprinting, 371 topological, 371 Third-generation scanner, 362 Threats. See also Attack(s) active attacks, 27 denial-of-service (DoS) attack, 30 masquerade, 27 modification of information, 27 network security, 124 passive attack, 25–27 release of contents, 25 replay, 27 service, 41 traffic analysis, 26 InDeX 461 man-in-the middle attacks, 224 network injection, 225 nontraditional networks, 224 Wireless security, 223–226 accessibility, 223 access points, 225 channel, 223 measures, 225 mobility, 223 networks, 224–226 resources, 223 threats, network, 224–225 transmissions, 224–225 encryption, 225 signal-hiding techniques, 225 Workstation hijacking, 397 Worm propagation model, 349–350 Worm technology, state of metamorphic, 351 multiexploit, 351 multiplatform, 351 polymorphic, 351 transport vehicles, 351 zero-day exploit, 351 X X.509 certificate, 139–146 certificate revocation list (CRL), 144 certificates, 140–142 certification authority (CA), 147 forward certificate, 143 introduction to, 139 issuer attributes, 146 key information, 145–146 path constraints, 146 policy information, 145–146 reverse certificate, 143 revocation of certificates, 144 subject attributes, 145 user's certificate, obtaining, 142–144 version 3, 144–145 X.800 standard recommendations, 24, 25, 27, 29–32 structure compression virus, 344, 345 simple virus, 344 traditional machine-executable virus code, 343 target, classification by boot sector infector, 346 file infector, 346 macro virus, 346 multipartite virus, 346 Vulnerability, passwords electronic monitoring, 397 exploiting multiple password use, 397 user mistakes, 397 offline dictionary attack, 396 password guessing against single user, 397 popular password attack, 396–397 specific account attack, 396 workstation hijacking, 397 W Web security, 184–185, 188–190. See also Internet security Web sites, 188, 189 Wide area network (WAN), 411, 423 Wi-Fi hotspots, 224 Wi-Fi Protected Access (WPA), 231, 237 Wireless Ethernet Compatibility Alliance (WECA), 231 Wireless networking components, 224 Wireless network security, 222–250 IEEE 802.11i LAN, 236–250 IEEE 802.11 LAN, 230–236 Robust Security Network (RSN), 237 Wi-Fi Protected Access

(WPA), 237 Wired Equivalent Privacy (WEP), 237 wireless security, 223–226 Wireless network threats, 224–225 accidental association, 224 ad hoc networks, 224 denial of service (DoS), 225 identity theft (MAC spoofing), 224 malicious association, 224 THE WILLIAM StALLINGs BOOKs ON COMPUtER Data And Computer Communications, Tenth Edition A comprehensive survey that has become the standard in the field, covering (1) data communications, including transmission, media, signal encoding, link control, and multiplexing; (2) communication networks, including wired and wireless WANs and LANs; (3) the TCP/IP protocol suite, including IPv6, TCP, MIME, and HTTP, as well as a detailed treatment of network security. Received the 2007 Text and Academic Authors Association (TAA) award for the best Computer Science and Engineering Textbook of the year. Wireless Communication Networks And Systems (with Cory Beard) A comprehensive, state-of-the-art survey. Covers fundamental wireless communications topics, including antennas and propagation, signal encoding techniques, spread spectrum, and error correction techniques. Examines satellite, cellular, wireless local loop networks and wireless LANs, including Bluetooth and 802.11. Covers wireless mobile networks and applications. Computer Security, Third Edition (with Lawrie Brown) A comprehensive treatment of computer security technology, including algorithms, protocols, and applications. Covers cryptography, authentication, access control, database security, cloud security, intrusion detection and prevention, malicious software, denial of service, firewalls, software security, physical security, human factors, auditing, legal and ethical aspects, and trusted systems. Received the 2008 TAA award for the best Computer Science and Engineering Textbook of the year. Operating Systems, Eighth Edition A state-of-the-art survey of operating system principles. Covers fundamental technology as well as contemporary design issues, such as threads, SMPs, multicore, real-time systems, multiprocessor scheduling, embedded OSs, distributed systems, clusters, security, and object-oriented design. Third, fourth and sixth editions received the TAA award for the best Computer Science and Engineering Textbook of the year. AND DATA COMMUNICATIONS TECHNOLOGY Foundations Of Modern Networking: SDN, NFV, QoE, IoT, and Cloud An in-depth up-to-date survey and tutorial on Software Defined Networking, Network Functions Virtualization, Quality of Experience, Internet of Things, and Cloud Computing and Networking. Examines standards, technologies, and deployment issues. Also treats security and career topics. Cryptography And Network Security, SEVENTH Edition A tutorial and survey on network security technology. Each of the basic building blocks of network security, including conventional and public-key cryptography, authentication, and digital signatures, are covered. Provides a thorough mathematical background for such algorithms as AES and RSA. The book covers important network security tools and applications, including S/MIME, IP Security, Kerberos, SSL/TLS, network access control, and Wi-Fi security. In addition, methods for countering hackers and viruses are explored. Second edition received the TAA award for the best Computer Science and Engineering Textbook of 1999. Business Data Communications, Seventh Edition (with Tom Case) A comprehensive presentation of data communications and telecommunications from a business perspective. Covers voice, data, image, and video communications and applications technology and includes a number of case studies. Topics covered include data communications, TCP/IP, cloud computing, Internet protocols and applications, LANs and WANs, network security, and network management. Computer Organization And Architecture, Tenth Edition A unified view of this broad field. Covers fundamentals such as CPU, control unit, microprogramming, instruction set, I/O, and memory. Also covers advanced topics such as multicore, superscalar, and parallel organization. Five-time

**winner of the TAA award for the best Computer Science and Engineering Textbook of the year.**