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.

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 problem-solving 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.

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.

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 Balasubramaniyan, 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 Koblentz, M. “NIDX—An Expert System for Real-Time Network Intrusion Detection.” *Proceedings, Computer Networking Symposium*, April 1988.

BELL90 Bellovin, 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 Bellovin, 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.

CERT01 CERT Coordination Center. “Denial of Service Attacks.” June 2001. 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.

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.

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.

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.

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.

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. Dobb'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.

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.

CREDITS

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 Key-Clustering 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/Iec 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.

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.