Bibliography

Chapter 1

Footnotes

1. MIMOSO, MICHAEL & THREATPOST, THE KASPERSKY LAB SECURITY NEWS SERVICE. (2013). *BREACH Compression Attack Steals HTTPS Secrets in Under 30 Seconds*. [Online] 5th August 2013. Available from: http://threatpost.com/breach-compression-attack-steals-https-secrets-in-under-30-seconds/101579.
2. FISHER, DENNIS & THREATPOST, THE KASPERSKY LAB SECURITY NEWS. (2013). *Most Surprising NSA Capability: Defeating the Collective Security Prowess of Silicon Valley*. [Online] 30th December 2013. Available from: http://threatpost.com/the-year-in-nsa/103329.
3. SYMANTEC CORPORATION. (2014). *2013 Norton Report*. [Online] Available from: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013
4. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2014). *Management System Standards*. [Online] Available from: http://www.iso.org/iso/home/standards/management-standards.htm

References

5. ABBATE, JANET ELLEN. (1994*). From ARPANET to Internet: A history of ARPA-sponsored computer networks, 1966–1988.*
6. CORBATO FERNANDO, J. & VICTOR A. VYSSOTSKY. (1965). Introduction and overview of the Multics system. *Proceedings of the November 30–December 1, 1965, fall joint computer conference, part I*. ACM.
7. BERNERS-LEE, TIM., CAILLIAU, R., GROFF, J.F., & POLLERMANN, B. (1992). World-Wide Web: the information universe. *Internet Research* 2.1. pp. 52–58.
8. BERNERS-LEE, TIM, ET AL. (1993). *The World Wide Web initiative.* [Online] Available from: http://info.cern.ch/hypertext/WWW/TheProject.html

Chapter 2
Footnotes

1. LEESON, PETER T. & CHRISTOPHER J COYNE. (2005). The Economics of Computer Hacking. *Journal of Economics & Policy*, p. 511.
2. CERT, SOFTWARE ENGINEERING INSTITUTE, CMU, TIMOTHY J. SHIMEALL & JONATHAN SPRING. (2014). *Introduction to Information Security: A Strategic-Based Approach.* [Online] Available from: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=88289
3. GARFINKEL, SIMSON. (2002). The FNI's Cybercrime Crackdown. *Technology Review: Manchester NH 105.9* pp. 66–75
4. KAHN, DAVID. (1996). *The Codebreakers – The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Revised ed. New York: Scribner.
5. MENKE, RICHARD. (2000). Telegraphic Realism: Henry James' In the Cage. *Publications of the Modern Language Association of America* pp. 975–990.
6. AGNEW, JAMES B. (1973). *The Great War that Almost Was: The Crimea, 1853-1856, pp. 83–102.* Birkhauser Basel.
7. RAKUS-ANDERSSON, ELISABETH. (2003). The Brains Behind the Enigma Code Breaking Before the Second World War. *Mathematics and War*. Birkhäuser Basel, pp. 83–102.
8. KRUH, LOUIS & DEAVOURS, CIPHER. (2002). The commercial Enigma: Beginnings of machine cryptography. *Cryptologia 26.1* pp. 1–16.
9. DIRK RIJMENANTS. *Photograph - The German Wehrmacht Enigma Cipher Machine*. [Online] Available from: http://users.telenet.be/d.rijmenants/en/enigma.htm
10. SHORT, KRISTI & DAGAN, AHARON. (2013). An Examination of the Components and Mathematics of the Enigma Electromechanical Rotor Ciphers. *Journal of Young Investigators, May 2013, Vol 25, No.5, pp. 33–40.*
11. COLIN SMITH. (2011). *Photograph - Alan Turing Statue near to Stoughton, Surrey, Great Britain.* [Online] Available from: http://www.geograph.org.uk/photo/2597296
12. CORBATO, FERNANDO J. & VYSSOTSKY, VICTOR A. (1965). Introduction and Overview of the Multics System. *Proceedings of the November 30-December 1, 1965, Fall Joint Computer Conference, Part I. ACM, 1965.*
13. BAKER, W.E., DUDONIS, R.M. & KEE, J.H. (1978). Transaction Network, Telephones and Terminals. *The Bell System Technical Journal, Vol. 57, No.10, December 1978.*
14. LAPSELY, PHIL. (2013). *Phreaking Out Ma Bell.* [Online] Available from: http://spectrum.ieee.org/telecom/standards/phreaking-out-ma-bell
15. BREEN, C. & DAHLBOM, C.A. (1960). Signaling System for Control of Telephone Switching. *The Bell System Technical Journal, Volume 39, November 1960, Number 6.* [Online] Available from: https://archive.org/details/bstj39-6-1381
16. BEATRICE COMPANIES, INC. *About Bell System Memorial, Photograph of John Draper*. Copyright of The Porticus Centre, Beatrice Technologies. [Online] Available from: http://www.beatriceco.com/bti/porticus/bell/about.html

17. SIMPSON, IAN & ROSHAN, MEDINA. (2013). *U.S. Soldier Manning Gets 35 Years for Passing Documents to WikiLeaks.* [Online] Available from: http://www.reuters.com/article/2013/08/21/us-usa-wikileaks-manning-idUSBRE97J0JI20130821

18. WIKILEAKS. (2013). *Statement by Julian Assange on today's sentencing of Bradley Manning.* [Online] Available from: https://wikileaks.org/Statement-by-Julian-Assange-on,267.html

19. A&E Television Networks, LLC. (2014). *Edward Snowden Biography*. [Online] Available from: http://www.biography.com/people/edward-snowden-21262897#synopsis

20. DEMOCRACY NOW. (2010). *Is WikiLeaks' Julian Assange a Hero? Glenn Greenwald Debates Steven Aftergood of Secrecy News*. [Online] Available from: http://www.democracynow.org/2010/12/3/is_wikileaks_julian_assange_a_hero

Additional References

- LUDLOW, PETER. (2010). WikiLeaks and Hacktivist Culture. *The Nation, October 4th, 2010.*
- BURGHARDT, TOM. (2013). ECHELON Today: The Evolution of an NSA Black Program. *Global Research.*
- A&E TELEVISION NETWORKS, LLC. *Edward Snowden, Biography*. [Online] Available from: http://www.biography.com/people/edward-snowden-21262897
- KARHULA, PAIVIKKI. (2011). *What is the Effect of WikiLeaks for Freedom of Information?* [Online] Available from: http://www.ifla.org/publications/what-is-the-effect-of-wikileaks-for-freedom-of-information
- NAKASHIMA, ELLEN. MARKON, JERRY, & WASHINGTON POST STAFF WRITERS. (2010). WikiLeaks Founder Could be Charged Under Espionage Act. *Washington Post: November 30th, 2010.* [Online] Available from: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112905973.html
- TAYLOR, MARISA. (2014). U.S. Spy Agency's Push for Secrecy Seen as Another Failing of Obama's Transparency Pledge. *McClatchy Washington Bureau*. [Online] Available from: http://www.kansas.com/2014/01/15/3228179/us-spy-agencys-push-for-secrecy.html
- ROSENBAUM, RON. *Secrets of the Little Blue Box.* [Online] Available from: http://www.webcrunchers.com/crunch/esq-art.html
- WESOLKOWSKI, SLAWO. (2009). The Invention of Enigma and How the Polish Broke It Before the Start of WWII.*University of Waterloo*.
- GOODELL, JEFF. (1996). *The Cyberthief and the Samurai: The True Story of Kevin Mitnick and the Man Who Hunted Him Down*.

Chapter 3

Footnotes

1. PERRIN, C. (2008). *Understanding layered security and defense in depth by Chad Perrin in IT Security.* [Online] Available from: http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/

2. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (Various). *Information technology—Security techniques—Information security management systems–Requirements (ISO/IEC 27001:2013) Standard; Information technology—Security techniques—Code of practice for information security controls (ISO/IEC 27002:2013); Standards/Guidelines from International Organization for Standardization.* [Online] Available from: www.iso.org/

3. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2011 & 2013). *Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View & 800-53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations.* [Online] Available from: http://csrc.nist.gov/publications/nistpubs/.

4. THE SABSA INSTITUTE, John Sherwood, Andrew Clark & David Lynas. (2009). *SABSA® White Paper on Enterprise Security Architecture.* [Online] Available from: http://www.sabsa.org/white_paper

5. ORAM, A. & JOHN VIEGA. (2009). *Beautiful Security*. First Edition. Sebastopol, CA: O'Reilly Media, Inc.

6. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2007). *Special Publication 800-100: Information Security Handbook: A Guide for Managers–Chapter 8.* [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

7. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2014). *ISO/IEC 27000:2014 -Information technology—Security techniques—Information security management systems—Overview and vocabulary*. [Online] Available from: http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip

8. INFORMATION SYSTEMS SECURITY ASSOCIATION & DONN B. PARKER. (2010). Our Excessively Simplistic Information Security Model and How to Fix It. Volume 8 Issue 7, July 2010. *ISSA Journal.* [Online] Available from: http://www.bluetoad.com/publication/?i=41813&page=1

9. SOFTWARE ENGINEERING INSTITUTE. (2005). *OCTAVE–S Implementation Guide, Version 1.* [Online] Available from: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6795

10. INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. (2009). *Risk IT Practitioner Guide.* [Online] Available from: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ The-Risk-IT-Framework.aspx

11. $(ISC)^2$. (2011). *2011 Frost & Sullivan Market Survey Sponsored by (ISC)2 and prepared by Robert Ayoub, CISSP Global Program Director, Information Security carried out in the fall 2010.* [Online] Available from: http://searchsecurity.techtarget.com/news/1527643/ISC2-survey-reveals-need-for-secure-application-development-skills

12. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (1996). Special Publication 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Chapter 4

Footnotes

1. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2014). *Special publication 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations.* [Online] Available from: http://csrc.nist.gov/publications/PubsSPs.html

Chapter 5

Footnotes

1. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2004). *Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199.* [Online] Available from: http://csrc.nist.gov/publications/PubsFIPS.html.

2. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2012). *Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments.* [Online] Available from: http://csrc.nist.gov/publications/PubsSPs.html.

3. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2012). *Special Publication 800-61 Rev. 2 Computer Security Incident Handling Guide.* [Online] Available from: http://csrc.nist.gov/publications/PubsSPs.html.

4. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2010). *Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems.* [Online] Available from: http://csrc.nist.gov/publications/PubsSPs.html.

Chapter 6

Footnotes

1. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, DOLORES R. WALLACE & D. RICHARD KUHN. (2014). *Failure Modes in Medical Device Software: An Analysis of 15 years of Recall Data.* [Online] Available from: www.scholar.google.com

2. THE SYDNEY MORNING HERALD TRAVELLER. (22nd March 2014). *Air India Dreamliner flight from Melbourne makes emergency landing due to 'glitches.'* [Online] Available from: http://www.smh.com.au/travel/travel- incidents/air-india-dreamliner-flight-from-melbourne-makes-emergency- landing-due-to-glitches-20140206-322wh.html

3. HINDUSTAN TIMES, NEW DELHI. (5th Feb 2014). *AI flight makes emergency landing in Kuala Lumpur.* [Online] Available from: http://www.hindustantimes.com/india-news/ai-flight-makes-emergency-landing- in-kuala-lumpur/article1-1180854.aspx

4. GOLEM TECHNOLOGIES. (2014). *Shell Injection & Command Injection.* [Online] Available from: https://www.golemtechnologies.com/articles/shell-injection

Additional References

- BOYD, STEPHEN W. & ANGELOS D. KEROMYTIS. (2004). SQLrand: Preventing SQL injection attacks. *Applied Cryptography and Network Security*. Springer Berlin Heidelberg.
- YODER, JOSEPH & JEFFREY BARCALOW. (1998). Architectural patterns for enabling application security. *Urbana 51 (1998): 61801*.
- YIP, ALEXANDER, ET AL. (2009). Improving application security with data flow assertions. *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles*. ACM, 2009.
- MCGRAW, GARY. (2004). Software security. *Security & Privacy, IEEE 2.2 (2004): 80–83*.

Chapter 7

Footnotes

1. KNAPP, M. (2014). *Hacked: Apple's Helpful Security Service Turned Harmful – By Mark Knapp dt. 27-May-2014.* [Online] Available from: http://wallstcheatsheet.com/technology/hacked-apples-helpful-security-service-turned-harmful.html/

2. USENIX – THE ADVANCED COMPUTING SYSTEMS ASSOCIATION, EVAN COOKE, FARNAM JAHANIAN & DANNY MCPHERSON. (2014). *Technical Paper The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets.* [Online] Available from: https://www.usenix.org/legacy/event/sruti05/tech/full_papers/cooke/cooke_html/

3. KERNER, S.M. (2013). *Internet of Things Could Bring On Attack of the Killer Toaster Botnet.* [Online] Available from: http://www.eweek.com/blogs/security-watch/internet-of-things-could-bring-on-attack-of-the-killer-toaster-botnet.html (Posted 2013-10-10)

4. EWEEK. (2002). *Trail of Destruction: The History of the Virus.* [Online] Available from: http://www.eweek.com/c/a/Web-Services-Web-20-and-SOA/Trail-of-Destruction-The-History-of-the-Virus/ (Posted 2002-03-22) & SEAN MICHAEL KERNER. (2013). *eWEEK 30: Computer Viruses Evolve from Minor Nuisances to Costly Pests.* [Online] Available at: http://www.eweek.com/security/eweek-30-computer-viruses-evolve-from-minor-nuisances-to-costly-pests.html (Posted 2013-11-15)

5. SYMANTEC CORPORATION. (2013). *Symantec Corporation's Symantec Threat Report 2013 - Volume 18.* [Online] Available from: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-18

6. MCAFEE LABS. (2014). McAfee Labs Threats Report – Fourth Quarter 2013. [Online] Available from: http://www.mcafee.com/in/security-awareness/articles/mcafee-labs-threats-report-q4-2013.aspx

7. MCAFEE LABS. (2013). McAfee Labs 2014 Threats Predictions Report. [Online] Available from: http://www.mcafee.com/in/security-awareness/articles/the-top-internet-security-threats-for-2014.aspx

8. SYMANTEC CORPORATION. (2014). *Norton Antivirus Product Details.* [Online] Available from: http://in.norton.com/360/ (accessed on 30th March 2014)

9. MCAFEE, INC. (2014). McAfee Antivirus Product Details. [Online] Available from: http://home.mcafee.com/store/total-protection (Accessed on 30th March 2014)

10. KASPERSKY LAB ZAO. (2014). Kaspersky Antivirus Product Details. [Online] Available from: http://www.kaspersky.co.in/kaspersky-pure

11. TECHMEDIA NETWORK | INTENDERS. (2014). *Top Ten Antivirus Reviews.* [Online] Available from: http://anti-virus-software-review.toptenreviews.com/

12. BITDEFENDER.COM. (2014). Bitdefender Antivirus Product Details. [Online] Available at: http://www.bitdefender.com/media/html/launch2014/?pid=in_nocover&sem_region=IN&utm_source=Google&utm_campaign=IN_Bitdefender&sem_type=search&sem_placement=&utm_content=38150774619&utm_term=bitdefender%20antivirus&gclid=CJnei73TvLOCFeIb4god6VoAYw & HERMAN STREET. (2014). [Online] Available from: http://store.hermanstreet.com/index.php?p=np&page_id=bitdefender-antivirus&ICID=bitdefender-2013-10-16&ofm

13. AVG TECHNOLOGIES. (2014). AVG Antivirus Product Details. http://www.avg.com/in-en/internet-security & HARMAN STREET. (2014). [Online] Available from: http://store.hermanstreet.com/pc-software/avg-anti-virus-2014-download/?&ICID=pin-AVG%20AntiVirus%202013-9-17bas&ofm (both accessed on 30th March 2014)

14. GRAVES, KIMBERLY. (2010). CEH Certified Ethical Hacker Study Guide. New Delhi: Wiley India Pvt. Ltd.

Chapter 8

Footnotes

1. INTERNET ENGINEERING TASK FORCE. (1998). *RFC 2440 - Open PGP Message Format.* [Online] Available from: http://www.rfc-editor.org/info/rfc2440

2. KAHN, DAVID. (1996). *The Codebreakers. The Codebreakers – The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Revised ed. New York: Scribner.

3. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2001). *Advanced Encryption Standard.* [Online] Available from: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

4. INTERNET ENGINEERING TASK FORCE, C. Adams of Entrust Technologies. (1997). *RFC 2144 - The CAST-128 Encryption Algorithm.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc2144.txt

5. INTERNET ENGINEERING TASK FORCE, C. Adams & J. Gilchrist of Entrust Technologies. (1999). *RFC 2612 - The CAST-256 Encryption Algorithm.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc2612.txt

6. INTERNET ENGINEERING TASK FORCE, R. Rivest of MIT Laboratory for Computer Science and Data Security, Inc. (1998). *RFC 2268 – A description of the RC2(r) Encryption Algorithm.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc2268.txt

7. INTERNET ENGINEERING TASK FORCE, R Baldwin of RSA Data Security, Inc & R Rivest of MIT Laboratory for Computer Science and RSA Data Security, Inc. (1996). *RFC 2040 - The RC5, RC5-CBC, RC5-CBC-Pad and RC5-CTS Algorithms.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc2040.txt

8. SCHNEIER, BRUCE. (1994). *The Blowfish Encryption Algorithm.* [Online] Available from: https://www.schneier.com/blowfish.html

9. SCHNEIER, BRUCE. (1998). *Twofish.* [Online] Available from: https://www.schneier.com/twofish.html

10. INTERNET ENGINEERING TASK FORCE, M. Matsui & J. Nakajima. (2004). *RFC 3713 - A description of the Camellia Encryption Algorithm.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc3713.txt

11. INTERNET ENGINEERING TASK FORCE, H Ohta & M Matsui of Mitsubishi Electric Corporation. (2000). *RFC 2994 - A Description of the MISTY1 Encryption Algorithms.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc2994.txt

12. INTERNET ENGINEERING TASK FORCE, H.J. Lee, S.J. Lee, J.H. Yoon, D.H. Cheon, J.I. Lee of KISA. (2005). *RFC 4269 - The SEED Encryption Algorithm.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc4269.txt

13. INTERNET ENGINEERING TASK FORCE, J. Lee, J. Lee, J. Kim, D. Kwon, C. Kim of NSRI. (2010). *RFC 5794 - A Description of the ARIA Encryption Algorithm.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc5794.txt

14. INTERNET ENGINEERING TASK FORCE, M. Katagi & S. Moriai of Sony Corporation. (2011). *RFC 6114 - The 128-bit Blockcipher CLEFIA.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc6114.txt

15. INTERNET ENGINEERING TASK FORCE, S. Kiyomoto & W. Shin of KDDI R&D Laboratories, Inc. (2013). *RFC 7008 - A Description of the KCipher-2 Encryption Algorithm.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc7008.txt

16. THE SANS INSTITUTE. (2001). *The GSM Standard.* [Online] Available from: http://www.sans.org/reading-room/whitepapers/telephone/gsm-standard-an-overview-security-317

17. MITSUBISHI ELECTRIC CORPORATION. *Cellular Algorithms-Encryption Algorithms.* [Online] Available from: http://www.etsi.org/services/security-algorithms/cellular-algorithms

18. INTERNET ENGINEERING TASK FORCE, J. Jonsson & B. Kaliski of RSA Laboratories. (2003). *RFC 3447 - RSA Cryptography Specification.* [Online] Available from: http://www.rfc-editor.org/rfc/rfc3447.txt

19. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2014). *RSA Validation List.* [Online] Available from: http://csrc.nist.gov/groups/STM/cavp/documents/dss/rsanewval.html

20. INTERNET ENGINEERING TASK FORCE, D. McGrew of Cisco Systems, K. Igoe & M. Salter of National Security Agency. RFC 6090 - Fundamental Elliptic Curve Cryptography Algorithm. [Online] Available from: http://www.rfc-editor.org/rfc/rfc6090.txt

21. INTERNET ENGINEERING TASK FORCE, B. Kaliski of RSA Laboratories. (1992). RFC 1319 - The MD2 Message-Digest Algorithm. [Online] Available from: http://www.rfc-editor.org/rfc/rfc1319.txt

22. INTERNET ENGINEERING TASK FORCE, D. Eastlake 3rd, T. Hansen of AT&T Labs. (2006). *RFC 4634 – US Secure Hash Algorithms (SHA and HMAC-SHA)*. [Online] Available from: http://www.rfc-editor.org/rfc/rfc4634.txt

23. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2012). *SHA-3 Competition (2007-2012)*. [Online] Available from: http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

24. TIMBERLINE TECHNOLOGIES. (2009). *Alphabetical List of Public Key Infrastructure Products*. [Online] Available from: http://www.timberlinetechnologies.com/products/pki.html

25. INTERNATIONAL TELECOMMUNICATION UNION. (2012). *X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*. [Online] Available from: https://www.itu.int/rec/T-REC-X.509/en

26. NATIONAL INSTITUTE OF TECHNOLOGY AND STANDARDS. (1993). *Capstone Chip Technology*. [Online] Available from: http://csrc.nist.gov/keyrecovery/cap.txt

27. ELECTRONIC PRIVACY INFORMATION CENTER. (1993). *The Clipper Chip*. [Online] Available from: http://epic.org/crypto/clipper/

28. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (Various). *Federal Information Processing Standards*. [Online] Available from: http://csrc.nist.gov/publications/PubsFIPS.html

29. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2008). *FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC)*. [Online] Available from: http://csrc.nist.gov/publications/PubsFIPS.html

30. SOURCEFORGE. (2014). *TrueCrypt – Migrating from TrueCrypt to BitLocker*. [Online] Available from: http://truecrypt.sourceforge.net/

Additional References

- DIFFIE, WHITFIELD, & MARTIN E. HELLMAN. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on* 22.6 (1976): 644-654.
- ODED, GOLDREICH. (2001). *Foundations of Cryptography, Volume 1: Basic Tools*. Cambridge University Press.
- MERRIAM-WEBSTER. *Cryptology (definition). Merriam-Webster's Collegiate Dictionary*. 11th edition. [Online] Available from: http://www.merriam-webster.com/dictionary/cryptology. Retrieved 2008-02-01.
- SCHNEIER, BRUCE. (1996). *Applied Cryptography*. Second Edition. J. Wiley and Sons.
- STALLINGS, WILLIAM. (2003). *Cryptography and Network Security, Principles and Practice*. Third edition. Prentice Hall.
- JOHNSON, J. & B. KALISKI. (2003). *RFC 3447 - Public-Key Cryptography Standards (PKCS): RSA Cryptography Specifications Version 2.1*. [Online] Available from: https://www.ietf.org/rfc/rfc3447.txt

- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2001). *Federal Information Processing Standards (FIPS) 140-2 - Security Requirements for Cryptographic Modules.* [Online] Available from: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- INTERNET ENGINEERING TASK FORCE. (2008). An Open Specification for Pretty Good Privacy (openpgp). [Online] Available from: http://datatracker.ietf.org/wg/openpgp/charter/
- SCHNEIER, B. (1996). *Applied Cryptography*. 2nd edition. New York: John Wiley & Sons.
- SCHNEIER, B. (2000). *Secrets & Lies: Digital Security in a Networked World.* New York: John Wiley & Sons.
- STALLINGS, W. (2014). *Cryptography and Network Security: Principles and Practice.* 6th edition. Dorling Kindersley (India) Pvt. Ltd.

Chapter 9

Footnotes

1. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. About ISO, What are Standards? [Online] Available from: http://www.iso.org/iso/home/about.htm
2. INTERNATIONAL TELECOMMUNICATION UNION. (1994). *X.200: Information technology - Open Systems Interconnection - Basic Reference Model: The basic model.* [Online] Available from: http://www.itu.int/rec/T-REC-X.200-199407-I/en
3. INTERNET ENGINEERING TASK FORCE, R. BRADEN. *RFC 1122* - Requirements for Internet Hosts - Communication Layers. [Online] Available from: http://www.ietf.org/rfc/rfc1122.txt
4. INTERNET ENGINEERING TASK FORCE. *RFC 791 – Internet Protocol – DARPA Internet Program Protocol Specification.* [Online] Available from: http://www.ietf.org/rfc/rfc791.txt
5. INTERNET ENGINEERING TASK FORCE. *RFC 793 – Transmission Control Protocol – DARPA Internet Program Protocol Specification.* [Online] Available from: http://www.ietf.org/rfc/rfc793.txt
6. MICROSOFT CORPORATION. *TCP/IP Protocol Architecture.* [Online] Available at: http://technet.microsoft.com/en-us/library/cc958821.aspx
7. CBS INTERACTIVE (ZDNET). (2012). *HSBC banking websites recover from DoS attack.* [Online] Available from: http://www.zdnet.com/uk/hsbc-banking-websites-recover-from-dos-attack-7000006063/.
8. PCMAG DIGITAL GROUP, JAY MUNRO. (2004). *MyDoom.A: Fastest Spreading Virus in History.* [Online] Available from: http://www.pcmag.com/article2/0,2817,1485719,00.asp
9. INTERNET ENGINEERING TASK FORCE, W. EDDY OF VERIZON. *RFC 4987 – TCP SYN Flooding Attacks and Common Mitigations.* [Online] Available from: http://www.ietf.org/rfc/rfc4987.txt

Additional References

- STEVENS, W.R. (1994). *TCP/IP Illustrated, Volume I: The Protocols*. Addison-Wesley.
- MILLER, M. (1999). *Troubleshooting TCP/IP*. John Wiley & Sons.
- CAPPELL, L.A. & E. TITTEL. (2004). *Guide to TCP/IP*. Second Edition. Thomson Course Technology.
- FEIT, S. (2000). *TCP/IP: Architecture, Protocols, and Implementation with IPv6 and IP Security*. McGraw-Hill.
- COMER, D. (1991). *Internetworking with TCP/IP, Vol. I: Principles, Protocols, and Architecture*. Second Edition. Prentice-Hall.

Chapter 10

Footnotes

1. [Online] Available from: http://postscapes.com/internet-of-things-market-size
2. [Online] Available from: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html
3. INTERNET ENGINEERING TASK FORCE. *RFC 791 – Internet Protocol – DARPA Internet Program Protocol Specification.* [Online] Available from: http://www.ietf.org/rfc/rfc791.txt
4. INTERNET ENGINEERING TASK FORCE. *RFC 793 – Transmission Control Protocol – DARPA Internet Program Protocol Specification.* [Online] Available from: http://www.ietf.org/rfc/rfc793.txt
5. INTERNET ENGINEERING TASK FORCE, K. EGEVANG of Cray Communications & P. FRANCIS of NTT. RFC 1631 – *The IP Network Address Translator (NAT).* [Online] Available from: http://www.ietf.org/rfc/rfc1631.txt
6. INTERNET ENGINEERING TASK FORCE, Y. REKHTER of CISCO Systems, B. MOSKOWITZ of Chrysler Corp, D. KARRENBERG of RIPE NCC, G. J. DE GROOT of RIPE NCC & E. LEAR of Silicon Graphics, Inc. *RFC 1918 – Address Allocation for Private Internets.* [Online] Available from: http://www.ietf.org/rfc/rfc1918.txt

Additional References

- CISCO SYSTEMS. *Cisco Firewall best Practices*. [Online] Available from: http://www.cisco.com/web/about/security/intelligence/firewall-best-practices.html
- THE SANS INSTITUTE. *SANS Security Consensus Operational Readiness Evaluation, Firewall Checklist*. [Online] Available from: http://www.sans.org/score/checklists/FirewallChecklist.pdf
- DARBY, R. (2012). Cyber Defence in Focus: Enemies Near and Far–or Just Behind the Firewall: The Case for Knowledge Management. *Defence Studies, 12(4), 523-538*.
- NICHO, M. (2012). Incorporating COBIT Best Practices in PCI DSS V2.0 for Effective Compliance. *ISACA Journal, 1, 42*.

- SINGH, A. N., PICOT, A., KRANZ, J., GUPTA, M. P., & OJHA, A. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal of Flexible Systems Management, 14(4), 225-239.*
- ROBERTSON, R. A. (2012). Security Auditing: The Need for Policies and Practices. *Journal of Information Privacy & Security, 8(1).*
- WEEK, J., IVANOVA, P., WEEK, S., & MCLEOD, A. (2011). A Firewall Data Log Analysis of Unauthorized and Suspicious Traffic. *Journal of Information System Security, 7(3).*

Chapter 11

Footnotes

1. SANS INSTITUTE – INFOSEC READING ROOM, ALLISON HRIVNAK. *Host Based Intrusion Detection: An Overview of Tripwire and Intruder Alert.* [Online] Available from: http://www.sans.org/reading-room/whitepapers/detection/host-based-intrusion-detection-overview-tripwire-intruder-alert-353
2. MCAFEE NETWORK SECURITY TECHNOLOGIES GROUP, DR. FENGMIN GONG. (2002). *Next Generation Intrusion Detection Systems (IDS).* [Online] Available from: https://www.mcafee.com/japan/products/pdf/IntruVert-NextGenerationIDSWhitePaper_en.pdf
3. MCAFEE NETWORK SECURITY TECHNOLOGIES GROUP, DR. FENGMIN GONG. (2003). *Deciphering Detection Techniques: Part II Anomaly-Based Intrusion Detection.* [Online] Available from: https://secure.mcafee.com/japan/products/pdf/Deciphering_Detection_Techniques-Anomaly-Based_Detection_WP_en.pdf
4. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, KAREN SCARFONE & PETER MELL. (2007). *Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS).* [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Additional References

- MCAFEE NETWORK SECURITY TECHNOLOGIES GROUP & DR. FENGMIN GONG. *Deciphering Detection Techniques: Part III Denial of Service Detection.* [Online] Available from: http://www.mcafee.com/japan/products/pdf/deciphering_detection_techniques-dos_detection_wp_en.pdf
- MUKKAMALA, SRINIVAS & ANDREW SUGAND AJITH ABRAHAM. Designing Intrusion Detection Systems: Architectures, Challenges and Perspectives. *Department of Computer Science, Oklahoma State University, USA*. [Online] Available from: http://wstst05.softcomputing.net/iec.pdf
- BACE, REBECCA GURLEY. (2000). *Intrusion Detection*. Macmillan Technical Publishing.
- BRACKNEY, R. (1998). Cyber-Intrusion Response. *Reliable Distributed Systems.*
- THE SANS INSTITUTE. (2008). *Network IDS & IPS Deployment Strategies.* [Online] Available from: http://www.sans.org/reading-room/whitepapers/intrusion/network-ids-ips-deployment-strategies-2143
- GARCIA-TEODORO, PEDRO, ET AL. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security 28.1 (2009): 18-28.*

- THE SANS INSTITUTE. (2001). *Understanding Intrusion Detection Systems.* [Online] Available from: http://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337
- THE SANS INSTITUTE. (2004). *Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth.* [Online] Available from: http://www.sans.org/reading-room/whitepapers/detection/understanding-ips-ids-ips-ids-defense-in-depth-1381

Chapter 12
Footnotes

1. INTERNET ENGINEERING TASK FORCE, W. SIMPSON of Daydreamer. (1994). *RFC 1661 - The Point-to-Point Protocol.* [Online] Available from: http://www.ietf.org/rfc/rfc1661.txt
2. INTERNET ENGINEERING TASK FORCE, K. HAMZEH of Ascend Communications, G. PALL of Microsoft Corporation, W. VERTHEIN of 3Com, J. TAARUD of Copper Mountain Networks, W. LITTLE of ECI Telematics & G. ZORN of Microsoft Corporation. (1999). *RFC 2637 - Point-to-Point Tunneling Protocol (PPTP).* [Online] Available from: http://www.ietf.org/rfc/rfc2637.txt
3. INTERNET ENGINEERING TASK FORCE, W.SIMPSON of Daydreamer. (1994). *RFC 1661 - The Point-to-Point protocol (PPPP).* [Online] Available from: http://www.ietf.org/rfc/rfc1661.txt
4. INTERNET ENGINEERING TASK FORCE, W.SIMPSON of Daydreamer. (1996). *RFC 1994 - PPP Challenge Handshake Authentication Protocol (CHAP*). [Online] Available from: http://www.ietf.org/rfc/rfc1994.txt
5. INTERNET ENGINEERING TASK FORCE, W. TOWNSLEY & A. VALENCIA of Cisco Systems, A. RUBENS of Ascend Communications, G. PALL & G. ZORN of Microsoft Corporation & B. PALTER of Redback Networks. (1999). *RFC 2661 - Layer Two Tunneling Protocol "L2TP".* [Online] Available from: http://www.ietf.org/rfc/rfc2661.txt
6. INTERNET ENGINEERING TASK FORCE, G. DOMMETY of Cisco Systems. (2000). *RFC 2890 - Key and Sequence Number Extensions to GRE*. [Online] Available from: http://www.ietf.org/rfc/rfc2890.txt
7. INTERNET ENGINEERING TASK FORCE, S. KENT of BBN Corp & R. ATKINSON of @ Home Network. (1998). *RFC 2401 - Security Architecture for the Internet Protocol.* [Online] Available from: http://www.ietf.org/rfc/rfc2401.txt
8. INTERNET ENGINEERING TASK FORCE, S. KENT & K. SEO of BBN Technologies. (2005). *RFC 4301 - Security Architecture for Internet Protocol.* [Online] Available from: http://www.ietf.org/rfc/rfc4301.txt
9. INTERNET ENGINEERING TASK FORCE, S. KENT of BBN Technologies. (2005). *RFC 4302 - IP Authentication Header.* [Online] Available from: http://www.ietf.org/rfc/rfc4302.txt
10. INTERNET ENGINEERING TASK FORCE, S. KENT of BBN Technologies. (2005). *RFC4303 - IP Encapsulating Security Payload (ESP)*. [Online] Available from: http://www.ietf.org/rfc/rfc4303.txt
11. INTERNET ENGINEERING TASK FORCE, C. KAUFMAN, Ed. of Microsoft. (2005). *RFC 4306 - Internet Key Exchange (IKEv2) Protocol*. [Online] Available from: http://www.ietf.org/rfc/rfc4306.txt

12. INTERNET ENGINEERING TASK FORCE, E. ROSEN of Cisco Systems, Inc., A. VISWANATHAN of Force10 Networks, Inc. & R. CALLON of Juniper Networks, Inc. (2001). *RFC 3031 – Multiprotocol Label Switching Architecture.* [Online] Available from: http://www.ietf.org/rfc/rfc3031.txt

13. INTERNET ENGINEERING TASK FORCE, E. ROSEN of Cisco Systems, Inc. & Y. REKHTER of Juniper Networks, Inc. (2006). *RFC 4364 - BGP/MPLS IP Virtual Private Networks (VPNs).* [Online] Available from: http://www.ietf.org/rfc/rfc4364.txt

Additional References

- GLEESON, B., A. LIN, J. HEINANEN, G. ARMITAGE, A. MALIS & INTERNET ENGINEERING TASK FORCE. (2000). *RFC 2764 - A Framework for IP Based Virtual Private Networks.* [Online] Available from: http://tools.ietf.org/html/rfc2764
- HANKS, S., T. LI, D. FARINACCI, P. TRAINA & INTERNET ENGINEERING TASK FORCE. (1994). *RFC1701 - Generic Routing Encapsulation.* [Online] Available from: http://tools.ietf.org/html/rfc1701
- HANKS, S., T. LI, D. FARINACCI, P. TRAINA & INTERNET ENGINEERING TASK FORCE. (1994). *RFC1702 - Generic Routing Encapsulation over IPv4 networks.* [Online] Available from: http://tools.ietf.org/html/rfc1702
- SHENKER, S., C. PATRIDGE, R. GUERIN & INTERNET ENGINEERING TASK FORCE. (1997). *RFC2212 - Specification of Guaranteed Quality of Service.* [Online] Available from: http://tools.ietf.org/html/rfc2212
- PERKINS, D. OF CMU & INTERNET ENGINEERING TASK FORCE. (1990). *RFC 1171 - The Point-to-Point Protocol for the Transmission of Multi-Protocol Datagrams Over Point-to-Point Links.* [Online] Available from: http://tools.ietf.org/html/rfc1171
- HAMZEH, K., ET AL., & INTERNET ENGINEERING TASK FORCE. (1999). *RFC 2637 - Point-to-Point Tunneling Protocol (PPTP).* [Online] Available from: http://tools.ietf.org/html/rfc2637
- SIMPSON, W., OF DAYDREAMER & INTERNET ENGINEERING TASK FORCE. (1994). *RFC 1661 - The Point-to-Point protocol (PPPP).* [Online] Available from: http://tools.ietf.org/html/rfc1661
- ZORN, G., OF MICROSOFT CORP & INTERNET ENGINEERING TASK FORCE. (1999). *RFC 2484 - PPP LCP International Configuration Option.* [Online] Available from: http://tools.ietf.org/html/rfc2484
- TOWNSLEY, W., ET AL, & INTERNET ENGINEERING TASK FORCE. (1999). *RFC 2661 - Layer Two Tunneling Protocol.* [Online] Available from: http://tools.ietf.org/html/rfc2661
- DOMMETY, G., & INTERNET ENGINEERING TASK FORCE. (2000). *RFC 2890 - Generic Routing Encapsulation (GRE).* [Online] Available from: http://tools.ietf.org/html/rfc2890
- KENT, S., R. ATKINSON & INTERNET ENGINEERING TASK FORCE. (1998). *RFC 2401 - Security Architecture for the Internet Protocol.* [Online] Available from: http://tools.ietf.org/html/rfc2401

- KENT, S., & INTERNET ENGINEERING TASK FORCE. (2005). *RFC 4302 - IP Authentication Header.* [Online] Available from: http://tools.ietf.org/html/rfc4302
- KENT, S., R. ATKINSON & INTERNET ENGINEERING TASK FORCE. *RFC 2406 & RFC4303 - IP Encapsulating Security Payload (ESP).* [Online] Available from: http://tools.ietf.org/html/rfc2406
- HARKINS, D., D. CARREL & INTERNET ENGINEERING TASK FORCE. (1998). *RFC 2409, RFC 4306 - The Internet Key Exchange (IKE).* [Online] Available from: http://tools.ietf.org/html/rfc2409
- KENT, S., K. SEO & INTERNET ENGINEERING TAKS FORCE. (2005). *RFC 4301, RFC 2401 - Security Architecture for the IP.* [Online] Available from: http://tools.ietf.org/html/rfc4301
- ROSEN, E., A. VISWANATHAN, R. CALLON & INTERNET ENGINEERING TASK FORCE. (2001). *RFC 3031 - MPLS Architecture.* [Online] Available from: http://tools.ietf.org/html/rfc3031
- ROSEN, E., Y. REKHTER & INTERNET ENGINEERING TASK FORCE. *RFC 4364 - BGP/MPLS VPNs.* [Online] Available from: http://tools.ietf.org/html/rfc4364
- INTERNET ENGINEERING TASK FORCE. (2006). *RFC 4364 - BGP/MPLS IP Virtual Private Networks (VPNs).* [Online] Available from: http://tools.ietf.org/html/rfc4364
- CHANDRA, R., P. TRAINA, T. LI & INTERNET ENGINEERING TASK FORCE. (1996). *RFC1997 - BGP Communities Attribute.* [Online] Available from: http://tools.ietf.org/html/rfc1997
- CHEN, E., T. BATES & INTERNET ENGINEERING TASK FORCE. (1996). *RFC1998 - An Application of the BGP Community Attribute in Multi-home Routing.* [Online] Available from: http://tools.ietf.org/html/rfc1998
- WAITZMAN, D., C. PARTRIDGE, S. DEERING & INTERNET ENGINEERING TASK FORCE. (1988). *RFC1075 - Distance Vector Multicast Routing Protocol.* [Online] Available from: http://tools.ietf.org/html/rfc1075
- INTERNET ENGINEERING TASK FORCE. (2005). *IP Security Protocol.* [Online] Available from: http://www.ietf.org/html.charters/ipsec-charter.html
- RAJA, P. & F5 NETWORKS, INC. (2006). *Rolling out New SSL VPN Service.* [Online] Available from: https://www.f5.com/pdf/white-papers/sslvpn-sp-wp.pdf.

Chapter 13

Footnotes

1. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2011). Special Publication 800-145: The NIST Definition of Cloud Computing. [Online] Available from: http://csrc.nist.gov/publications/PubsSPs.html
2. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2011). Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing.[Online] Available from: http://csrc.nist.gov/publications/PubsSPs.html

3. KRUTZ, L. & RUSSELL DEAN VINES. (2010). *Cloud Security – A Comprehensive Guide to Secure Cloud Computing*. New Delhi - Wiley India Pvt. Ltd.

4. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2012). *Special Publication 800-146: Cloud Computing Synopsis and Recommendations*. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-146/SP800-146.pdf

References

1. KRUTZ, R.L. & RUSSELL DEAN VINES. (2004). Second Edition. The CISSP Prep Guide. New Delhi - Wiley dreamtech India Pvt. Ltd.

Chapter 14

Footnotes

1. PARKER, D.B. (1998). *Fighting Computer Crime*. New York: John Wiley and Sons Inc. pp. 250–251.

References

2. SINHA, G.R. & SANDEEP B PATIL. *Biometrics: Concepts and Applications*. New Delhi: Wiley India Pvt. Ltd.

3. GREGORY, P. & MICHAEL A. SIMON. (2008). *Biometrics for Dummies*. Hoboken, NJ: Wiley Publishing, Inc.

Additional References

- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Special Publication 800-12: Introduction to Computer Security: The NIST Handbook – Chapter 15*. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter15.html

- JAIN, A. K., A. ROSS, & S. PRABHAKAR. (2004). An Introduction to Biometric Recognition. *IEEE Trans. on Circuits and Systems for Video Technology, Special Issue on Image and Video-Based Biometrics, vol. 14, no. 1, pp. 4-20, January 2004*. [Online] Available from: http://ieeexplore.ieee.org/iel5/76/28212/01262027.pdf

Chapter 15

Footnotes

1. GRAVES, KIMBERLY. (2010). CEH Certified Ethical Hacker Study Guide. New Delhi: Wiley India Pvt. Ltd.

Additional References

- LUO, XIN (ROBERT), RICHARD BRODY., ALESSANDRO SEAZZU., & STEPHEN BURD - ALL OF THE UNIVERSITY OF NEW MEXICO, USA. (2011). Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal, 24(3), 1-8, July-September 2011.* [Online] Available from: http://scholar.google.co.in/scholar?q=social+engineering+neglected+human+factor&btnG=&hl=en&as_sdt=0%2C5&as_ylo=2010/IRMJ2011.pdf
- DIMKOV., T., WOLTER PIETERS, PIETER HARTEL OF UNIVERSITY OF TWENTE, THE NETHERLANDS. (2010). *Two methodologies for physical penetration testing using social engineering.* [Online] Available from: http://scholar.google.co.in/scholar?q=social+engineering+two+methodologies+for+physical+penetration+testing&btnG=&hl=en&as_sdt=0%2C5&as_ylo=2010
- MAAN., P.S., MANISH SHARMA. OF DAV INSTITUTE OF ENGINEERING AND TECHNOLOGY, PUNJAB TECHNICAL UNIVERSTIY, INDIA. (2012). Social Engineering: A Partial Technical Attack. *IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012.* [Online] Available from: http://scholar.google.co.in/scholar?q=social+engineering+a+partial+technical+attack&btnG=&hl=en&as_sdt=0%2C5&as_ylo=2010
- HASAN, M., NILESH PRAJAPATI, & SAFVAN VOHARA OF BVM ENGINEERING COLLEGE, INDIA. Case Study On Social Engineering Techniques For Persuasion. *International journal on applications of graph theory in wireless ad hoc networks and sensor networks.* [Online] Available from: http://scholar.google.co.in/scholar?as_ylo=2010&q=case+study+on+social+engineering&hl=en&as_sdt=0,5

Chapter 16

Footnotes

1. NATIONAL SECURITY AGENCY, UNITED STATES OF AMERICA - SYSTEMS AND NETWORK ANALYSIS CENTER, INFORMATION ASSURANCE DIRECTORATE. *Bluetooth Security.* [Online] Available from: http://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&sqi=2&ved=0CFQQFjAJ&url=http%3A%2F%2Fwww.nsa.gov%2Fia%2F_files%2Ffactsheets%2FI732-016R-07.pdf&ei=d294U9XHB8aLuATj_YJ4&usg=AFQjCNFc2CXHzjfl27QVF7gBZuZonc9tKQ