

## Student Research References Network and Digital Forensics

### Network Forensic Analysis

- Anson, S., & Bunting, S. (2007). *Mastering Windows network forensics and investigation*. Hoboken, NJ: Sybex.
- Corey, V., Peterman, C., Shearin, S., Greenburg, M., & Bokkelen, J. (2002, November-December). Network forensics analysis. *IEEE Internet Computing*.
- Garfinkel, S. (2002). *Network forensics: tapping the Internet*, O'Reilly Network.
- Krasser, S., Conti, G., Grizzard, J., Gribshaw, J., & Owen, H. (2005, June 15-17). *Real-time and forensic network data analysis using animated and coordinated visualization*. Paper presented at the Sixth Annual IEEE Information Assurance Workshop (IAW '05).
- Layton, T. (2006). *Information security: design, implementation, measurement, and compliance*. New York: Auerbach.
- Mueller, P. (2007, June 25). How's your forensics strategy? *Network Computing*, 18, 18-18.
- Mukkamala, S., & Sung, A. (2003). Identifying significant features for network forensics analysis using artificial intelligent techniques. *International Journal of Digital Evidence*, 1(4).
- Neville, A. (2003, January 20). *IDS logs in forensics investigations: An analysis of a compromised honeypot*, from <http://www.securityfocus.com/infocus/1676>
- Perry, S. (2006, December). Network forensics and the inside job. *Network Security*, 2006, 11-13.
- Sandstorm Inc. (2007). Addressing data breeches with NetIntercept, from <http://www.knowledgestorm.com>
- Schiffman, M., Pennington, B., Pollino, D., & O'Donnell, A. (2002). *Hacker's Challenge 2: test your network security & forensics skills* (2nd ed.). New York, NY: McGraw Hill/Osborne.

## Network Forensic Analysis (Continued)

Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security (TISSEC)*, 2(2), 159-176.

Shanmugasundaram, K. (2004). *ForNet: A Distributed Forensics Network*.

Shipley, G. (2004). Body of evidence (network forensic tools). *Network Computing*.

Siles, R. (2007, January 2). *Wireless forensics: tapping the air*. Retrieved September 14, 2007, from <http://www.securityfocus.com/infocus/1884>

Wylter, N., Potter, B., & Hurley, C. (2005). *Aggressive network self-defense*. Rockland, MA: Syngress.

## Anti-Forensic Technology

Berghel, H. (2007). Hiding data, forensics, and anti-forensics. *Communications of the ACM*, 50(4), 15-20.

## Computer and Digital Media Forensics

Bunting, S., & Wei, W. (2006). *EnCase computer forensics: the official EnCE study guide*. Edison, NJ: Sybex.

Casey, E. (2004). *Digital evidence and computer crime* (Second Edition ed.): Elsevier.

Guillermo, F., Trifas, M., Brown, D., Francia, R., & Scott, C. (2006). *Visualization and management of digital forensics data*. Paper presented at the 3rd Annual Conference on Information Security Curriculum Development.

Kruse, W., & Heise, J. (2001). *Computer forensics: incident response essentials*. Boston: Addison-Wesley Professional.

Liebrock, L., Marreno, N., Burton, D., Prine, R., Cornelius, E., Shakamuri, M., et al. (2007). *A preliminary design for digital forensics analysis of terabyte size data sets*. Paper presented at the ACM Symposium on Applied Computing.

## Computer and Digital Media Forensics (Continued)

Obialero, R. (2006). Forensic analysis of a compromised Intranet server. Bethesda: SANS Institute.

Steel, C. (2006). *Windows forensics: the field guide for corporate computer investigations*. Edison, NJ: Wiley.

## Incident Response and Investigation

Ames, B. (2007, August 29). Monster outlines anti-fraud measures. *PC World*.

Casey, E. (2006). Investigating sophisticated security breaches. *Communications of the ACM*, 49(2), 48-55.

Chen, P., Laih, C., Pouget, F., & Dacier, M. (2005). Comparative survey of local honeypot sensors to assist network forensics. *IEEE*.

Dunn, J. (2007). Criminals operating malware supermarkets, *NetworkWorld.com*.

Howell, B., & Rubin, S. (2007, May). What every lawyer should know about digital forensics (but may not know to ask). *Computer & Internet Lawyer*, 24, 12-15.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response* (No. NIST 800-86): National Institute of Standards and Technology (NIST).

National Institute of Justice. (2001). *Electronic crime scene investigation, a guide for first responders*: Department of Justice.

Nolan, R., Baker, M., Branson, J., Hammerstein, J., Rush, K., Waits, C., et al. (2005). First responders guide to computer forensics: advanced topics. *CERT*.

Schweitzer, D. (2003). *Incident response: computer forensics toolkit*. Edison, NJ: Wiley.

Wong, J., Kirovski, D., & Potkonjak, M. (2004). Computational forensic techniques for intellectual Property protection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits And Systems*, 23(6).

## Information Security

- Allen, J. (2001). *CERT(R) guide to system and network security practices (SEI Series in Software Engineering)*. Boston: Addison-Wesley Professional.
- Layton, T. (2006). *Information security: design, implementation, measurement, and compliance*. New York: Auerbach.
- Landoll, D. (2005). *The security risk assessment handbook: a complete guide for performing security risk assessments*. London: CRC Press.
- Locasto, M., Wang, K., Keromytis, A., & Stolfo, S. (2005). *FLIPS: hybrid adaptive intrusion prevention*: Columbia University.
- National Institute of Standards and Technology. (2000). *Digital Signature Standard (DSS) (No. FIPS PUB 186-2)*. Washington, D.C.
- Northcutt, S. (2005). *Inside network perimeter security*. Indianapolis: SAMS.
- Northcutt, S., & Novak, J. (2002). *Network intrusion detection*. Indianapolis: New Riders Publishing.
- Peltier, T. (2001). *Information security policies, procedures, and standards: guidelines for effective information security management*. New York: Auerbach.
- Pollino, D., Pennington, B., Bradley, T., & Dwivedi, H. (2006). *Hacker's challenge 3 (hacking exposed)*: McGraw Hill.
- Specht, S., & Lee, R. (2004). *Distributed denial of service: Taxonomies of attacks, tools, and countermeasures*. Paper presented at the 17<sup>th</sup> International Conference on Parallel and Distributed Computing Systems.