Course Recommended Reading

Recommended Reading for L1:

i. The DDOS that almost Broke the Internet
ii. Practical Network Support for IP Traceback
iii. A DoS-limiting Network Architecture

Recommended Reading for L2:

Spamalytics: An Empirical Analysis of Spam Marketing Conversion
PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs

Recommended Reading for L3:

The Hacker Playbook – Practical Guide to Penetration Testing, by Peter Kim

Recommended Readings for L4 and L5:

A Look Back at "Security Problems in the TCP/IP Protocol Suite"
Steve Friedl's Unixwiz.net Tech Tips: An Illustrated Guide to the Kaminsky DNS Vulnerability
BGP Security in Partial Deployment

Recommended Readings for L6:

Securing Frame Communication in Browsers
The Security Architecture of the Chromium Browser
Exposing Private Information by Timing Web Applications
An Introduction to Content Security Policy
Play safely in sandboxed IFrames
The Basics of Web Workers
Using CORS
Secure Session Management With Cookies for Web Applications
Origin Cookies: Session Integrity for Web Applications

ForceHTTPS: Protecting High-Security Web Sites from Network Attacks
Towards Short-Lived Certificates

Recommended reading for L7

1. Ether: Malware Analysis via Hardware Virtualization Extensions.

2. Artem Dinaburg, Paul Royal, Monirul Sharif, and Wenke Lee.

3. In Proceedings of The 15th ACM Conference on Computer and Communications Security (CCS 2008), Alexandria, VA, October 2008.

4. http://ether.gtisc.gatech.edu/

5. Automatic Reverse Engineering of Malware Emulators. Monirul Sharif, Andrea Lanzi, Jon Giffin, and Wenke Lee. In Proceedings of The 2009 IEEE Symposium on Security and Privacy, Oakland, CA, May 2009. http://old.iseclab.org/people/andrew/download/oakland09.pdf

6. Exploring Multiple Execution Paths for Malware Analysis. Andreas Moser, Christopher Kruegel, and Engin Kirda. In Proceedings of The 2007 IEEE Symposium on Security and Privacy, Oakland, CA, May 2007.

   https://www.auto.tuwien.ac.at/~chris/research/doc/oakland07_explore.pdf

Recommended reading L8 (other than the papers already listed on slides, please add):

Jekyll on iOS: When Benign Apps Become Evil.
Tielei Wang, Kangjie Lu, Long Lu, Simon Chung, and Wenke Lee.
In Proceedings of The 22nd USENIX Security Symposium. Washington DC. August 2013.

These papers are listed on the video called 'Mobile Malware Protection":

On Lightweight Mobile Phone Application Certification
Mitigating Android Software Misuse Before It Happens

Recommended Reading for Lesson 9

1. BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation. Guofei Gu, Phillip Porras, Vinod Yegneswaran, Martin Fong, Wenke Lee. In Proceedings of The 16th USENIX Security Symposium (Security'07), Boston, MA, August 2007. http://faculty.cs.tamu.edu/guofei/paper/Gu_Security07_botHunter.pdf

2. BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection. Guofei Gu, Roberto Perdisci, Junjie Zhang, and Wenke Lee. In Proceedings of The 17th USENIX Security Symposium (Security'08), San Jose, CA, July 2008. https://www.usenix.org/legacy/event/sec08/tech/full_papers/gu/gu_html/

3. Modeling Botnet Propagation Using Time Zones. David Dagon, Cliff Zou, and Wenke Lee. In Proceedings of The 13th Annual Network and Distributed System Security Symposium (NDSS 2006), San Diego, CA, February

2006. http://www.cs.ucf.edu/~czou/research/botnet_tzmodel_NDSS06.pdf

Recommended Reading for Lesson 10

Zakir Durumeric, Eric Wustrow, and J. Alex Halderamn. ZMap: Fast Internet-Wide Scanning and its Security Applications.
In Proceedings of the 22nd USENIX Security Symposium

Recommended Reading for Lesson 11

1. Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster. Building a Dynamic Reputation System for DNS. In Proceedings of The 19th USENIX Security Symposium, Washington, DC, August 2010.

2. Manos Antonakakis, Roberto Perdisci, Wenke Lee, Nikolaos Vasiloglou II, and David Dagon. Detecting Malware Domains at the Upper DNS Hierarchy. In Proceedings of The 20th USENIX Security Symposium, San Francisco, August 2011.

3. Charles Lever, Manos Antonakakis, Bradley Reaves, Patrick Traynor and Wenke Lee. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. In Proceedings of The 20th Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2013.

4. Yacin Nadji, Manos Antonakakis, Roberto Perdisci, and Wenke Lee. Beheading Hydras: Performing Effective Botnet Takedowns. In Proceedings of The 20th ACM Conference on Computer and Communications Security (CCS), Berlin, Germany, November 2013.

Recommended Reading for Lesson 12a and 12b

Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction

by Arvind Narayanan, Joseph Bonneau, Ed Felten, Andrew Miller, and Steven Goldfeder

Recommended Reading for Lesson 13a

1. Tom Mitchell, Machine Learning, McGraw-Hill, 1997

2. Wenke Lee and Sal Stolfo. A Framework for Constructing Features and Models for Intrusion Detection Systems Wenke Lee and Sal Stolfo. ACM Transactions on Information and System Security, 3(4), November