Tentative Syllabus

These topics are tentative and subject to change without warning. If I don't discuss something you're interested in, ask about it! I may very well add it or modify what I'm covering to include it.

I am revising the textbook, so some readings will be from the second edition. They are identified as such below, and are available on SmartSite. These are still under revision (but are very near final form), so if you see any typographical errors or other problems, please let me know.

lec	date	topic	reading	due
1.	Jan 4	Introduction, overview of security	§1*	
2.	Jan 6	*to be arranged*		
3.	Jan 8	*to be arranged*		
4.	Jan 11	Access control matrix, instantiations	§2*, 16**	
5.	Jan 13	*to be arranged*		
6.	Jan 15	*to be arranged*		
—.	Jan 18	*no class; Martin Luther King Day*		
7.	Jan 20	Policies and policy languages	§4*, [1]	
8.	Jan 22	Example policy models	§5*, 6.1, 6.4, [21]	project selection
9.	Jan 25	Basic cryptography	§10†	homework 1
10.	Jan 27	Protocols and key management	§10, 11, [11, 15]	
11.	Jan 29	PGP, TLS, IPSec	§11.4, [14]	
12.	Feb 1	Identity	§14	
13.	Feb 3	Information flow 1	§16.1, 16.3–16.5	
14.	Feb 5	Information flow 2	§16.1, 16.3–16.5	homework 2
15.	Feb 8	Confinement problem	§17.2	project progress report
16.	Feb 10	Covert (side) channels 1	§17.3, [9]	
17.	Feb 12	Covert (side) channels 2	§17.3	
—.	Feb 15	*no class; Presidents' Day*		
18.	Feb 17	Malware 1	§22, [6, 17]	homework 3
19.	Feb 19	Malware 2	§22	
20.	Feb 22	Vulnerability models	§23.3, 23.4, [10]	
21.	Feb 24	Attack models	[13, 19]	
22.	Feb 26	Penetration testing	§23.2, [16]	
23.	Feb 29	Auditing	§24	homework 4
24.	Mar 2	Intrusion detection	§25, [7, 20, 23]	
25.	Mar 4	Designing for security	§14‡	
26.	Mar 7	Basic assurance	§18	
27.	Mar 9	Topics: elections and e-voting systems	[2, 4, 18]	
28.	Mar 11	Topics: insider threat	[3, 5, 8]	homework 5
29.	Mar 14	Topics: human aspects of security	[12, 22, 24]	completed project
—.	Mar 18	***Final examination period (not held)***		

Notes

* This is the handout of a chapter in the second edition
** Chapter 15 in the first edition; this is the handout of the chapter in the second edition
† Chapter 9 in the first edition; this is the handout of the chapter in the second edition
‡ Chapter 13 in the first edition; this is the handout of the chapter in the second edition

References

[1] B. L. A. Batista and M. P. Fernandez, "PonderFlow: A Policy Specification Language for Openflow Networks," *Proceedings of the 13th International Conference on Networks* pp. 204–209 (Feb. 2014). url: `http://www.thinkmind.org/index.php?view=article&articleid=icn_2014_9_10_30047`.

[2] M. Bishop, *Overview of Red Team Reports*, Office of the California Secretary of State, Sacramento, CA, USA (July 2007). url: http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/red-overview.pdf.

[3] M. Bishop, S. Engle, S. Peisert, S. Whalen, and C. Gates, "We Have Met the Enemy and He Is Us," *Proceedings of the 2008 Workshop on New Security Paradigms* (*NSPW '08*) pp. 1–12 (Sep. 2008). doi: 10.1145/1595676.1595678.

[4] M. Bishop, S. Peisert, C. Hoke, M. Graff, and D. Jefferson, "E-Voting and Forensics: Prying Open the Black Box," *Proceedings of the 2009 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections* pp. 3:1–3:20 (Aug. 2009). url: https://www.usenix.org/legacy/events/evtwote09/tech/full_papers/bishop.pdf.

[5] B. M. Bowen, M. Ben Salem, S. Hershkop, A. D. Keromytis, and S. J. Stolfo, "Designing Host and Network Sensors to Mitigate the Insider Threat," *IEEE Security and Privacy* **7**(6) pp. 22–29 (Nov. 2009). doi: 10.1109/MSP.2009.109.

[6] D. Brumley, "Invisible Intruders: Rootkits in Practice," *;login:* **24**(9) (Sep. 1999). url: https://www.usenix.org/publications/login/apr15/brumley.

[7] L. T. Heberlein, *Why Anomaly Detection Sucks*, Technical Report TR-2005-02-01, Net Squared, Inc., Davis, CA, USA (Feb. 2005). url: http://www.netsq.com/Research/Single.php?stuff=papers&num=17.

[8] J. Hunker and C. W. Probst, "Insiders and Insider Threats—An Overview of Definitions and Mitigation Techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* **2**(1) pp. 4–27 (June 2011). url: http://isyou.info/jowua/abstracts/jowua-v2n1-1.htm.

[9] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *Advances in Cryptology—CRYPTO '99 Proceedings* (*Lecture Notes in Computer Science* **1666**) pp. 388–397 (Aug. 1999). doi: 10.1007/3-540-48405-1_25.

[10] J. A. Kupsch and B. P. Miller, "Manual vs. Automated Vulnerability Assessment: A Case Study," *Proceedings of the First International Workshop on Managing Insider Security Threats* pp. 83–97 (June 2009). url: http://pages.cs.wisc.edu/~kupsch/va/ManVsAutoVulnAssessment.pdf.

[11] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter, *Ron Was Wrong, Whit Is Right*, eprint 2012/064, International Association for Cryptologic Research (Feb. 2012). url: http://ia.cr/2012/064.

[12] H. R. Lipford and M. E. Zurko, "Someone to Watch over Me," *Proceedings of the 2012 Workshop on New Security Paradigms* pp. 67–76 (Sep. 2012). doi: 10.1145/2413296.2413303.

[13] C. Meadows, "A Procedure for Verifying Security Against Type Confusion Attacks," *Proceedings of the Sixteenth Computer Security Foundations Workshop* pp. 62–72 (June 2003). doi: 10.1109/CSFW.2003.1212705.

[14] B. Möller, T. Duong, and K. Kotowicz, *This POODLE Bites: Exploiting the SSL 3.0 Fallback*, Google, Mountain View, CA, USA (Sep. 2014). url: https://www.openssl.org/~bodo/ssl-poodle.pdf.

[15] W. T. Polk, N. E. Hastings, and A. Malpani, "Public Key Infrastructures that Satisfy Security Goals," *IEEE Internet Computing* **7**(4) pp. 60–67 (July 2003). doi: 10.1109/MIC.2003.1215661.

[16] M. Ramilli and M. Prandini, "An Integrated Application of Security Testing Methodologies to E-Voting Systems," *Proceedings of the Second IFIP WG 8.5 International Conference on Electronic Participation* (*Lecture Notes in Computer Science* **6229**) pp. 225–236 (Aug. 2010). doi: 10.1007/978-3-642-15158-3_19.

[17] H. Shacham, "The Geometry of Innocent Flesh on the Bone: Return-Into-Libc Without Function Calls (On the x86)," *Proceedings of the 14th ACM Conference on Computer and Communications Security* (*CCS '07*) pp. 552–561 (2007). doi: 10.1145/1315245.1315313.

[18] B. I. Simidchieva, S. J. Engle, M. Clifford, A. C. Jones, S. Peisert, M. Bishop, L. A. Clarke, and L. J. Osterweil, "Modeling and Analyzing Faults to Improve Election Process Robustness," *Proceedings of the 2010 Electronic Voting Technology/Workshop on Trustworthy Elections* (Aug. 2010). url: https://www.usenix.org/legacy/events/evtwote10/tech/full_papers/Simidchieva.pdf.

[19] S. J. Templeton and K. Levitt, "A Requires/Provides Model for Computer Attacks," *Proceedings of the 2000 New Security Paradigms Workshop* (*NSPW '00*) pp. 31–38 (2000). doi: 10.1145/366173.366187.

[20] D. Wagner and P. Soto, "Mimicry Attacks on Host-Based Intrusion Detection Systems," *Proceedings of the 9th ACM Conference on Computer and Communications Security* (*CCS '02*) pp. 255–264 (Nov. 2002). doi: 10.1145/586110.586145.

[21] T. Walcott and M. Bishop, "Traducement: A Model for Record Security," *ACM Transactions on Information System Security* **7**(4) pp. 576–590 (Nov. 2004). doi: 10.1145/1042031.1042035.

[22] K.-P. Yee, "User Interaction Design for Secure Systems," *Proceedings of the Fourth International Conference on Information and Communications Security* (*Lecture Notes in Computer Science* **2513**) pp. 278–290 (2002). doi: 10.1007/3-540-36159-6_24.

[23] J. Zhou, M. Heckman, B. Reynolds, A. Carlson, and M. Bishop, "Modeling Network Intrusion Detection Alerts for Correlation," *ACM Transactions on Information System Security* **10**(1) pp. 1–31 (Feb. 2007). doi: 10.1145/1210263.1210267.

[24] M. E. Zurko and R. T. Simon, "User-Centered Security," *Proceedings of the 1996 Workshop on New Security Paradigms* pp. 27–33 (Sep. 1996). doi: 10.1145/304851.304859.