Syllabus

Week 1: **Dates**: Oct. 2
Topics: Overview of computer security; access control matrix
Reading: *text*, §1, 2

Week 2: **Dates**: Oct. 7, Oct 9
Topics: HRU result; ACL, C-lists, lock-and-key, PACLs
Reading: *text*, §3.1–3.2, 15; paper [TL13]

Week 3: **Dates**: Oct. 14, Oct. 16
Topics: Policy models: general, confidentiality, integrity, availability; domain-specific
Reading: *text*, §4.1–4.4, 5.1–5.2.2, 5.3, 6.1–6.2, 6.4, 7; papers [PS04, WB04]
Due: Project selection (due Oct. 16); Homework 1 (due Oct. 16)

Week 4: **Dates**: Oct. 21, Oct. 23
Topics: Malware; vulnerabilities: models, classification schemes
Reading: *text*, §22, 23; papers [KCR+10, KWG+12]

Week 5: **Dates**: Oct. 28, Oct. 30
Topics: Assurance and formal verification
Reading: *text*, §18; paper [M79]
Due: Homework 2 (due Oct. 30)

Week 6: **Dates**: Nov. 4, Nov. 6
Topics: Basic cryptography: classical, public key, digital signatures
Reading: *text*, §9, 10; papers [M78, RSA78]
Due: Project progress report (due Nov. 6)

Week 7: **Dates**: Nov. 13; *no class* on Nov. 11 (Veteran's Day)
Topics: Authentication
Reading: *text*, §12; paper [HO12]
Due: Homework 3 (due Nov. 13)

Week 8: **Dates**: Nov. 18, Nov. 20
Topics: Basic intrusion detection: types, methods
Reading: *text*, §25

Week 9: **Dates**: Nov. 25; *no class* on Nov. 27 (Thanksgiving Day)
Topics: Information flow
Reading: *text*, §16; paper [BDU07]
Due: Homework 4 (due Nov. 25)

Week 10: **Dates**: Dec. 2, Dec. 4
Topics: Network security: firewalls, servers, protocols, architectures; network attacks
Reading: papers [CJM05, YCM+06]

Week 11: **Dates**: Dec. 9, Dec. 11
Topics: Special topics: cyber-physical systems, insiders, elections
Reading: papers [BSH+09, SEC+10]
Due: Homework 5 (due Dec. 11)

Dec. 15: **Due**: Completed project due at 10:00am

References

[BDU07] M. Backes, M. Dümuth, and D. Unruh, "Information Flow in the Peer-Reviewing Process (Extended Abstract)," *Proceedings of the 2007 IEEE Symposium on Security and Privacy* pp. 187–191 (May 2007). doi: 10.1109/SP.2007.24

[BSH+09] B. Bowen, M. Ben Salem, S. Hershkop, A. Keromytis, and S. Stolfo, "Designing Host and Network Sensors to Mitigate the Insider Threat," *IEEE Security & Privacy* **7**(6) pp. 22–29 (Nov. 2009). doi: 10.1109/MSP.2009.109

[CJM05] E. Cooke, F. Jahanian, and D. McPherson, "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets," *Proceedings of the USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet* pp. 39–44 (July 2005). url: http://www.usenix.org/legacy/events/sruti05/tech/cooke.html

[HO12] C. Herley and P. van Oorschot, "A Research Agenda Acknowledging the Persistence of Passwords," *IEEE Security & Privacy* **10**(1) pp. 28–36 (Jan.-Feb. 2012). doi: 10.1109/MSP.2011.150

[KWG+12] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles," *Proceedings of Infotech@Aerospace* paper AIAA 2012-2438 (June 2012). doi: 10.2514/6.2012-2438

[KCR+10] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," *Proceedings of the 2010 IEEE Symposium on Security and Privacy* pp. 447–462 (May 2010). doi: 10.1109/SP.2010.34

[M78] R. Merkle, "Secure Communications Over Insecure Channels," *Communications of the ACM* **21**(4) pp. 294–299 (Apr. 1978). doi: 10.1145/359460.359473

[M79] J. Millen, "Operating System Security Verification," *unpublished* (1979).

[PS04] J. Park and R. Sandhu, "The UCON_{ABC} Usage Control Model," *ACM Transactions on Information and System Security* **7**(1) pp. 128–174 (Feb. 2004). doi: 10.1145/984334.984339

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* **21**(2) pp. 120–126 (Feb. 1978). doi: 10.1145/359340.359342

[SEC+10] B. Simidchieva, S. Engle, M. Clifford, A. Jones, S. Peisert, M. Bishop, L. Clarke, and L. Osterweil, "Modeling and Analyzing Faults to Improve Election Process Robustness," *Proceedings of the 2010 USENIX/ACCURATE Electronic Voting Technology Workshop* (Aug. 2010). url: http://www.usenix.org/events/evtwote10/tech/full_papers/Simidchieva.pdf

[TL13] M. Tripunitara and N. Li, "The Foundational Work of Harrison-Ruzzo-Ullman Revisited," *IEEE Transactions on Dependable and Secure Computing* **10**(1) pp. 28–39 (Jan.-Feb. 2013). doi: 10.1109/TDSC.2012.77

[WB04] T. Walcott and M. Bishop, "Traducement: A Model for Record Security," *ACM Transactions on Information and System Security* **7**(4) pp. 576–590 (Nov. 2004). doi: 10.1145/1042031.1042035

[YCM+06] L. Yuan, H. Chen. J. Mai, C.-N. Chuah, Z. Su, and P. Mohapatra, "FIREMAN: A Toolkit for Firewall Modeling and Analysis," *Proceedings of the 2006 IEEE Symposium on Security and Privacy* (May 2006). doi: 10.1109/SP.2006.16