Tentative Syllabus

This syllabus is *tentative* and will undoubtedly continue to change as the quarter progresses. If there is a topic you're interested in but not shown, please let me know; I may well change things to cover it. All readings are from the text unless otherwise indicated.

Week 1: **Lec 1–2**
Dates: Sep 21, Sep 23
Topics: Introduction, principles of secure design, threats and policies
Reading: *text*, §1, 14; papers [Sm12,MA19]

Week 2: **Lec 3–5**
Dates: Sep 26, Sep 28, Sep 30
Topics: Basic policy models: Bell-LaPadula, Biba, Clark-Wilson
Reading: *text*, §5.1–5.2.2, 5.3, 6.2, 6.4; paper [Sa93]

Week 3: **Lec 6–8**
Dates: Oct 3, Oct 5, Oct 7
Topics: Symmetric and public key cryptography
Reading: *text*, §10
Due: Oct 5: homework 1; Oct 7: project selection

Week 4: **Lec 9–11**
Dates: Oct 10, Oct 12, Oct 14
Topics: Protocols, authentication
Reading: *text*, §11.1, 12.1, 12.4, 12.5, 13; papers [Ke93]

Week 5: **Lec 12–14**
Dates: Oct 17, Oct 19, Oct 21
Topics: Access control mechanisms, confinement problem, reference monitor
Reading: *text*, §16.1–16.3, 18.1–18.2, 20.1.2.2; papers [HS16]
Due: Oct 21: homework 2

Week 6: **Lec 15–17**
Dates: Oct 24, Oct 26, Oct 28
Topics: Confinement problem, vulnerabilities
Reading: *text*, §18.2, 24.3–24.4; papers [La73,Li75]

Week 7: **Lec 18–20**
Dates: Oct 31, Nov 2, Nov 4
Topics: Penetration testing, malware
Reading: *text*, §24.1–24.2, 23.1–23.6.1; papers [B+07]
Due: Nov 4: progress report

Week 8: **Lec 20–21**
Dates: Nov 7, Nov 9, Nov 11 **[Nov 11 is Veterans Day (a university holiday)]**
Topics: Elections and e-voting, malware
Reading: *text*, §23.6.2–23.7, 23.9, 26.1–26.3, 28.1, 28.3; papers [Bi00,O+17]
Due: Nov 9: homework 3

Week 9: **Lec 22–24**
Dates: Nov 14, Nov 16, Nov 18
Topics: Network security, firewalls, intrusion detection, entropy, information flow
Reading: *text*, §23.9.7, C, 17.1, 17.3–17.6; papers [B+07, De87]

Week 10: **Lec 25–26**
Dates: Nov 21, Nov 23, Nov 25 **[Nov 25 is Thanksgiving (a university holiday)]**
Topics: Information flow, identity
Reading: §15
Due: Nov 23: homework 4

Week 11: **Lec 27–29**
Dates: Nov 28, Nov 30, Dec 2 **[Dec 2 is the last class]**
Topics: Identity, anonymity, onion routing
Reading: §15
Due: Dec 2: homework 5

Dec 8: **Due**: Completed project due at 3:00pm

References

[Bi00] M. Bishop, "Analysis of the ILOVEYOU Worm," Unpublished paper, Dept. of Computer Science, University of California Davis, Davis, CA 95616 (May 5, 2000).

[B+07] 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

[De87] D. Denning, "An Intrusion-Detection Model," *IEEE Transactions on Software Engineering* **SE-13**(2) pp. 222–232 (Feb. 1987). DOI: 10.1109/TSE.1987.232894

[HS16] M. Heckman and R. Schell, "Using Proven Reference Monitor Patterns for Security Evaluation," *Information* **7**(2) pp. 23ff (Apr. 2016). DOI: 10.3390/info7020023

[Ke93] S. Kent, "Internet Privacy Enhanced Mail," *Communications of the ACM* **36**(8) pp. 48–60 (Aug. 1993). DOI: 10.1145/163381.163390

[La73] B. Lampson "A Note on the Confinement Problem," *Communications of the ACM* **16**(10) pp. 63–615 (Oct. 1973) DOI: 10.1145/362375.362389

[Li75] . S. Lipner, "A Comment on the Confinement Problem," *Proceedings of the Fifth ACM Symposium on Operating System Principles (SOSP '75)* pp. 192–196 (Nov. 1975). DOI: 10.1145/800213.806537

[MA19] M. Mesbah and M. Azer, "Cyber Threats and Policies for Industrial Control Systems," *Proceedings of the 2019 International Conference on Smart Applications, Communications and Networking (SmartNets)* (Dec. 2019). DOI: 10.1109/SmartNets48225.2019.9069761

[O+17] L. Osterweil, M. Bishop, H. Conboy, H. Phan. B. Simidchieva, G. Avrunin, L. Clarke, and S. Peisert, "Iterative Analysis to Improve Key Properties of Critical Human-Intensive Processes: An Election Security Example," *ACM Transactions on Privacy and Security* **20**(2) pp. 5:1–5:31 (Mar. 2017). doi: 10.1145/3041041

[Sa93] R. Sandhu, "Lattice-Based Access Control Models," *IEEE Computer* **26**(11) pp. 9–19 (Nov. 1993). doi: 10.1109/2.241422

[Sm12] R. Smith, "A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles," *IEEE Security and Privacy* **10**(6) pp. 20–25 (Nov.-Dec. 2012). DOI: 10.1109/MSP.2012.85