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:	**Dates**: Sep 27, Sep 29
Lec 1–2	**Topics**: Introduction, principles of secure design, threats and policies
	Reading: *text*, §1, 14; papers [Sm12,MA19]
Week 2:	**Dates**: Oct 2, Oct 4, Oct 6
Lec 3–5	**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:	**Dates**: Oct 9, Oct 11, Oct 13
Lec 6–8	**Topics**: Symmetric and public key cryptography
	Reading: *text*, §10
	Due: Oct 9: homework 1; Oct 11: project question
Week 4:	**Dates**: Oct 16, Oct 18, Oct 20
Lec 9–11	**Topics**: Protocols, authentication
	Reading: *text*, §11.1, 12.1, 12.4, 12.5, 13; papers [Ke93]
Week 5:	**Dates**: Oct 23, Oct 25, Oct 27
Lec 12–14	**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 23: homework 2; Oct 27: project background research
Week 6:	**Dates**: Oct 30, Nov 1, Nov 3
Lec 15–17	**Topics**: Confinement problem, vulnerabilities
	Reading: *text*, §18.2, 24.3–24.4; papers [La73,Li75]
Week 7:	**Dates**: Nov 6, Nov 8, Nov 10 **[Nov 10 is a university holiday, for Veterans' Day]**
Lec 18–20	**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 6: homework 3
Week 8:	**Dates**: Nov 13, Nov 15, Nov 17
Lec 20–22	**Topics**: Malware, penetration testing,
	Reading: *text*, §24.1–24.2, 23.1–23.6.1; papers [B+07]
Week 9:	**Dates**: Nov 20, Nov 22, Nov 24 **[Nov 25 is Thanksgiving (a university holiday]**
Lec 23–24	**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]
	Due: Nov 20: homework 4; Nov 22: project progress report
Week 10:	**Dates**: Nov 27, Nov 29, Dec 1
Lec 25–27	**Topics**: Information flow, identity
	Reading: §15
Week 11:	**Dates**: Dec 4, Dec 6 **[Dec 6 is the last class]**
Lec 28–29	**Topics**: Identity, anonymity, onion routing
	Reading: §15
	Due: Dec 6: homework 5
Dec 12:	**Due**: Completed project due

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[Bi00] M. Bishop, "Analysis of the ILOVEYOU Worm," Unpublished paper, Dept.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