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**: Jan 10, 12
Topics: Reference monitor, access control matrix, safety question, take-grant model, SPM
Reading: *text*, §2, 3–3.4, 20.1.2.2; papers [TL13, Z+05]

Week 2: **Dates**: Jan 17, Jan 19
Topics: Expressive power of models, comparing models, security policies
Reading: *text*, §3.4–3.7, 4; paper [Bi96]

Week 3: **Dates**: Jan 24, Jan 26
Topics: Confidentiality policies, Bell-LaPadula Model
Reading: *text*, §5.1–5.2, A; paper [Sa93]
Due: Jan 24: homework 1; Jan 26: project selection

Week 4: **Dates**: Jan 31, Feb 2
Topics: Tranquility, System Z, assurance overview, assurance in building systems, assurance in design
Reading: *text*, §5.3–5.6, 19, 20–20.2; papers [D+06, Mi79]

Week 5: **Dates**: Feb 7, Feb 9 **[No class on Feb 9]**
Topics: Assurance in implementation, integrity models, Biba, Clark-Wilson, trust models, availability models
Reading: *text*, §20.2–20.4, 6 (except 6.2), 7–7.2; papers [J+11, LO10]
Due: Feb 7: homework 2

Week 6: **Dates**: Feb 14, Feb 16
Topics: Availability models, hybrid models, Chinese Wall model, CISS model, ORCON, RBAC, Traducement
Reading: *text*, §7.3–7.4, 8; papers [A+10, E+03, WB04]
Due: Feb 14: project progress report

Week 7: **Dates**: Feb 21, Feb 23
Topics: Basic policy composition, noninterference, unwinding theorem, nondeducibility, restrictiveness
Reading: *text*, §9; paper [B+07]
Due: Feb 21: homework 3

Week 8: **Dates**: Feb 28, Mar 2
Topics: Entropy, information flow
Reading: *text*, §17, C; paper [SA06]

Week 9: **Dates**: Mar 7, Mar 9
Topics: Principles of secure design, confinement problem, isolation
Reading: §14, 18–18.2; papers [S+06,KR02]

Week 10: **Dates**: Mar 14, Mar 16 **[Mar 16 is last class]**
Topics: Covert channel analysis, malware
Reading: §18.3, 23.8; paper [D+11]
Due: Mar 14: homework 4

Mar 24: **Due**: Completed project due at 10:00am

References

[A+10] C. Ardagna, S. di Vimercati, S. Foresti, T. Grandison, S. Jajodia, and P. Samarati, "Access Control for Smarter Healthcare Using Policy Spaces," *Computers & Security* **29**(8) pp. 848–858 (Nov. 2010). DOI: 10.1016/j.cose.2010.07.001

[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

[Bi96] M. Bishop, "Conspiracy and Information Flow in the Take-Grant Protection Model," *Journal of Computer Security* **4**(4) pp. 331–359 (1996).
DOI: 10.3233/JCS-1996-4404

[D+11] A. Datta, J. Franklin, D. Garg, L. Jia, and D. Kaynar, "On Adversary Models and Compositional Security," *IEEE Security & Privacy* **9**(3) pp. 26–32 (May 2011).
DOI: 10.1109/MSP.2010.203

[D+06] P. Derrin, K. Elphinstone, G. Klein, D. Cock, and M. Chakravaty, "Running the Manual: An Approach to High-assurance Microkernel Development," *Proceedings of the 2006 ACM SIGPLAN Workshop on Haskell* pp. 60–71 (Sep. 2006).
DOI: 10.1145/1159842.1159850

[E+03] A. El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel, and G. Trouessin, "Organization Based Access Control," *Proceedings of the IEEE 4th International Workshop on Policies for Distributed Systems and Networks* pp. 120–131 (June 2003).
DOI: 10.1109/POLICY.2003.1206966.

[J+11] B. Javadi, D. Kondo, J.-M. Vincent, and D. Anderson, "Discovering Statistical Models of Availability in Large Distributed Systems: An Empirical Study of SETI@home," *IEEE Transactions on Parallel and Distributed Systems* **22**(11) pp. 1896–1903 (Nov. 2011).
DOI: 10.1109/TPDS.2011.50

[KR02] C. Ko and T. Redmond, "Noninterference and Intrusion Detection," *Proceedings of the 2002 IEEE Symposium on Security and Privacy* pp. 177–187 (May 2002).
DOI: 10.1109/SECPRI.2002.1004370

[LO10] G. Loukas and G. Öke, "Protection Against Denial of Service Attacks: A Survey," *The Computer Journal* **53**(7) pp. 1020–1037 (2010).
DOI: 10.1093/comjnl/bxp078

[Mi79] J. Millen, "Operating System Security Verification," MITRE Corp., Bedford, MA (1979).

[S+06] G. Shah, A. Molna, and M. Blaze, "Keyboards and Covert Channels," *Proceedings of the 15th USENIX Security Symposium* pp. 59–78 (Aug. 2006).
URL: https://www.usenix.org/legacy/event/sec06/tech/shah/shah.pdf

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

[SA06] J. Soon and J. Alves-Foss, "Covert Timing Channel Analysis of Rate Monotonic Real-Time Scheduling Algorithm in MLS Systems," *Proceedings of the 2006 IEEE Information Assurance Workshop* pp. 361–368 (June 2006).
DOI: 10.1109/IAW.2006.1652117

[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. 2011).
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

[Z+05] X. Zhang, Y. Li, and D. Nalla, "An Attribute-Based Access Matrix Model," *Proceedings of the 2005 ACM Symposium on Applied Computing* pp. 359–363 (Mar. 2005).
DOI: 10.1145/1066677.1066760