# Syllabus

**Week 1**: **Dates**: Apr. 3, Apr. 5, Apr. 7
**Topics**: Access control matrix, safety question
**Reading**: *Chapters from revised text*, §2, 3.1–3.4; papers [TL13,Z+05]

**Week 2**: **Dates**: Apr. 10, Apr. 12, Apr. 14
**Topics**: Expressive power of models; security policies
**Reading**: *Chapters from revised text*, §3.5, 4; paper [Bi96]

**Week 3**: **Dates**: Apr. 17, Apr. 19, Apr. 21
**Topics**: Confidentiality policies; assurance
**Reading**: *Chapters from revised text*, §5, A; *text*, §18; papers [D+06,Sa93,Mi79]
**Due**: Apr. 17: homework #1; Apr. 19: select project

**Week 4**: **Dates**: Apr. 24, Apr. 26, Apr. 28;
**Topics**: More assurance; integrity, availability policies
**Reading**: *Chapters from revised text*, §6–6.2, 6.4; *text*, 19; paper [E+03]

**Week 5**: **Dates**: May 1, May 3, May 5
**Topics**: Availability, hybrid policies
**Reading**: *Chapters from revised text*, §8; papers [J+11,Li89,LO10]
**Due**: May 1: homework #2

**Week 6**: **Dates**: May 8, May 10, May 12
**Topics**: Other policy models, information flow policies
**Reading**: *Chapters from revised text*, §8, 17; papers [A+10,WB04]
**Due**: May 12: project progress report

**Week 7**: **Dates**: May 15, May 17, May 19
**Topics**: Information flow mechanisms, covert channels
**Reading**: *Chapters from revised text*, §17, 18; papers [B+07,S+06,SA06]
**Due**: May 15: homework #3

**Week 8**: **Dates**: May 22, May 24, May 26
**Topics**: Noninterference, nondeducibility, restrictiveness
**Reading**: *text*, §8; papers [D+11,KR02,Ma02]

**Week 9**: **Dates**: May 31, June 2 **[May 29: Memorial Day (university holiday)]**
**Topics**: *to be arranged*
**Reading**: *to be arranged*

**Week 10**: **Dates**: June 5, June 7 **[June 7 is last class]**
**Topics**: Insider threat; elections and voting
**Reading**: papers [B+09,HP11,O+17]
**Due**: June 5: homework #4

**June 7**: **Due**: Completed project due at 8:00pm

**Note.** The "chapters from revised text" are in files that begin with the chapter number.

## 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

[B+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

[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.

[HP11] J. Hunker and C. 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 (2011). url: http://isyou.info/jowua/papers/jowua-v2n1-1.pdf

[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

[Li89] T. Lin, "Chinese Wall Security Policy—An Aggressive Model," *Proceedings of the 5th Annual Computer Security Applications Conference* pp. 282–289 (Dec. 1989). doi: 10.1109/CSAC.1989.81064

[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

[Ma02] H. Mantel, "On the Composition of Secure Systems," *Proceedings of the 2002 IEEE Symposium on Security and Privacy* pp. 88–101 (May 2002). doi: 10.1109/SECPRI.2002.1004364

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

[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

[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