# Tentative Syllabus

Because I teach to the students, and not to the syllabus, these topics are tentative and subject to change without warning. In particular, if I don't discuss something you're interested in, ask about it! I may very well add it or modify what I'm covering to include it.

| lecture | topic | reading |
|---|---|---|
| 1. | Introduction, overview of security | §1 |
| 2. | Access control matrix model | §2 |
| 3. | Safety question and the HRU result | §3.1, 3.2 |
| 4. | Take-Grant Protection Model: *de jure* rules | §3.3 |
| 5. | Take-Grant Protection Model: *de facto* rules | [Bi96] |
| 6. | Schematic Protection Model | §3.4 |
| 7. | Expressive power of models, ESPM, TAM, MTAM | §3.5; [Z+05] |
| 8. | Security policies, mechanisms | §4; [LT05] |
| 9. | Bell-LaPadula Policy Model | §5.1–5.2.2; [Sa93] |
| 10. | Bell-LaPadula Policy Model (*con't*) | §5.2.3, 5.2..4 |
| 11. | System Z, Biba Integrity Policy Model | §5.3, 5.4, 6.2 |
| 12. | Clark-Wilson Integrity Policy Model | §6.4 |
| 13. | Chinese Wall Policy Model | §7.1 |
| 14. | Other Policy Models | §7.2; [WB04] |
| 15. | ORCON, RBAC Access Control Models | §7.3, 7.4 |
| 16. | Deterministic Noninterference | §8.1, 8.2; [KR02] |
| 17. | Deterministic Noninterference (*con't*) | §8.2.1–8.2.4 |
| 18. | Nondeducibility, generalized non-interference | §8.3, 8.4 |
| 19. | Restrictiveness and composition of systems | §8.5; [Ma02] |
| 20. | Concepts of information flow | §16.1, 32 |
| 21. | Non-lattice and non-transitive policies | §16.2; [HS97] |
| 22. | Compiler-based flow mechanisms | §16.3 |
| 23. | Execution-based flow mechanisms | §16.4, 16.5 |
| 24. | Covert channels and isolation | §17.1, 17.2; [S+06] |
| 25. | Analyzing covert channels | §17.3–17.3.1 |
| 26. | Analyzing covert channels (*con't*) | §17.3.2, 17.3.3 |
| 27. | *to be arranged* | |
| 28. | *to be arranged* | |
| 29. | *to be arranged* | |

## Dates

Although instruction begins on Jan. 5, I will be at a conference for that week. Therefore, the first lecture will be on Jan. 12. As this class is being recorded, I will record three lectures sometime during the term, and you can view them at your leisure.

Jan. 19 is Martin Luther King, Jr. Day and Feb. 16 is Presidents' Day. As these are University holidays, there will be no class then.

## References

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

[HS97] T. Himdi and R. Sandhu, "Lattice-Based Models for Controlled Sharing of Confidential Information in the Saudi Hajj System," Proceedings of the 13th Annual Computer Security Applications Conference pp. 164–174 (Dec. 1997).

[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).

[LT05] N. Li and M. Tripunitara, "On Safety in Discretionary Access Control," *Proceedings of the 2005 IEEE Symposium on Security and Privacy* pp. 96–109 (May 2005).

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

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

[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)

[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).

[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).