CS 564/559: Schedule of Readings

September 4, 2012

Tu, 28 Aug Needham and Schroeder, *Using Encryption for Authentication in Large Networks of Computers.* CACM, Dec 1978. `papers/needhamSchroeder78.pdf`

Th, 30 Aug Dolev and Yao, *On the Security of Public-Key Protocols.* IEEE Transactions on Information Theory. 1983. `papers/dolev_yao.pdf`
Gavin Lowe, *An Attack on the Needham-Schroeder Public Key Authentication Protocol.* Information Processing Letters, 1995.
(Francis) `papers/lowe95.pdf`

Tu, 4 Sep Abadi and Needham, *Prudent Engineering Practice for Cryptographic Protocols.* IEEE S&P, 1994.
(Zhenhao) `papers/AbadiNeedham.pdf`

Th, 6 Sep *To be rescheduled.*

Tu, 11 Sep Thayer, Herzog, and Guttman, *Strand Spaces: Why is a Security Protocol Correct?* IEEE S&P, 1998.
(David) `papers/oakland_strands.pdf`

Th, 13 Sep Lowe, *Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR*, TACAS, 1996.
(Yuncheng) `papers/lowe96breaking.pdf`

Tu, 18 Sep Blanchet, *An Efficient Protocol Verifier based on Prolog Rules*, CSFW 2001.
(Guo) `papers/blanchet_csfw01.pdf`