Description

Security is a diverse and rapidly advancing field. In order to give a broad sampling of the different topics in
the field, the class will break up into teams of two members and each team will read a paper on a topic of their
choosing. A 20-30 minute summary of these papers will be presented (with Powerpoint slides) to the class. Some
potential topics (and potential papers for consideration) include (but certainly are not limited to...)

Network Security:

- Secure Border Gateway Protocol (S-BGP) Real World Performance and Deployment Issues, by Stephen
  Kent, Charles Lynn, Joanne Mikkelson, and Karen Seo
- Security Problems in the TCP/IP Protocol Suite, by S.M. Bellovin
- Bro: A System for Detecting Network Intruders in Real-Time by Vern Paxson
  Berger, Hari Balakrishnan
- Traffic Analysis
- IP Traceback

Computer Security:

- Design and Implementation of a TCG-Based Integrity Measurement Architecture by Reiner Sailer, Xiaolan
  Zhang, Trent Jaeger, Leendert Van Doorn (IBM Research Report)
- Secure Electronic Voting

General Wireless Security:

- Security Considerations for IEEE 802.15.4 Networks, by Sastry and Wagner.

Wireless Ad Hoc Security:

- Trust Evaluation in Ad-Hoc Networks, by George Theodorakopoulos and John S. Baras
- SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, by Yih-Chun Hu,
  David B. Johnson, and Adrian Perrig

Sensor Network Security:

- Random Key Predistribution Schemes for Sensor Networks, by Chan, Perrig, and Song.
- An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data Injection in Sensor Networks,
  by Sencun Zhu, Sanjeev Setia, Sushil Jajodia, Peng Ning

Theoretical Foundations of Security:

- Wyner’s Wiretap Problem
- Key Escrow

To find other papers that might be of interest, students might want to examine papers from past IEEE Sym-
posium on Security and Privacy, ACM Conference on Computer and Communications Security, ACM Workshop
on Wireless Security, and CRYPTO/EUROCRYPT.