

Tentative topics for student presentations:

- (1) Wireless security
- (2) Adhoc Wireless Security
- (3) DNS Security
- (4) Intrusion detection software
- (5) Firewalls and other edge devices
- (6) Routing attacks and BGP security
- (7) Authentication mechanisms, Kerberos
- (8) Key Distribution mechanisms
- (9) Secure Remote access techniques
- (10) Cryptanalysis of AES (Rijndael)
- (11) Attack tools and scripts
- (12) Email security
- (13) Buffer Overflow attacks
- (14) SSL and transport security
- (15) Secure voting – current systems (Diebold), attacks and critique
- (16) Elliptic Curve Cryptography
- (17) iSCSI, networked storage and security
- (18) Code obfuscation: methods and limitations
- (19) Secure Group communication
- (20) Secure Broadcasting
- (21) Low-impact Security protocols for overlay networks: issues & design approaches
- (22) Secure peer-to-peer computing: high-performance computation in untrusted environments
- (23) RFID: privacy and security issues

If you have an idea for a presentation topic outside the above list, discuss it with the faculty and get approval. Here is what each team needs to do:

- (a) Give three topics of interest to you in order of priorities
- (b) For each topic, identify at least 2 papers that you would like to talk about so that we know what you are talking about (give URLs for papers where possible).

We will look through all the proposals and assign you a topic so that there is no overlap in presentations. We will also tell you the date of presentation at that time. Presentations will start after Spring Break.

Due date: 2nd March