Preliminaries

You can work on teams of two people to complete a class project of your own choosing. The project can be an extension of all the topics we have discussed in class, or any other topic related to security that you wish to investigate. You are expected to generate a final report and do a final in-class presentation that will last for about 35 mins including questions.

Important Dates: Final report is due **Tuesday May 6th** in class before your presentation.

A non exhaustive list of suggested topics (you may propose your own)

1. The insecurity of the Wired Equivalent Privacy (WEP) protocol – Analysis of the insecurities of the WEP protocol used to secure wifi connections. Paper to read: FLUHRER, S., MANTIN, I., AND SHAMIR, A. Weaknesses in the key scheduling algorithm of RC4. Eighth Annual Workshop on Selected Areas in Cryptography, Aug. 2001.

2. Comparison of key distribution schemes for wireless sensor networks – Comparison of random, deterministic and deployment knowledge key predistribution schemes in terms of security and resource overhead.

3. Key management for multicast services in ad hoc networks (or wired networks) -- Schemes for distributing and updating keys in dynamic groups that receive a multicast service.

4. Anonymization of communications via Mixnets -- Explore the different types of Mixnets available and the level of anonymity that they provide.

5. Implementation and Security Analysis of Elliptic Curve Cryptography methods – Perform cryptanalysis on an elliptic curve public key cryptosystem.

6. Primality testing – Based on the paper M. Agrawal, N. Kayal and N. Saxena, "PRIMES in P," Ann. of Math. (2), 160:2 (2004) 781--793.

7. Security of Diffie-Hellman, RSA, ElGamal -- Describe different attacks against any scheme of your choosing and create a program that breaks each one when keys of small sizes are used.

8. Hashing -- Find collisions in hashes with small ranges and domains.

Final Report Guidelines

Each team should provide a self-contained, readable final report. The following format is suggested but you do not have to follow it exactly.

1. Abstract.
2. Introduction -- Include background material and discuss the scope and limitations of your project.
3. Threat Model – Describe the type of adversary you assume and what types of attacks it can perform. Also clearly state what the goals of the adversary.
4. Main Body – Describe that different methods used or compared in your project and also present any analysis involved.
5. Evaluation – Any simulation results.
6. Conclusions.
7. Future work and open problems.
8. References.
9. Appendices, including supporting material as needed.

Presentation guidelines

Plan to give a 35 minute presentation. Presentations should be self-contained, and should be clear and precise. Briefly introduce the topic including any background information, describe the investigation, development, or experimentation that was conducted, and provide any demonstrations developed as part of the project, or describe the results of the investigation or experimentation. The following format is suggested:

1. Title -- Name the project and all the team members
2. Outline -- Summarize the full presentation
3. Introduction -- Introduce the purpose and goals of the project. Provide any background material necessary to understand the presentation.
4. Investigation, development, or experimentation conducted -- Describe the methods and findings regarding your problem.
5. Results -- Show any demonstrations developed or results achieved during the project.
6. Conclusion.
7. Questions and discussion.