Final Project

Yinqian Zhang

Topic

- Theme of the project: Man-in-the-Middle attacks and defenses
  - Any project related to man-in-the-middle
    - May assume a man-in-the-middle position already
    - May leverage existing open-source projects
  - Develop a useful tool (for attackers or defenders)
  - Quality of the code: an open source project on github
  - Be creative
- Timeline
  - Mar 2: One slides presentation of the project
  - Mar 23: One slides presentation of the progress
  - Apr 20 & 23: Project presentation and demo

Example projects

- Example 1: Man-in-the-middle attacks against SSH
  - Tools that can perform a complete MITM attacks against SSH connections
    - Attack the Diffie-Hellman key exchange protocol
    - Complete control of the SSH connect: inject, modify, delete messages
  - May assume the tool is run by the network admin
  - Demo to show that SSH client can be fooled to connect to an SSH server with an adversary sitting in the middle.

Example projects (Con’t)

- Example 2: Cookie hijacking in HTTP/HTTPS traffic
  - Eavesdropping network traffic and extract cookies (and organized in a database)
  - Attack websites that support both HTTP and HTTPS and use the same authentication cookie for both
    - Steal cookies by injecting HTML tags in the HTTP stream to trigger HTTP request to the target website

Example projects (Con’t)

- Example 3: Real-world padding oracle attacks
  - Demonstrate real-world padding oracle attacks
  - For example, implement POODLE attacks against SSL v3.
  - Or, implement padding oracle attack against TLS 1.2
    - Well, this one needs to find new oracles.

Example projects (Con’t)

- Example 4: MITM defense
  - For example, how to detect MITM attacks?
    - E.g., timing
  - How to prevent MITM attacks?