CSci530: Computer Security Systems
Wireless Technologies and Implications
26 November 2003

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute

Administrative

- All proposals replied to. If you do not have a response send a follow-up message to csci530@usc.edu.
- End-of-term exam next Wednesday 9:30 AM.
- Research paper officially due the same day, but no penalty if turned in up to one week late.
- See web site for additional guidance on research paper.

What's Different

- Easy (but wrong) answer:
  - Wireless communication involves transmission of data by radio or similar means, and this allows an attacker to read the data more readily without requiring physical access to the network.
- The problem with this explanation:
  - If you have been paying attention during this course, you will likely note that we have been assuming it is easy for an attacker to intercept data anyway, even on wired networks. Good security design should assume this. Yes, it is a little easier for an attacker to eavesdrop with wireless, but there are so many other ways to get the data that wireless doesn't really change this part.

What's Different

- The real answer:
  - Wireless communications devices are often disconnected.
  - Such devices may have limited storage or limited computation abilities.
  - Such systems CAN be deployed in ways that create greater vulnerabilities if the basic protocols running on such systems have not applied confidentiality protection.
  - Such systems may be more vulnerable to jamming.
  - Such systems create a less accountable path into the network.

A False Sense of Security

- Solutions that provide encryption at the network layer or below provide a false sense of security.
  - WEP: Wired Equivalent Protocol is just that.
    - Doesn't solve the end to end problems.
    - Wires aren't that hard to tap anyway.
  - Attacks on WEP
    - Repeated IV on encryption enables recovery of the key stream.
    - Authentication reveals secret.

A False Claim of Security

- Beware of papers like the Bluetooth paper in the assigned readings.
  - These kinds of papers appear all the time, pointing to vulnerabilities in competing products or protocols and showing how their solution does not exhibit these weakness.
  - Keep in mind that weakness and vulnerabilities are usually approach specific. That an alternative doesn't exhibit the SAME vulnerabilities is not at all surprising.

Bluetooth Vulnerabilities

- Bluetooth exhibits serious vulnerabilities in its interface to the user.
  - Similar to SSL URL authentication problems.
    - i.e. that you know the name of the server you were talking to, but not that it was the right server.
  - SNARF Attack
    - Connect to device without alerting owner
  - Backdoor Attack
    - Establish trust by pairing, but remove from list of pair devices.
  - Problem is to few protection domains.
    - Connection grants access to most data on the device.

Wireless to Improve Security

- Wireless promotes less constrained reconfiguration.
  - Topology of network is not constrained by physical wires.
  - Examples in sensor nets.
    - Home burglary example
- Spread spectrum can be used as a security tool.
  - If codes secret, useful to hide communication.
  - Resistant to jamming.

Peer to Peer and Ad Hoc Security

- Security protocols may have phases independent of central infrastructure.
- Services may be provided by untrusted nodes.
- Messages need to be relayed by untrusted nodes.
- Devices may be overrun.
- Collusion is possible (Byzantine failure).

Review for Final Exam - Cryptography

- Basic Crypto
  - Transposition, Substitution
  - Mathematical
- Modes of operation
  - Block cipher ECB
  - Streams
    - CBC, CFB, OFB
  - Some systems
  - RSA, DES, 3DES, AES
  - Digital Signatures
- Key Sizes

Review for Final Exam – Authentication and Key Management

- Choosing Keys
- Authentication and Key Distribution
  - PKI
  - Kerberos
- Group Key Management

Review for Final Exam - Authorization

- Access Matrix
- Policy Models
  - Bell Lapadula, Biba, Chinese Wall
  - MAC – Mandatory Access Controls
  - Clark Wilson
  - Role Based Access Controls
  - Least Privelege
- Distributed Mechanisms
  - Proxies
  - GAA-API

Review for Final Exam - Intrusions

- Detection - how
  - Signature based
  - Anomaly based
- Detection - where
  - Network based
  - Host based
  - Application based
- Coordination of detection
- Response
- Recovery
- Forensics

Review for Final Exam - Wireless

- The real differences
  - Devices and connectivity
- Some of the benefits
  - Redundancy of communication paths
  - Autonomy
- WEP as examples of vulnerabilities
- Need for end-to-end security

Summary

- Be critical
  - Look for the vulnerabilities in systems.
    - Protocol errors.
    - Vulnerabilities in administration.
    - Incorrect assumptions about the environment.
    - Failure to meet the high level goals even if the system functions perfectly.
  - Assume that there will be failures
    - Defense in depth
    - Mitigation