Prolog to Lecture 7
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

How Can Man-in-the-Middle Attacks Really Occur?

- Man-in-the-middle attacks require an attacker to intercept and replace messages
- How can that happen in real world scenarios?
- How do attackers “lay hands” on our messages?

Active Eavesdropping

- Generally only possible on broadcast media
  - 802.11, true Ethernet, etc.
- Everyone (nearby) can hear the messages
- Often, they can forge low level addresses and identifiers

How Else Could It Happen?

- Through name translations
  - Alter translation of some name at a higher level to the wrong lower level entity
- Through routing control
  - Route network traffic through nodes under your control

ARP Poisoning

- A name translation attack
- On an Ethernet
- Alter the translation from the network to link layer
  - IP address to MAC address
- Persuade the switch to use the wrong translation

DNS Mistranslations

- Users work with user level names
  - Typically DNS names
- If attacker can alter the translation, he gets the messages
  - Which he can later forward to the real destination
- How do you fiddle a DNS translation?

DNS Attacks

- Corrupt a DNS server
  - Change entry at server to the wrong translation
- Spoof replies from a DNS server
  - Create fake reply to a legit DNS request
  - If it beats response from real server, fake one is used
  - If response cached, it persists
    - DNS cache poisoning

Routing Attacks

- Generally, BGP routing changes not well authenticated
  - Several cases of bogus requests resulting in traffic diversion
  - In 2010, China "accidentally" diverted much US traffic
- Attacks based on direct source addressing

Direct Source Addressing Attacks

- Attacker provides a direct source address to a target
  - Spoofing someone else's source address
  - But including attacker's real address in the source routing
- Responses will probably go through attacker
- Allowing him to be in the middle

The General Issue

- There are network paths at multiple levels
- If attacker can divert any of them through him, he might get in the middle
- New technologies might open new possibilities