Advanced Unix System Administration

Lecture 17
April 4, 2007

Steven Luo
<sluo+decal@OCF.Berkeley.EDU>

Some Network Attacks

- A good lot of what's on for today's networks was designed in the 1970s and 1980s for trusted networks
- This has unfortunate consequences for those of us working on a hostile Internet in the 21st century
  - Difficult to fix some of these problems without breaking backwards compatibility
  - Other problems can be fixed, but the fixes look fairly ugly

Some Network Attacks

- Host-spoofing attacks
  - Various techniques, but the idea is always the same: pretend to be someone else on the network
  - If the remote service grants access based on the identity of the host, might be able to do damage
- Man-in-the-middle attacks
  - Read/modify traffic going in between hosts
  - Can be done as a router, or with a two-way host spoofing attack

Some Network Attacks

- Promiscuous mode
  - Normally, an Ethernet adapter only reads traffic destined to its MAC address
  - In promiscuous mode, the adapter reads all traffic regardless of MAC address
    - On unswitched and wireless networks, this is all traffic!

Some Network Attacks

- ARP cache poisoning attack
  - Recall that hosts make an ARP announcement broadcast when they plug into the network
  - By broadcasting a fake ARP announcement, we might be able to get a host to “update” its ARP cache with bad values
  - We then (hopefully) get all traffic for this IP
  - This works on switched networks too

Some Network Attacks

- TCP initial sequence prediction
  - Recall the TCP three-way handshake: client SYN (with client ISN), server SYN/ACK (with server ISN, acknowledging client ISN), client ACK (acknowledging server ISN)
  - If the client can predict the server's ISN, it doesn't need to receive the server's SYN/ACK to be able to complete this connection sequence
  - This allows us to spoof being another host
  - See RFC 1948 for the classic solution

Some Network Attacks

- SYN flood
  - To be able to finish the three-way handshake, a host (conventionally) needs to store state for each SYN it receives
  - This “SYN queue” can't be allowed to grow without bound
  - By filling up a host's SYN queue, we can prevent it from taking further TCP connections
    - This requires a much smaller number of packets than a straight flood
  - Classic solution: TCP syncookies

Some Network Attacks

- DNS cache poisoning
  - A few different ways of introducing bad entries:
    - We may be able to spoof a response from a recursive lookup
    - We could also return a fake NS record for the target domain's nameserver when the server looks up something from us
  - This bad entry then lives in the cache for the specified TTL
  - Impact similar to the ARP cache poisoning attack, except at a different layer

Some Network Attacks

- Morals of the story
  - You **cannot** trust information you receive from the network without some verification!
  - You **cannot** trust the identity of the host you're talking to without some form of higher-layer authentication!
  - You don't want to allocate resources based on the initial stages of a connection
  - Segmenting your physical networks is a good idea