Advanced Unix System Administration

Lecture 19
April 28, 2008

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

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