Network Attacks and Defenses

Tuesday, November 25, 2008
Sources: Skoudis, CounterHack; S&M Chapter 5 (including many images)

CS342 Computer Security
Department of Computer Science
Wellesley College

Networks Complicate Security

Smith and Marchesini, p. 96:

If we go back and think of the OS as a collection of states, we see some interesting properties emerge when the network becomes part of the OS. Without the network, the typical OS state space and the avenues for interacting with it are quite large. Adding users and applications to the systems increases the state and interaction space, as both interact with the OS (e.g., via syscalls). Accordingly, most OSes put much effort into authentication and authorization so that users and applications can only affect the OS's state space in a well-defined manner; of course, this is not always successful.

However, adding the network to the OS explodes things. Any packet coming from any other entity must be processed by the receiving OS. Anyone on the network becomes a potential requester of OS services; any service the OS offers over the net is offered potentially to the whole world; any flaw in any API or implementation is exposed to the whole world. The network gives attackers the ability to remotely affect the target OS's state, either by causing unexpected transitions or by injecting new states. This "feature" of computer networks is what has traditionally made them the medium that attackers rely on to get into a victim machine (we discuss this in Section 5.3).
Attack Phases

1. **Reconnaissance:** learn about target system
2. **Scan:** “rattle doorknobs”, looking for opening
3. **Gain Access**
4. **Maintain Access**
5. **Covering Tracks and Hiding**

Reconnaissance

Ways for attacker to learn about the target organization/system:

- social engineering
- dumpster diving
- physical break-in
- search the fine web (STFW)
- social networking sites, blogs, etc.
- whois databases
- DNS
Scanning

Goals of scanning:
• network topology of target system
• OSs used by target system
• which ports/services running on individual machines

Techniques:
• send TCP/UDP packets to standard port numbers to see if active
• banner grabbing from active ports
• TCP stack fingerprinting to deduce target machine OS
• search for application-level remote procedure calls (RPC) on target
• ping sweeping/traceroute to determine network topology
• nmap and other high-level tools automate some steps

Scanning Defense: Disabling & Firewalls

Disable nonessential services/ports especially ones with known problems (e.g. FTP, Telnet)

Use firewall on individual machines and/or network border to filter undesirable packets.

Some firewalls can perform state-based packet filtering
Scanning Defense: Subnets and DMZs

Bad idea to depend only on firewall at network boundary. Provide defense in depth by decomposing internal network into subnets.

Put publicly accessible Web servers in a demilitarized zone (DMZ) outside firewall.

Scanning Defense: Other Approaches

Vulnerability scanners: scan own system with tools like SARA, SAINT, VLAD the Scanner, Nessus.

Intrusion detection systems (IDS): tools like Snort can match real-time network traffic against signatures = known attack patterns.

Problems:
- Arms race between attackers and targets
- Attacker triggers false attack detected by IDS, and then launches real attack.
- Clever use of IP fragmenting can evade IDS.
- Packet flooding can overwhelm IDS

Host-based intrusion prevention systems (HIPS): IDS on end host that can analyze and block traffic in real time.

Honeypots: Distract attackers (and learn about their attacks) with unsecured decoys.
Bad idea to depend only on firewall at network boundary. Provide defense in depth by decomposing internal network into subnets.

Put publicly accessible Web servers in a demilitarized zone (DMZ) outside firewall.

Scanning for Access Points

Old days: war dialing to find modems connected to intranet networks

Today: war driving to find unsecured access points, especially rogue access points connected to organization intranet
**War Driving**

**War Driving in Wellesley**

Outfitted with a Sony Viao, a Lucent Orinoco wireless network, a MaxRad antenna, and Netstumbler software, we jumped into a car with the antenna on the roof and were on our way to find some networks.

<table>
<thead>
<tr>
<th>Default SSIDs</th>
<th>31 of 55</th>
<th>56.4%</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP disabled</td>
<td>41 of 55</td>
<td>74.5%</td>
</tr>
</tbody>
</table>

**World Wide War Drive**

<table>
<thead>
<tr>
<th></th>
<th>2001</th>
<th>2002</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP Disabled</td>
<td>69.86%</td>
<td>72.87%</td>
<td>+2.21%</td>
</tr>
<tr>
<td>SSIDs Default</td>
<td>29.53%</td>
<td>35.24%</td>
<td>+5.71%</td>
</tr>
<tr>
<td>WEP Disabled AND SSID Default</td>
<td>26.64%</td>
<td>31.44%</td>
<td>+4.8</td>
</tr>
</tbody>
</table>

**Wireless Protection**

Require supplicant to authenticate by MAC address and/or password (but MAC addresses can be spoofed).

Put wireless access points outside organization firewall.
Gaining Access

- Implementation attacks: buffer overflow, printf exploits, etc.
- Password attacks
- Application attacks
- Sniffing attacks - tools like Wireshark allow sniffing traffic, which can find usernames/passwords, especially on unsecured wireless networks.

Wireless Sniffing in a Hotel

Wireless access points in public places are often unsecured.

Figure 5.13 Wireless sniffing in a hotel room at a conference revealed much interesting traffic, including this packet. The user whose session we sniffer was also doing employment-related browsing; it would not have been difficult to determine the user's identity.
Wireless Sniffing in a Dormitory

Even though many dorm rooms have wired internet access, students prefer the convenience of wireless access. But this is often much less secure!

Sniffing Defense

Wired world:
- Use switches rather than hubs. But still problems
  - MAC flooding
  - ARP cache poisoning
- Encrypt traffic - e.g. SSH, SSL/TLS, etc.

Wireless world:
- Encrypt traffic
  - Wired Equivalent Privacy (WEP) is easily crackable
  - Wi-Fi Protected Access (WPA) is much stronger
**Maintaining Access**

- Backdoors
- Trojan horses
- Keyloggers
- Rootkits

More coverage in malware lecture (next), individual presentations.

**Covering Tracks and Hiding**

Alter event logs & history files.

Defenses:
- set proper file permissions
- append-only log files
- redirect logs to separate logging server
- encrypt log files
- write-once log media

Create obscure/hidden files

Defense: integrity-checking tools (e.g. Tripwire)

Covert channels for communicating with cracked system:
- squirrel information away in protocols
- steganography