Security issues in networks

- What is security in context of networks?
- What are potential attacks?
- What can an attacker gain?
Security principles

- **Confidentiality**
  - Content is hidden
- **Authentication**
  - Source is verified
- **Message integrity and non-repudiation**
  - Message is unchanged and undeniable
- **Availability and access control**
  - Legitimate users should have access
- **Today:** availability; next lecture: “CIA triad”

Attack types

- **Classification of attacks by target:**
  
<table>
<thead>
<tr>
<th>Attack target</th>
<th>Goal of attack</th>
<th>Attack examples</th>
<th>Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-system</td>
<td>Data access and modification</td>
<td>Hacking, phishing, espionage, etc.</td>
<td>Virus scanner, firewall, network intrusion detection system, etc.</td>
</tr>
<tr>
<td>Control plane</td>
<td>Denial-of-service</td>
<td>Denial-of-service attack via botnets, etc.</td>
<td>Secure routing protocols (e.g., DNSSEC), etc.</td>
</tr>
<tr>
<td>Data plane</td>
<td>Data access and modification</td>
<td>Malicious DNS announcement, DNS cache poisoning, etc.</td>
<td>Secure DNS (DNSSEC), etc.</td>
</tr>
<tr>
<td></td>
<td>Denial-of-service</td>
<td>DNS recursion attack, etc.</td>
<td>Secure SNI protocol, etc.</td>
</tr>
<tr>
<td></td>
<td>Data access and modification</td>
<td>Eavesdropping, man-in-the-middle attack, etc.</td>
<td>Processing monitors, etc.</td>
</tr>
<tr>
<td></td>
<td>Denial-of-service</td>
<td>Exploit of vulnerable packet processing code</td>
<td></td>
</tr>
</tbody>
</table>
End system attacks

- End-system intrusion
  - Exploit software vulnerabilities to gain access
  - Steal data or control system to launch attacks
- Denial of service
  - Overwhelm system with traffic
- Defenses
  - Firewalls
  - Intrusion detection systems

Control plane attacks

- Mapping
  - Analysis of target domain (network topology, contact info)
    Tools: ping, traceroute, port scanners
- Hijacking of connections
  - Eavesdrop on connection state
  - DoS attack on one side
  - Spoof towards other side
- DNS attacks
  - DoS attack on root server
Control plane attacks

1 March 2007

Factsheet
Root server attack on 6 February 2007

Executive summary
- The Internet sustained a significant distributed denial of service attack, originating from the Asia-Pacific region, that lasted up to 8 hours.
- Six of the 13 root servers that form the foundation of the Internet were affected, two briefly. The two worst affected were located in a country that does not have any Reserved Technology status.
- The attackers highlighted the vulnerability of the Internet’s root name system technology.
- The attack was halted before full impact was realized.
- Full server operation resumed from backup data files.
- Root zone operation was restored.

On 6 February 2007, starting at 13:00 (UTC 16:00 PST), for approximately two and a half hours, the system that underpins the Internet (root server attack). Within a half-hour after the attack stopped, a second attack, this time lasting five hours, began.

Fortunately, thanks to the determined efforts of engineers across the globe and a new technology developed and implemented after the last DNS attack of this type, on 21 October 2002, the attack had a very limited impact on actual Internet users.

This factsheet provides the most important details of the attack and briefly explains how the domain name system works and the systems in place to protect it. It also outlines how such attacks are possible and discusses possible solutions to future attacks.

What happened?

The root DNS servers of the Internet were targeted at a significant distributed denial of service attack (DDoS). In such an attack, filtered network data packets are repeatedly sent towards a network in order to overwhelm them with requests and to disrupt the smooth running of the Internet.

The Internet works by splitting up information into very small packets, and...
Denial of Service attacks

- Denial of service (DoS) attack
  - SYN flooding
    - TCP state exhaustion
  - Smurf attack
    - ICMP echo request converge on single host
  - Distributed DoS (DDoS) attacks
    - Large number of hosts attack single node
    - Much better scalability of attack
    - Often based on botnets

Botnets

- Geographic distribution of botnets
DoS attack for economic gain

PC World: Web of Crime
August 22, 2005

“We were getting a lot of panic attacks from our customers saying they were under attack and they were being held for ransom and could we help them,” Quintana says. Prolexic, a company founded in 2003 that protects businesses against DDoS attacks, repels at least one major version every week, according to chief technical officer Barrett Lyon. Of those, slightly less than half involve one business attacking a competitor, as happened to Export Satellite, he says. Most of the rest are extortion attempts, where a criminal may threaten a DDoS attack unless a company pays protection money (as much as $250,000). Very few attacks occur without financial motivation, Lyon says.

Saad Echouafni, head of a satellite communications company, is wanted in Los Angeles, California for allegedly hiring computer hackers to launch attacks against his company’s competitors. On August 29, 2006, Echouafni was indicted by a federal grand jury in Los Angeles in connection with the first successful investigation of a large-scale distributed denial of service attack (DDoS) used for a commercial purpose in the United States. In a

DoS attack as cyber warfare

The New Front Line
Estonia under Cyberassault

Estonia and its neighbors today face large and growing threats to...
Network attacks

- Internet is based on “on-by-default” principle
  - Any node can send traffic to any other node
- Open approach is good for cooperative environment
  - Difficult to deal with malicious users
- Some network attacks can be solved with crypto
  - Confidentiality, integrity, authentication in protocols
- Availability of resources still an open problem
  - New network architectures aim to address security at core