ISP Security

Michael Behringer <mbehring@cisco.com>
The Internet Today

• NetAid’s October 9th Event

  System architecture:
  - for 60 million hits per hour
  - just over 16,000 transactions per second
  - to support 50,000,000 users over a multi-day event

Consistent probes and attacks!!
What do ISPs need to do?

• Protect themselves
• Help protect their customers from the Internet
• Protect the Internet from their customers
ISP Security
- Agenda -

• Hacking and Attacks
  ... what the bad guys do

• Network Element Security
  ... routers, switches, etc.

• Network Security
  ... design, routing, filtering, etc.

• Incident Handling
  ... working with customers, other ISPs, CERTs, etc.
Hacking and Attacks
## Types of Attacks

<table>
<thead>
<tr>
<th></th>
<th>Gets Access</th>
<th>Gets no Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authorised User</strong></td>
<td>✔</td>
<td>DoS</td>
</tr>
<tr>
<td><strong>Unauthorised User</strong></td>
<td>Intrusion</td>
<td>✔</td>
</tr>
</tbody>
</table>

• **Location of Attacks: Layer 1 - 7**
Network Element Security
Network Element Security

• No unnecessary services
• Secure Access (IPsec, SSH, OOB)
• AAA on device
• Secure management (SNMP, syslog, TFTP server, ...)
• Site security
Network Security
Network Security

- Packet filtering / RPF
- Routing:
  - prefix / prefix length / AS path filtering
  - peer authentication (!)
  - dampening
- Redundancy (for availability)
- Netflow, syslog, SNMP, security audit
- Rate limiting: ICMP, maybe UDP
- Secure Management / Site Security
Incident Handling
How an ISP Detects an Incident

• Technical:
  - Intrusion Detection Systems
  - Network monitoring
  - syslogs, SNMP, netflow, ...
  - (plus evaluation s/w)

• Non-Technical
  - Alert from customer / ISP / 3rd party
  - Alert from a CERT
What To Do in an Incident

- Alarm (customers, ISPs, CERTs, …)
- Block the attack (if possible)
  Access lists, CAR, IDS
- Trace the attacker
  routing, syslog, netflow
- Notify authorities, gather evidence
Wrap Up and Summary
There is no 100% Security

“"The first day of summer vacations is the best example for a DDoS attack against the highway system"