Introduction to Computer & Networking Security

Dr. Guofei Gu
http://faculty.cse.tamu.edu/guofei/
Some Bedtime Stories

Denial of Service
Estonia recovers from massive denial-of-service attack


A spree of denial-of-service (DDoS) attacks against Web sites in Estonia appears to be subsiding, as the government calls for greater response mechanisms to cyber attacks within the European Union.

The attacks, which started around April 27, have crippled Web sites for Estonia’s prime minister, banks, and less-trafficked sites run by small schools, said Hilar Aarelaid, CTO for Estonia’s Computer Emergency Response Team (CERT), on Thursday. But most of the affected Web sites have been able to restore service.

“Yes, it’s a serious problem, but we are up and running,” Aarelaid said.

Aarelaid said analysts have found postings on Web sites indicating Russian hackers may be involved in the attacks. However, analysis of the malicious traffic shows that computers from the United States, Canada, Brazil, Vietnam and others have been used in the attacks, he said.
Your YouTube Traffic: Pwned!

Insecure routing redirects YouTube to Pakistan
By @itsch van Beinum | Published: February 25, 2008 - 03:31AM CT

On Sunday, YouTube became unreachable from most, if not all, of the Internet. No "sorry we're down" or cutey kitten with screwdriver page, nothing. What happened was that packets sent to YouTube were flowing to Pakistan. Which was curious, because the Pakistan government had just instituted a ban on the popular video sharing site. What apparently happened is that Pakistan Telecom routed the address block that YouTube's servers are into a "black hole" as a simple measure to filter access to the service. However, this routing information escaped from Pakistan Telecom to its ISP PCCW in Hong Kong, which propagated the route to the rest of the world. So any packets for YouTube would end up in Pakistan Telecom's black hole instead.

On the North American Network Operators Group (NANOG) mailing list, where many engineers in charge of Internet routing hang out, the consensus is that this was an accident. Only one or two people suggest that it may be a malicious act, possibly a trial of something bigger. So why was this incident so devastating to YouTube's reachability?

Attack on BGP Routing

- August 2008
- “Man-in-the-middle” attack
Phishing

• Spam: 95+% of all email traffic on the Internet (200 billion spam messages per day, as of January 2009)

• Unique phishing attacks rose 13% (to over 28k!) in for second quarter 2008

• 294 hijacked brands

• 442 unique malicious application variants in May 2008

Malware

Spyware:
It's not what every well-dressed spy is wearing
More…

- “Attack of the tweets: Major Twitter Flaw Exposed” – UK researcher says vulnerability in Twitter API lets an attacker take over a victim’s account – with a tweet. Aug 27, 2009 [Darkreading]
- Conficker worm:
Botnet – New Rising Threat
Sea-Change in Internet Attacks

- Computers on the Internet used to be *mere targets*
  - For fun and fame

- Now they are *Resources/Platforms*
  - For profit

- How big is the problem now?

---

**Top 5 Super Computer**

- June 2008 survey of super computers from [http://www.top500.org/list/2008/06/100](http://www.top500.org/list/2008/06/100)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Site</th>
<th>Computer/Year</th>
<th>Vendor</th>
<th>Cores</th>
<th>Rmax</th>
<th>Rpeak</th>
<th>Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DOE/NASALALHL United States</td>
<td>Roadrunner - Brookhaven National Laboratory Cluster Opteron 2.4 GHz, PowerPC 970 Extreme, 2004.5</td>
<td>IBM</td>
<td>12264</td>
<td>1026.00</td>
<td>1376.78</td>
<td>2346.50</td>
</tr>
<tr>
<td>2</td>
<td>DOE/NASALALHL United States</td>
<td>BlueGene/L - eServer Blue Gene Solution / IBM</td>
<td>IBM</td>
<td>212892</td>
<td>479.20</td>
<td>595.38</td>
<td>2329.60</td>
</tr>
<tr>
<td>3</td>
<td>Argonne National Laboratory United States</td>
<td>BlueGene/P - Blue Gene Solution / IBM</td>
<td>IBM</td>
<td>163340</td>
<td>459.30</td>
<td>557.95</td>
<td>1260.00</td>
</tr>
<tr>
<td>4</td>
<td>Texas Advanced Computing Center/UI of Texas United States</td>
<td>Ranger - SunBlade x8420, Opteron Cluster 2GHz, Infiniband 2008</td>
<td>Sun Microsystems</td>
<td>52076</td>
<td>325.00</td>
<td>503.81</td>
<td>2000.00</td>
</tr>
<tr>
<td>5</td>
<td>DOE/NASALALHL United States</td>
<td>Jaguar - Cray XT4 Clusters 2.1 GHz / Cray Inc.</td>
<td>Cray Inc.</td>
<td>30076</td>
<td>205.00</td>
<td>260.20</td>
<td>1680.71</td>
</tr>
</tbody>
</table>
Storm Worm for Comparison

- “…the Storm cluster has the equivalent of one to 10 million 2.8 GHz Pentium 4 processors with one to 10 million petabytes worth of RAM. ... To put the size of a petabyte into perspective, Google, as of Aug. 2007, uses between 20 and 200 petabytes of disk space, according to Wikipedia.com. In comparison, Gutmann said, BlueGene/L currently contains 128,000 computer processor cores, and has a paltry 32 terabytes of RAM. A terabyte is about 1,000 times smaller than a petabyte.”


What is Storm?

- A malware instance, more precisely, a botnet
- Using P2P techniques for its C&C channels
- Mainly used to send spam

- We are lucky because Storm is mainly used for sending spam…
Botnets: Current Single largest Internet Threat

- “Attack of zombie computers is growing threat”  
  (New York Times)
- “Why we are losing the botnet battle”  
  (Network World)
- “Botnet could eat the internet”  
  (Silicon.com)
- “25% of Internet PCs are part of a botnet”  
  (Vint Cerf)

What are Bots/Botnets?

- Bot (Zombie)
  - Compromised computer controlled by botcode (malware) without owner consent/knowledge
  - Professionally written; self-propagating
- Botnets (Bot Armies): Networks of bots controlled by criminals
  - Definition: “A coordinated group of malware instances that are controlled via C&C channels”.
  - Architectures: centralized (e.g., IRC, HTTP), distributed (e.g., P2P)
  - Key platform for fraud and other for-profit exploits
Botnet Epidemic

- More than 95% of all spam
- All distributed denial of service (DDoS) attacks
- Click fraud
- Phishing & pharming attacks
- Key logging & data/identity theft
- Distributing other malware, e.g., spyware
- Anonymized terrorist & criminal communication

Number of Bots Are Increasing!

Source: shadowserver.org, 2008
Internet Security: Broken Assumptions

• Internet infrastructure (e.g., DNS, BGP) is trustworthy
  – DNS is more vulnerable than you think …
• Computers are secure when using up-to-date AV tools and firewall
  – Not really
• Attackers are for fun and fame
  – Profit, profit, profit!
• Attackers have limited/bounded computing power
  – They have almost unbounded(?) power
• Attacks from isolated computers
  – The network is attacking you

• Where are we? Any hope to win this game?

AV industry in 1998

AV industry in 2008
What is Security?

• [Informally] Security is the prevention of certain types of intentional actions from occurring
  
  – These potential actions are threats
  – Threats that are carried out are attacks
  – Intentional attacks are carried out by an attacker
  – Objects of attacks are assets
Security: Definition

- **Security** is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable.

- Security rests on confidentiality, authenticity, integrity, and availability.

Basic Components

- **Confidentiality** is the concealment of information or resources
  - Keeping data and resources hidden. Privacy.

- **Authenticity** is the identification and assurance of the origin of information.

- **Integrity** refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes
  - Preventing unauthorized changes to data or resources.

- **Availability** refers to the ability to use the information or resource desired
  - Enabling access to data and resources.
Security Threats and Attacks

- A threat is a *potential* violation of security
  - Flaws in design, implementation, and operation

- An attack is any *action* that violates security
  - Active vs. passive attacks

Vulnerabilities (Attack Vectors)

- A vulnerability is a systematic artifact that exposes the user, data, or system to a threat
  - E.g., buffer-overflow, WEP key leakage

- What is the source of a vulnerability?
  - Bad software (or hardware)
  - Bad design, requirements
  - Bad policy/configuration
  - System Misuse
  - Unintended purpose or environment
    - E.g., student IDs for liquor store
Eavesdropping - Message Interception (Attack on Confidentiality)

- Unauthorized access to information
- Packet sniffers and wiretappers
- Illicit copying of files and programs

Full Packet Capture (Passive)

Example: OC3Mon

- Rack-mounted PC
- Optical splitter
- Data Acquisition and Generation (DAG) card

Source: endace.com
Eavesdropping Attack: Example

- tcpdump with promiscuous network interface
  - On a switched network, what can you see?

- What might the following traffic types reveal about communications?
  - DNS lookups (and replies)
  - IP packets without payloads (headers only)
  - Payloads

Integrity Attack - Tampering

- Stop the flow of the message
- Delay and optionally modify the message
- Release the message again

Diagram:

A -> B
Perpetrator
Authenticity Attack - Fabrication

- Unauthorized assumption of other’s identity
- Generate and distribute objects under this identity

Masquerader: from A

Man-In-The-Middle: Example

- Passive tapping
  - Listen to communication without altering contents.
- Active wire tapping
  - Modify data being transmitted
  - Example:

User

Intruder

Server

Intruder takes over identity of user (masquerading)
Attack on Availability

- Destroy hardware (cutting fiber) or software
- Modify software in a subtle way (alias commands)
- Corrupt packets in transit

Blatant *denial of service* (DoS):
- Crashing the server
- Overwhelm the server (use up its resource)

Goals of Security

**Prevention**
- Prevent attackers from violating security policy

**Detection**
- Detect attackers’ violation of security policy

**Recovery**
- Stop attack, assess and repair damage

**Survivability**
- Continue to function correctly even if attack succeeds
My Overall Research Problems

• How to make our computer, network, and Internet more secure?

Prevent  Detect  React/
Survive

Security principles: Defense–in-Depth, layered mechanisms

Interested? Want to know more?

• Consider taking CSCE 465 “Computer & Network Security” next spring that I’ll teach.