Agenda

- The rest of the semester: network security
- Focus on 3 major problems (inter-related)
  - Distributed Denial of Service (DDoS)
  - Buffer-Overflow
  - Worms

What is Denial of Service?

- Technically
  - DoS attack occurs when the attacker tries to prevent legitimate users from using a service by overflowing some resource(s) (CPU cycles, memory, bandwidth, ...) at the target
  - DDoS is DoS from multiple sources
- What's an example of DoS in everyday's life?
- What's an example of DDoS in everyday's life?

A Selective History of (D)DoS Attacks (1)

- **1996**: first appearance of SYN-flooding attacks
- **1997**: large DoS on IRC networks
  - Tools: *teardrop, boink, bonk* (attack Windows)
  - Undernet's IRC servers taken down by a Romanian teenage with SYN-flooding
  - Other attacks took advantage of TCP/IP implementation bugs (in fragmentation/defragmentation)
  - *Smurf attacks* (also called *reflection attack*) started to appear. Idea: bounce packets off various networks toward the target
- **1998**: tools for OS fingerprinting started to appear

A Selective History of (D)DoS Attacks (2)

- **1999**: first large scale use of new DoS tools
  - Trinoo, Tribe Flood Network (TFN, TFN2K), Stacheldraht, Shaft
  - Newer versions of these are still in use today
  - Targets were mostly IRC servers or clients
  - U. of Minnesota's IRC server attacked with a DDoS [tons of UDP packets with 2-byte payload from about 4000 hosts], network unavailable for almost 3 days (*I was at U of M at the time!*)
  - CERT organized a workshop in response, resulted in a very important report
  - Remember, this was near Y2K, lots of panicked people

A Selective History of (D)DoS Attacks (3)

- **2000**: many attacks on famous servers and networks
  - Jan 18, 2000: ISP Oz.Net in Seattle got hit with a Smurf
  - Feb 2000: eBay, Yahoo, E*Trade, Buy.com, Amazon.com, Excite.com, CNN all hit by another Smurf attack
  - Even FBI's own website got hit by a DDoS in Feb
- **2001**:
  - futuresite.register.com hit by a reflection attack from DNS servers around the world, this lasted for about a week
  - Microsoft got hit a few times, some unsuccessfully
- **2002**: all 13 DNS root servers were attacked for only an hour (then it stopped by itself)

A Selective History of (D)DoS Attacks (4)

- **2003**:
  - Spammers went distributed, started attacking anti-spam websites
  - Some attacks were made with extortion in mind
  - During Iraq war, Al Jazeera's website was hit, their DNS name was hijacked and redirected to a pro-American website
  - SCO's website hit (after its legal action against Linux)
- 2004:
  - Agobot and Phatbot became popular

Basic DDoS Attack Strategy

- From attacker's machine:
  - Need IP spoofing
  - Need very powerful machine & huge bandwidth
- DDoS
  - Probably still want IP spoofing
  - Recruit a large number of agent (slave) machines
  - Infect the slave machines with attack code (can be fully automated)
  - Run attack codes

A Taxonomy of DDoS Attacks

Can be classified from multiple perspectives [Mirkovic, Martin, Reiher – SIGCOMM 2004]

- Degree of automation
- Exploited vulnerability
- Attack rate dynamics
- Impact

1. Degree of Automation

- Manual: these are old, primitive
- Semi-automatic:
  - Automatic scripts to compromise slave machines
  - Manually indicate a target and run attack codes
  - *Attacks with direct communications*: slave and handler machines communicate directly during attacks (hard-coded IP addresses in malicious codes)
  - *Attacks with indirect communications*: one or two levels of indirect communication to collaborate the attack, e.g. communications done via IRC channels which are somewhat anonymous
- Automatic: time & target pre-programmed, no need for communication to trigger

Scanning and Propagation Mechanisms

- To (semi-) automatically *recruit* slave machines, attack code often needs to do scanning and propagating
- Scanning: to identify potential slaves
  - Strategies: random (Code Red), hit list, topological (all email worms), permutation (not yet deployed), local-subnet (Code Red II and Nimda)
- Propagation mechanism
  - Central source propagation (li0n worm)
  - Back-chaining propagation (Ramen, Morris worms)
  - Autonomous propagation (Code Red, Warhol, and most email worms)

2. Exploited Vulnerability

- Brute-force attacks
  - Filterable: ICMP Smurf, UDP flood
  - Non-filterable: HTTP request flood, DNS request flood
- Protocol attacks
  - SYN-flood
  - CGI request attack: consume CPU time by issuing multiple CGI requests
  - Authentication server attack: authenticating takes much longer than generating a bogus signature

3. Attack Rate Dynamics

- Continuous rate
- Variable rate – makes detection harder
  - Increasing rate
  - Fluctuating rate

4. Impact

- Disruptive attacks
  - Completely deny the victim's service
- Degrading attacks
  - Consume some portion of the victim's resource
  - It could remain undetected for a long period of time (Think about the economics involved)

A Taxonomy of DDoS Defense Mechanisms

Classification can be done by

- Activity level
- Deployment location

1. Deployment Location

- Victim-Network
  - Resource accounting
  - Protocol security
- Intermediate Networks
  - Intermediate networks provide infrastructural service to a large number of hosts; victims contact service for protection and/or compensation
  - E.g., push-back and trace-back techniques
- Source-Network
  - Prevent the network from generating the attack
  - Low level of motivation for deployment

2. Activity Level - Preventive

- Attack prevention
  - System security: anti-virus, software patches, firewalls, access lists, capability-based systems, ...
  - Protocol security: design better protocols
- DoS prevention
  - Resource accounting: avoid identity theft, provide legitimate users with fair services, ...
  - Resource multiplication: over-provision resources (multiple servers, more bandwidth, ...)

2. Activity Level – Reactive

- Detection strategy
  - Pattern attack detection: signature-based
  - Anomaly attack detection: track system usage for anomalies, often suffered from false positives vs. false negatives problem
  - Hybrid attack detection: pattern + anomaly
  - Third party attack detection: trace-back mechanisms
- Response strategy
  - Slave identification: trace-back techniques
  - Rate-limiting: limit rate on detected stream
  - Filtering: completely filter out the bad stream
  - Reconfiguration: reconfigure the victim's network or intermediate networks (say – overlay networks)

2. Activity Level – Cooperation Level

- Autonomous
  - Independent attack detection and response (firewall, IDS)
- Cooperative
  - Can operate autonomously, but can improve performance with cooperation
  - Cooperate with other entities for detection & response (e.g., push-back mechanism)
- Interdependent
  - Require full cooperation of other entities (e.g., trace-back technique)