

Distributed Denial of Service

Dr. Arjan Durrezi
Louisiana State University
Baton Rouge, LA 70810
Durrezi@Csc.LSU.Edu

These slides are available at:

http://www.csc.lsu.edu/~durrezi/CSC7502_04/



- ❑ The DoS project's trinoo distributed denial of service attack tool, by David Dittrich
- ❑ A Framework for Classifying Denial of Service Attacks, by Alefiya Hussain, John Heidemann, and Christos Papadopoulos, SIGCOM 2003

DDoS

- ❑ The goal of a denial of service attack is to deny legitimate users access to a particular resource.
- ❑ An incident is considered an attack if a malicious user intentionally disrupts service to a computer or network resource.
- ❑ Resource exhaustion

Resource Exhaustion

- ❑ Disk Space
- ❑ CPU Cycles
- ❑ Memory
- ❑ Network Bandwidth
- ❑ Application Resources
 - TCP Stack
 - Web Connections

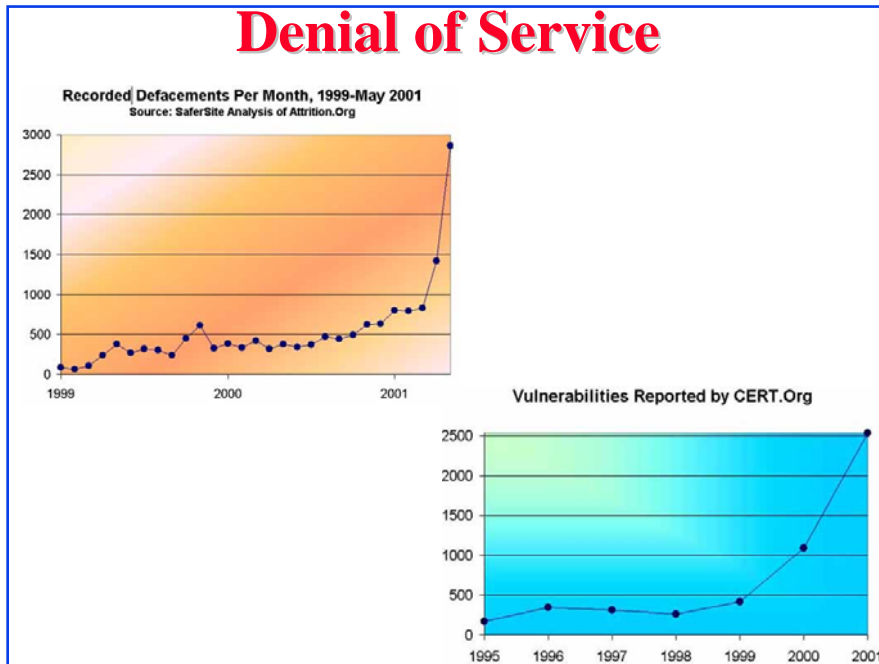
What's the Harm?

- ❑ Financial loss can be difficult to estimate
 - Lost business
 - Bad publicity and damaged reputation
- ❑ 2002 CSI/FBI Survey
 - 40% of reported attacks are DOS
 - Average cost per attack is >\$1 million
- ❑ Distributed DOS attacks (February 2000)
 - Amazon, CNN, E-Trade, eBay, etc...
 - Estimated losses were “several millions to billions of dollars”
- ❑ DOS can also be used to cover-up “real” attacks
- ❑ Nations critical infrastructure is also at risk

DDoS

- ❑ Denial of Service in pervasive networks
 - Power-draining attacks
 - Bandwidth-usage attacks
 - CPU-usage attack

Denial of Service



Why are DOS attacks possible?

- ❑ IP employs an open architecture
 - No authentication of sender's IP address
 - Easy to forge any address, hard to detect offender
 - IP traceback, ingress/egress filters (later)
- ❑ No resource regulation in the network
 - Employ QOS techniques to mitigate impact (later)

Denial of Service Attacks

- ❑ Most involve either resource exhaustion or corruption of the operating system runtime environment.
- ❑ UDP bombing
- ❑ tcp SYN flooding
- ❑ ping of death
- ❑ smurf attack

Types of attacks

- ❑ ping of death: network flood, single very large ping packet, or a flood of large or small ping packets
- ❑ smurf attack: amplified network flood, exploits ICMP and broadcats, pings with faked return address (broadcast address)
- ❑ syn flood: overload the machine instead of the network, exploit connection establishment in TCP

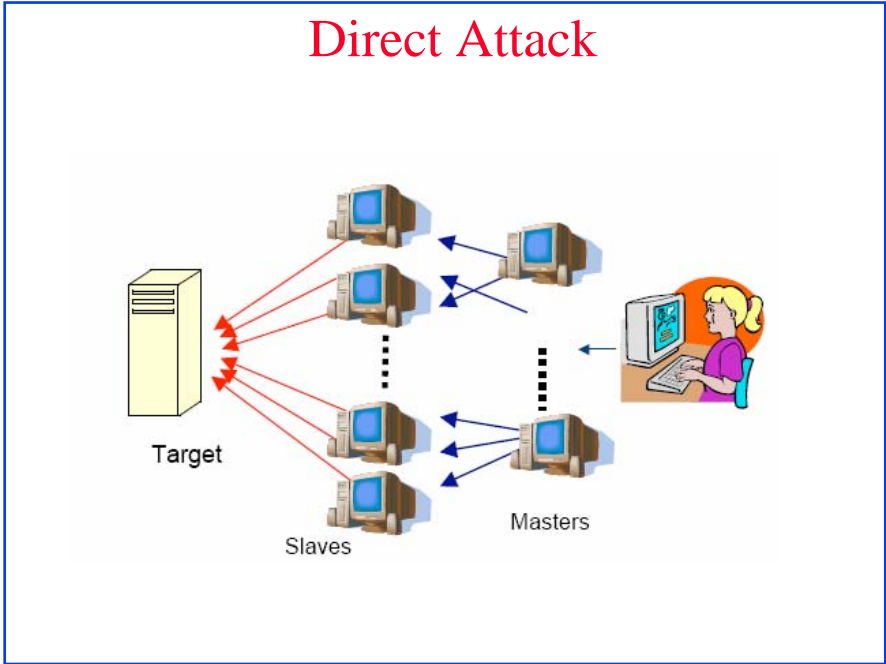
DDoS

- ❑ Exploit protocols vulnerabilities: TCP SYN, ICMP, etc.
- ❑ Flooding-based attacks
 - Single-source attacks
 - Multiple-source attacks
 - Reflector attacks (particular case of multiple-source attacks)

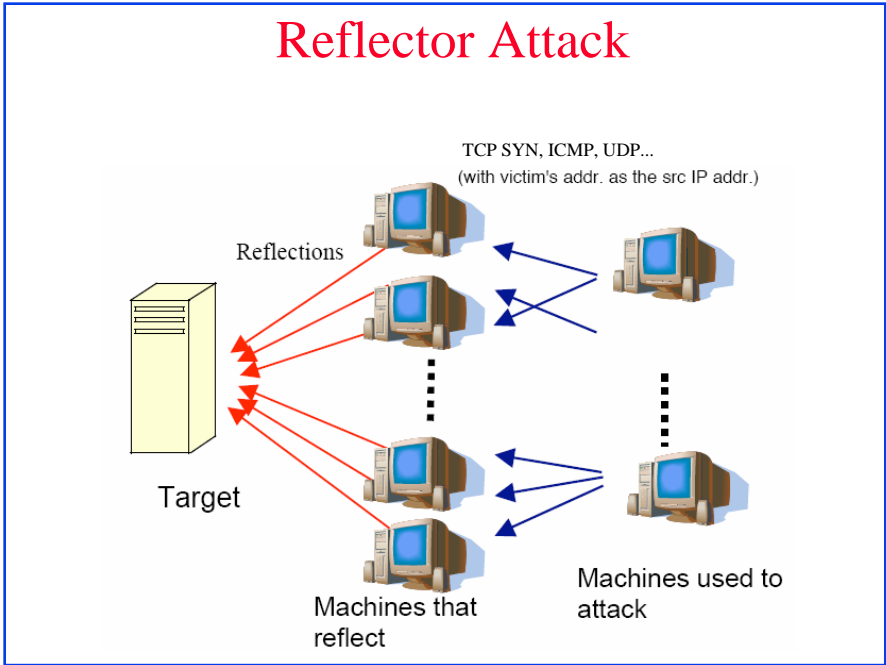
DDoS Tools

- ❑ DDoS: MORE POWERFUL, distributed attack, employs a combination of attacks, can attack one machine or more
- ❑ Examples:
 - Trin00, UDP
 - Tribe Flood Network, (TFN)UDP, ICMP, SYN, Smurf
 - Stacheldrucht, UDP, ICMP, SYN, Smurf
 - TFN, 2K UDP, ICMP, SYN, Smurf
 - Shaft, UDP, ICMP, SYN
 - Trinity, UDP, SYN

Direct Attack



Reflector Attack



Trinoo

- ❑ Attackers take over a set of machines exploiting well-known holes, install master agents on them.
- ❑ Attacker-machines communication is TCP-based
- ❑ Masters and daemons communication is UDPbased
- ❑ Password authentication
- ❑ Certain commands are also protected
- ❑ Sometime encryption is used (Blowfish)
- ❑ All passwords are protected using crypt, however, most of them are sent in clear over the network

Attack using Trinoo

- ❑ In August 1999, a network of > 2,200 systems took University of Minnesota offline for 3 days
- ❑ Tools found cached at Canadian firm
- ❑ Steps:
 - scan for known vulnerabilities, then attack
 - once host compromised, script the installation of the DDoS master agents
- ❑ According to the incident report: it took about 3 seconds to get root access (in 4 hours, set up about 2,200 agents)

Is Your Computer Used in an Attack?

- ❑ **last**: shows you what accounts intruders were using, where they were coming from, and when they were in your system.
- ❑ **ls**: shows their files.
- ❑ **ps**: shows the sniffer, password cracking program, etc.
- ❑ **netstat**: shows you the current network connections and ports...
- ❑ **ifconfig**: shows if the ethernet interface was in promiscuous mode, making visible to the intruder's sniffer program all network traffic.
- ❑ **YOU WISH THAT WAS TRUE!!!! BUT IT'S NOT!**

Is Your Computer Used in an Attack?

- ❑ **Attackers modify most programs you rely on to get information: You think they're doing what they were supposed to, but they're not**
- ❑ **Example: ls will not show attacker's files**

Security Mechanisms

- ❑ Normally, not a single silver bullet
- ❑ Develop multiple layers of defense
- ❑ Employ as many layers of defense as needed – risk, resource profiles
- ❑ Castle, moat, drawbridge, mountain-top lookout, perimeter wall, inner wall, ruler decoy etc.
- ❑ Firewall, resource managers, app. Level security, logging, antivirus, remote backups, egress filters...

Security Analogy



Defenses

- ❑ Victim network
- ❑ Intermediate network
- ❑ Source network
- ❑ Attack is **observed close to victim**
- ❑ Attack **must be stopped close to the source**
- ❑ Intermediate network used to “**traceback**” the attack
- ❑ **Reactive** (after the attack) and **proactive** (prevents the attack) methods

Two Security Philosophies

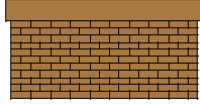


Super Protection – very expensive, could be broken



Prevention Power of punishment

Defense Methods at Victim



- ❑ Intrusion detection and firewall: detect packets that look like attacks (known attack signature).
- ❑ Make the attack costly for attacker: for example have clients to solve puzzles if they want to access server's resources
- ❑ Increase server resources: distributed clusters

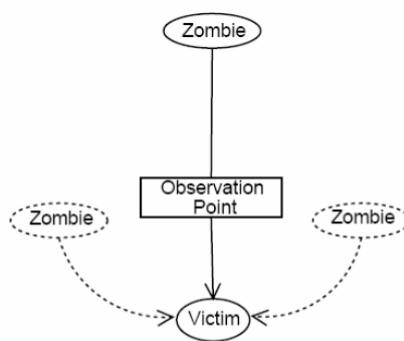
Intermediate Network

- ❑ IP traceback: where is the attack coming from (forensics)
- ❑ Push-back mechanism
- ❑ Route-based packet filtering
- ❑ We will look at these methods class.



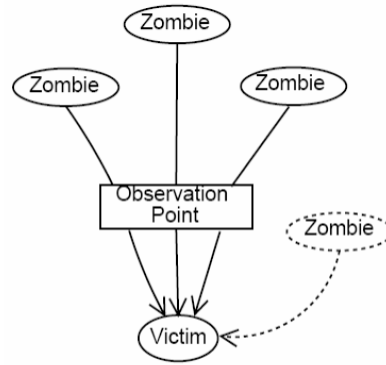
Classifying Denial of Service Attacks

Single-Source



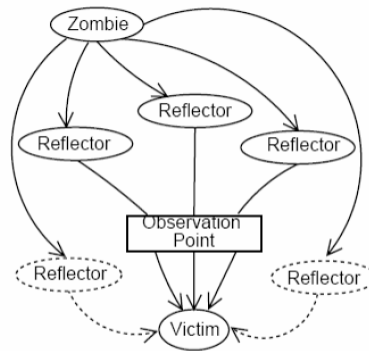
(a) Single-source

Multiple sources



(b) Multi-source

Reflector



(c) Reflector

Attack Classification Methods

- ❑ Analyze header content
- ❑ Transient ramp-up behavior
- ❑ Spectral characteristics

Header Analysis

- ❑ Source address can be easily spoofed
- ❑ Use other header fields:
 - Fragment identification field (ID)
 - Time-to-live field (TTL)
- ❑ OS usually sequentially increments ID field for each successive packet
- ❑ Assuming routes remain relatively stable, TTL value will remain constant

Header Analysis (cont.)

- ❑ Estimate the number of attackers by counting the number of distinct ID sequences present in attack
- ❑ Packets are considered to belong to the same ID sequence if :
 - ID values are separated by less than an *idgap* (=16)
 - TTL are the same

Ramp-up Behavior

- ❑ If multi-source attack , ramp-up of the attacks intensity noticed because of
 - Variation in path latency
 - Weak synchronization of local clocks at zombies
- ❑ No ramp-up usually indicates single source attack
- ❑ Cannot robustly identify single-source attacks.

Spectral Characteristics

- ❑ Attack streams have markedly different spectral content that varies depending on number of attackers
 - Single source attacks have a linear cumulative spectrum due to dominant frequencies spread across the spectrum.
 - Multi-source attacks shift spectrum to lower frequencies.
- ❑ Use quintile, $F(p)$, as a numerical method of comparing power spectral graphs.
- ❑ Compare the $F(60\%)$ values of attacks:
 - 240-296Hz ‡ single source
 - 142-210Hz ‡ multiple source

Applications of Classifying DDoS

- ❑ **Automating Attack Detection:** useful in selecting the appropriate response mechanism.
- ❑ **Modeling Attacks:** help in understanding DDoS dynamics and design better attack detection and response mechanisms.
- ❑ **Inferring DoS Activity in the Internet:** approximate attack prevalence; requires increasing the size and duration of the monitored region.

Summary



- ❑ DDoS tools
- ❑ Defenses
- ❑ Classification of attacks

Next Lecture

- ❑ Thursday: IP Traceback
- ❑ A: **Practical Network Support for IP Traceback.** Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson. SIGCOMM 2000.
- ❑ B: **Advanced and Authenticated Marking Schemes for IP Traceback.** Dawn X. Song, Adrian Perrig. Proceedings IEEE Infocomm 2001

Thank You!

