Computer Security
Denial-of-Service Attacks

Erland Jonsson (based on material from Lawrie Brown)
Department of Computer Science and Engineering
Chalmers University of Technology
Sweden

Denial of Service

- **denial of service** (DoS) an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space
- attacks
  - network bandwidth
  - system resources
  - application resources
- have been an issue for some time
- DoS can also be accomplished by “killing” the server

The New York Times

Twitter Restores Service Af

www.nytimes.com/2009/08/07/technolo

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

The New York Times

Internet

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Search Technology

Go

Inside Technology

Internet | Start-Ups | Business Computing | Companies

Bits Blog

Online Attack Silences Twitter for Much of Day

By JENNA WORTHAM
Published: August 6, 2009

TWITTER
LINKEDIN
E-MAIL
PRINT
REPRINTS
SHARE

Twitter, the popular microblogging site, was out of service much of the day Thursday as it worked to defend itself against a Web attack, but service appeared to have been restored by late evening.

Many of Twitter's 45 million legitimate visitors were unable to use the service for hours. Analysts characterized the disruption as a denial-of-service attack, in which hackers overwhelm a Web site by sending it a deluge of junk requests, and one suggested the attack might have originated in Russia or Georgia.

Facebook and Google fended off similar attacks on Thursday.

Most computer security analysts did not cite a specific source of the attack on Twitter.

But Bill Woodcock, research director of the Packet Clearing House, a nonprofit technical organization that tracks Internet traffic, said the attack was an extension of the conflict between Russia and Georgia.

It was not clear who initiated the attack, Mr. Woodcock said, but it was likely that "one side put up propaganda, the other side figured this out and is attacking them." He said

Related

Bits: Twitter Attack Said to Target Blogger (August 7, 2009)

Bits: Twitter Service Spotty as Attacks Continue

Times Topics: Twitter

Post a Comment on Bits

www.toptechnews.com/article/index.php?story_id=01300170PJY5

News & Product Reviews for Tech Leaders

TOP TECH NEWS CIO TODAY DATA STORAGE TODAY MOBILE TECH TODAY

Search...

TOP TECH NEWS

HOME TECH TRENDS NETWORK SECURITY CLOUD COMPUTING HARDWARE APPLICATIONS MICROSOFT/WINDOWS APPLE/MAC MORE

MORE ON THIS SITE:

MOBILE TECH WORLD WIDE WEB BIG DATA UNIFIED COMMUNICATIONS CHIPS & PROCESSORS SMALL BUSINESS CRM SYSTEMS PERSONAL TECH PRESS RELEASES

TRENDING TOPICS: CES • Security • Cybercrime • Microsoft • Google • Data Centers • Android • Apple

WORLD WIDE WEB

Xbox Live Network Hit by Lizard Squad DDoS Attack

Posted December 2, 2014

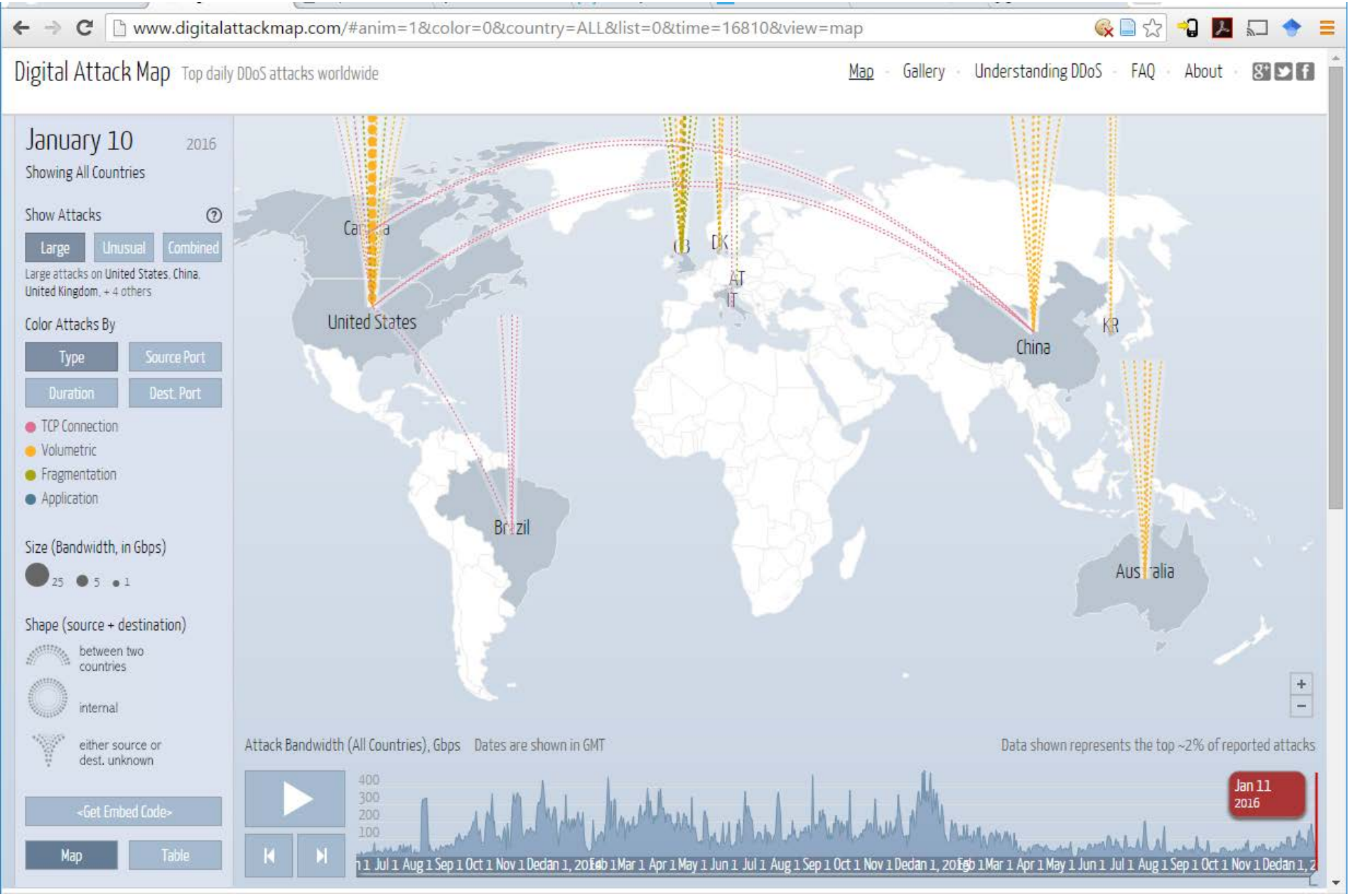
2015

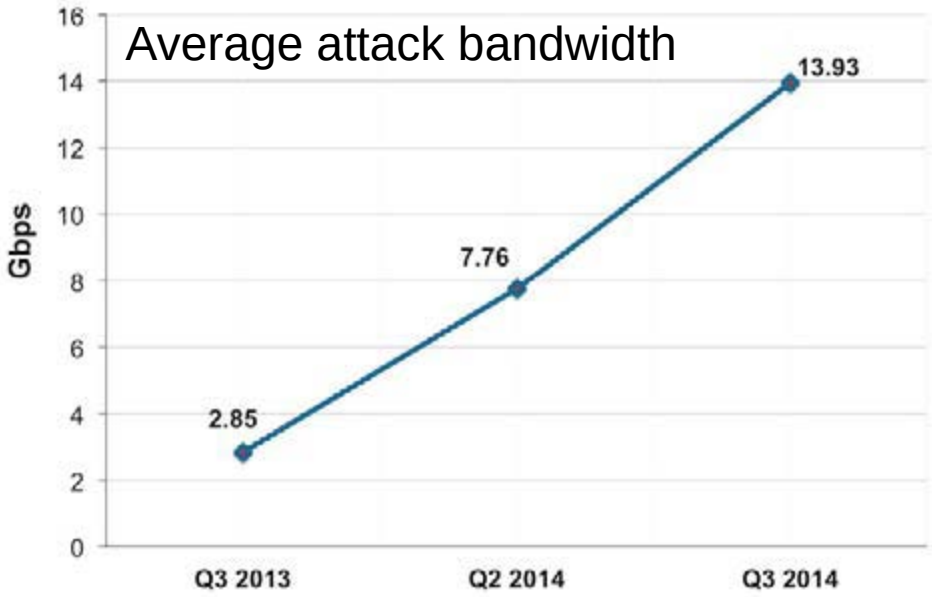
Arbor Networks Detects Largest Ever DDoS Attack in Q1 2015 DDoS Report

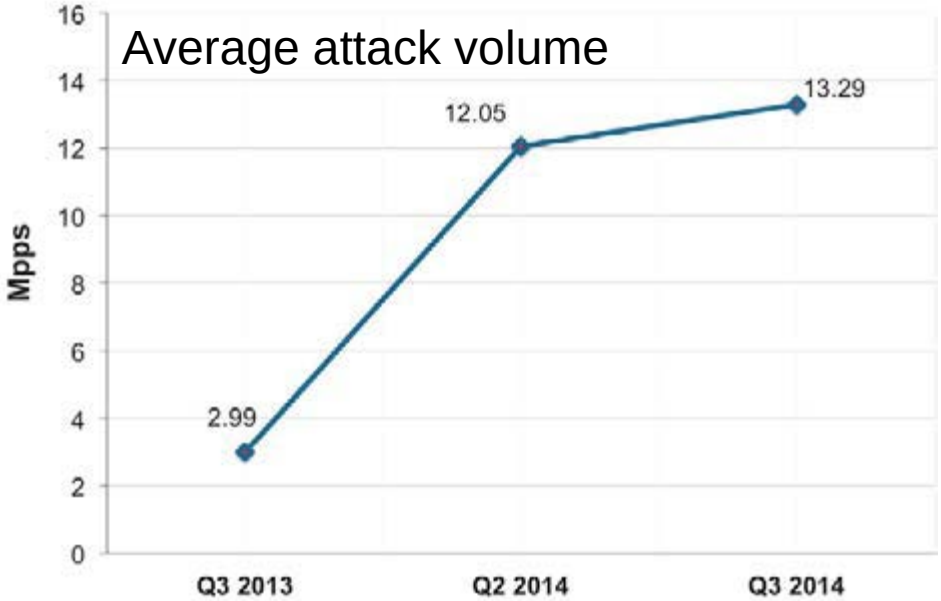
BURLINGTON, MA., April 28, 2015 – Arbor Networks Inc. , a leading provider of DDoS and advanced threat protection solutions for enterprise and service provider networks, today released Q1 2015 global DDoS attack data that shows a continuation of extremely high volume attacks, including the largest attack ever detected by Arbor's ATLAS threat intelligence infrastructure, a 334Gbps attack targeting a network operator Asia. In Q1 2015, there were 25 attacks larger than 100Gbps globally.

In the past year, Arbor has documented a dramatic increase in DDoS activity. The majority of recent very large attacks leverage a reflection amplification technique using the Network Time Protocol (NTP), Simple Service Discovery Protocol (SSDP) and DNS servers, with large numbers of significant attacks being detected all around the world.

Reflection amplification is a technique that allows an attacker to both magnify the amount of traffic they can generate, and obfuscate the original sources of that attack traffic. This technique relies on two unfortunate realities: firstly,


www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=16810&view=map
Digital Attack Map
Top daily DDoS attacks worldwide
Map
Gallery
Understanding DDoS
FAQ
About
January 10
2016
Showing All Countries
Show Attacks
Large
Unusual
Combined
Large attacks on United States, China, United Kingdom, + 4 others
Color Attacks By
Type
Source Port
Duration
Dest. Port
TCP Connection
Volumetric
Fragmentation
Application
Size (Bandwidth, in Gbps)
25
5
1
Shape (source + destination)
between two countries
internal
either source or dest. unknown
<Get Embed Code>
Map
Table
United States
China
KR
Attack Bandwidth (All Countries), Gbps
Dates are shown in GMT
Data shown represents the top ~2% of reported attacks
400
300
200
100
Jan 11
2016





- For example, the highest packet-per-second rate attack that Akamai mitigated this quarter was 169 million packets per second (Mpps) and peaked at a substantial 232 Gbps.
- To achieve this result the attackers leveraged two vectors:
  - a padded **syn flood** with extra bandwidth-consuming data and
  - a **udp flood** with a single byte of data.
  - **Reflection** and **amplification-based** attacks have also played a major role in the increase in attack volume.
- This rising trend in average peak volume is expected to continue.

https://www.stateoftheinternet.com/downloads/pdfs/2014-internet-security-report-q3.pdf

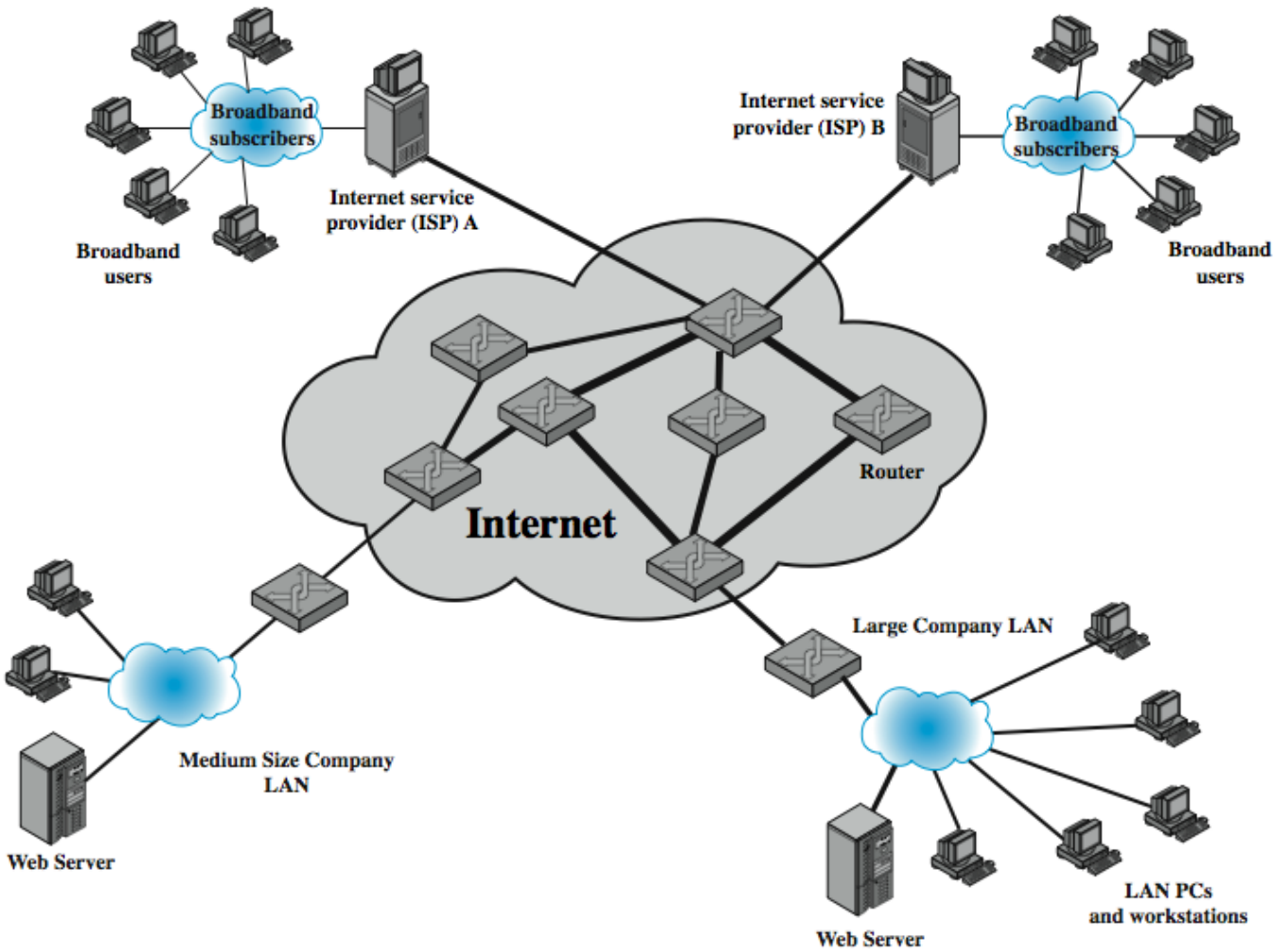
Classic Denial of Service Attacks

1) Overload/Flooding
   - from higher capacity network link to lower
   - causing loss of traffic
   - can use simple *flooding ping* (ping flood)
     - ICMP Flood, UDP Flood, TCP Syn Flood
   - source of flood traffic easily identified
     - Alternative: SYN Spoofing targeting system resources/code/memory (page 248-->)
2) Crash/Kill
   - Trigger bug in system (poison packet)
   - Ping-of-death, land attack

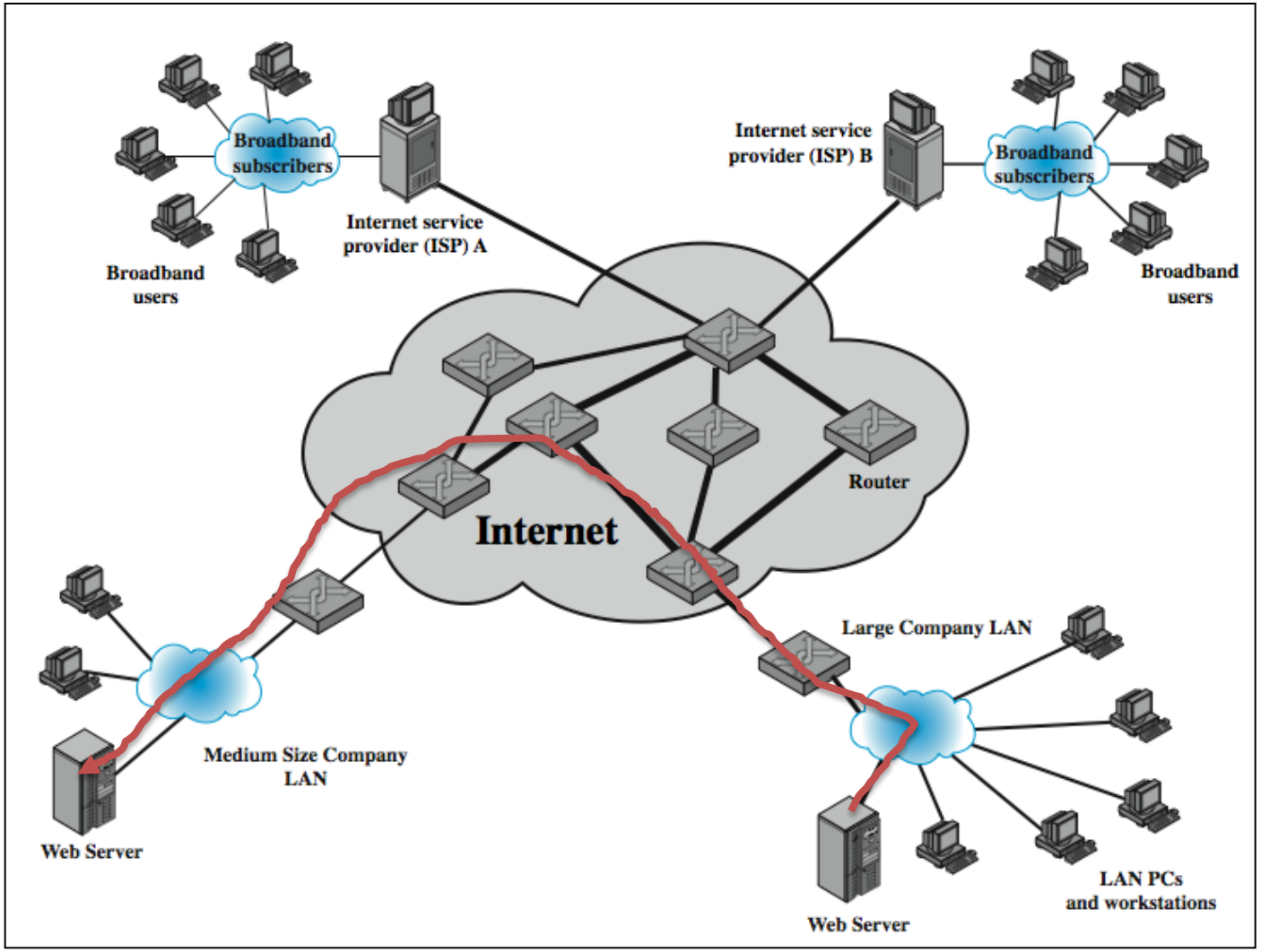
Classic Denial of Service Attacks

1) Overload/Flooding
   - from higher capacity network link to lower
   - causing loss of traffic
   - can use simple *flooding ping* (ping flood)
     - ICMP Flood, UDP Flood, **TCP Syn Flood**
   - source of flood traffic easily identified
     - Alternative: **SYN Spoofing** [illegible] system resources (page 248-->)
2) Crash/Kill
   - Trigger bug in system (poison packet)
   - Ping-of-death, land attack

Classic Denial of Service Attacks



Classic Denial of Service Attacks

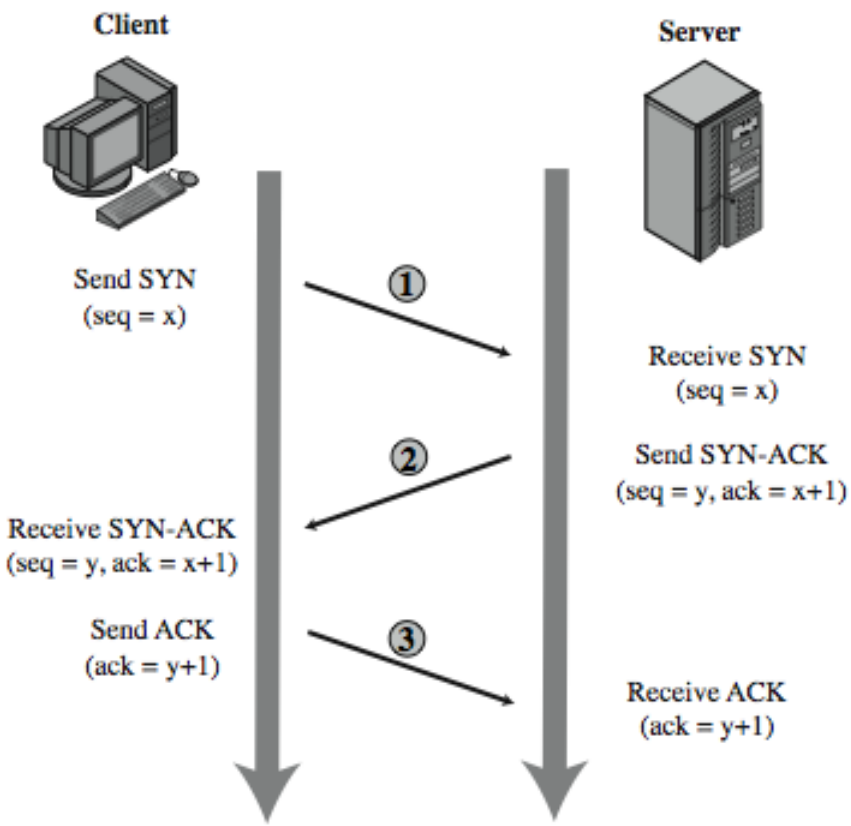


Types of Flooding Attacks

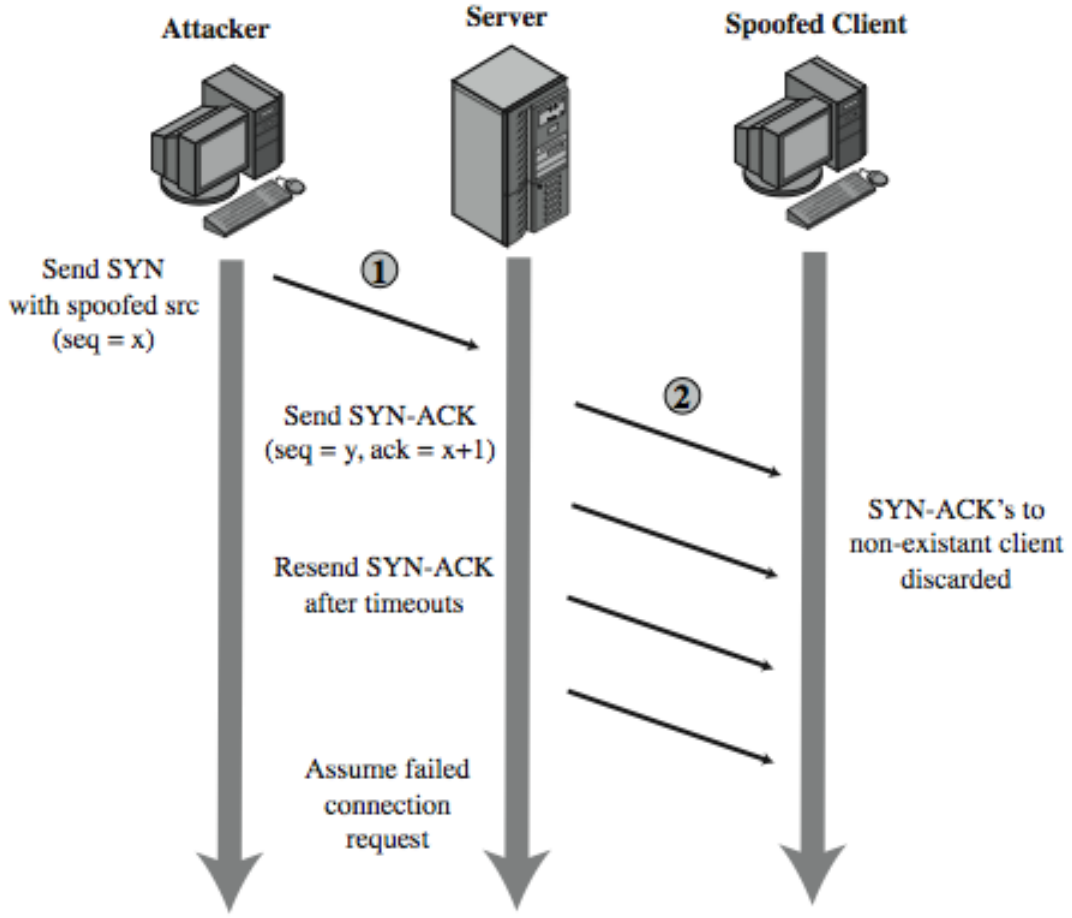
- classified based on network protocol used
- ICMP Flood
  - uses ICMP packets, eg echo request
  - typically allowed through, some required
- UDP Flood
  - alternative uses UDP packets to some port
- TCP SYN Flood
  - use TCP SYN (connection request) packets
  - (but for volume attack compare SYN Spoofing)

SYN Spoofing Attack

TCP Connection Handshake



SYN Spoofing Attack



SYN Spoofing Attack

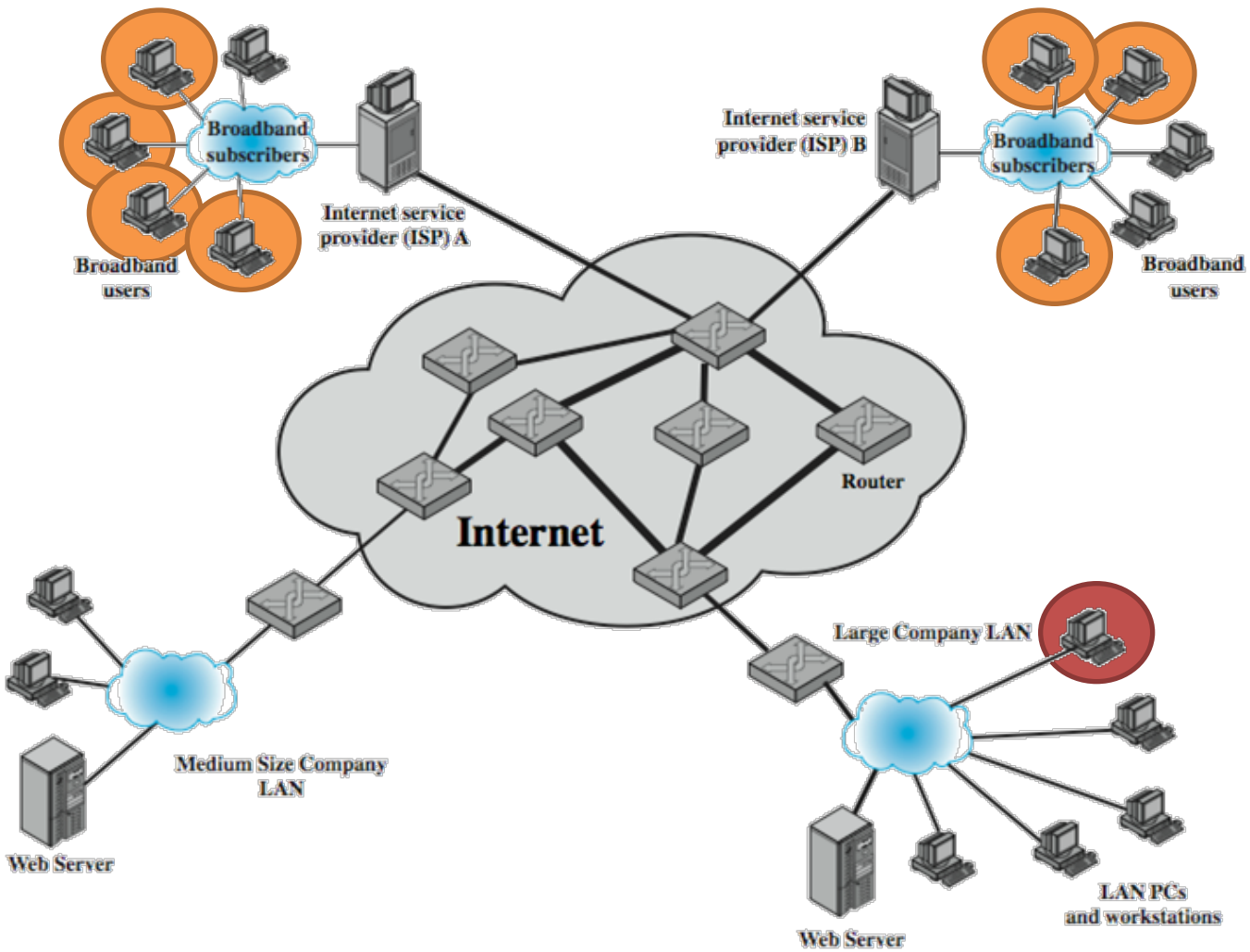
- attacker often uses either
  - random source addresses
  - or that of an overloaded server

  to block return of (most) reset packets
- has much lower traffic volume
  - attacker can be on a much lower capacity link

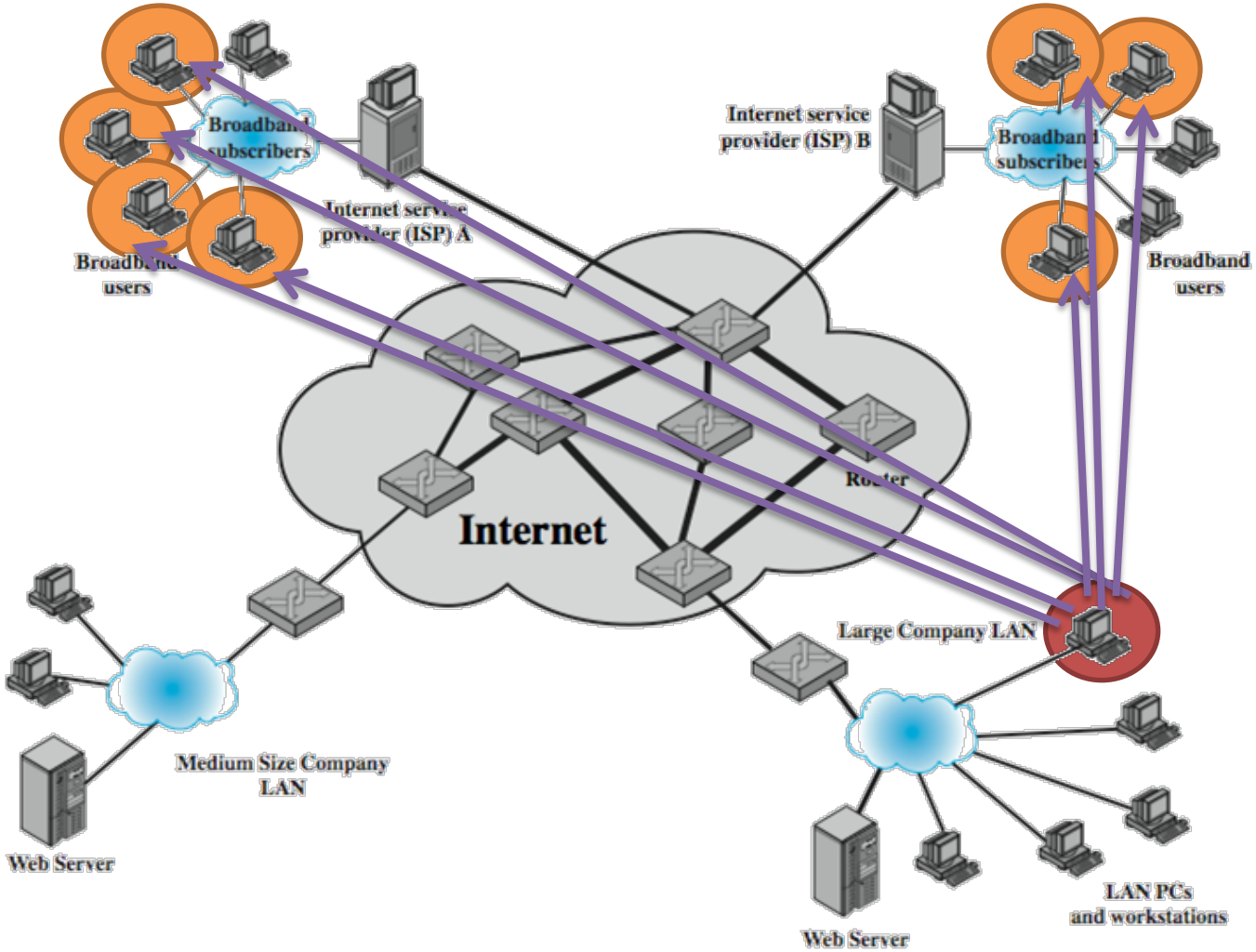
Distributed Denial of Service Attacks

- multiple systems allow much higher traffic volumes to form a Distributed Denial of Service (DDoS) Attack
- often compromised PC's / workstations
  - zombies with backdoor programs installed
  - forming a botnet
- e.g. Tribe Flood Network (TFN), TFN2K

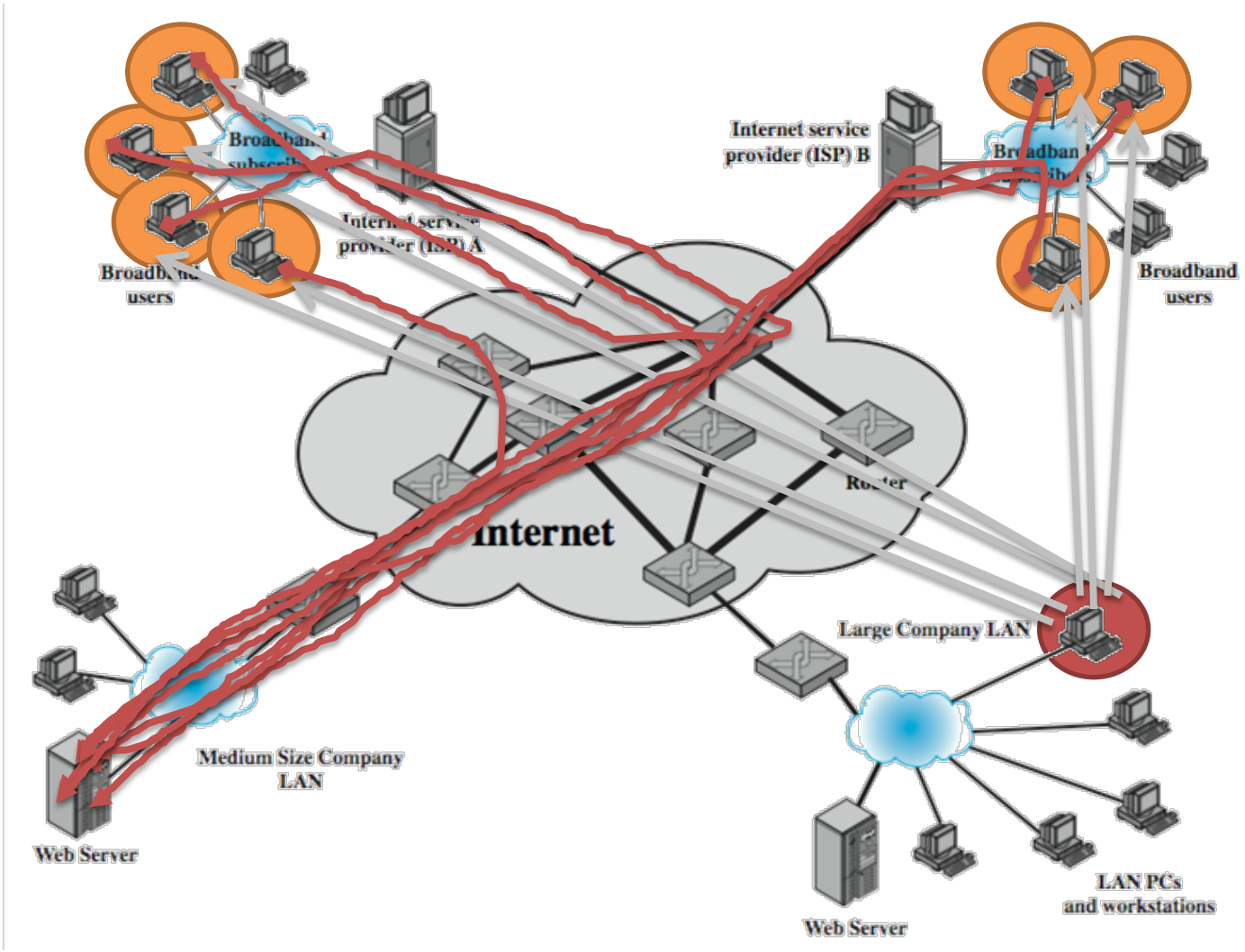
Distributed Denial of Service Attacks



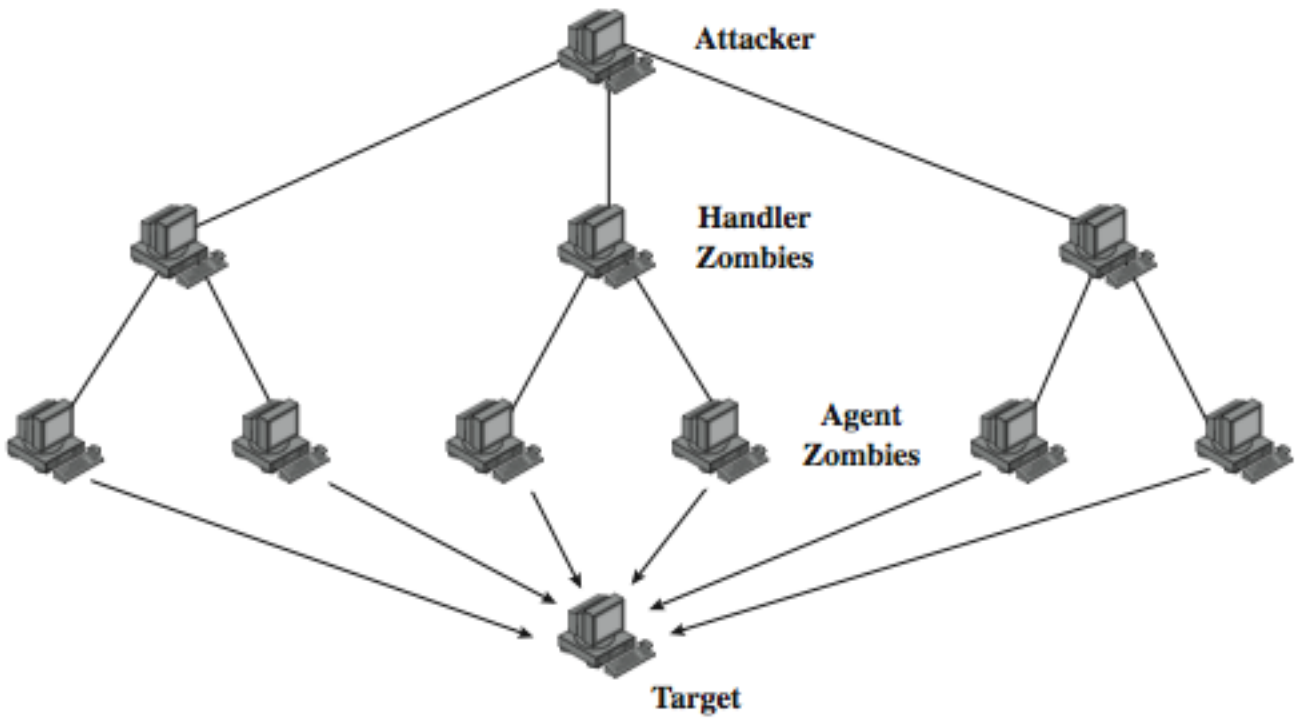
Distributed Denial of Service Attacks



Distributed Denial of Service Attacks



DDoS Control Hierarchy

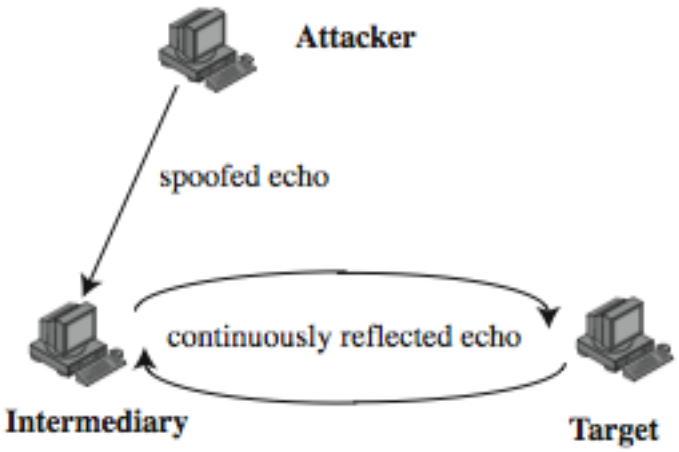


Reflection Attacks

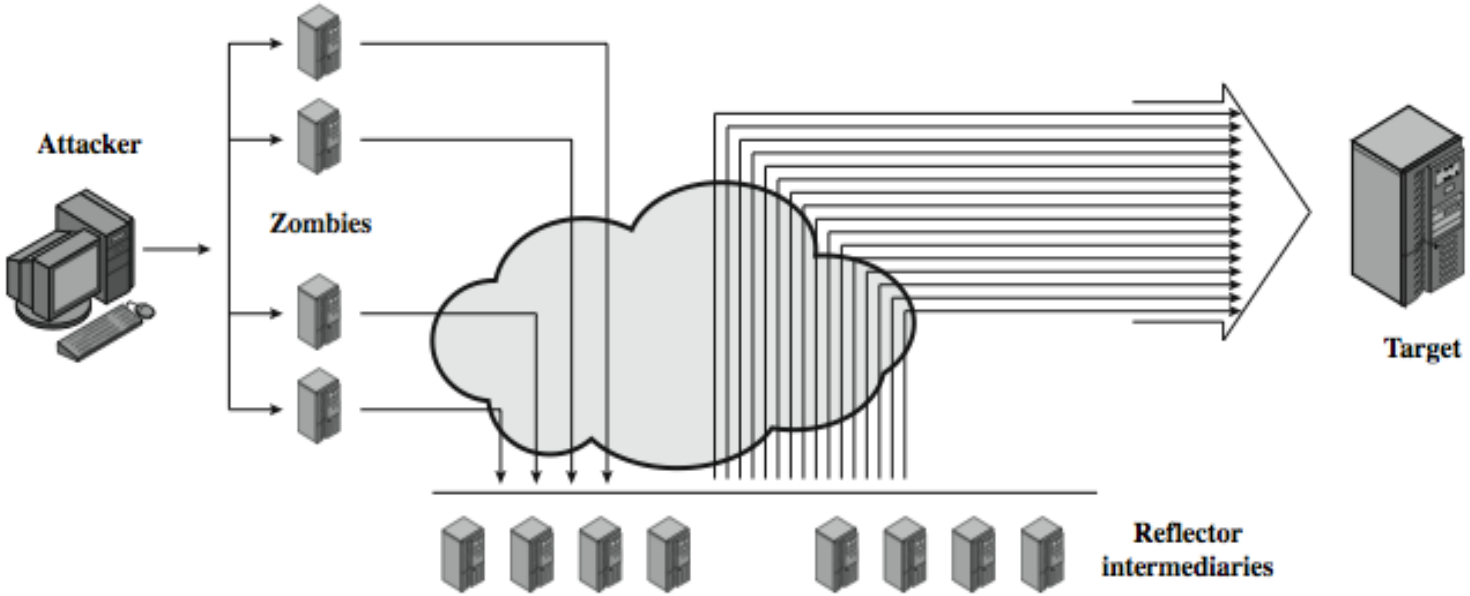
- use normal behavior of network
- attacker sends packet with spoofed source address being that of target to a server
- server response is directed at target
- if send many requests to multiple servers, response can flood target
- various protocols e.g. UDP or TCP/SYN

Reflection Attacks

- further variation creates a self-contained loop between intermediary and target
- fairly easy to filter and block



Amplification Attacks



DoS Attack Defenses

- high traffic volumes may be legitimate
  - result of high publicity
  - or to a very popular site, e.g. Olympics etc
- four lines of defense against (D)DoS:
  - attack prevention and preemption
  - attack detection and filtering
  - attack source traceback and identification
  - attack reaction (after attack) to curtail effects of an attack

Attack Prevention

- block spoofed source addresses
  - on routers as close to source as possible
  - still far too rarely implemented
- rate controls in upstream distribution nets
  - on specific packets types
  - e.g. some ICMP, some UDP, TCP/SYN
- use modified TCP connection handling
  - use SYN cookies when table full
  - or selective or random drop when table full

Attack Prevention

- block IP directed broadcasts
- block suspicious services & combinations
- manage application attacks with “puzzles” to distinguish legitimate human requests
- good general system security practices
- use mirrored and replicated servers when high-performance and reliability required

Responding to Attacks

- identify type of attack
  - capture and analyze packets
  - design filters to block attack traffic upstream
  - or identify and correct system/application bug
- have ISP trace packet flow back to source
  - may be difficult and time consuming
  - necessary if legal action desired
- implement contingency plan
- update incident response plan