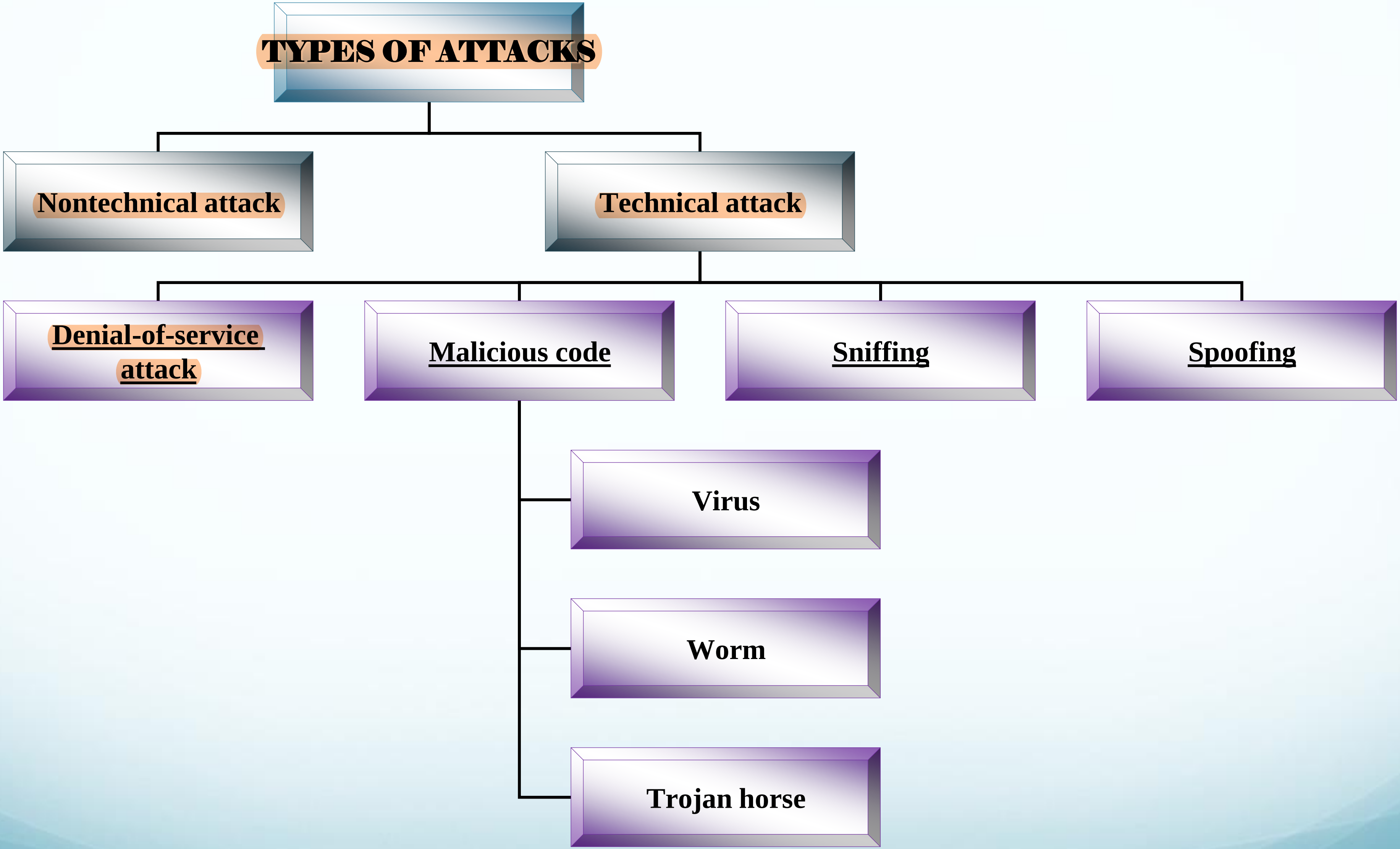
Denial of Service Attacks



TYPES OF ATTACKS

Nontechnical attack

Technical attack

Denial-of-service attack

Malicious code

Sniffing

Spoofing

Virus

Worm

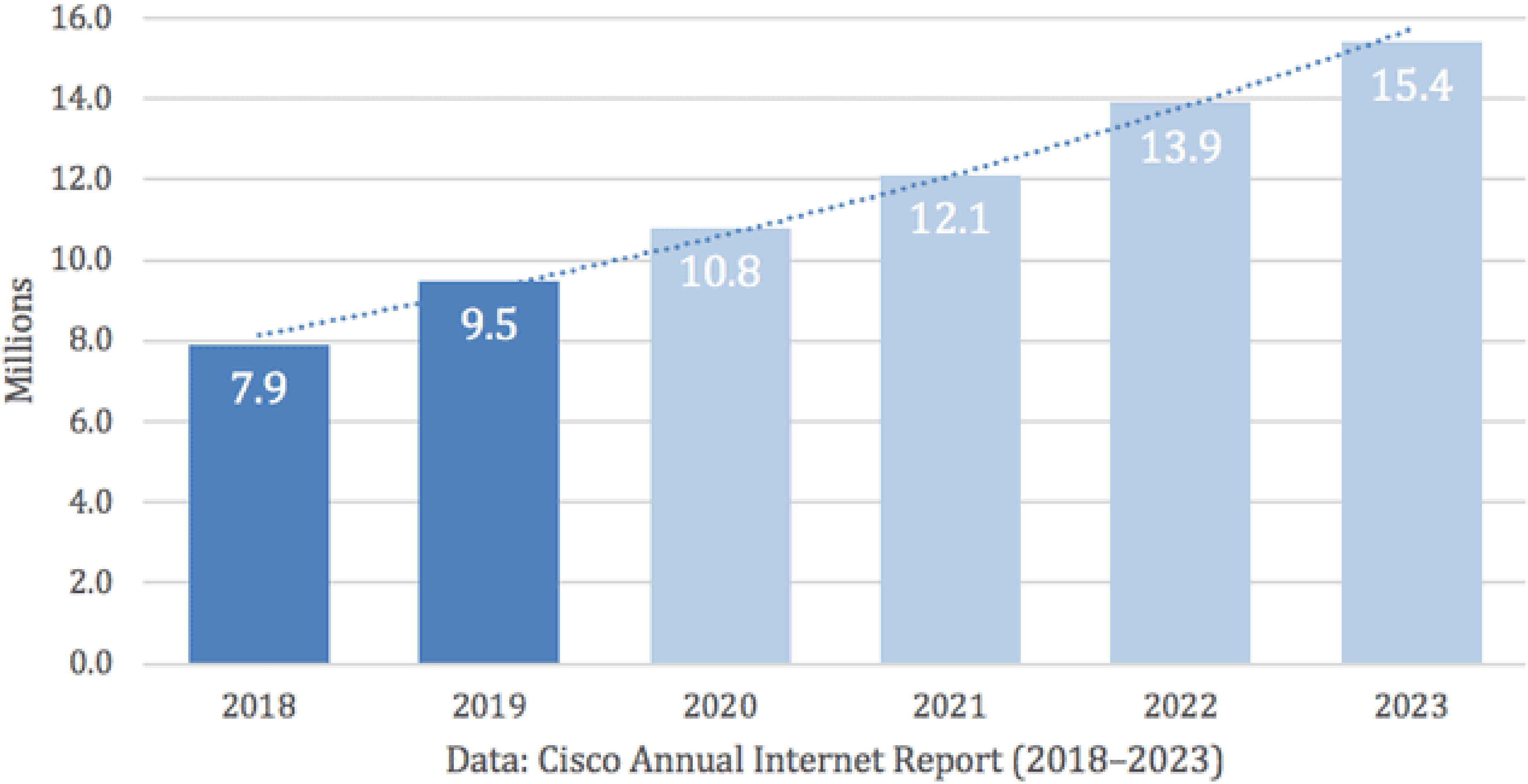
Trojan horse

Understanding Denial of Services

Cost of DOS/DDoS Attacks

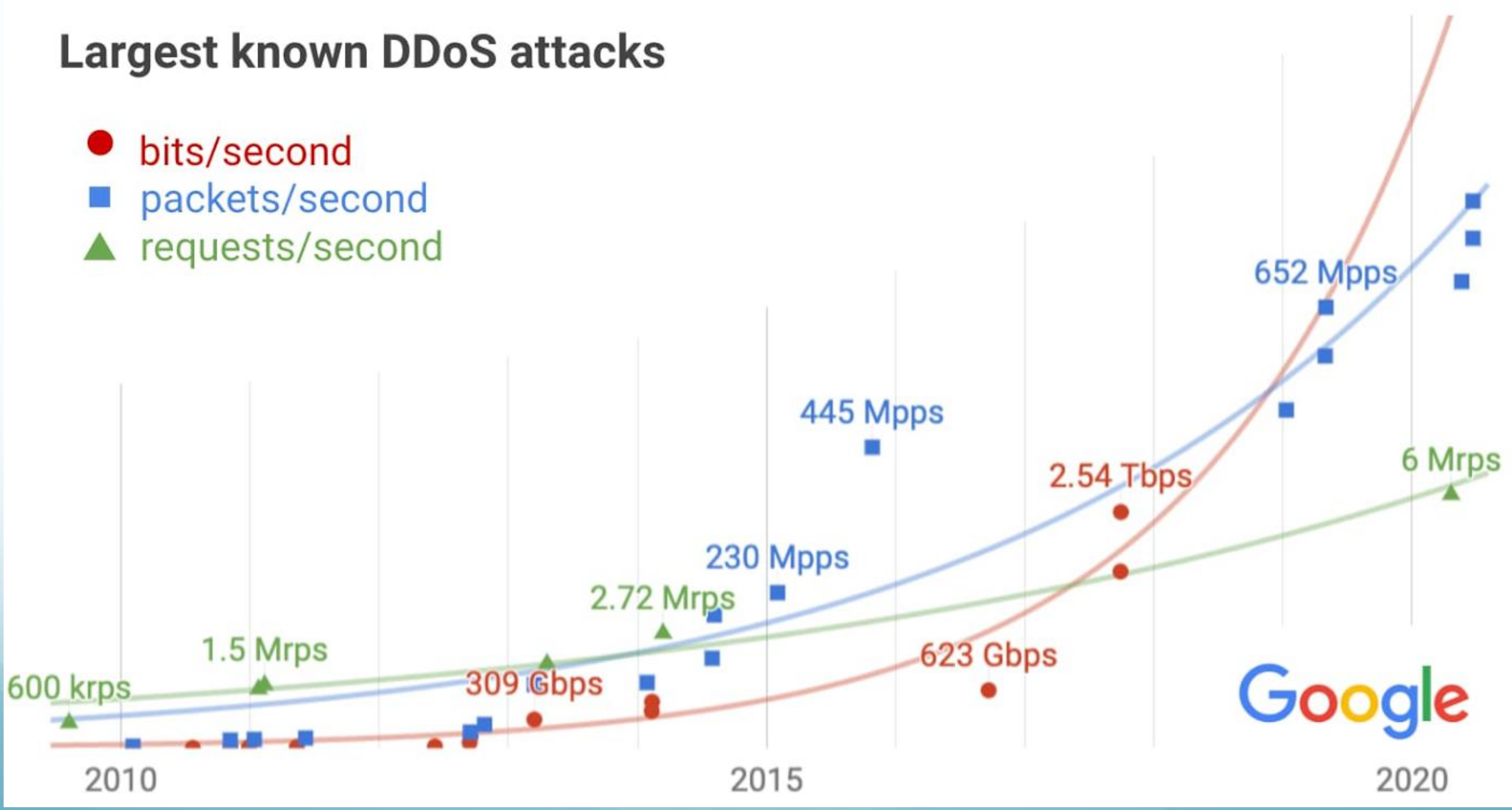
- Victims of (D)DoS attacks
  - Service-providers (in terms of time, money, resources, good will)
  - Legitimate users (deprived of availability of service)
- Hard to quantify
  - Incomplete data – Companies reluctant to admit they have been victimized
  - Lost business
  - Lost productivity

Cisco’s analysis of DDoS total attack history



Data: Cisco Annual Internet Report (2018–2023)

Largest Known DDoS Attacks



Why? Who?

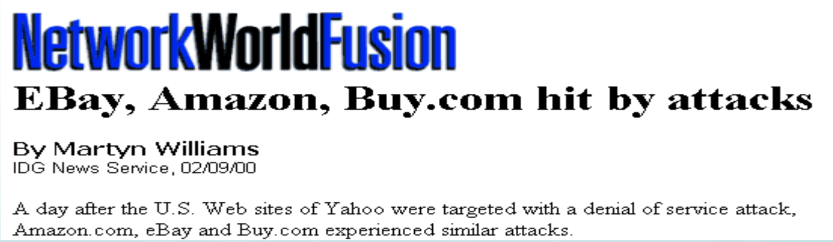
- **Several motives**
  - Earlier attacks were proofs of concepts
  - Political issues
  - Competition
  - Hired
- **Levels of attackers**
  - Highly proficient attackers who are rarely identified or caught
  - Script-kiddies

DoS Attacks Fast Facts

- Large-Scale DDoS Attack
  - CNN, Yahoo, E*Trade, eBay, Amazon.com, Buy.com
- Microsoft’s name sever infrastructure was disabled
- DDoS attack Root DNS
- DDoS for hire and Extortion
- DDoS against Estonia
- DDoS against Georgia during military conflict with Russia
- Ddos on Twitter and Facebook
- Ddos on VISA and Master Card

DoS Attacks

- In the past series of massive DoS attacks
  - Yahoo, Amazon, eBay, CNN, E*Trade, ZDNet, Datek and Buy.com all hit
- Attacks allegedly perpetrated by teenagers
- Used compromised systems at UCSB
- Yahoo : 3 hours down with $500,000 lost revenue
- Amazon: 10 hours down with $600,000 lost revenue



NetworkWorldFusion

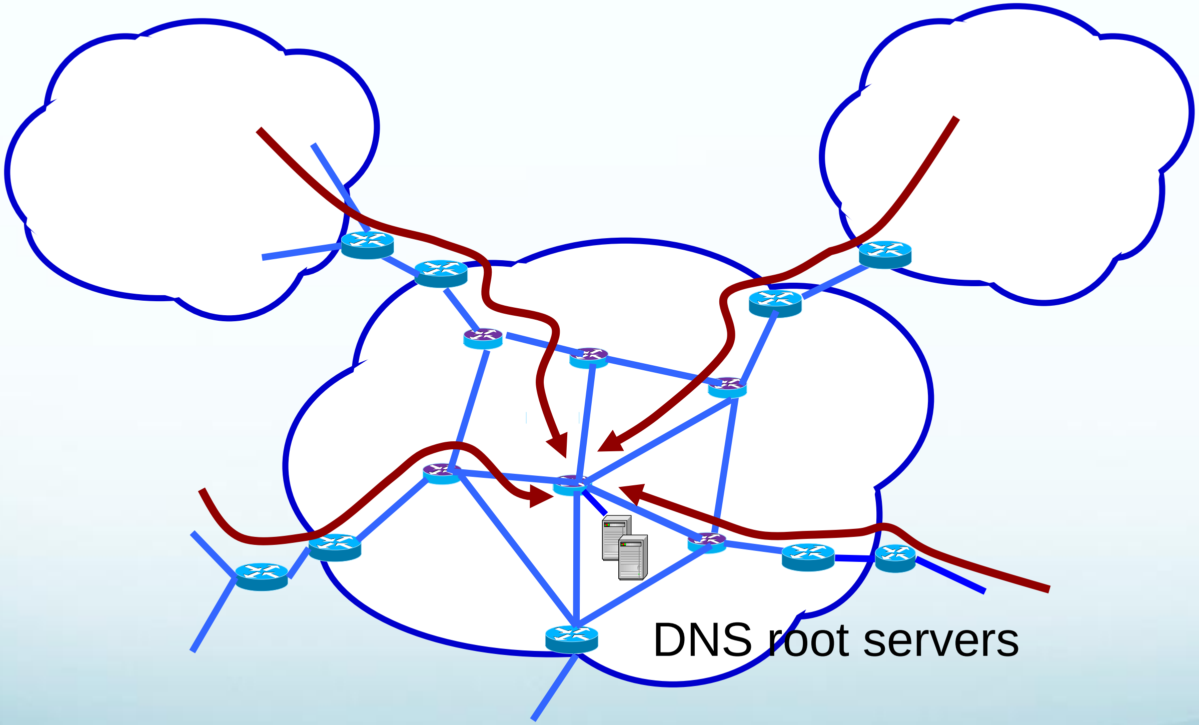
EBay, Amazon, Buy.com hit by attacks

By Martyn Williams
IDG News Service, 02/09/00

A day after the U.S. Web sites of Yahoo were targeted with a denial of service attack, Amazon.com, eBay and Buy.com experienced similar attacks.

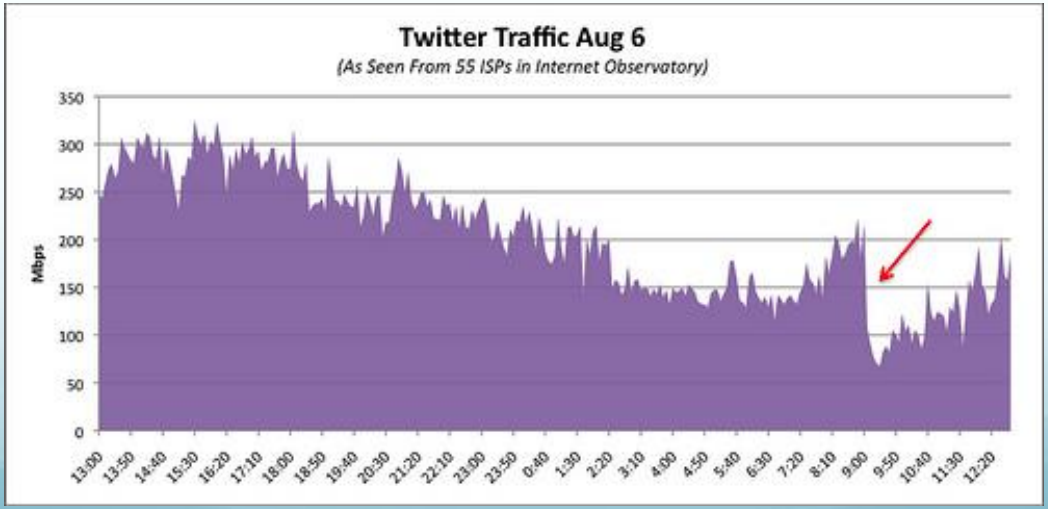
DNS DoS Attacks

- ICMP floods 150 Kbps (primitive attack)
- Took down 7 root servers (two hours)



DDoS on Twitter

- Hours-long service outage
  - 44 million users affected
- At the same time Facebook, LiveJournal, and YouTube were under attacked
  - some users experienced an outage



DDoS on Mastercard and Visa

- December 2010
- Targets: MasterCard, Visa, Amazon, Paypal, Swiss Postal Finance, and more

- Attack launched by a group of vigilantes called ***Anonymous*** (~5000 people)
  - DDoS tool is called LOIC or “Low Orbit Ion Cannon”
  - Bots recruited through social engineering
  - Directed to download DDoS software and take instructions from a master
  - Motivation: Payback, due to cut support of WikiLeaks after their founder was arrested on unrelated charges

How can a service be denied?

- Using up resources is the most common approach
- Several ways..
  - Crash the machine
  - Put it into an infinite loop
  - Crash routers on the path to the machine
  - Use up a machine resource
  - Use up a network resource
  - Deny another service needed for this one (e.g. DNS)

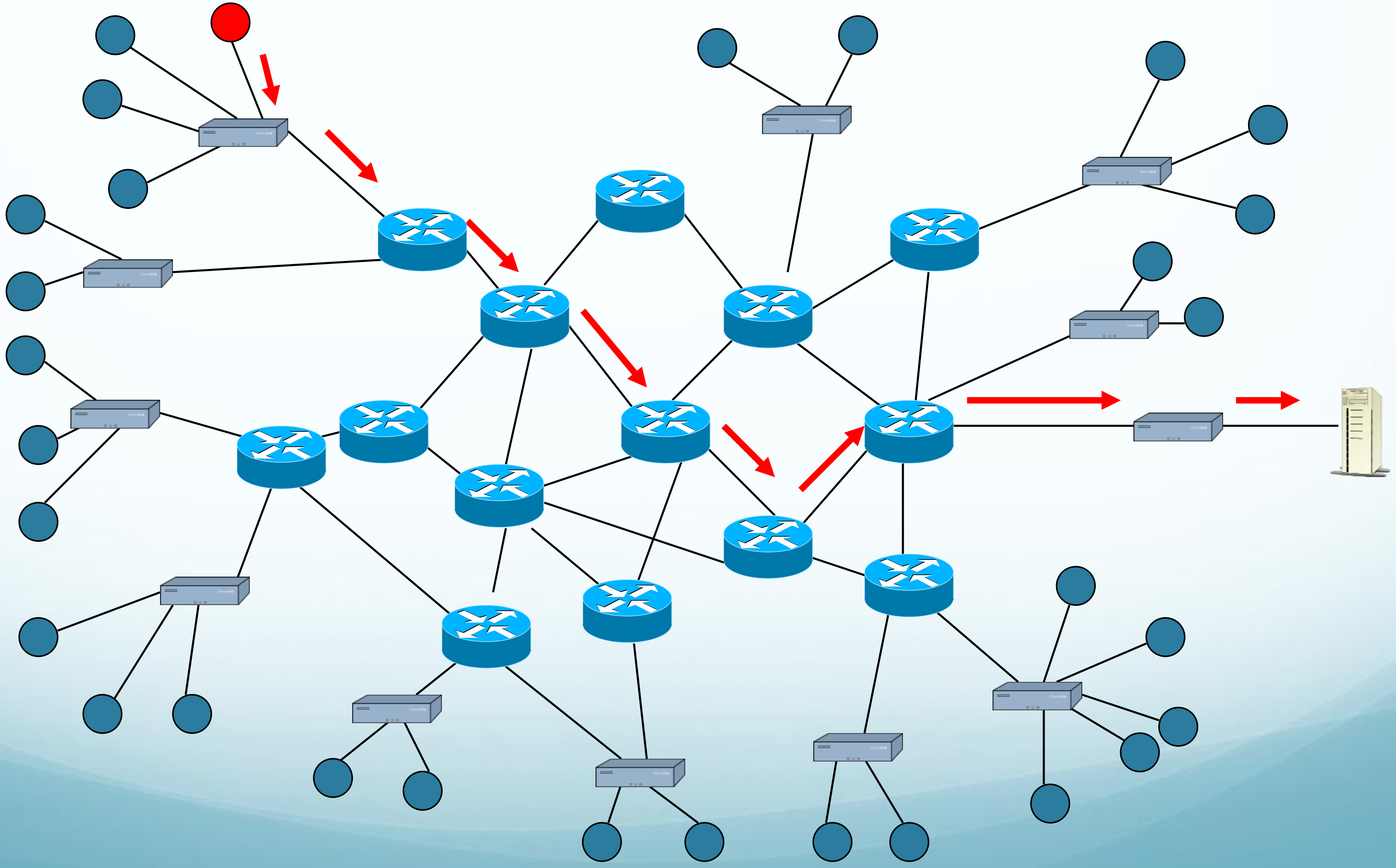
DDoS Attack

- The idea behind this attack is focusing Internet connection bandwidth of many machines upon one or a few machines. This way it is possible to use a large array of smaller (or “weaker”) widely distributed computers to create the big flood effect.

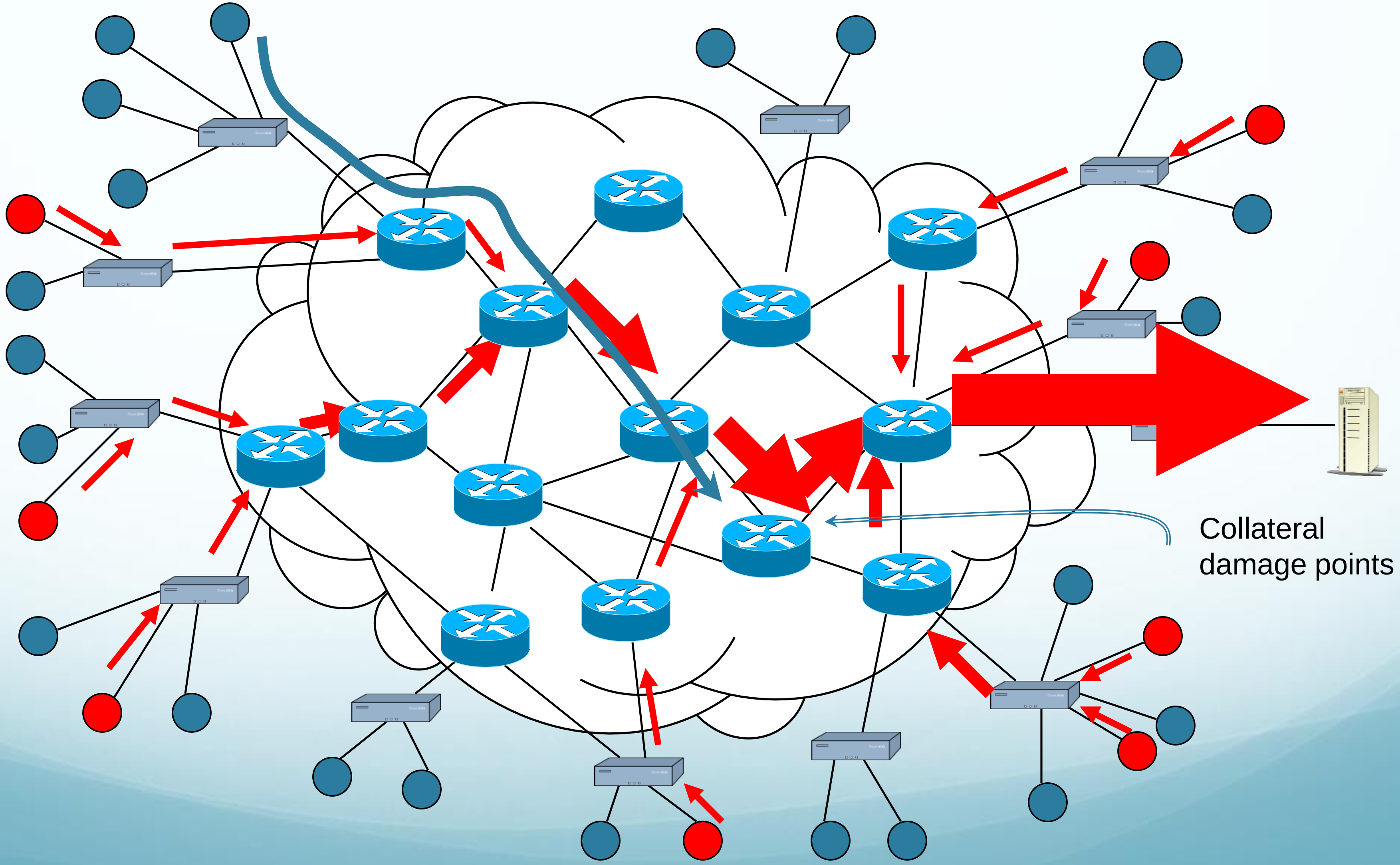
What is Denial of Service?

- **Denial of Service (DoS)**
  - Attack to disrupt the authorized use of networks, systems, or applications
- **Distributed Denial of Service (DDoS)**
  - Employ multiple compromised computers to perform a coordinated and widely distributed DoS attack

DoS Single Source



DDoS



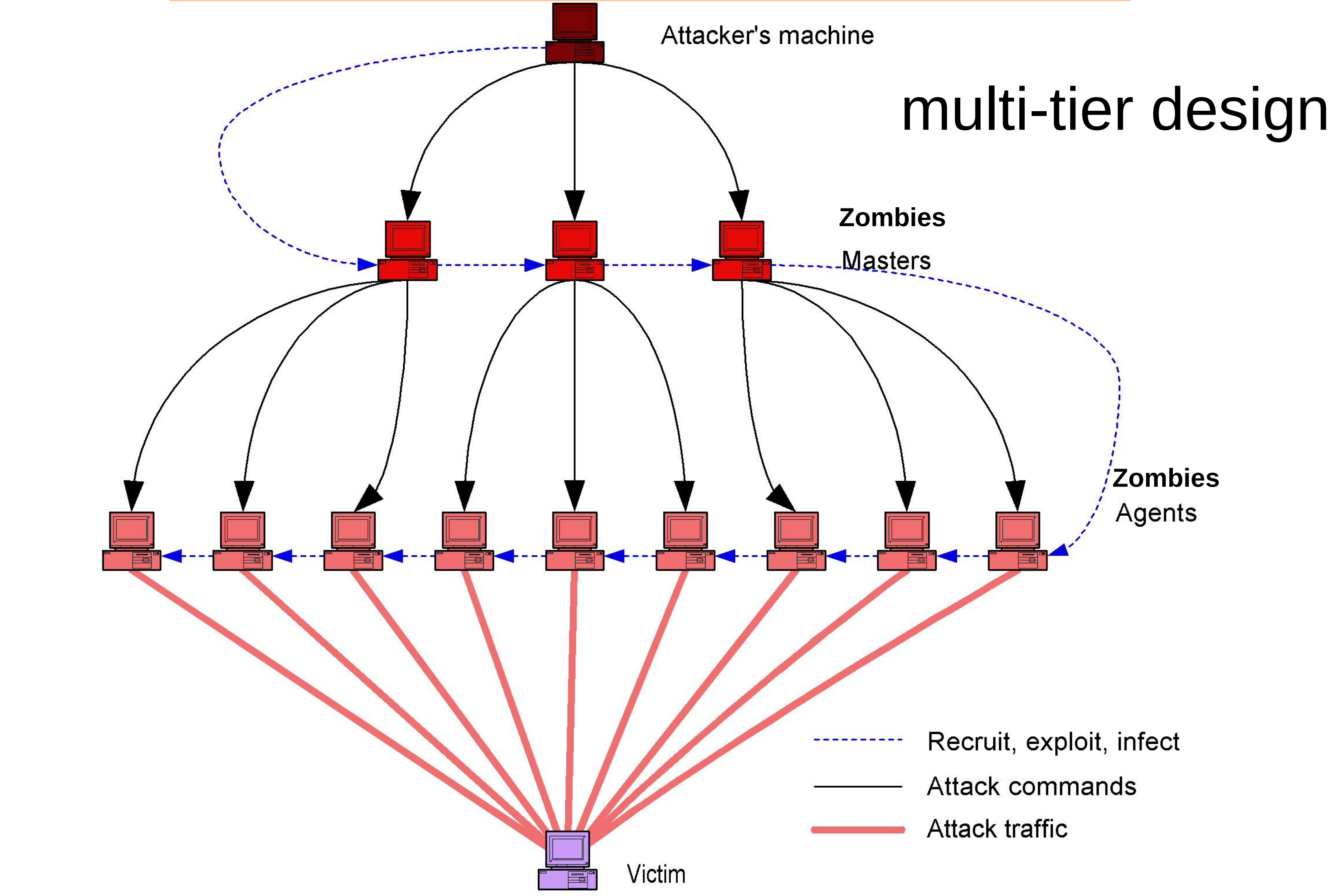
Collateral damage points

DDoS Botnets

- **Botnet**: Collection of compromised computers that are controlled for the purposes of carrying out DDoS attacks or other activities
- Can be large in number
- Systems join a botnet when they become infected by certain types of malware
  - Like a virus, but instead of harming the system, it wants to take it over and control it
  - Through email attachments, website links, or IM links
  - Through unpatched operating system vulnerabilities

Botnets Modus Operandi

multi-tier design



DDoS Attack Classification

Attack classification

1. Bandwidth/Throughput Attacks
2. Protocol Attacks
3. Software Vulnerability Attacks

DOS attack list

- **Flood attack**
  - TCP SYN flood
  - UDP flood
  - ICMP (PING) flood
  - Amplification (Smurf, Fraggle since 1998)

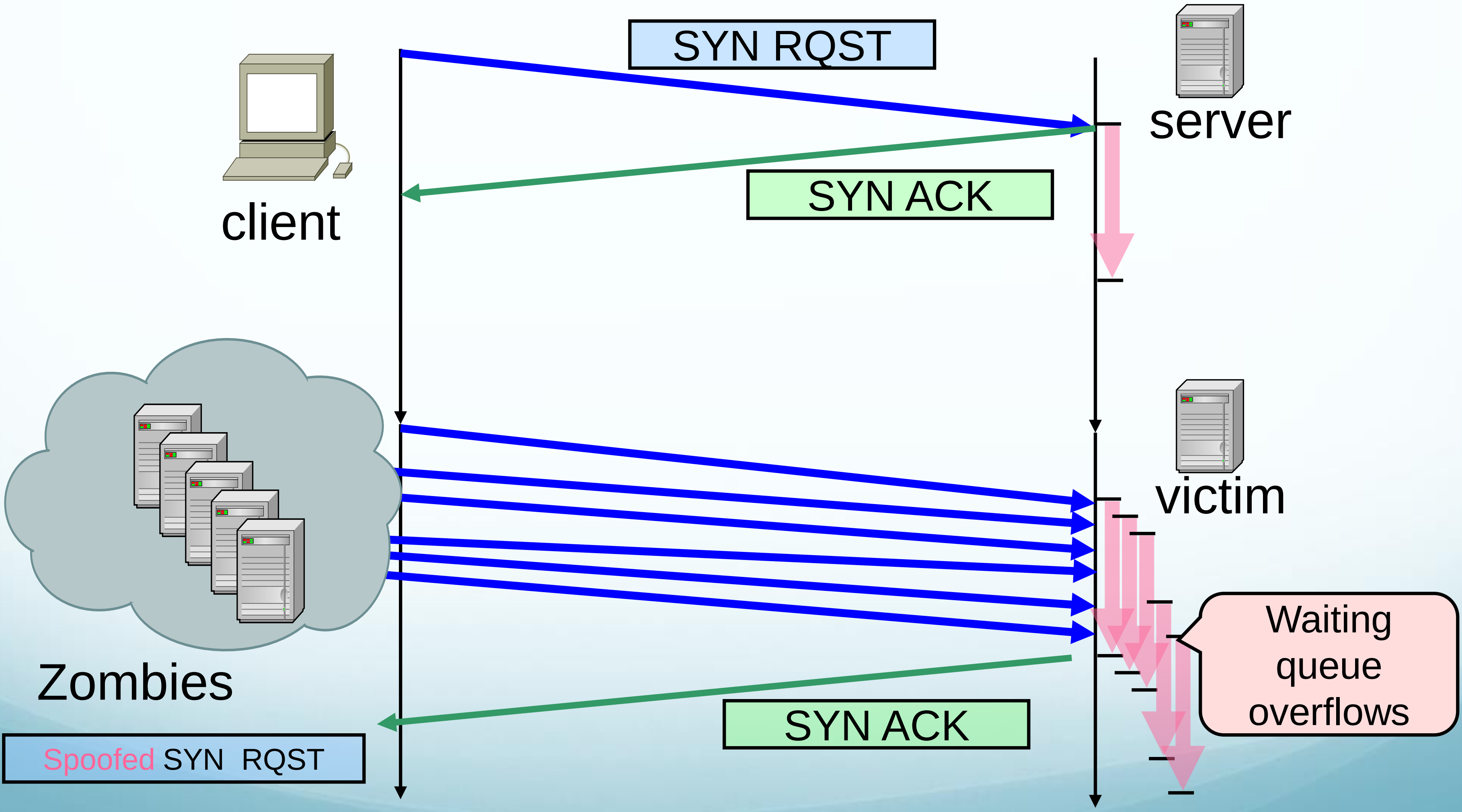
Flooding attack

- Commonly used DDoS attack
- Sending a vast number of messages whose processing consumes some key resource at the target
- The strength lies in the volume, rather than the content
- Implications :
  - The traffic look **legitimate**
  - **Large** traffic flow **large** enough to consume victim's resources
  - **High packet rate** sending

Vulnerability DoS attack

- *Vulnerability* : a bug in implementation or a bug in a default configuration of a service
- *Malicious messages* (exploits) : unexpected input that utilize the vulnerability are sent
- Consequences :
  - The system slows down or crashes or freezes or reboots
  - Target application goes into infinite loop
  - Consumes a vast amount of memory

TCP SYN flood



examples

- **Syn flood**
  - **TCP three-way handshake:**
    - **The client requests a connection by sending a SYN (*synchronize*) message to the server.**
    - **The server *acknowledges* this request by sending SYN-ACK back to the client, which,**
    - **Responds with an ACK, and the connection is established.**
- **How it work………???**
  - **1. attacker sends SYN packet to victim forging non-existent IP address**
  - **2. victim replies with Syn/Ack but neither receives Ack nor RST from non-existent IP address**
  - **3. victim keeps potential connection in a queue in Syn_Recv state, but the queue is small and takes some time to timeout and flush the queue, e.g 75 seconds**
  - **4. If a few SYN packets are sent by the attacker every 10 seconds, the victim will never clear the queue and stops to respond.**

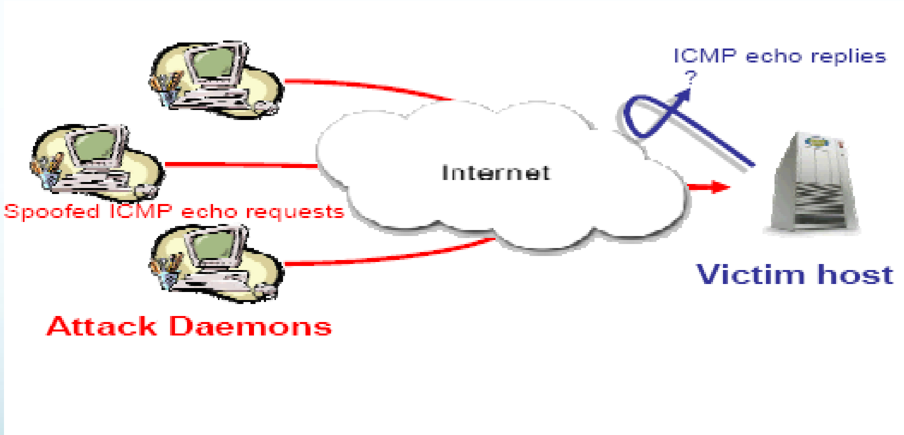
UDP Flood Attacks

- UDP protocol is a connectionless unreliable protocol which doesn't require session negotiation between client and server application. UDP provides easy to use interface for producing large quantity of packets.

- A common attack which exploits UDP simply floods the network with UDP packets destined to a victim's host. Due to the relative simplicity of this protocol an attacker can produce large bandwidth capacity with relatively small effort.

Ping Flood Attack

- An attempt by an attacker on a high bandwidth connection to saturate a network with ICMP echo request packets in order to slow or stop legitimate traffic going through the network.



Ping of Death: Oversized packets

- Ping of Death is an attempt by an attacker to crash, reboot or freeze a system by sending an illegal ICMP (over IP) packet to the host under attack.

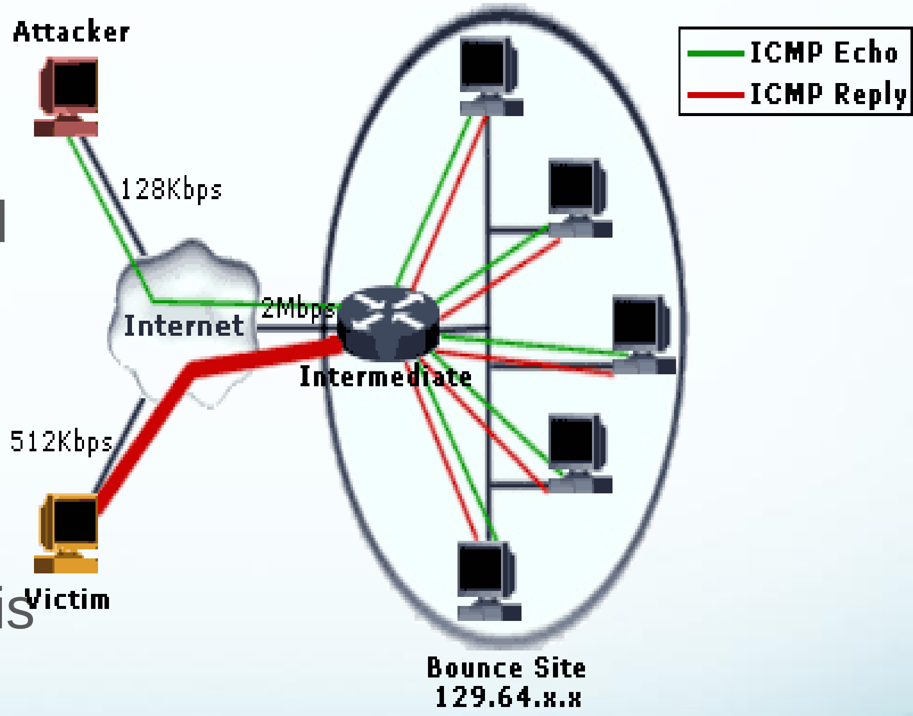
- The TCP/IP specification allows for a maximum packet size of up to 65536 octets. In some TCP stack implementation encountering packets of greater size may cause the victim's host to crash.

- Most implementations of the ICMP protocol use packet header size of 8 octets but allow the user to specify larger packet header sizes.

- In the attack, the ICMP packet is sent in the form of a fragmented message which, when reassembled is larger than the maximum legal IP packet size

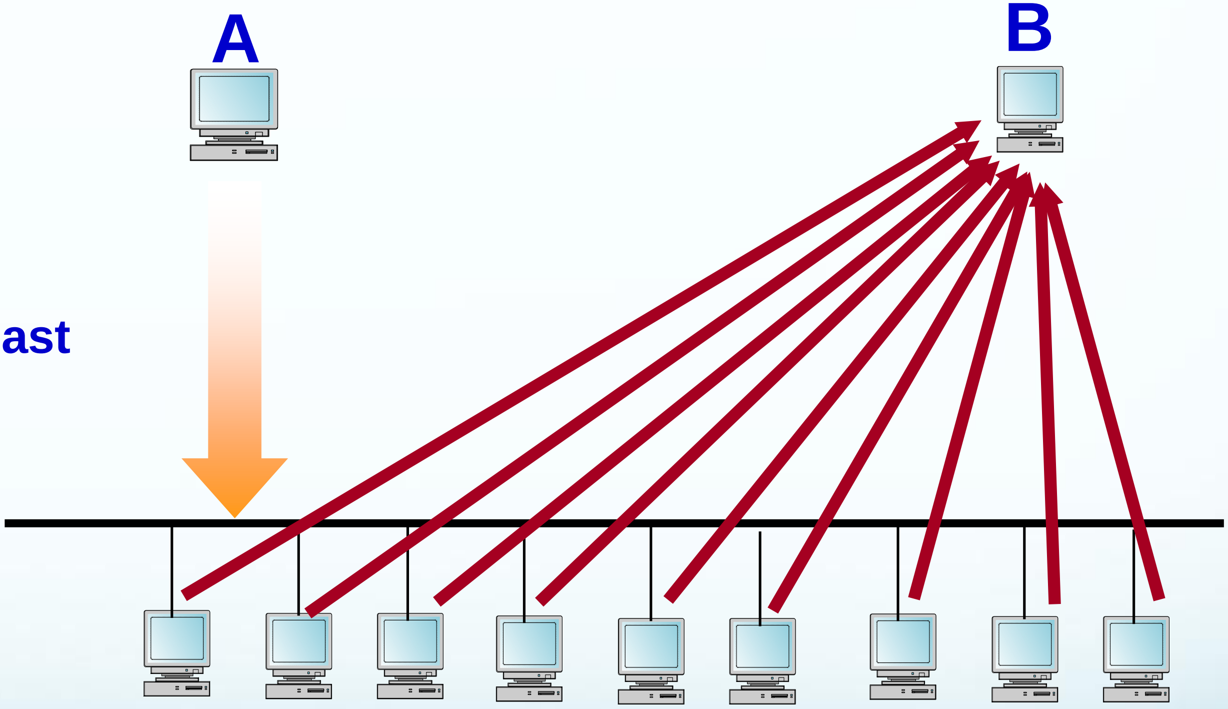
Smurf attack

- Amplification attack
  - Sends ICMP ECHO to network
  - Amplified network flood
  - widespread pings with faked return address (broadcast address)
  - Network sends response to victim system



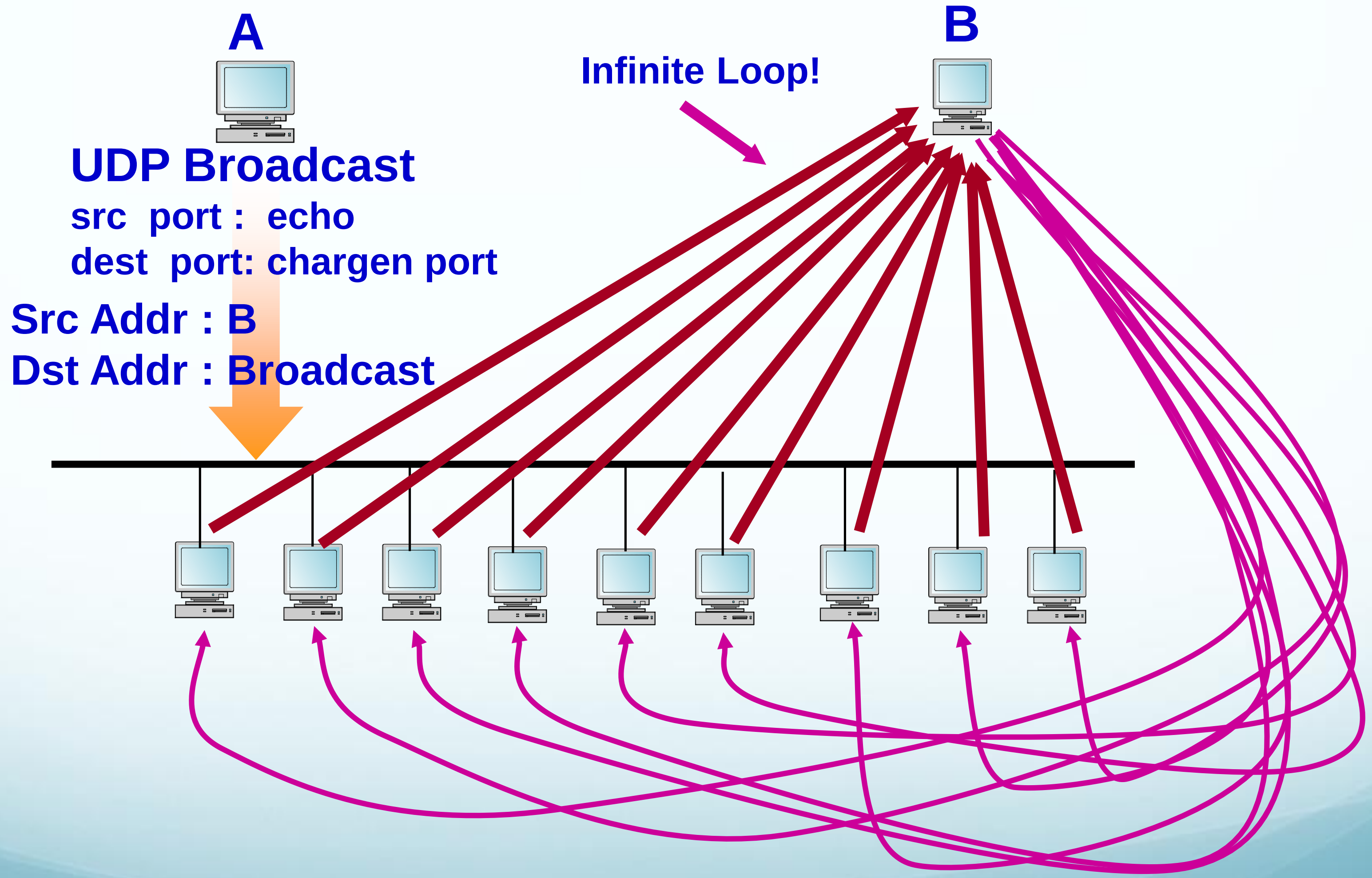
  - The "smurf" attack's cousin is called "fraggle", which uses UDP echo packets in the same fashion

DoS : Smurf



Ping Broadcast
Src Addr : B
Dst Addr : Broadcast

DoS : Fraggle



UDP Broadcast

src port : echo

dest port: chargen port

Src Addr : B

Dst Addr : Broadcast

- Well known exploit Echo/Chargen

LAND

- The attack involves sending a spoofed **TCP SYN packet** (connection initiation) with the target host's IP address as both source and destination.

DNS name server Attack

- The most common method seen involves an intruder sending a large number of UDP-based DNS requests to a Nameserver using a spoofed source IP address. Any Nameserver response is sent back to the spoofed IP address as the destination.

- In this scenario, the spoofed IP address represents the victim of the denial of service attack. The Nameserver is an intermediate party in the attack.

- The true source of the attack is difficult for an intermediate or a victim site to determine due to the use of spoofed source addresses.

Implications For the Future

- More complex attacks
- Recently seen trends:
  - Larger networks of attack machines
  - Rolling attacks from large number of machines
  - Attacks at higher semantic levels
  - Attacks on different types of network entities
  - Attacks on DDoS defense mechanisms
- Need flexible defenses that evolve with attacks

DDoS Defense

Are we safe from DDoS?

- **My machine are well secured**
  - It does not matter. The problem is not your machine but everyone else
- **I have a Firewall**
  - It does not matter. We slip with legitimate traffic or we bomb your firewall
- **I use VPN**
  - It does not matter. We can fill your VPN pipe
- **My system is very high provision**
  - It does not matter. We can get bigger resource than you have

Why DoS Defense is difficult

- **Conceptual difficulties**
  - Mostly random source packet
  - Moving filtering upstream requires communication
- **Practical difficulties**
  - Routers don’t have many spare cycles for analysis/filtering
  - Networks must remain stable—bias against infrastructure change
  - Attack tracking can cross administrative boundaries
  - End-users/victims often see attack differently (more urgently) than network operators
- **Nonetheless, need to:**
  - Maximize filtering of bad traffic
  - Minimize “collateral damage”

Defenses against DoS attacks

- DoS attacks cannot be prevented entirely
- Impractical to prevent without compromising network performance
- Three lines of defense against (D)DoS attacks
  - Attack prevention and preemption
  - Attack detection and filtering
  - Attack source traceback and identification
  - Role of ISP

Attack prevention

- Limit ability of systems to send spoofed packets
  - Filtering done as close to source as possible by routers/gateways
  - Reverse-path filtering ensure that the path back to claimed source is same as the current packet's path
    - Ex: On Cisco router "ip verify unicast reverse-path" command
- Block IP broadcasts

Responding to attacks

- Need good incident response plan
  - With contacts for ISP
- Ideally have network monitors and IDS
  - To detect and notify abnormal traffic patterns

Responding to attacks cont’d ….

- Identify the type of attack
  - Capture and analyze packets
  - Design filters to block attack traffic upstream
  - Identify and correct system application bugs
- 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

DDoS Attack Trends

- Attackers follow defense approaches, adjust their code to bypass defenses
- Use of subnet spoofing defeats ingress filtering
- Use of encryption and decoy packets, IRC or P2P obscures master-slave communication
- Encryption of attack packets defeats traffic analysis and signature detection
- Pulsing attacks defeat slow defenses and traceback
- Flash-crowd attacks generate application traffic