Network Security: Network Flooding

Seungwon Shin, KAIST

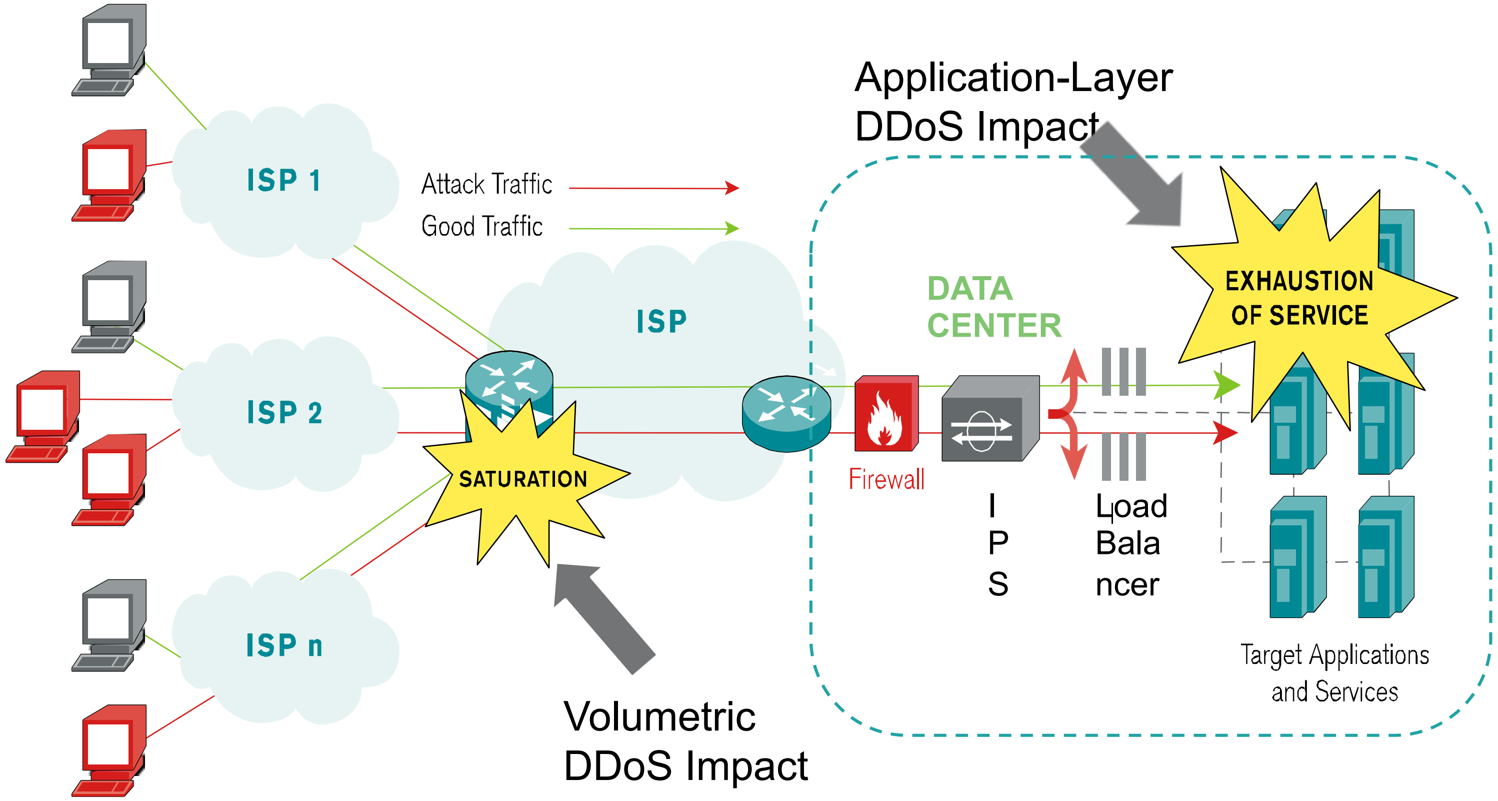
Most slides from Dr. Dan Boneh and Darren Anstee

What is a Denial of Service Attack?

- Goal
  - take out a large site with little computing work
    - Network Bandwidth
    - Computing Power
      - Processor
      - Memory
- How: Amplification
  - Small number of packets ⇒ big effect
- Two types of amplification attacks
  - DoS bug:
    - Design flaw allowing one machine to disrupt a service
  - DoS flood:
    - Command bot-net to generate flood of requests

What is a Denial of Service Attack

- An attempt to consume finite resources, exploit weaknesses in software design or implementation, or exploit lack of infrastructure capacity
- Effects the availability and utility of computing and network resources
- Attacks can be distributed for even more significant effect
- The collateral damage caused by an attack can be as bad, if not worse, than the attack itself



Application-Layer DDoS Impact

Volumetric DDoS Impact

DoS or DDoS

- DoS (Denial of Service)
  - A DoS attack is targeted at a particular node (machine).
  - Attempts to deny service to that node

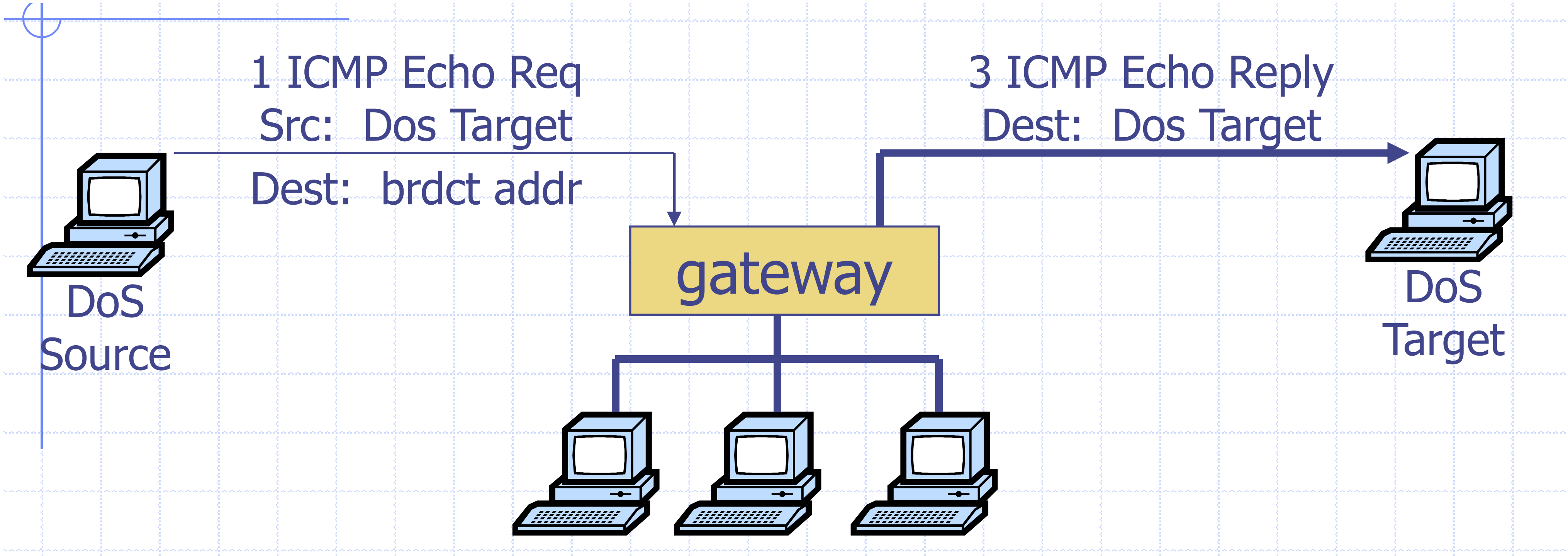
- Source of the attack:
  - Single node: DoS (Denial of Service) attack
  - Multiple nodes: DDoS (Distributed Denial of Service) attack

Which Layer?

- Sample Dos at different layers (by order)
  - Link
  - TCP/UDP
  - Application

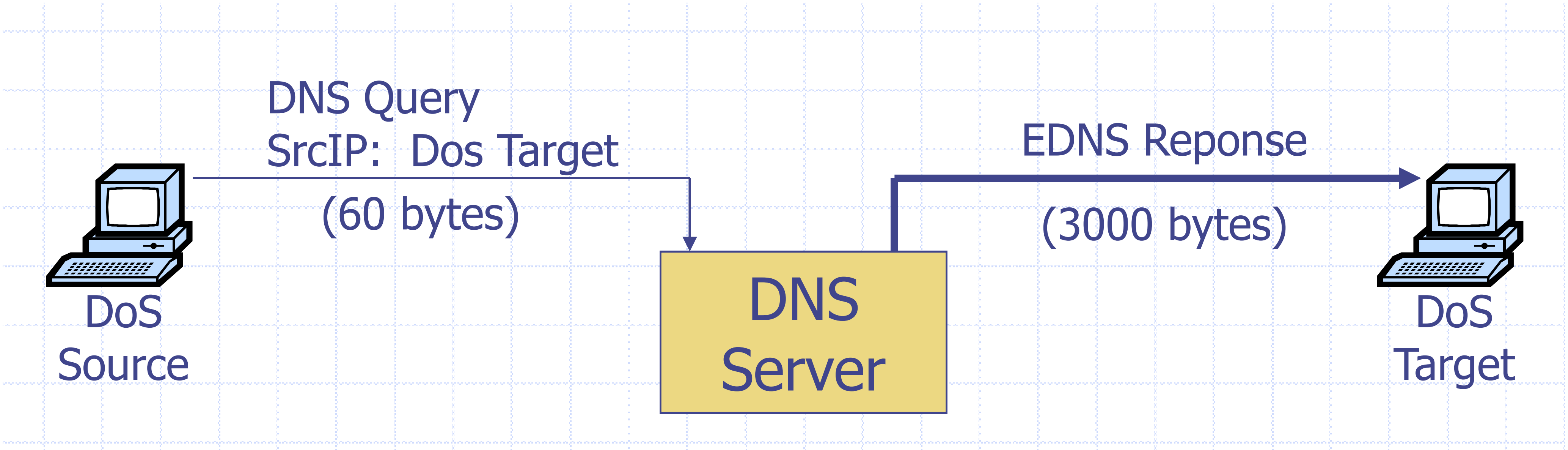
- Sad truth:
  - Current Internet… not designed to handle DDoS attacks

Smurf Attack

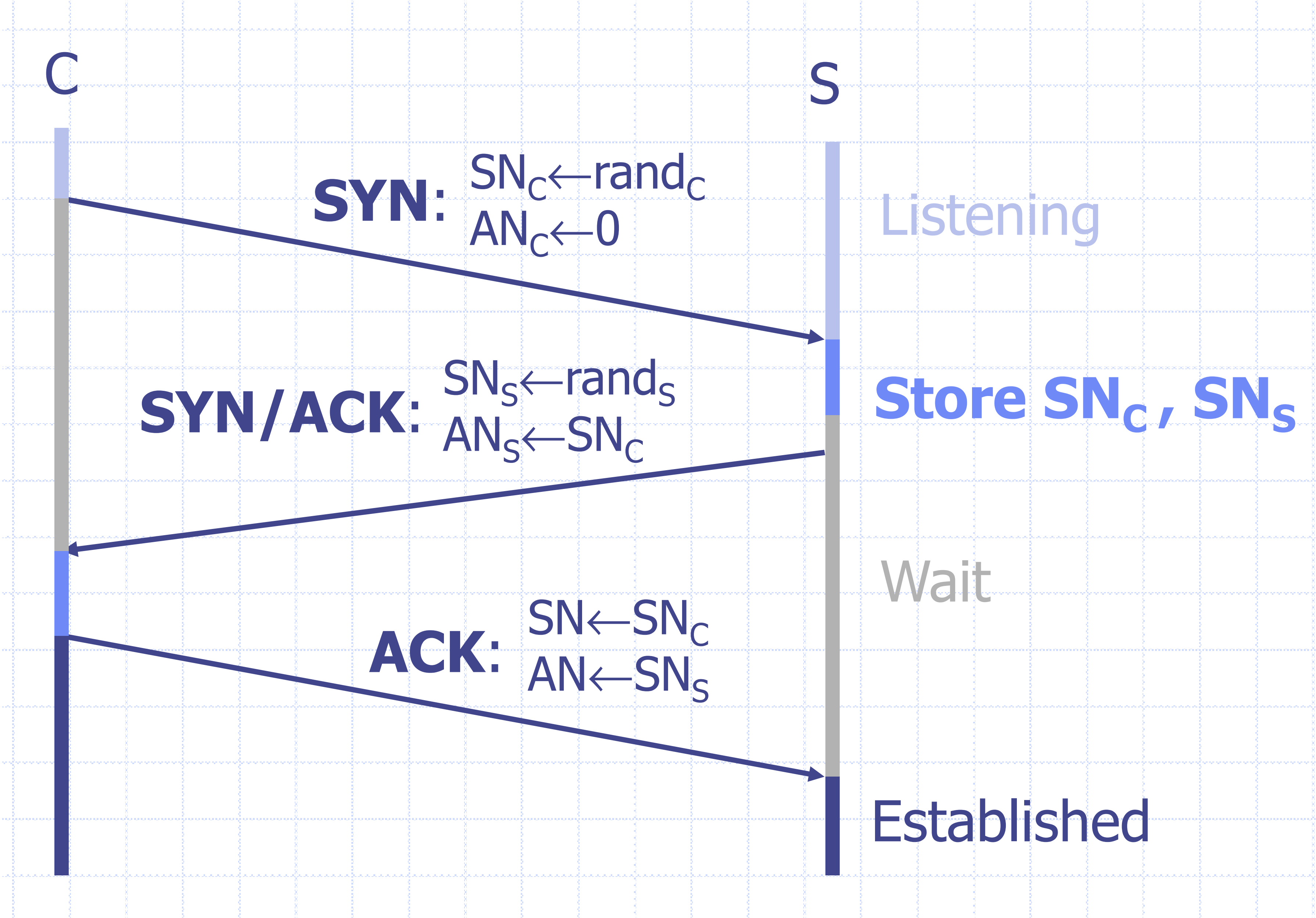


- Send ping request to broadcast address (ICMP Echo Req)
- Lots of responses:
  - Every host on target network generates a ping reply (ICMP Echo Reply) to victim

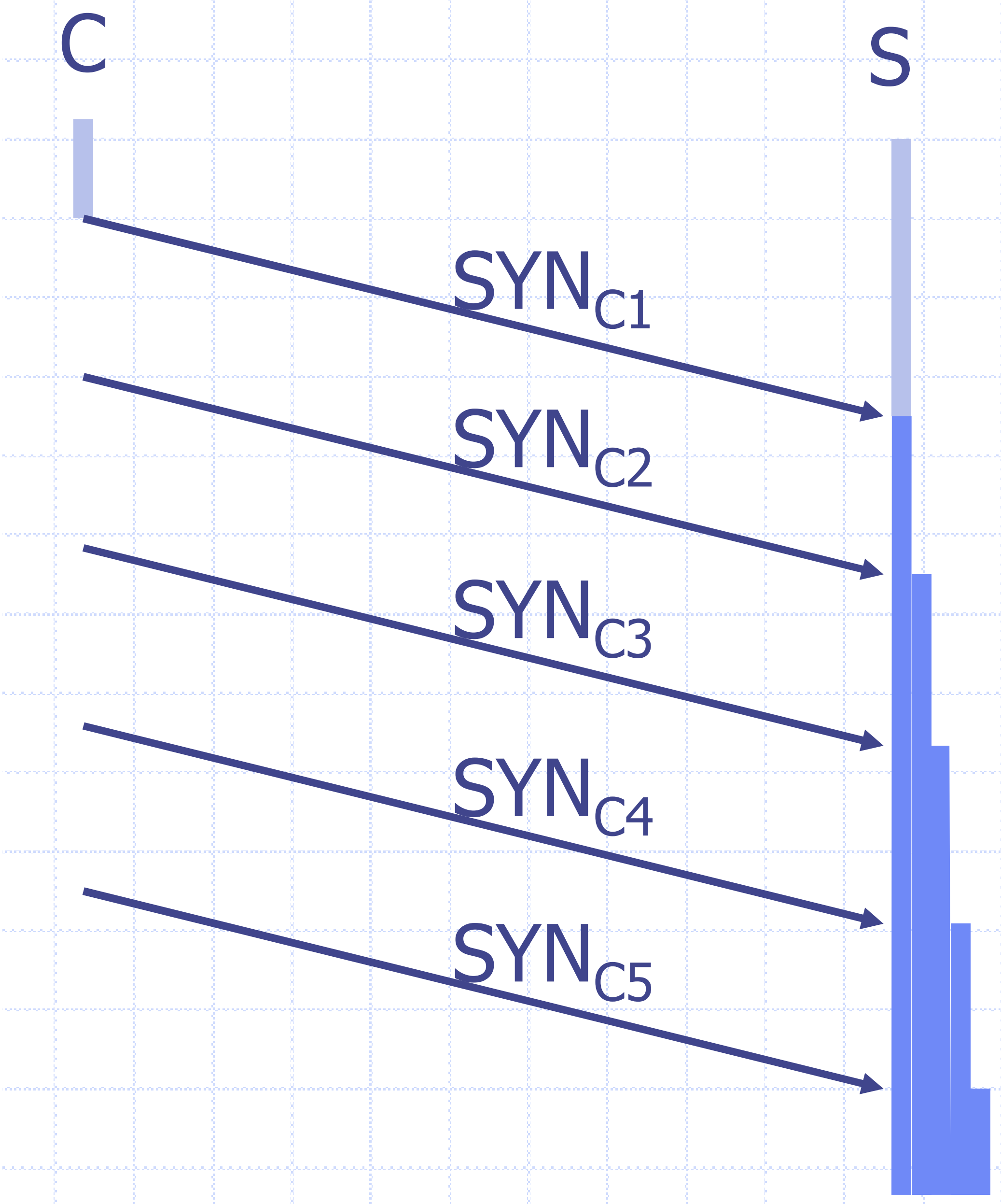
DNS Amplification Attack



TCP 3-way Handshake


C
S
SYN: $SN_C \leftarrow rand_C$ $AN_C \leftarrow 0$
Listening
SYN/ACK: $SN_S \leftarrow rand_S$ $AN_S \leftarrow SN_C$
Store SN_C , SN_S
Wait
ACK: $SN \leftarrow SN_C$ $AN \leftarrow SN_S$
Established

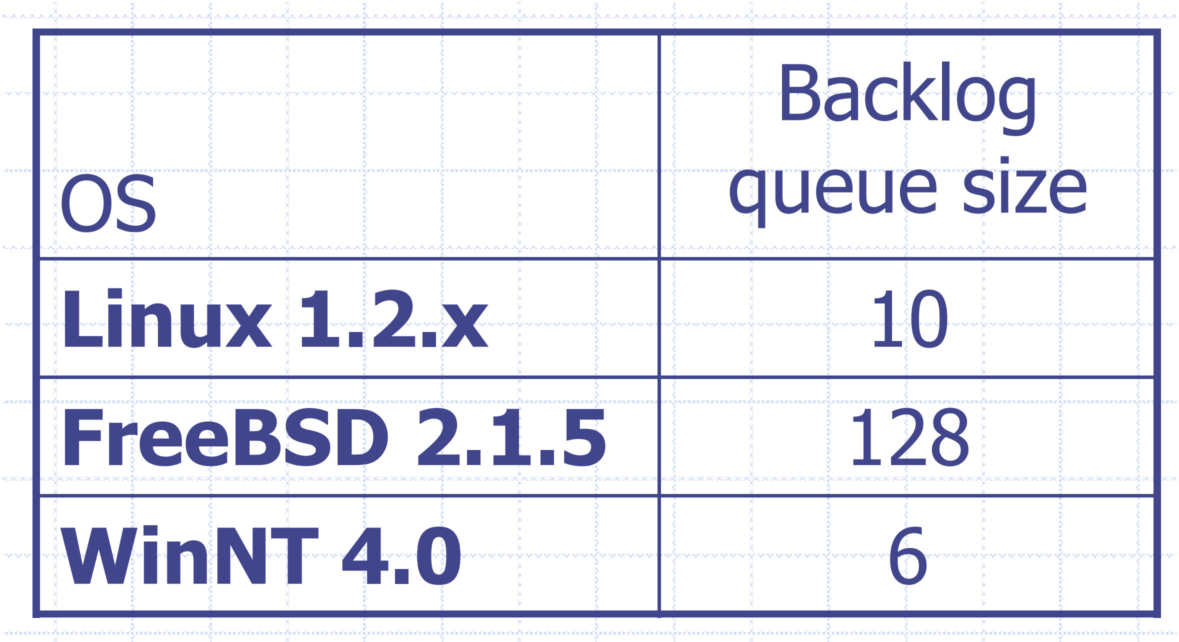
TCP SYN Flooding



Single machine:

- SYN Packets with **random source IP addresses**
- Fills up backlog queue on server
- No further connections possible

Why is it Vulnerable?



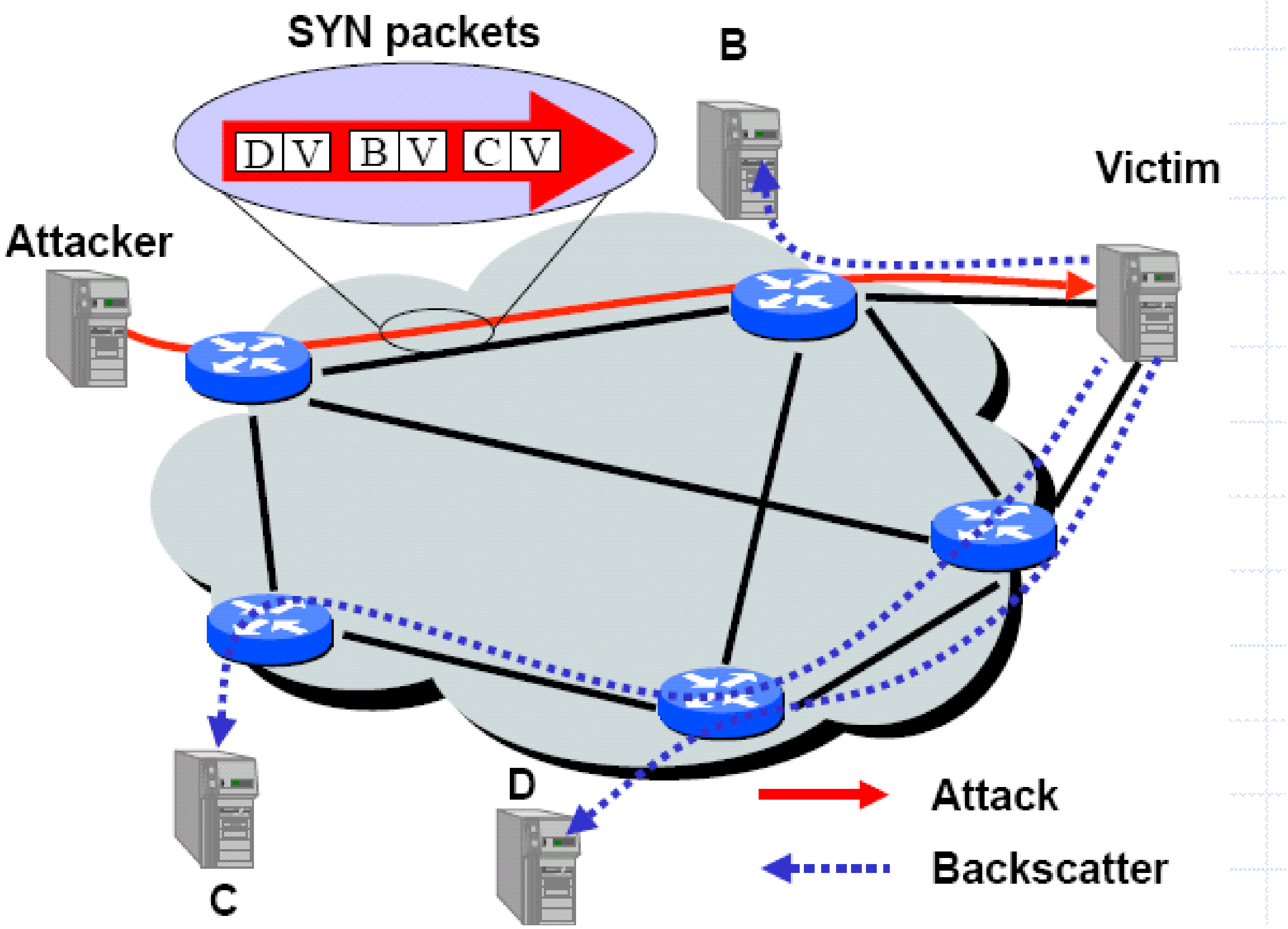
OS	Backlog queue size
Linux 1.2.x	10
FreeBSD 2.1.5	128
WinNT 4.0	6

Windows 2000 server: 80
Advanced Windows server: 400

- TCP backlog issue
  - Backlog timeout:
    - 3 minutes
  - Attacker need only send 128 SYN packets every 3 minutes.
    - Low rate SYN flood

```
Increase the backlog (Linux RedHat 7.3)
 # sysctl -w net.ipv4.tcp_max_syn_backlog="2048"
```

Backscatter Effect



- SYN with forged source IP ⇒ SYN/ACK to random host

TCP SYN Flood Case

- MS Blaster worm (2003)
  - Infected machines at noon on Aug 16th:
    - SYN flood on port 80 to windowsupdate.com
    - 50 SYN packets every second.
    - each packet is 40 bytes.
    - Spoofed source IP: a.b.X.Y where X,Y random.

- MS solution:
  - new name: windowsupdate.microsoft.com
  - Win update file delivered by Akamai

More Interesting Example: SQL Slammer

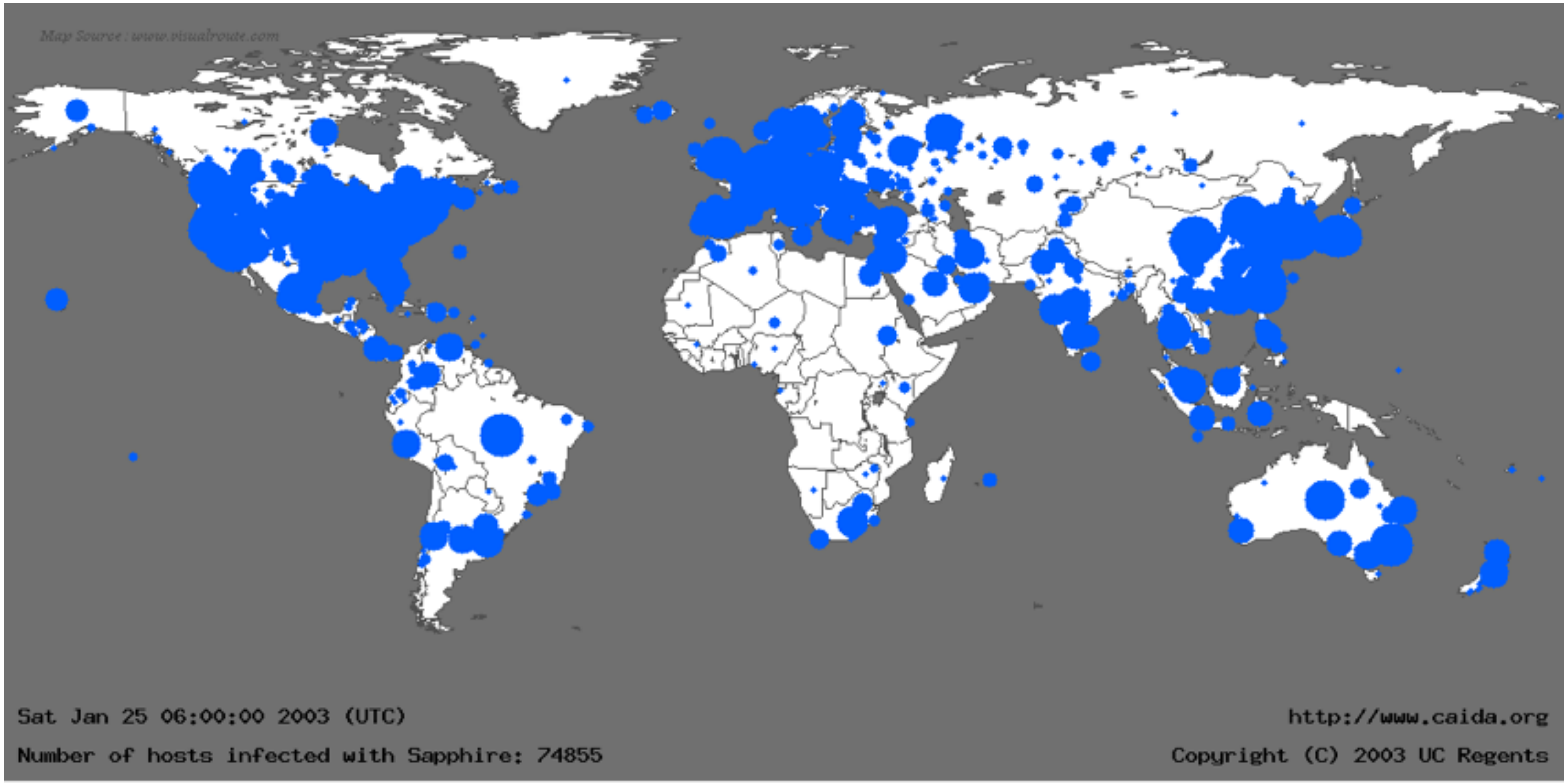
- Damage history (extract):
  - on Jan. 25, 2003
    - over 260,000 unique IP addresses infected by the Slammer worm within Internet Security Systems' monitored networks
    - Propagation of the worm overpowered Internet connections with millions of UDP/IP probes hours after the activity began.
    - ETH Zurich was not connected to the Internet for about 3 hours. Service for e-mail and web pages were only partially available.
  - On Feb. 5, 2003
    - (W)LAN for visitors and vendors at the Internet Expo in Zurich (with 330 vendors present) was not available due to SQL Slammer infections of vendor’s computers.

More Interesting Example: SQL Slammer

- How the SQL Slammer DDoS attack works
  - The amplifying network of zombies is built fast by worm spreading based on exploiting a system vulnerability
  - System vulnerability
    - Exploit Microsoft SQL Servers and MSDE- enabled products vulnerable to the SQL Server resolution service buffer overflow.
  - Slammer's main function is
    - propagation, sending 376 bytes of code across port 1434/UDP until the SQL Server shuts down
  - Scanning/infection/attack code is combined

- Countermeasures:
  - Patch the vulnerable SQL server installations
  - Filter attack traffic to port 1434/UDP

SQL Slammer



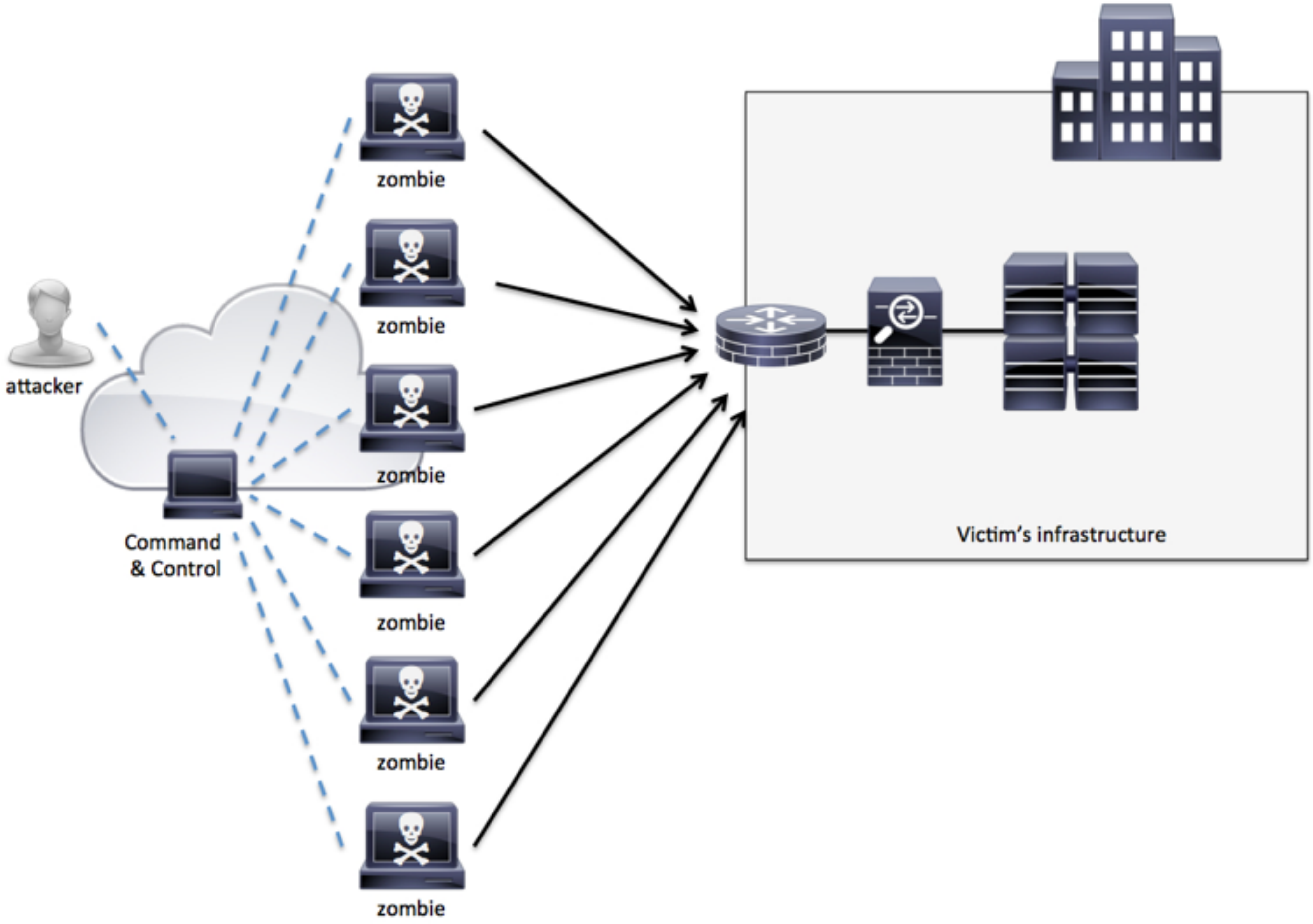
Map Source : www.visualroute.com

Sat Jan 25 06:00:00 2003 (UTC)

Number of hosts infected with Sapphire: 74855

http://www.caida.org

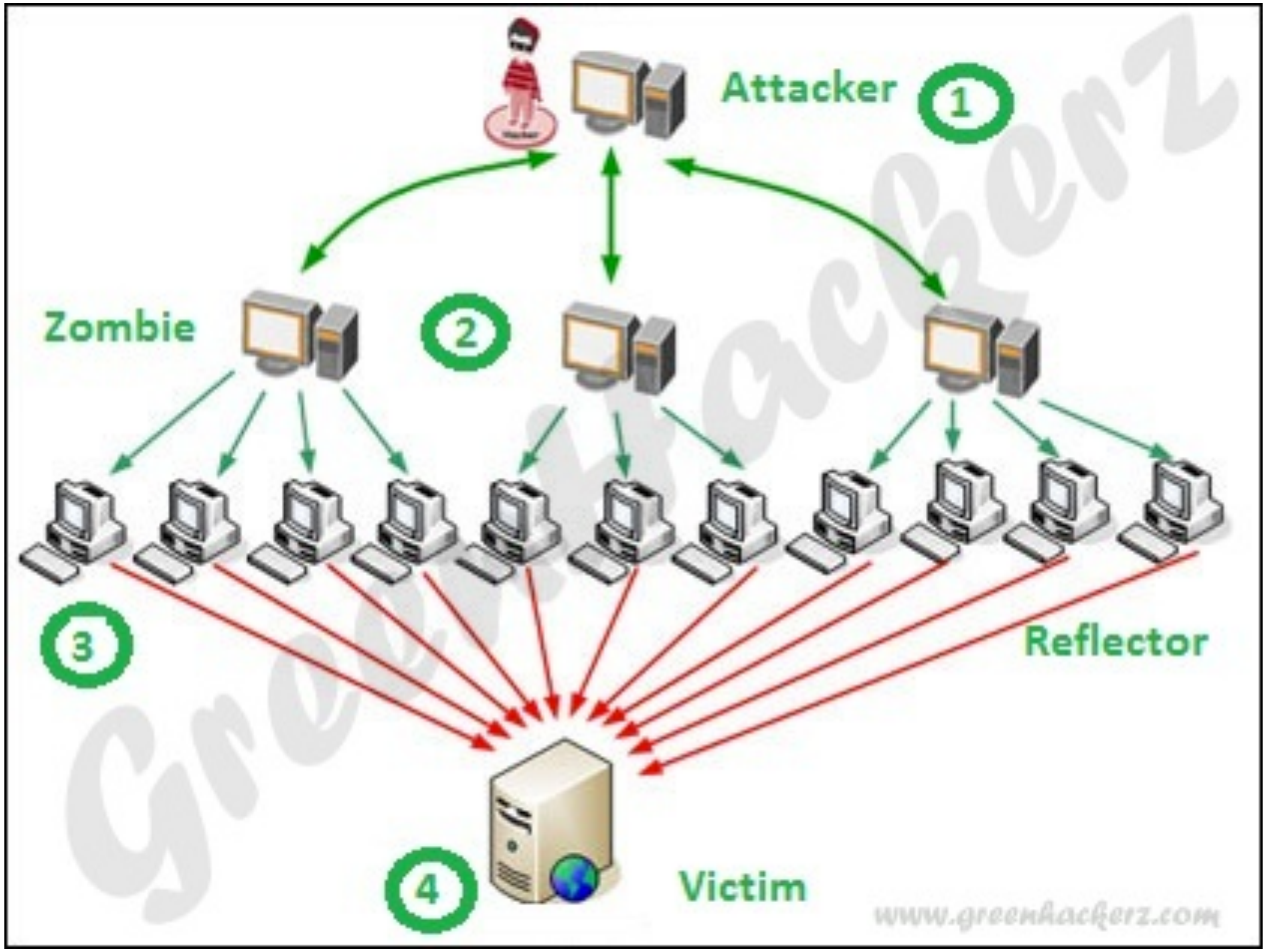
DDoS with Botnet



DRDoS with Botnet

- DRDoS Attack
  - Distributed Reflector Denial of Service
  - Reflectors are uncompromised machines.
  - The slave zombies send packets to the reflectors **with IP source addresses spoofed as the target**
    - **reflectors return packets to the target**
  - The reflectors carry out the flooding rather than the slaves.
  - More distributed than a typical DDoS attack.

DRDoS with Botnet

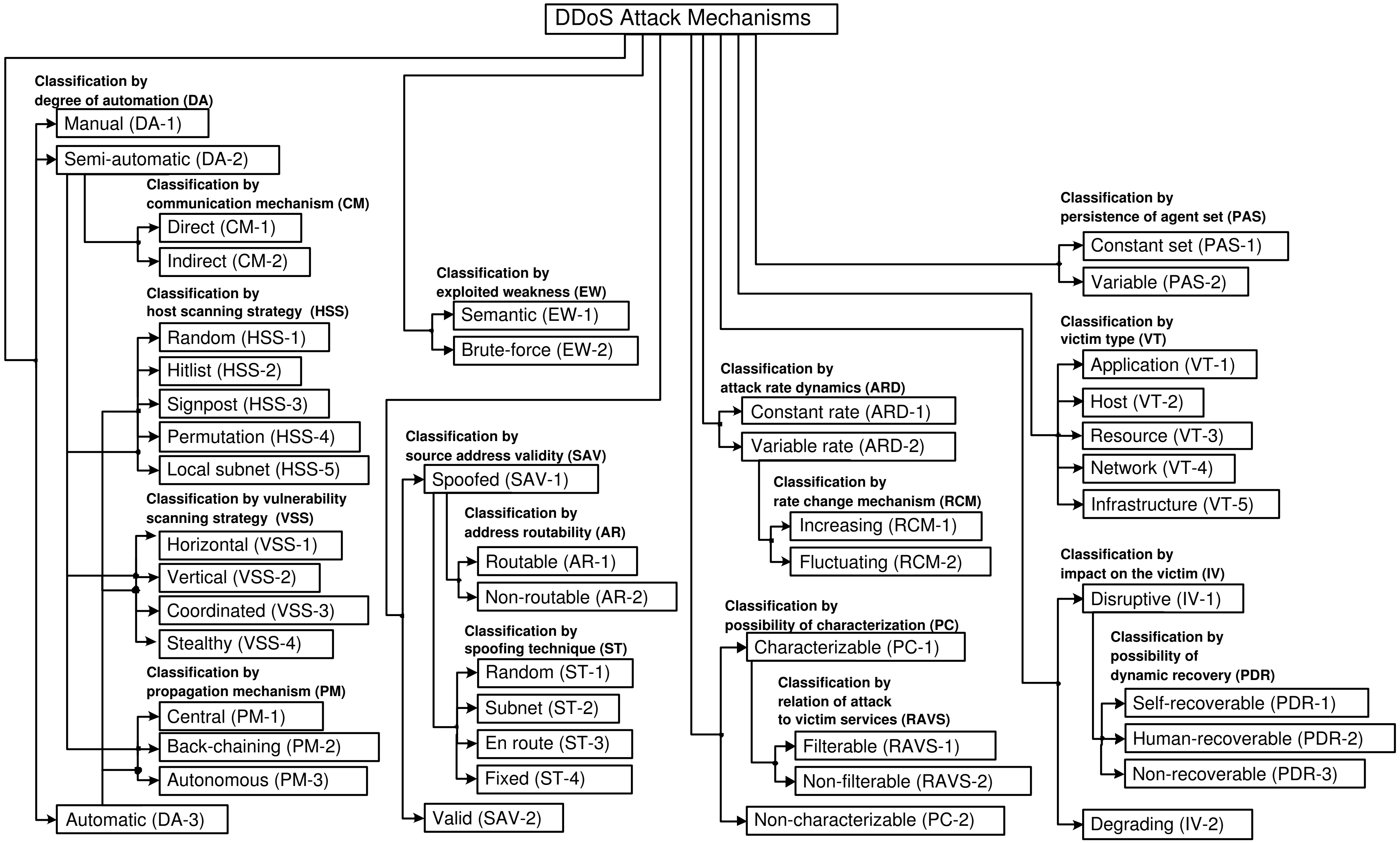


Application Level Attack

- Command bot army to do the following operations
  - make a TCP session
  - send short HTTP HEAD request to a target
  - keep sending
- It can evade detection approaches
  - TCP SYN flooding detection
- However,
  - attacker should use real IP addresses not spoofed ones
  - reason why an attacker uses bots

DDoS classification

- A Taxonomy of DDoS Attack and DDoS Defense Mechanisms
  - Mirkovic et al., ACM CCR 2004



DDoS Attack Mechanisms

Classification by degree of automation (DA)
Manual (DA-1)
Semi-automatic (DA-2)
Classification by communication mechanism (CM)
Direct (CM-1)
Indirect (CM-2)
Classification by host scanning strategy (HSS)
Random (HSS-1)
Hitlist (HSS-2)
Signpost (HSS-3)
Permutation (HSS-4)
Local subnet (HSS-5)
Classification by vulnerability scanning strategy (VSS)
Horizontal (VSS-1)
Vertical (VSS-2)
Coordinated (VSS-3)
Stealthy (VSS-4)
Classification by propagation mechanism (PM)
Central (PM-1)
Back-chaining (PM-2)
Autonomous (PM-3)
Automatic (DA-3)

Classification by exploited weakness (EW)
Semantic (EW-1)
Brute-force (EW-2)

Classification by source address validity (SAV)
Spoofed (SAV-1)
Classification by address routability (AR)
Routable (AR-1)
Non-routable (AR-2)
Classification by spoofing technique (ST)
Random (ST-1)
Subnet (ST-2)
En route (ST-3)
Fixed (ST-4)
Valid (SAV-2)

Classification by attack rate dynamics (ARD)
Constant rate (ARD-1)
Variable rate (ARD-2)
Classification by rate change mechanism (RCM)
Increasing (RCM-1)
Fluctuating (RCM-2)

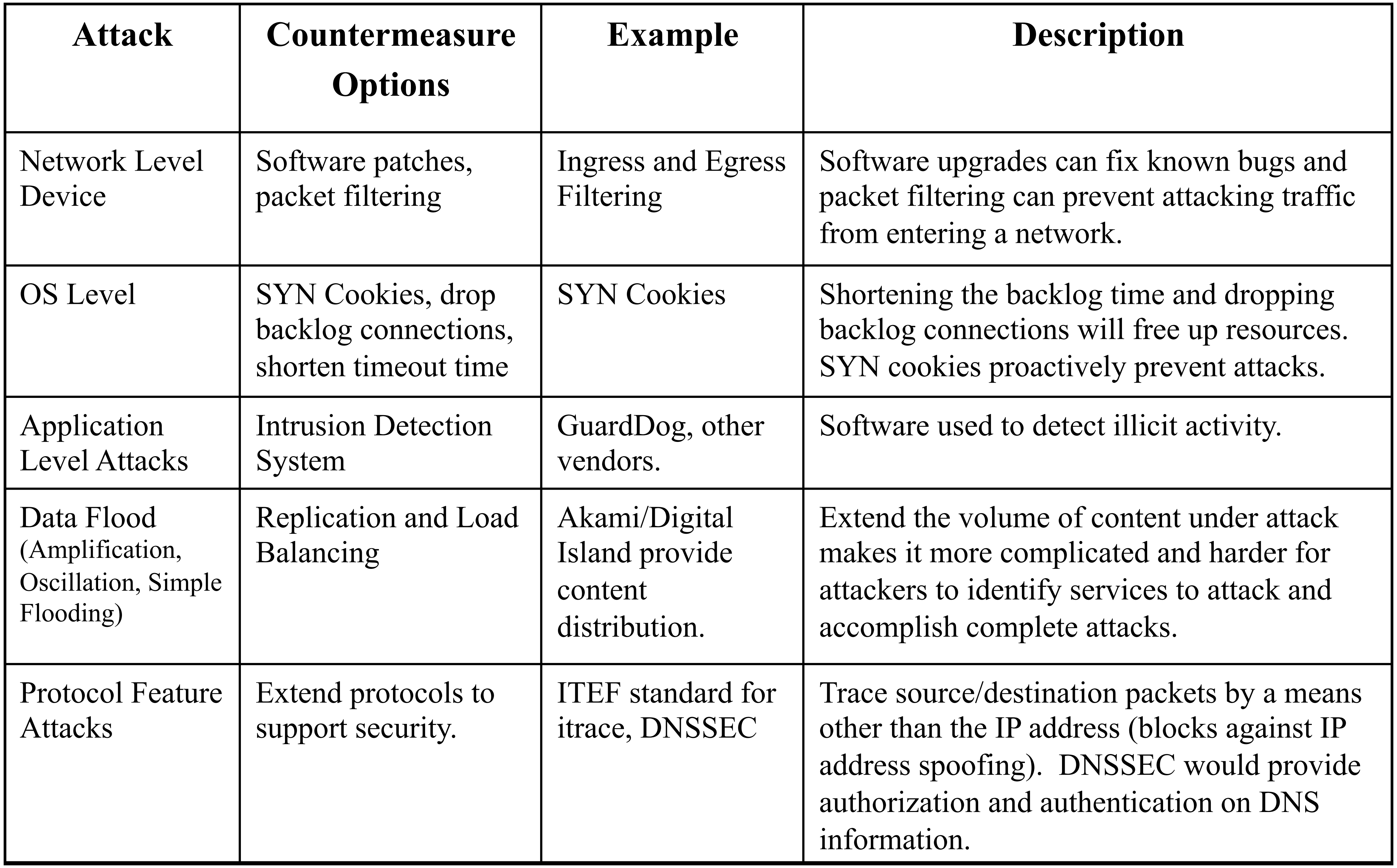
Classification by possibility of characterization (PC)
Characterizable (PC-1)
Classification by relation of attack to victim services (RAVS)
Filterable (RAVS-1)
Non-filterable (RAVS-2)
Non-characterizable (PC-2)

Classification by persistence of agent set (PAS)
Constant set (PAS-1)
Variable (PAS-2)

Classification by victim type (VT)
Application (VT-1)
Host (VT-2)
Resource (VT-3)
Network (VT-4)
Infrastructure (VT-5)

Classification by impact on the victim (IV)
Disruptive (IV-1)
Classification by possibility of dynamic recovery (PDR)
Self-recoverable (PDR-1)
Human-recoverable (PDR-2)
Non-recoverable (PDR-3)
Degrading (IV-2)

DDoS Defense - next class



Attack	Countermeasure Options	Example	Description
Network Level Device	Software patches, packet filtering	Ingress and Egress Filtering	Software upgrades can fix known bugs and packet filtering can prevent attacking traffic from entering a network.
OS Level	SYN Cookies, drop backlog connections, shorten timeout time	SYN Cookies	Shortening the backlog time and dropping backlog connections will free up resources. SYN cookies proactively prevent attacks.
Application Level Attacks	Intrusion Detection System	GuardDog, other vendors.	Software used to detect illicit activity.
Data Flood (Amplification, Oscillation, Simple Flooding)	Replication and Load Balancing	Akami/Digital Island provide content distribution.	Extend the volume of content under attack makes it more complicated and harder for attackers to identify services to attack and accomplish complete attacks.
Protocol Feature Attacks	Extend protocols to support security.	ITEF standard for itrace, DNSSEC	Trace source/destination packets by a means other than the IP address (blocks against IP address spoofing). DNSSEC would provide authorization and authentication on DNS information.

by Dr. Ruby Lee

DDoS Trend

DDoS Trend - CISCO

Distribution	Management	# Attackers (Bandwidth)	Type of attack	Protection
–Email attach –Download from questionable site –via "chat" –ICQ, AIM, IRC –Worms	Via botnets	**~X00,000 attackers** (X-X0 Gbps)	**•Legitimate requests** **•Infrastructure elements (DNS, SMTP, HTTP…)**	**•Blackhole (?)** **•ACL (?)** **•DDoS solutions** **•Anycast (?)**
–Email attach –via "chat" ICQ, AIM, IRC…	Manually	**~X00-X,000 Attackers** (X00 Mbps)	**•All type of applicatios (HTTP, DNS, SMTP)** **•Spoofed SYN**	**•ISP/IDC** **•Blackhole** **•ACL** **•DDoS solutions**
Manually (hack to servers)	Manually	**X0-X00 attackers** (X0 Mbps)	**Spoofed SYN** **Non critical Protocols (eg ICMP)**	**•Enterprise level** **•Firewall/** **•ACL access routers**

DDoS Trend - from Akamai Report (2015)

- Summary
  - DDoS attacks, Q4 2015 vs. Q4 2014
    - 148.85% increase in total DDoS attacks 168.82% increase in infrastructure layer
  - DDoS attacks, Q4 2015 vs. Q3 2015
    - 39.89% increase in total DDoS attacks 42.38% increase in infrastructure layer
  - Web application attacks, Q4 2015 vs. Q3 2015
    - 28.10% increase in total web application attacks 28.65% increase in web application
    - 12.19% increase in SQL attacks

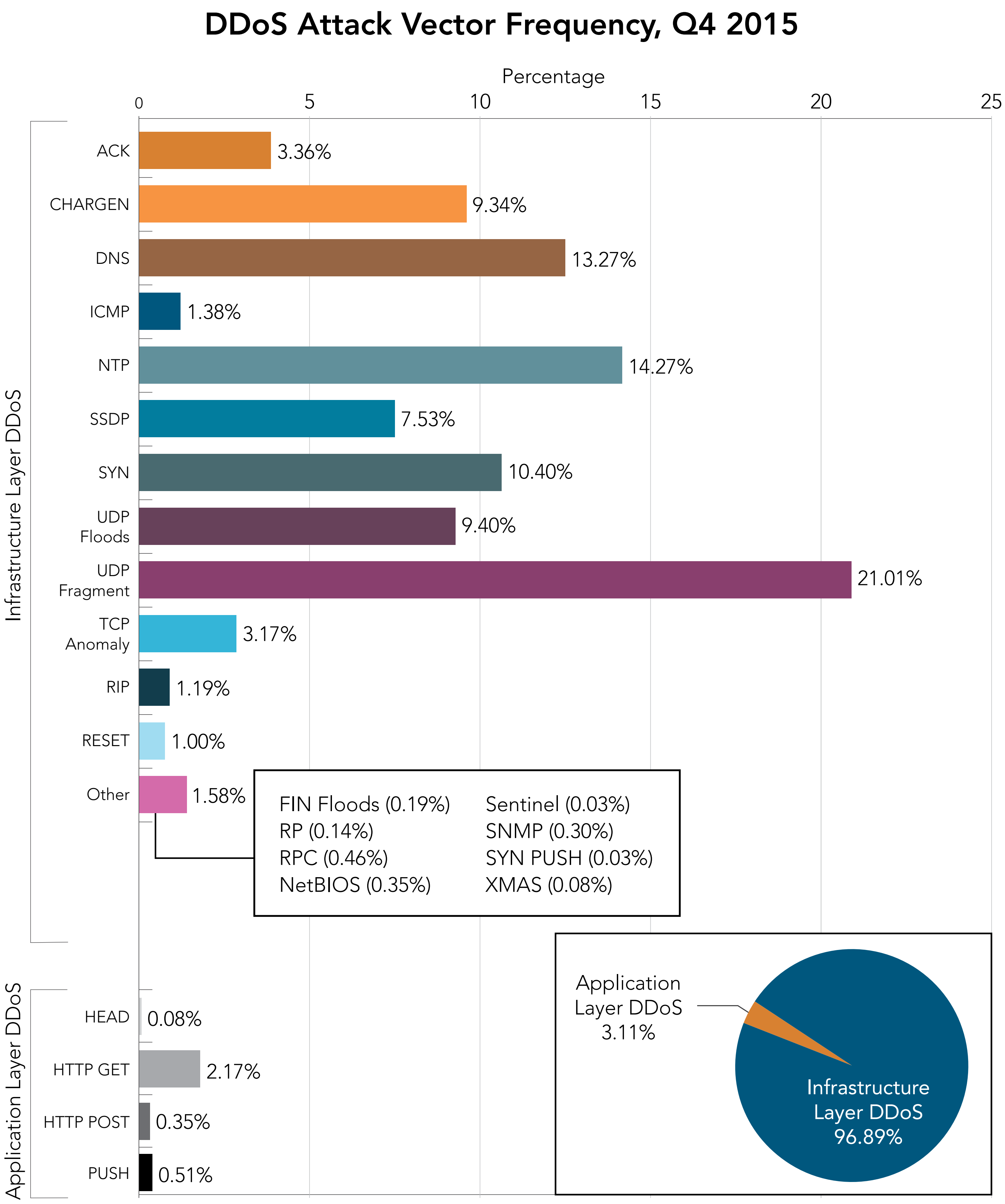


Figure 2-1: Of the 24 DDoS attack vectors tracked this quarter, four—UDP Fragment, NTP, SYN and DNS—made up almost 60% of the attacks

Top 10 Source Countries for DDoS Attacks, Q4 2015

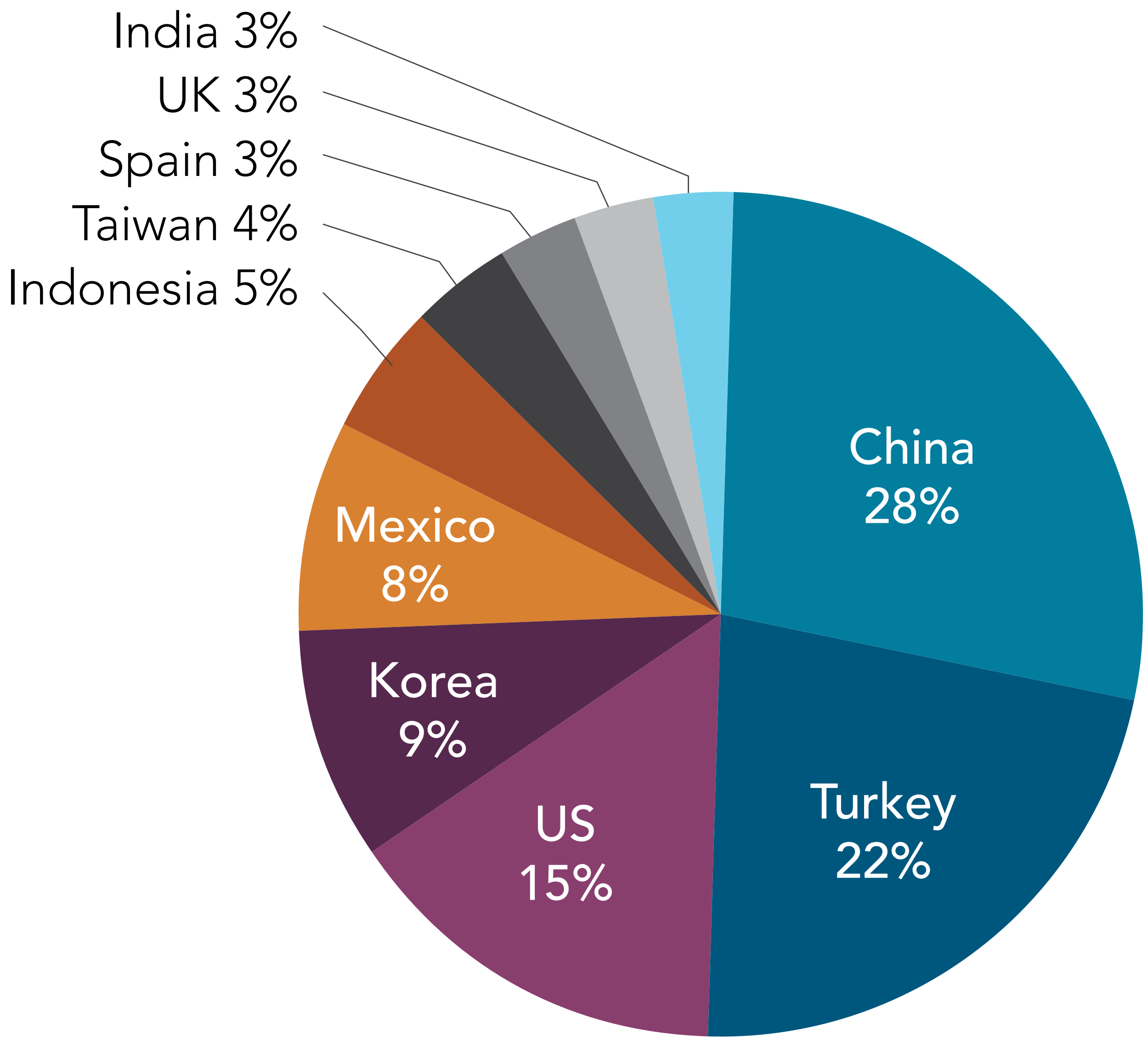


Figure 2-9: In Q4 2015, DDoS attacks were most commonly observed coming from China, Turkey and the US

Top 5 Source Countries for DDoS Attacks, Q4 2014–Q4 2015

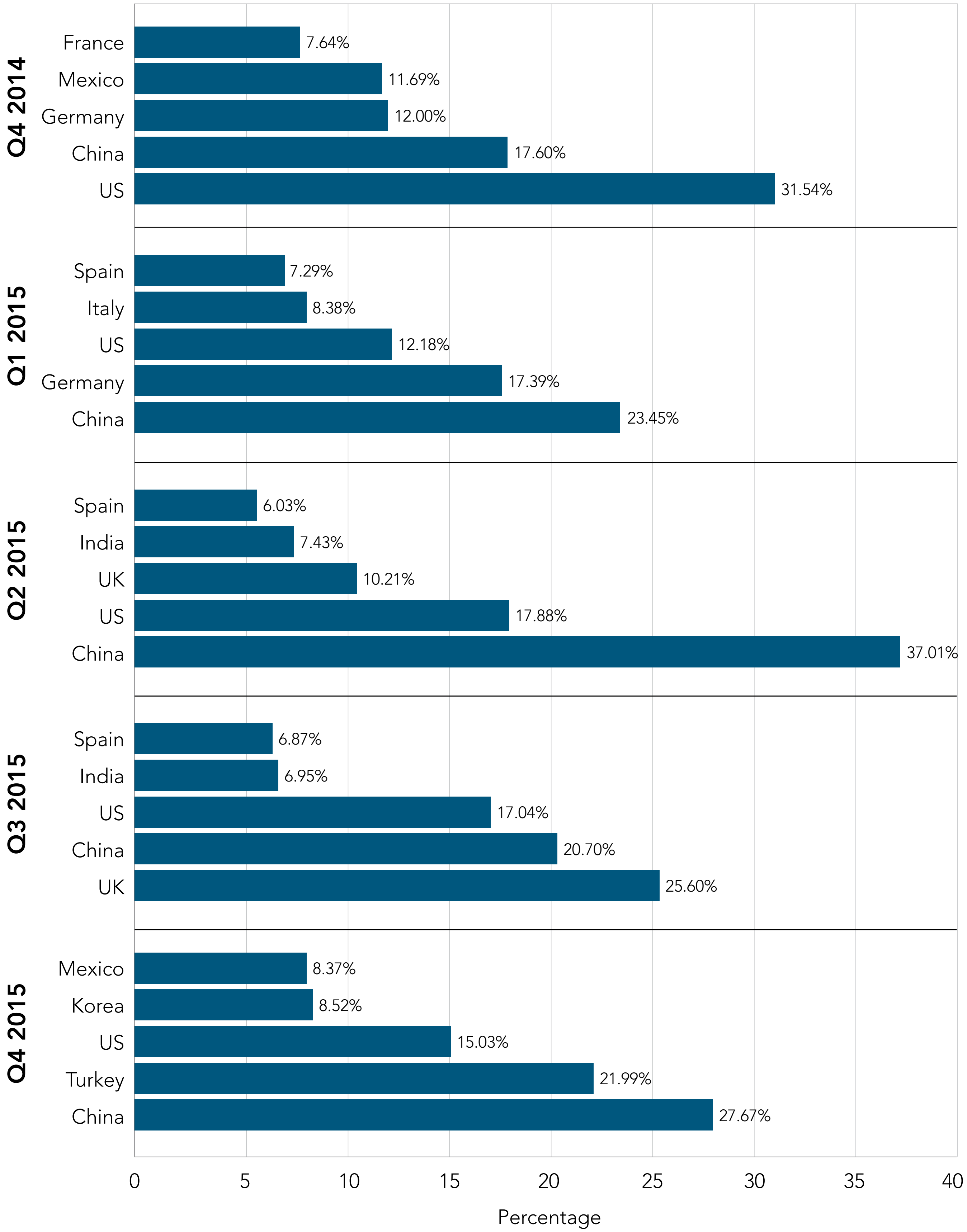


Figure 2-10: While the US and China have been in the top five every quarter, Q4 2015 marks the first time that Turkey has made the list

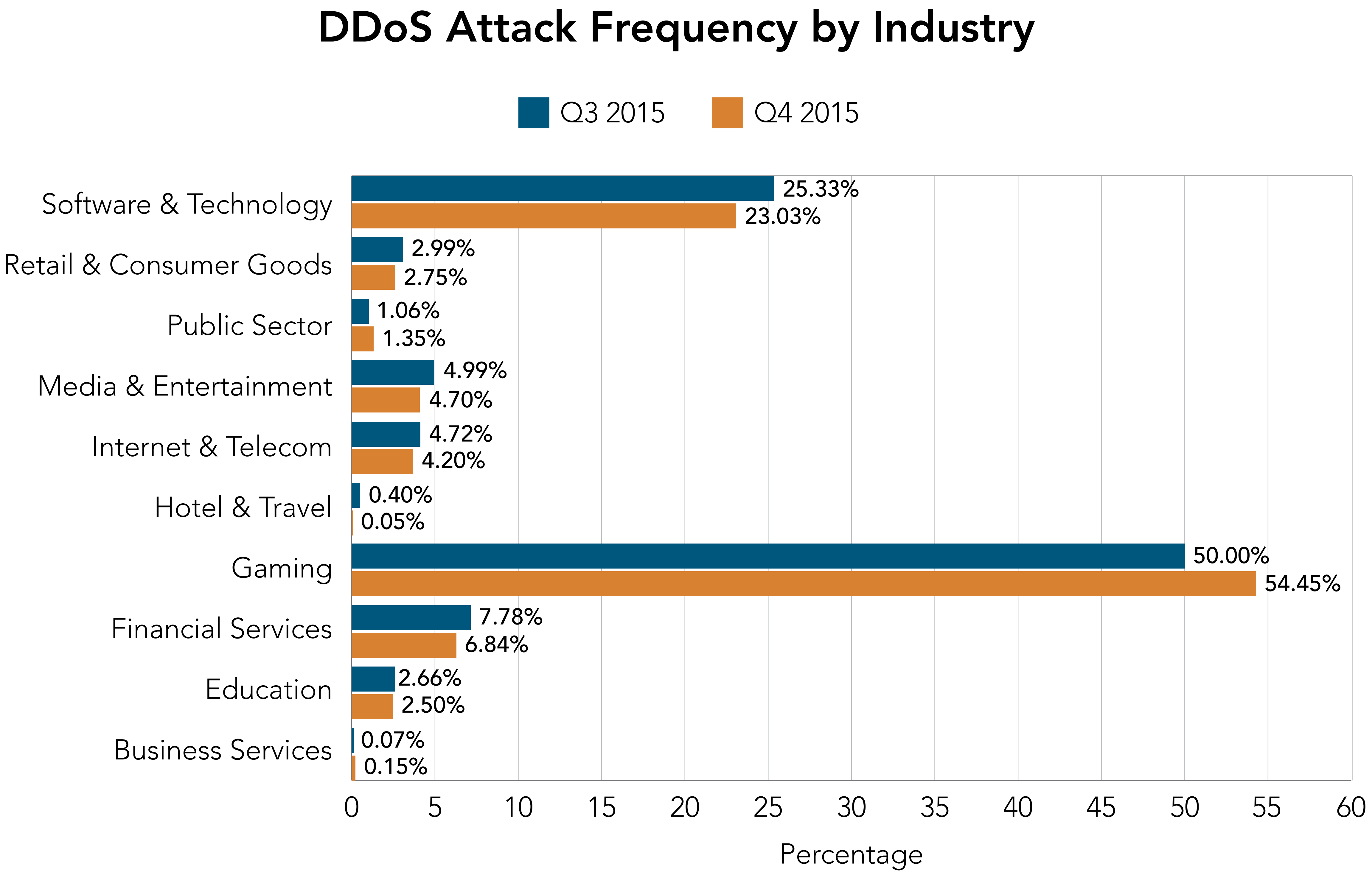


Figure 2-11: The gaming and software & technology industries were targeted 77% of the time in Q4 2015, up from 75% in Q3 2015

Reflection DDoS Attacks, Q4 2014–Q4 2015

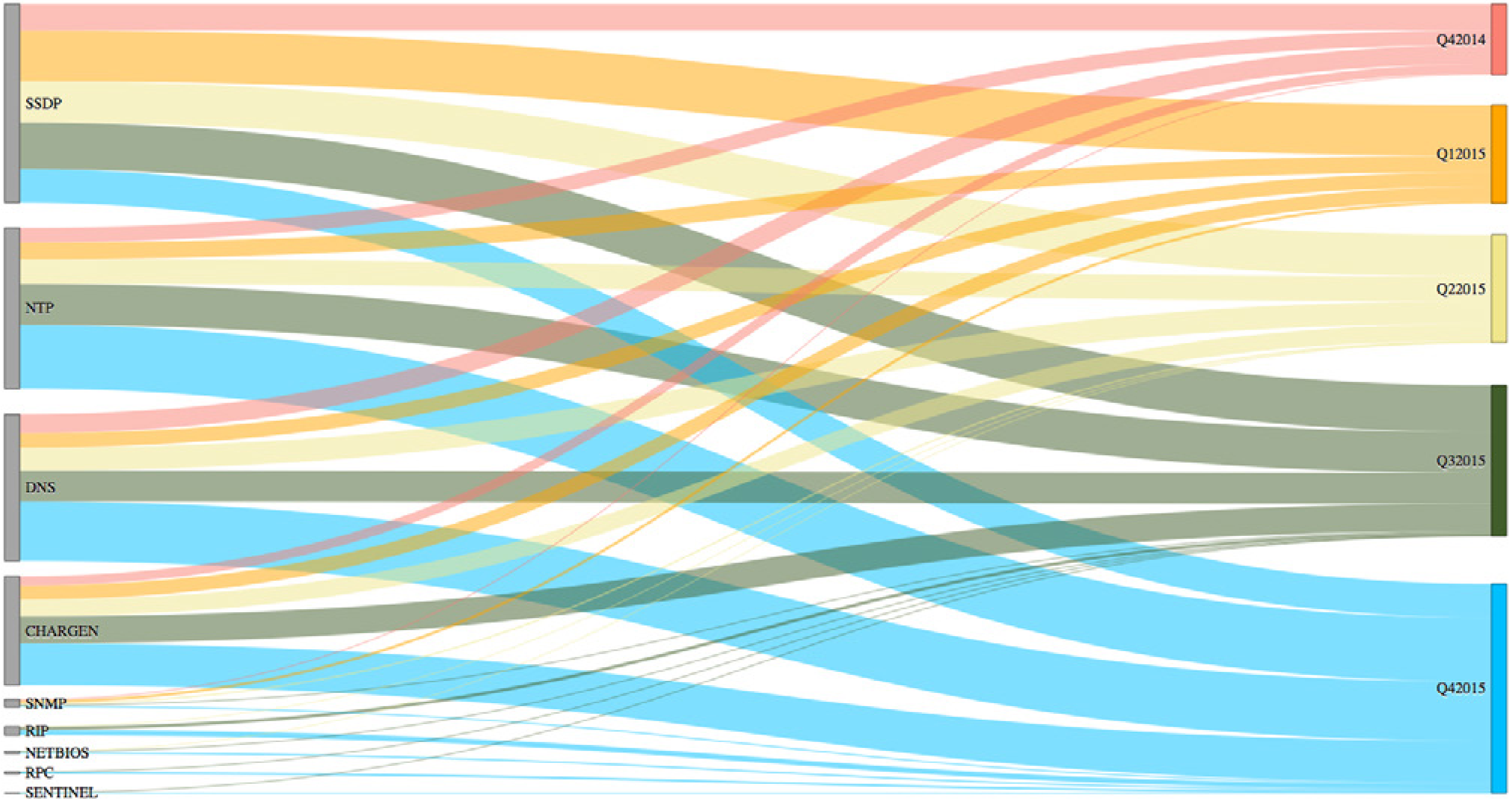


Figure 2-14: SSDP, NTP, DNS and CHARGEN have consistently been used as the most common reflection attack vectors, as can be seen on the left axis, and the use of reflection attacks has increased dramatically since Q4 2014, as shown on the right axis

DDoS Reflector Heat Map, Q4 2015

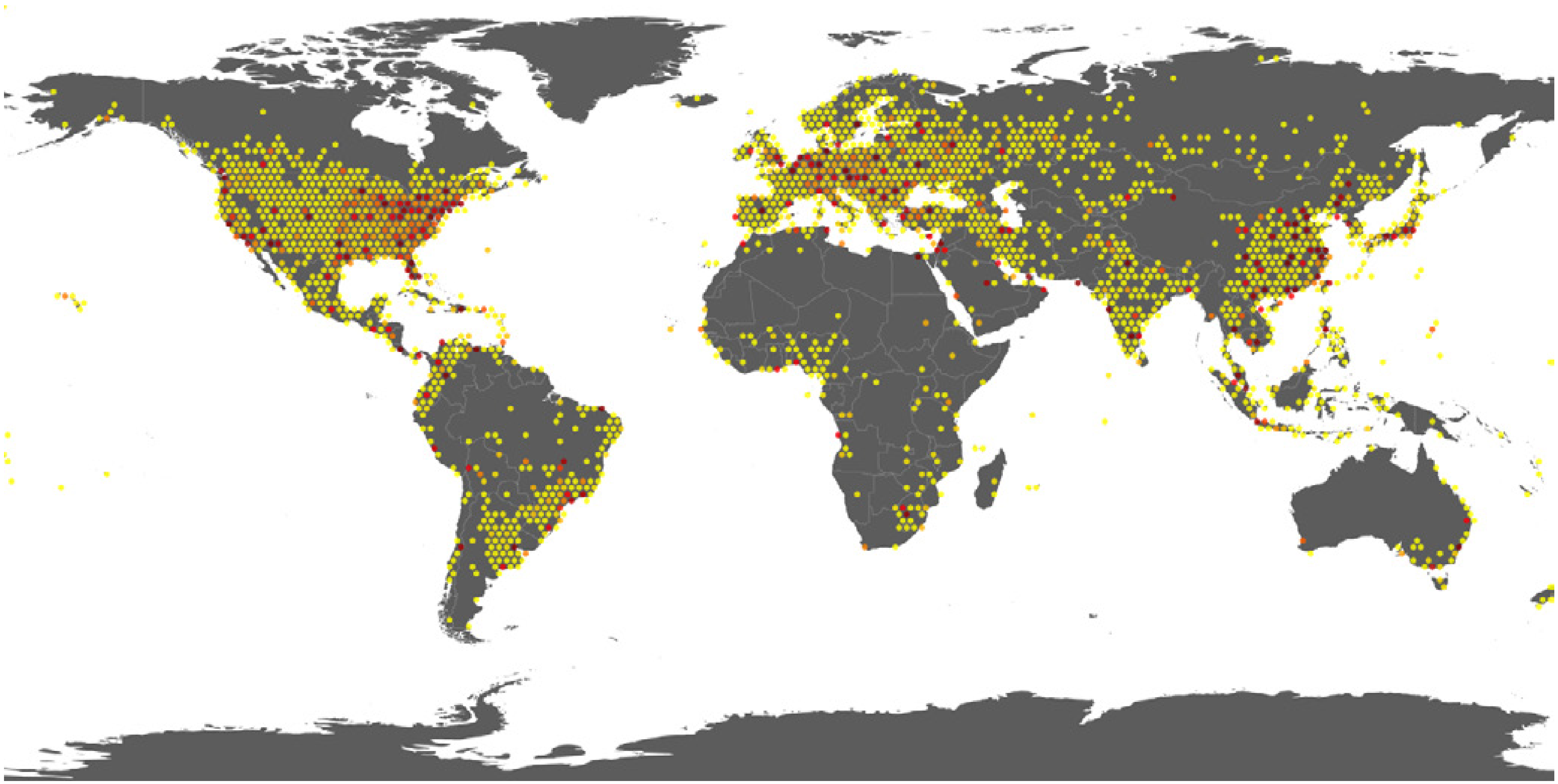


Figure 4-3: The location of vulnerable devices used in reflection-based attacks during Q4 2015 was concentrated in the US, Asia and Europe

Web Application Attacks Over HTTP vs. HTTPS

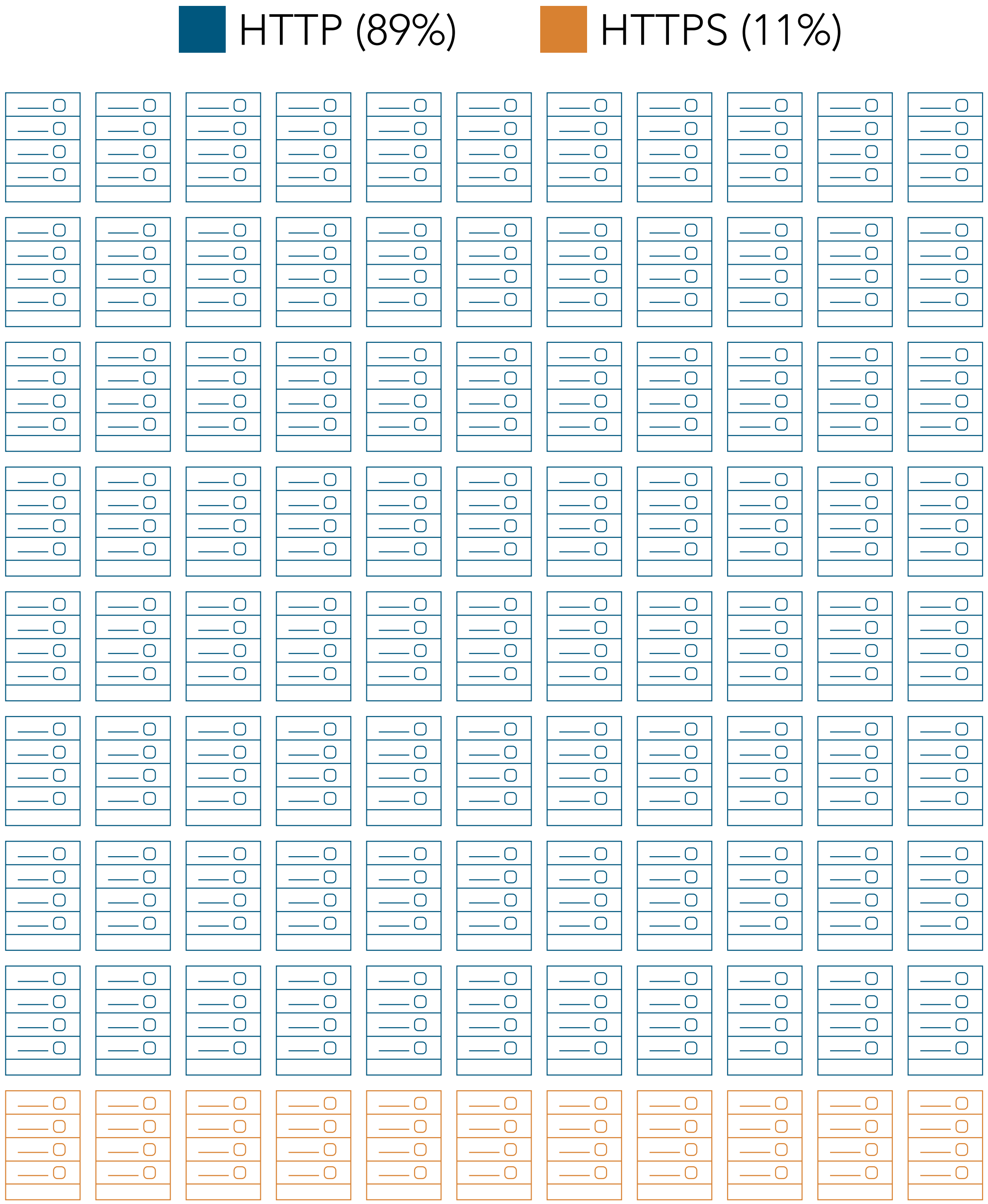


Figure 3-1: Only 11% of the web application attacks observed in Q4 2015 were over encrypted (HTTPS) connections

Web Application Attack Vectors Over HTTP, Q4 2015

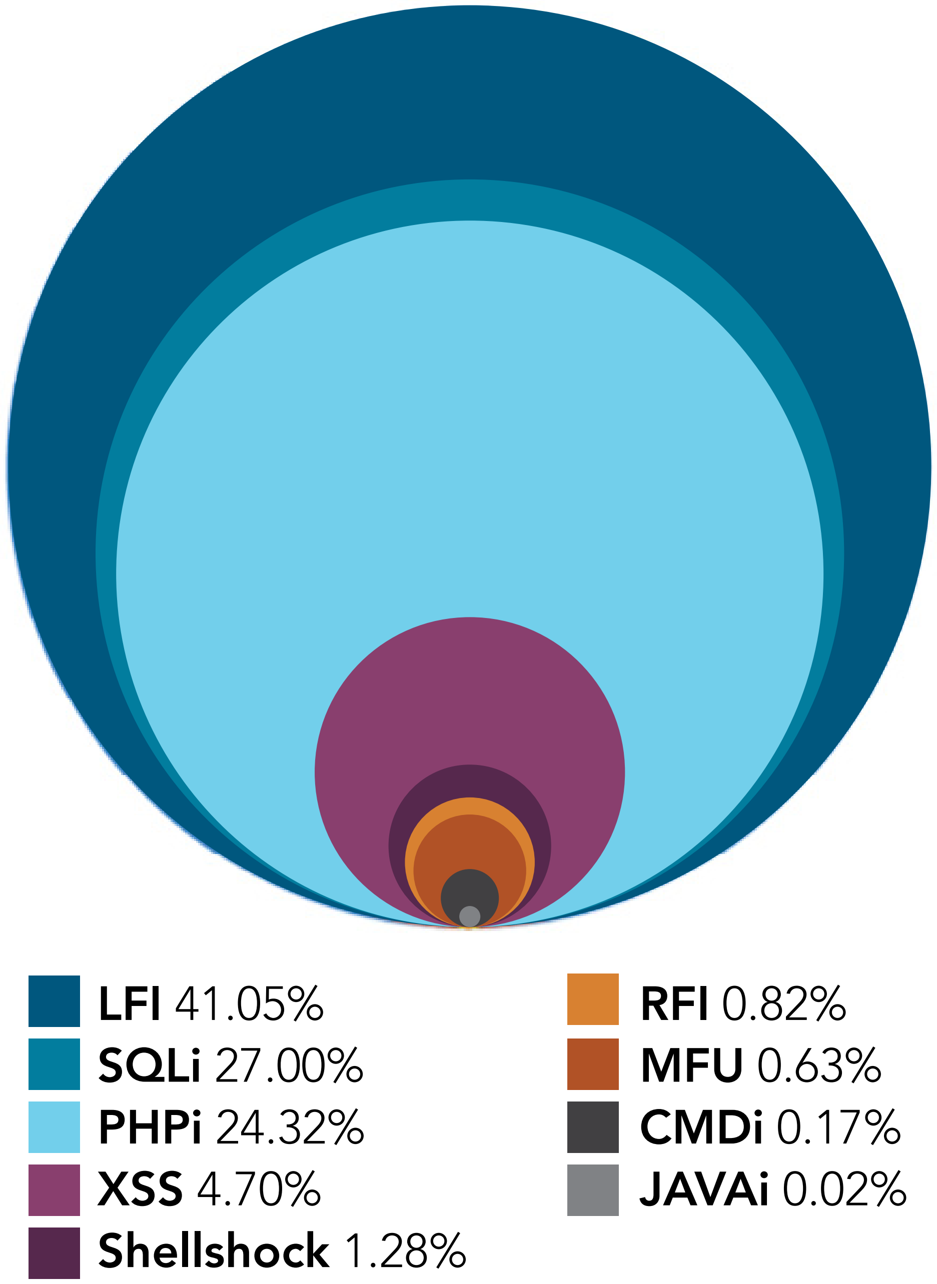


Figure 3-2: The three most popular attack vectors—LFI, SQLi and PHPi—were used in more than 92% of the attacks over HTTP