
ESTD1845
QUEEN'S
UNIVERSITY
BELFAST

Denial of Service - Part 1

Dr. Sandra Scott-Hayward

CSC3064 Lecture 17

School of Electronics, Electrical Engineering and Computer Science

Session Overview

- What is a (D)DoS?
- Attack techniques
- Example attacks

References:
Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.
Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.
Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2007

QUEEN'S UNIVERSITY BELFAST

(D)DoS Attacks

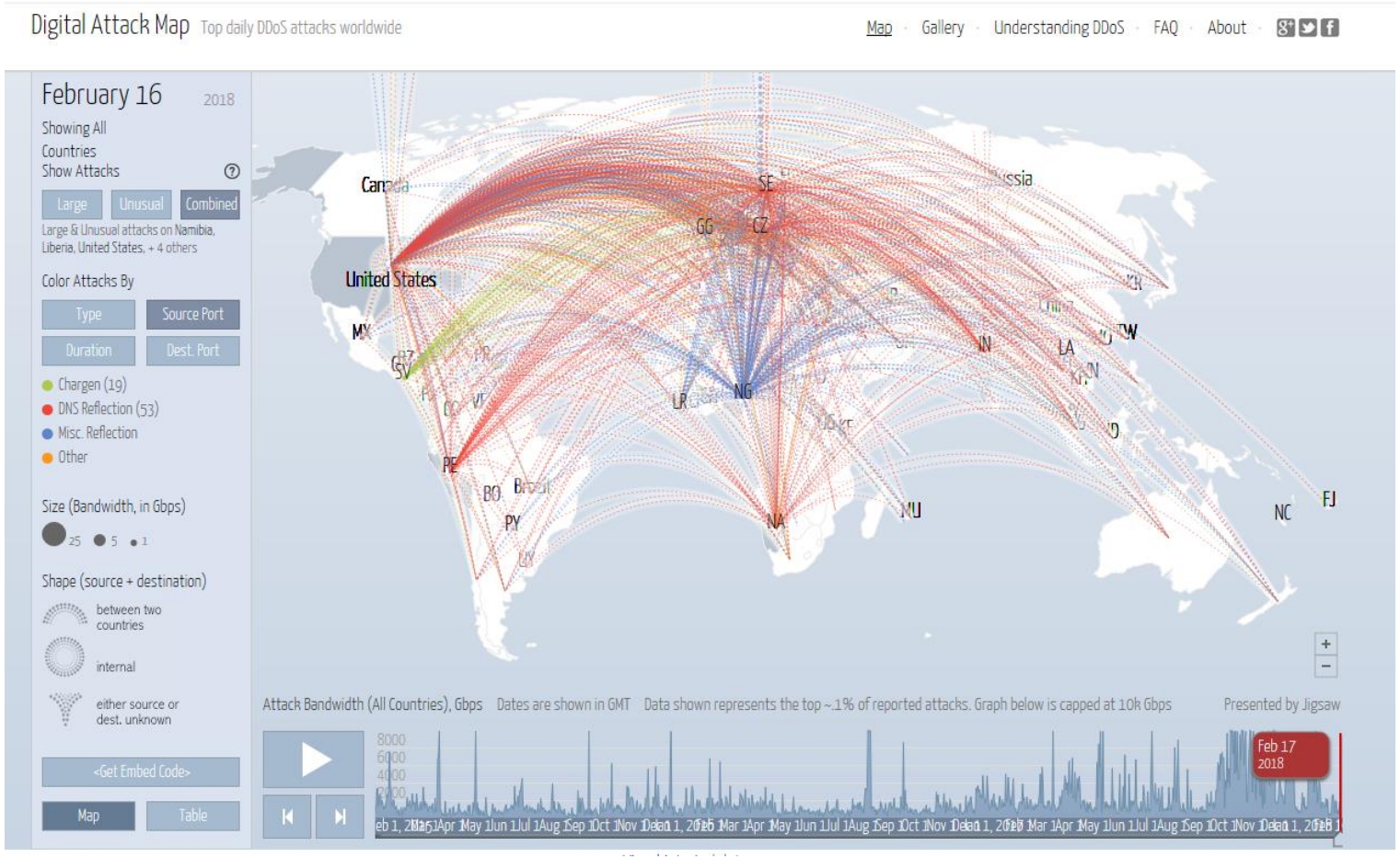
- Attacks that make computer systems inaccessible by flooding servers, networks, or even end-user systems with useless traffic so that legitimate users can no longer gain access to those resources

- One way to classify DDoS attacks is in terms of the type of resource that is consumed

- The resource consumed is either an ***internal host resource on the target system*** or ***data transmission capacity in the local network*** to which the target is attached

QUEEN'S UNIVERSITY BELFAST

How serious is the DDoS problem?



http://www.digitalattackmap.com

Current Internet not designed to handle DDoS attacks

QUEEN'S UNIVERSITY BELFAST

Attacking Techniques

Resource destruction by:

- Hacking into systems
- Making use of implementation weaknesses such as buffer overrun
- Deviation from proper protocol execution

Resource reservations that are never used (e.g. bandwidth)

E.g. TCP connections with window 0

Resource depletion by causing:

- Storage of (useless) state information
- High traffic load (requires high overall bandwidth from attacker)
- Expensive computations (“expensive cryptography”)

Origin of malicious traffic:

- Single source with single / multiple (forged) source addresses
- Multiple sources with forged / valid source addresses (Distributed DoS)

QUEEN'S UNIVERSITY BELFAST

Resource Destruction

Deviation from proper protocol execution – well known examples:

Ping-of-Death

- Attacker sends IP fragments that exceed the total size of 65,535 bytes
- After reassembly a buffer overflow occurs…

LAND attack

- TCP spoofing is used to send SYN packet
- Source & destination address equal
- OS may run in an infinite loop

Teardrop attack

- Exploits TCP/IP fragmentation reassembly
- https://security.radware.com/ddos-knowledge-center/ddospedia/teardrop-attack/

QUEEN'S UNIVERSITY BELFAST

Resource Depletion

Expensive computations (“expensive cryptography”)

- Often at “higher” layers
- At L3/L4: Parallel negotiation of many cryptographic connections
- Typical example: THC SSL DoS tool (performs permanent renegotiations) https://tools.kali.org/stress-testing/thc-ssl-dos

Storage of (useless) state information

- IP fragment attack
  - Attacker sends IP fragments that never form a complete packet
  - Receiver must store fragments until timeout
- TCP SYN Flooding

High traffic load (requires high bandwidth or amplification)

- Examples for amplification techniques:
  - Smurf attack
  - DNS & NTP amplification

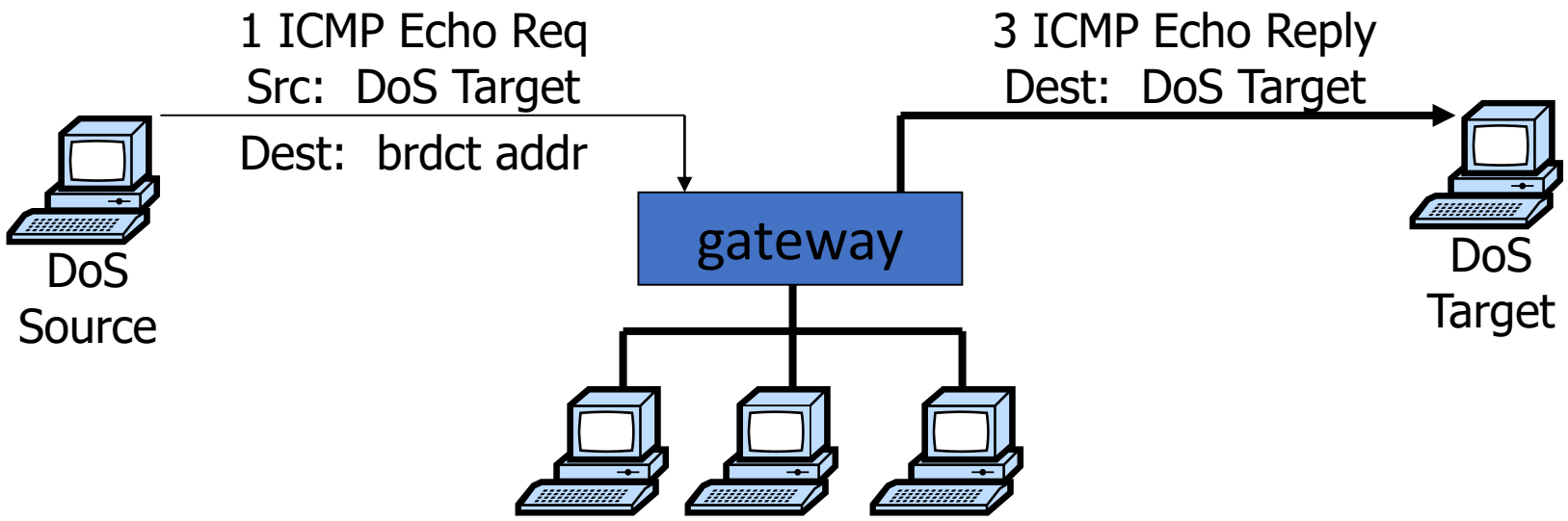
QUEEN'S UNIVERSITY BELFAST

The Threat …

Source: *Julie Sigwart -- the creator of the popular comic "Geeks"*

QUEEN'S UNIVERSITY BELFAST

Smurf amplification DoS attack

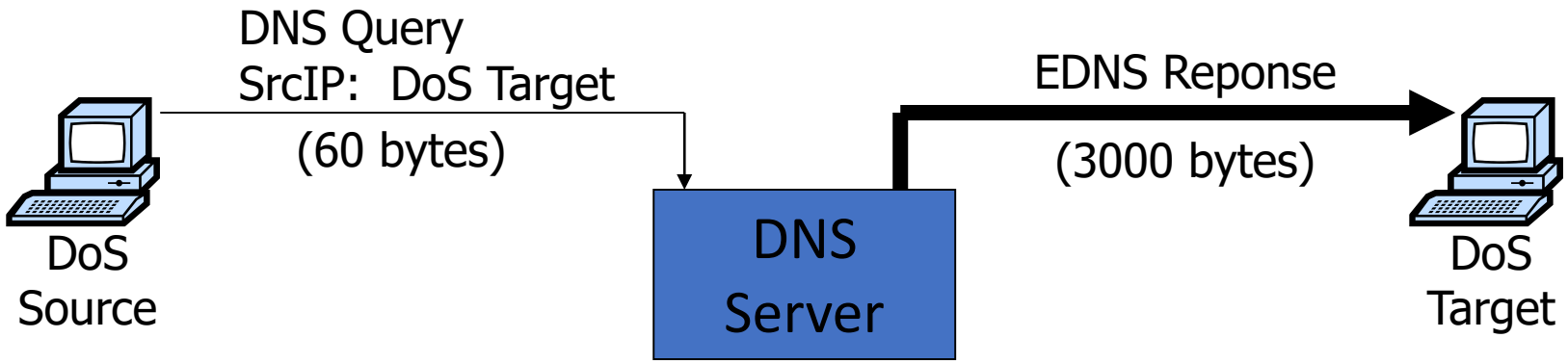


1. Send ping request to broadcast address (ICMP Echo Request)
2. Many responses:
   - Every host on target network generates a ping reply (ICMP Echo Reply) to victim

Prevention: reject external packets to broadcast address

QUEEN'S UNIVERSITY BELFAST

DNS amplification



2006: 0.58M open resolvers on Internet

2013: 22M open resolvers

⇒ 3/2013: DDoS attack generating 309 Gbps for 28 mins

(http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet)

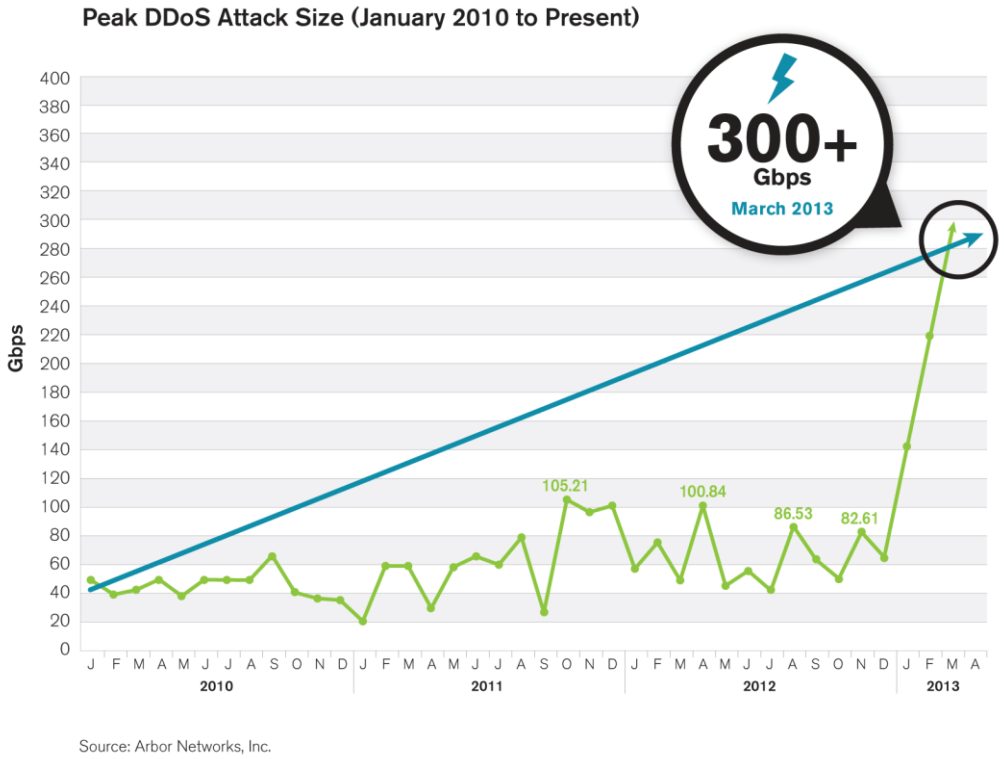
2018: 3M open resolvers

(https://dnsscan.shadowserver.org/stats/)

QUEEN'S UNIVERSITY BELFAST

NTP Amplification

Feb. 2014: 400 Gbps via NTP amplification (4500 NTP servers)



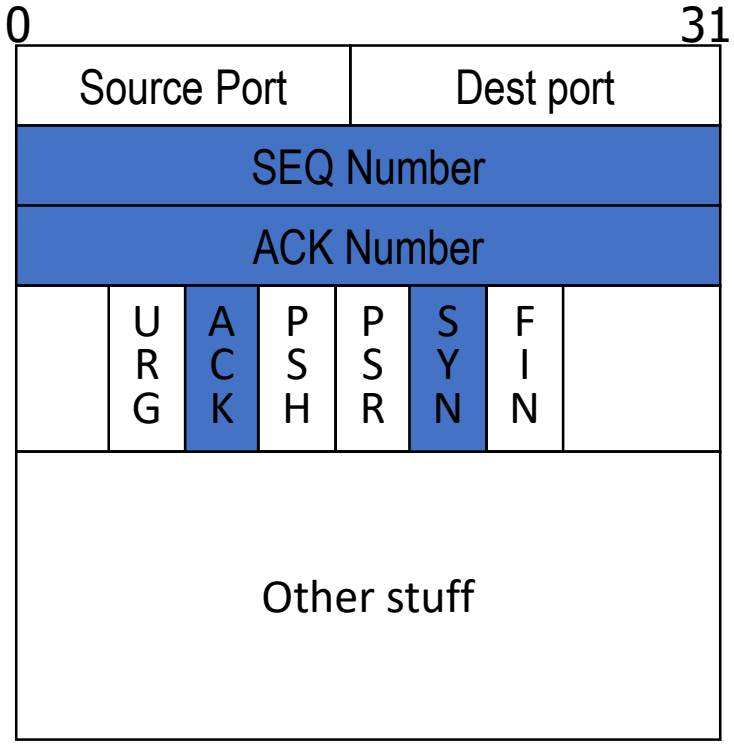
https://ntpscan.shadowserver.org/stats/

QUEEN'S UNIVERSITY BELFAST

Review: TCP header format

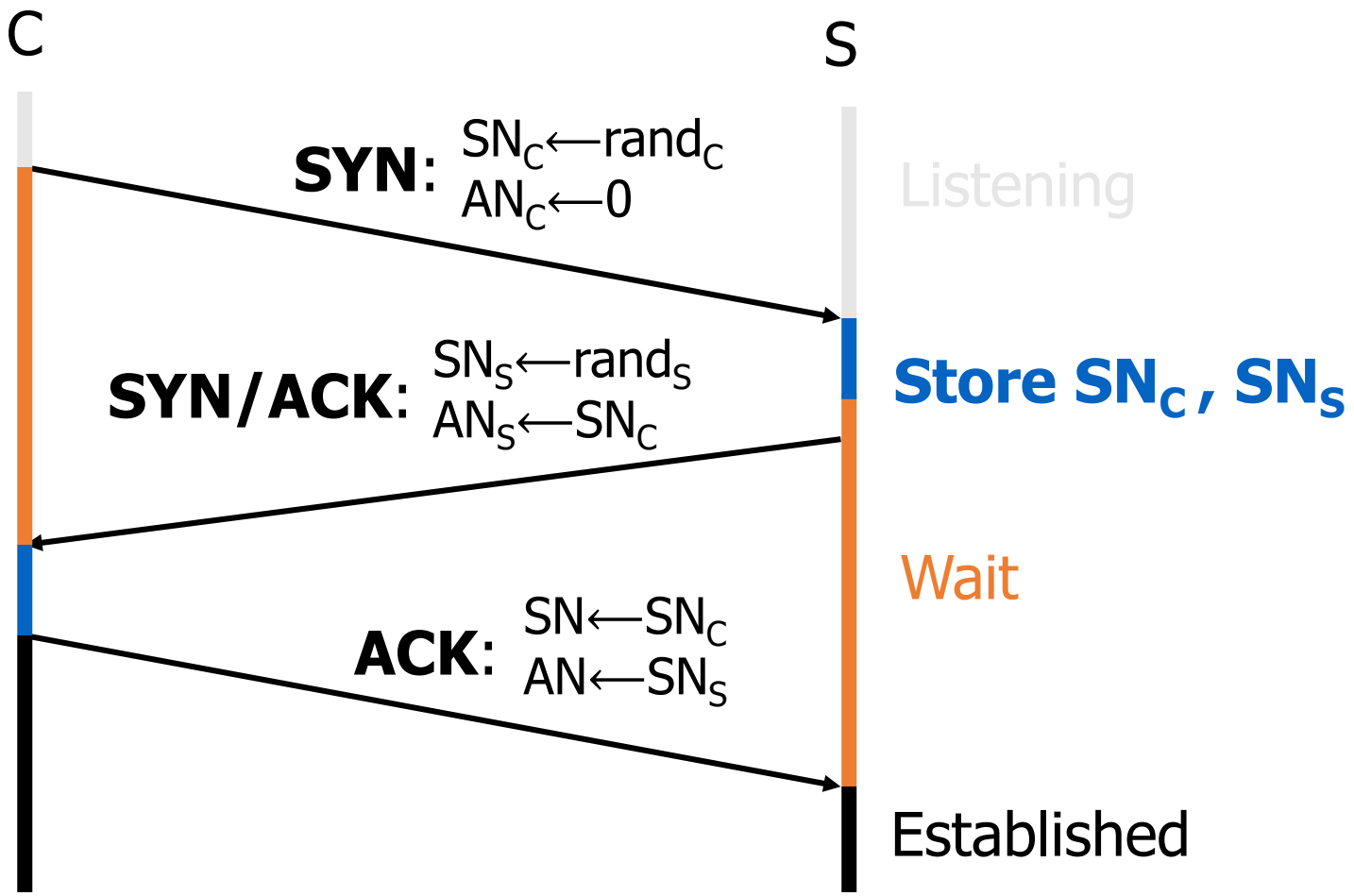
TCP:

- Session based
- Congestion control
- In order delivery



QUEEN'S UNIVERSITY BELFAST

Review: TCP Handshake



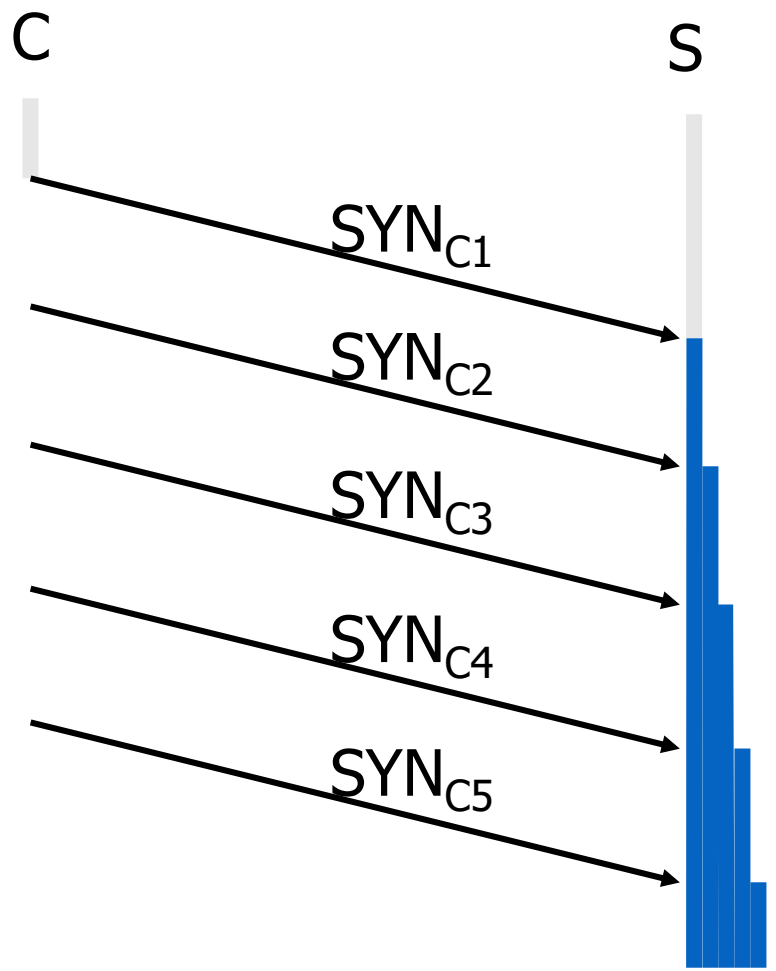
QUEEN'S UNIVERSITY BELFAST

TCP SYN Flood I - Low rate

Single machine:

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

Note: Number of SYN packets per minute depends on backlog queue size and eviction policy.



QUEEN'S UNIVERSITY BELFAST

Low rate SYN Flood defenses

Non-solution:

- Increase backlog queue size or decrease timeout

Correct solution (when under attack) :

- **SYN cookies**: remove state from server
- Small performance overhead

QUEEN'S UNIVERSITY BELFAST

Constructing the attack network

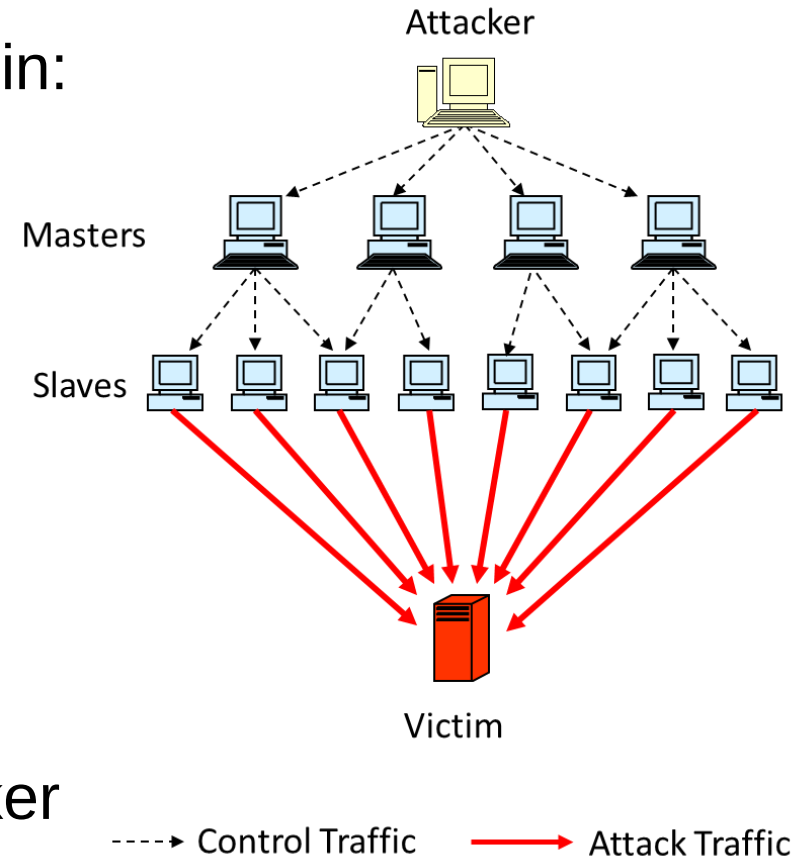
- The first step in a **DDoS** attack is for the attacker to infect a number of machines with zombie software that will ultimately be used to carry out the attack

- Essential ingredients:
  - Software that can carry out the DDoS attack
    - *E.g. “Rootkits” can be used to hide the existence of this software*
  - A vulnerability in a large number of systems
    - *E.g. Exploit known flaws*
  - A strategy for locating vulnerable machines (*scanning)*
    - *E.g. Random, Hit list, local*

QUEEN'S UNIVERSITY BELFAST

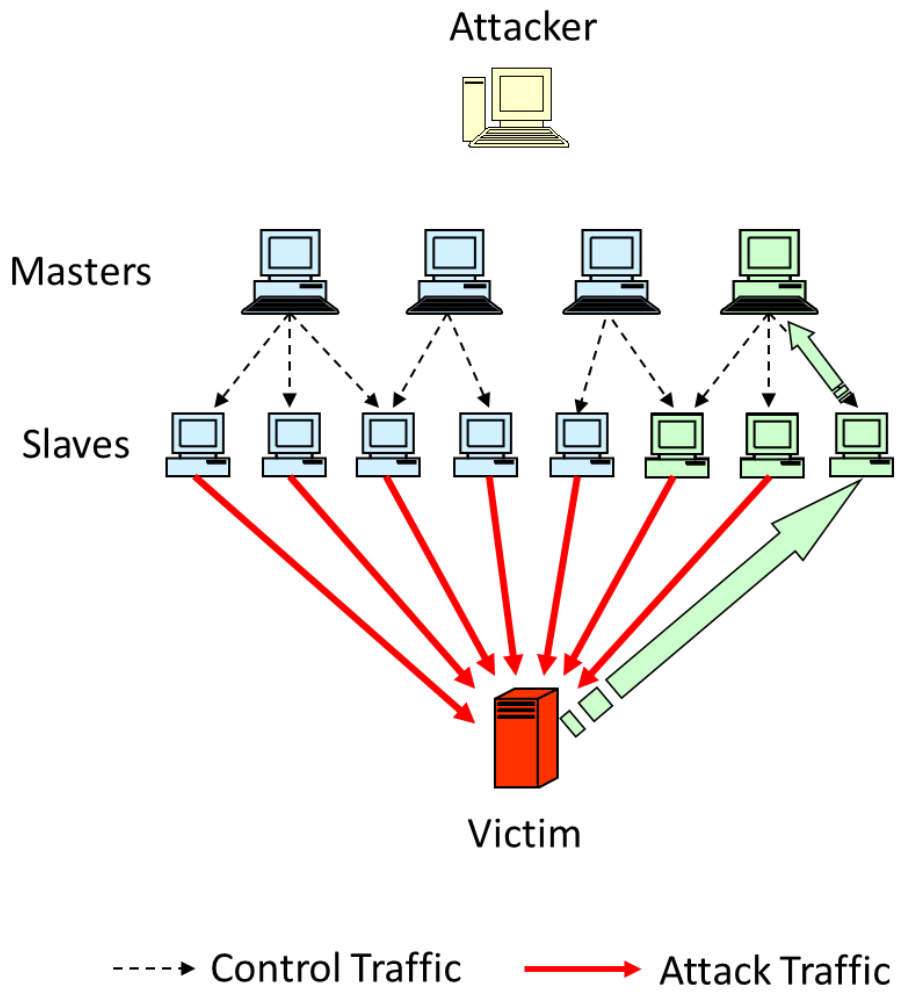
Botnet (Command and Control)

- The attacker classifies the compromised systems in:
  - Master systems
  - Slave systems
- Master systems:
  - Receive command data from attacker
  - Control the slaves
- Slave systems:
  - Launch the proper attack against the victim
- During the attack there is no traffic from the attacker



QUEEN'S UNIVERSITY BELFAST

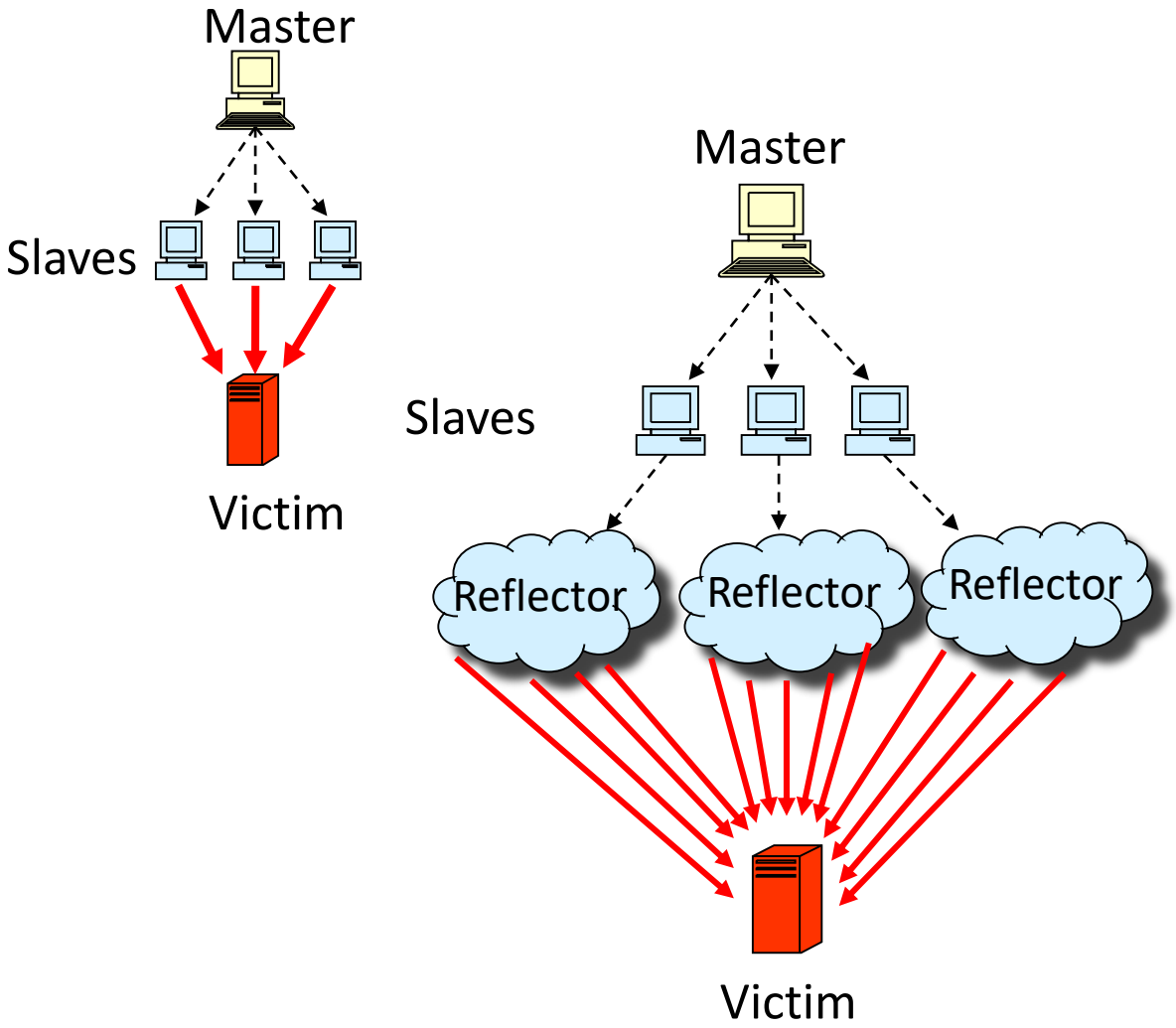
Botnet (Command and Control)

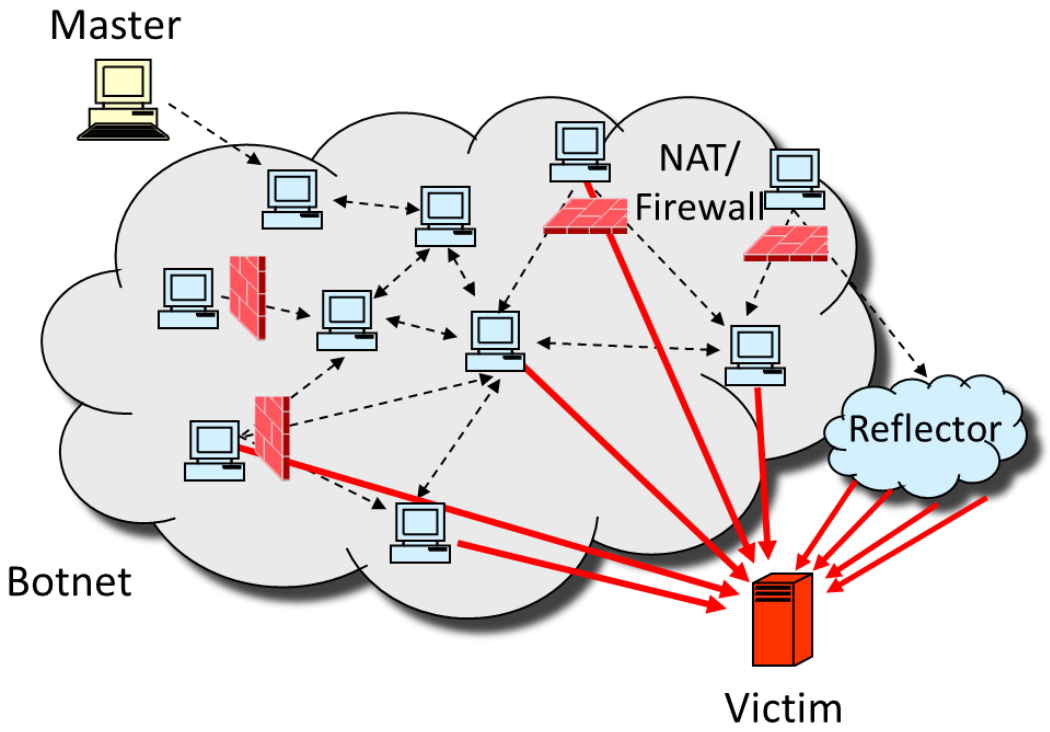


- Each master system only knows some slave systems
- Therefore, the network can handle partial failure, caused by detection of some slaves or masters

QUEEN'S UNIVERSITY BELFAST

Different attack network topologies



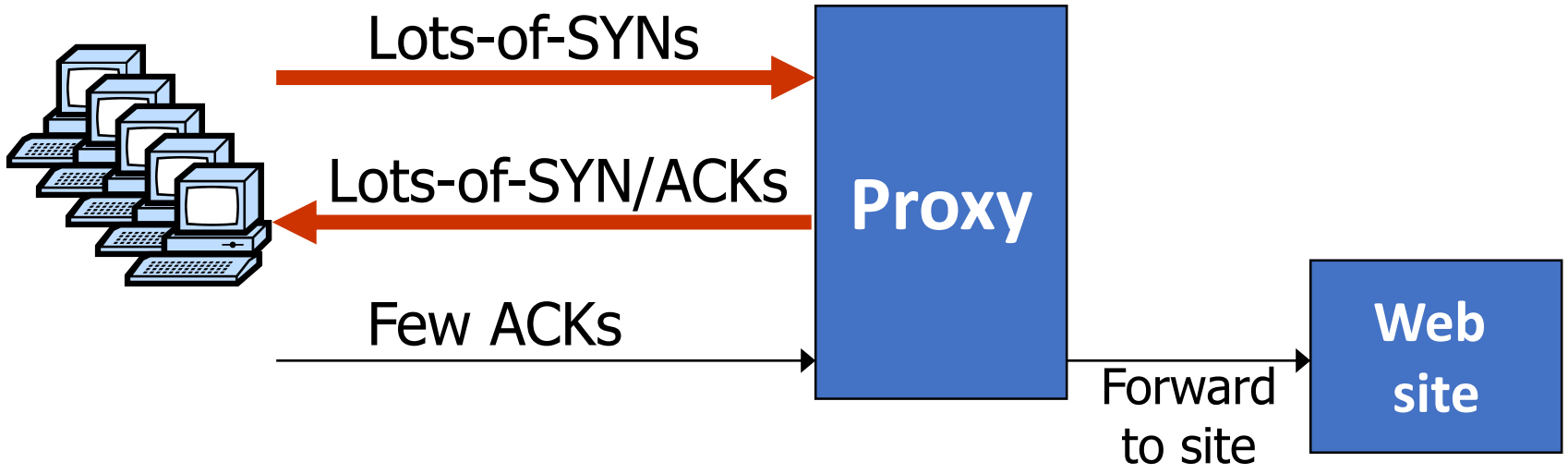


QUEEN'S UNIVERSITY BELFAST

SYN Floods II – Massive Flood

Attack: Command Bot army to flood specific target

Protection: Only forward established TCP connections to target site



QUEEN'S UNIVERSITY BELFAST

Other junk packets … filtering

Proxy must keep floods of these away from web site

Attack Packet	Victim Response
TCP SYN to open port	TCP SYN/ACK
TCP SYN to closed port	TCP RST
TCP ACK or TCP DATA	TCP RST
TCP RST	No response
TCP NULL	TCP RST
ICMP ECHO Request	ICMP ECHO Response
UDP to closed port	ICMP Port unreachable

QUEEN'S UNIVERSITY BELFAST

Stronger attacks

Command bot army to:

- Complete TCP connection to web site
- Send short HTTP HEAD request
- Repeat

Will bypass SYN flood protection proxy

… but:

Attacker can no longer use random source IPs.

- Reveals location of bot zombies

Proxy can now block or rate-limit bots.

QUEEN'S UNIVERSITY BELFAST

DNS DoS Attacks

- DNS runs on UDP port 53
  - DNS entry for victim.com   hosted at victim_isp.com

- DDoS attack:
  - flood victim_isp.com with requests for victim.com
  - **Random source IP address** in UDP packets

- Takes out entire DNS server: (collateral damage)

QUEEN'S UNIVERSITY BELFAST

DoS via route hijacking

YouTube is 208.65.152.0***/22*** (includes 2^{10} IP address)
youtube.com is 208.65.153.238, …

Feb. 2008:

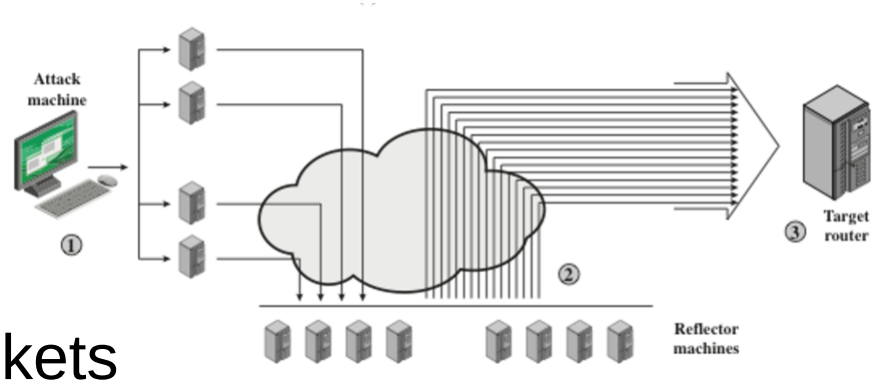
- Pakistan telecom advertised a BGP path for
  208.65.153.0***/24*** (includes 2^{8} IP address)
- Routing decisions use most specific prefix
- The entire Internet now thinks
  208.65.153.238 is in Pakistan

Outage resolved within two hours

- … but demonstrates the DoS vulnerability with no solution!

QUEEN'S UNIVERSITY BELFAST

DoS Reflector Attacks



Reflector:

- A network component that responds to packets
- Response sent to victim (spoofed source IP)

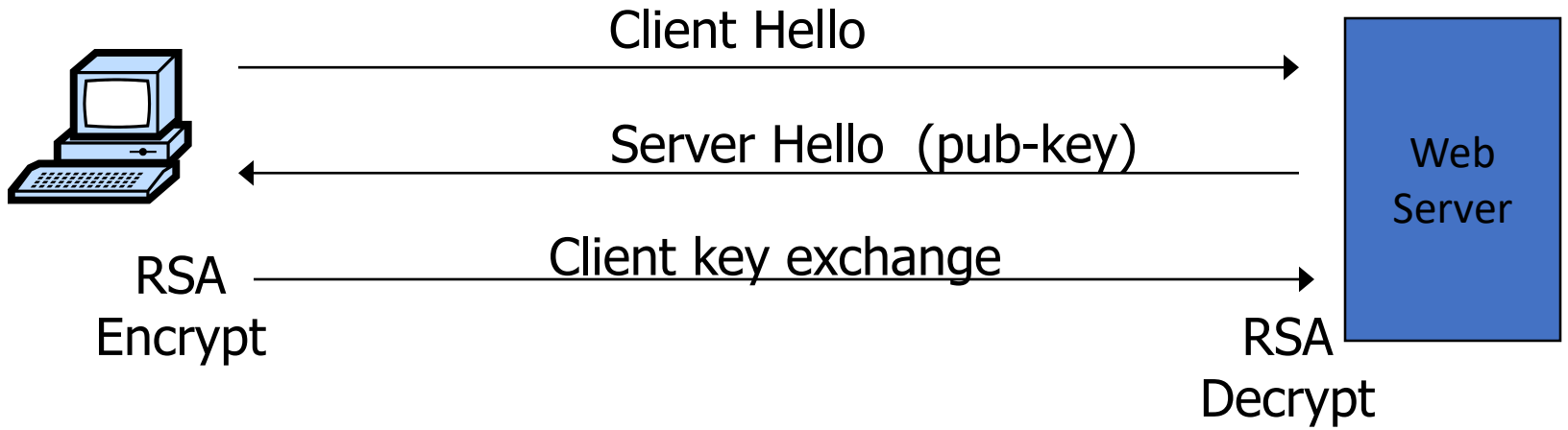
Examples:

- DNS Resolvers: UDP 53 with victim.com source
  - At victim: DNS response
- Web servers: TCP SYN 80 with victim.com source
  - At victim: TCP SYN ACK packet

QUEEN'S UNIVERSITY BELFAST

DoS at higher layers

SSL/TLS handshake



RSA-encrypt speed ≈ 10 × RSA-decrypt speed

⇒ Single machine can bring down ten web servers

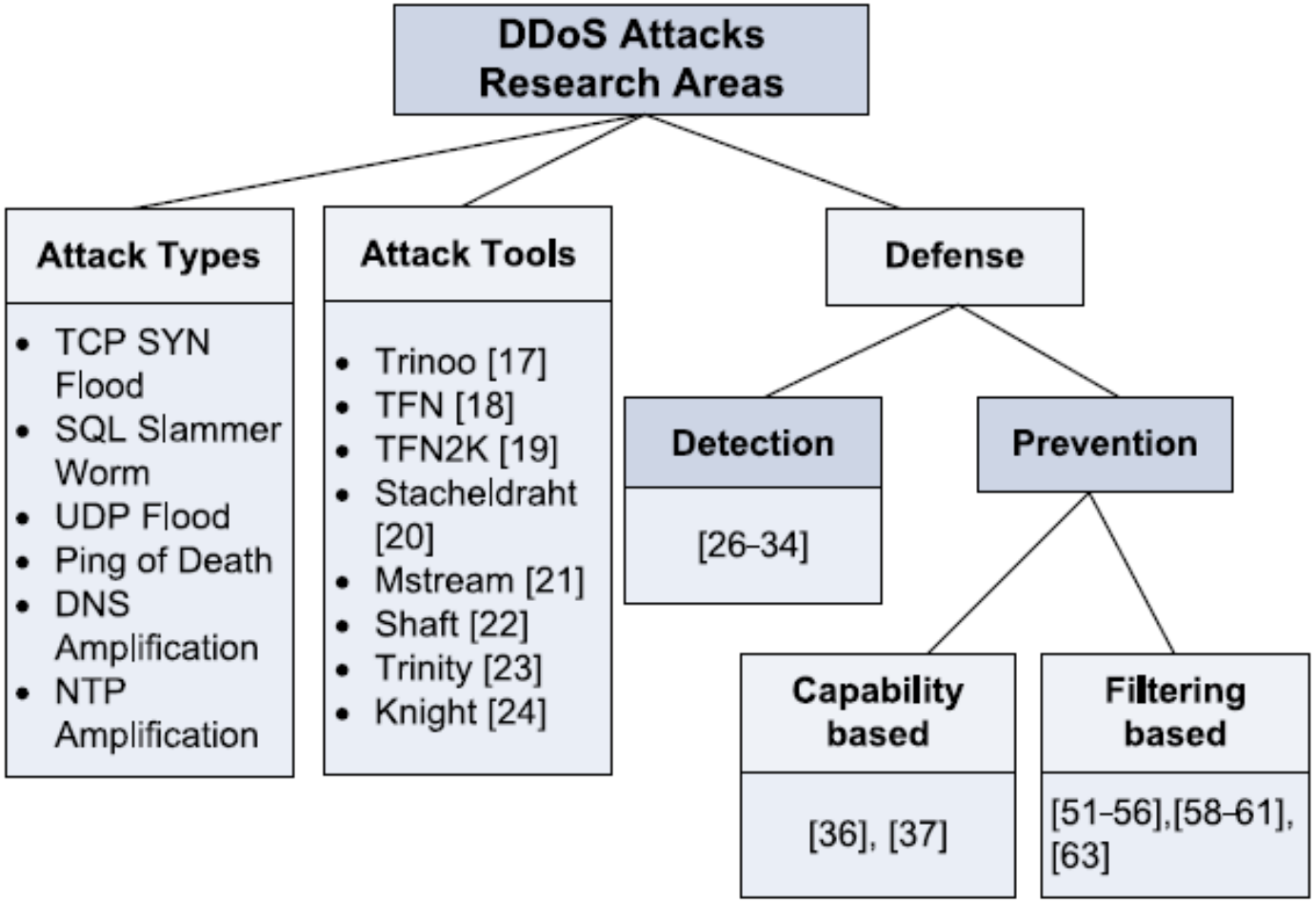
Similar problem with application DoS:

- Send HTTP request for some large PDF file
- Easy work for client, hard work for server

QUEEN'S UNIVERSITY BELFAST

Classification of DDoS attack studies

Background

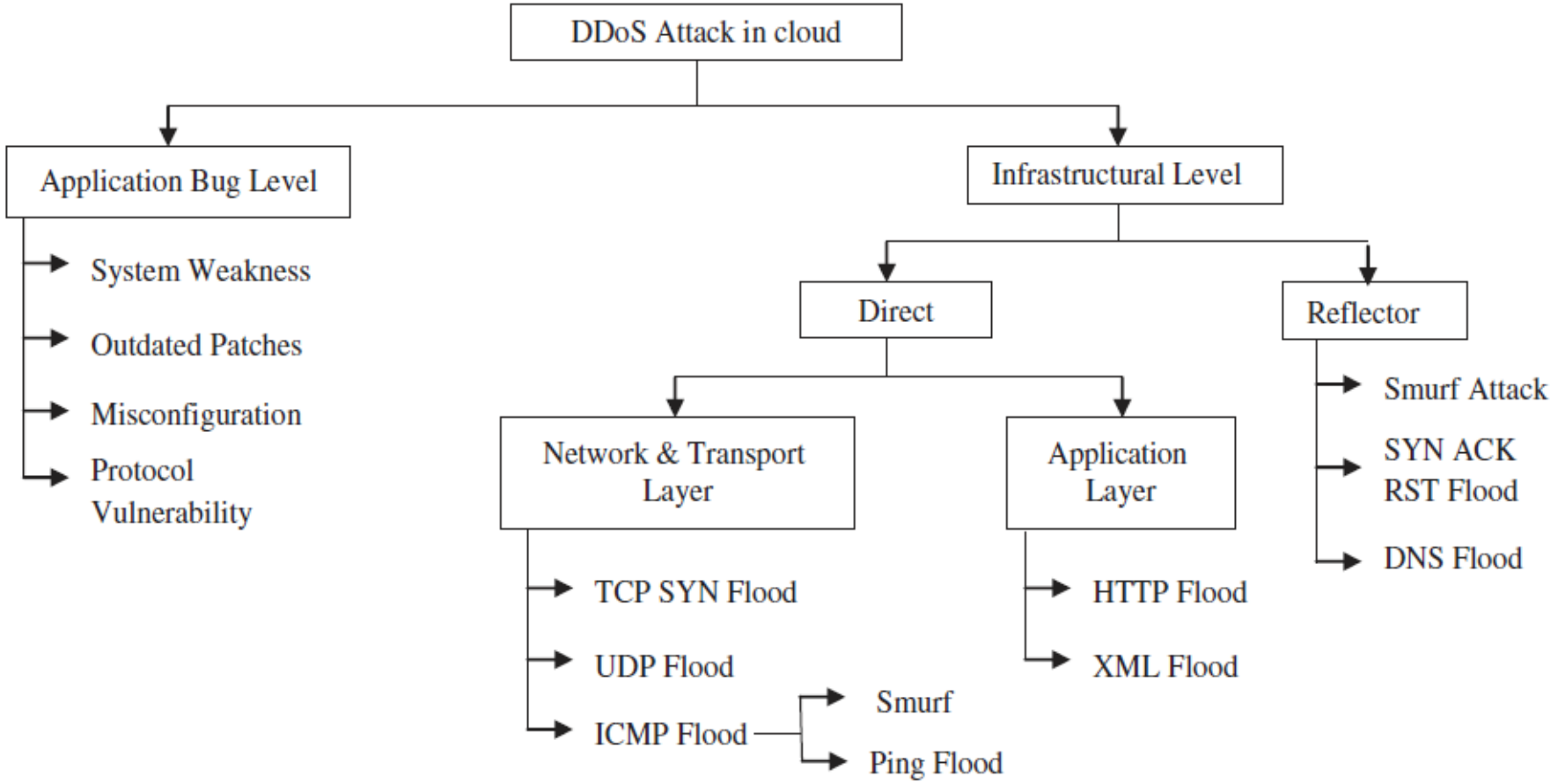


Kalkan, Kübra, Gürkan Gür, and Fatih Alagöz. "Filtering-based defense mechanisms against DDoS attacks: A survey." *IEEE Systems Journal* 11, no. 4 (2017): 2761-2773.

QUEEN'S UNIVERSITY BELFAST

Cloud Computing – DDoS Attack Topology

Background



Agrawal, Neha, and Shashikala Tapaswi. "Defense schemes for variants of distributed denial-of-service (ddos) attacks in cloud computing: A survey." *Information Security Journal: A Global Perspective* 26, no. 2 (2017): 61-73.

QUEEN'S UNIVERSITY BELFAST

Summary

- What is a (D)DoS?
- Attack techniques
    - Resource destruction, reservation, depletion
- Attack types
    - Amplification attacks
    - SYN Flooding attacks – low rate, massive
    - DNS DoS
    - DoS via route hijacking
    - DoS at higher layers
- Attack network topologies

QUEEN'S UNIVERSITY BELFAST

Questions?

Next Session: Denial of Service – Part 2

Friday, 22 March 2019

QUEEN'S UNIVERSITY BELFAST