DDoS Mitigation and Economics

Krassimir Tzvetanov

krassi@fastly.com

July 5-6

Introduction

ICC International Cybersecurity Congress

- Who am I?
- Who are you?
- What is the target audience of this tutorial?
- Let me know if I speak too fast!
- Let’s make it interactive!

Overview

ICC International Cybersecurity Congress

- What is DDoS?
- Terminology
- Factors supporting and accelerating DDoS

What is DoS/DDoS?

What is Denial of Service?

ICC International Cybersecurity Congress

- Discussion
- Resource exhaustion… which leads to lack of availability
- Consider:
  - How is it different from The Guardian pointing to somebody's web site?
  - How is that different from company's primary Internet connection going down?

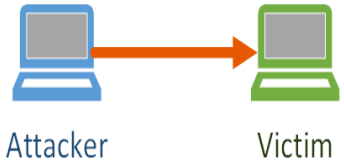
What is Denial of Service?

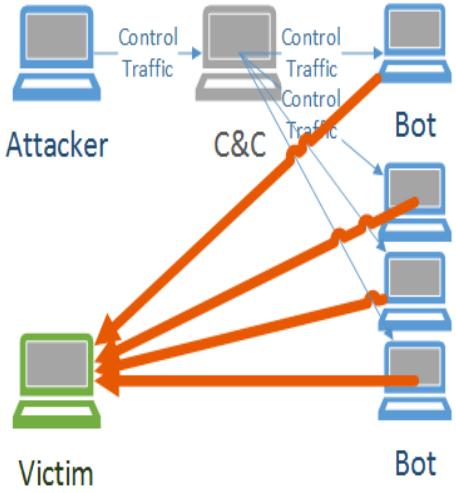
ICC International Cybersecurity Congress

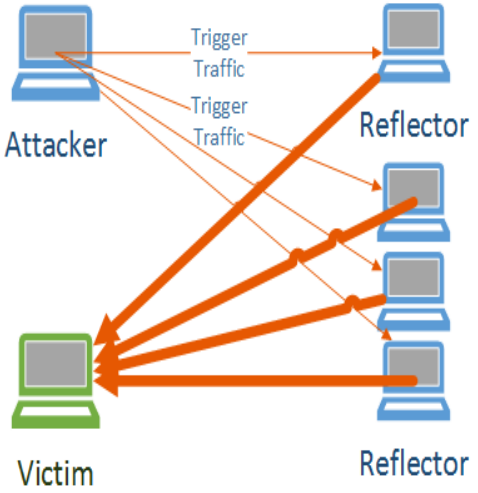
- From security point of view?
  - Decreased availability
- From operations point of view?
  - An outage
- From business point of view?
  - Financial losses

DoS vs. DDoS

- What is the difference?
  - One system is sending the traffic vs many systems
  - Consider reflected attacks
- How does that change the attacks volume?
  - More systems – more capacity







DDoS Volume Factors

Additional factors supporting and accelerating DDoS

- Overall bandwidth
- Reflectors
- IoT/Embedded devices
- Content management systems
- Booters/Stressors (lowers threshold)
- Accessible information

Home routers

ICC International Cybersecurity Congress

- Embedded home and SOHO devices
  - Default username/password
  - Open DNS recursive resolvers
  - NetUSB bug
  - Network diagnostic tools
  - Some do not allow the user to turn off DNS
- XBOX and Sony attacks over Christmas (2014)
  - Krebs on security:
    http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/
  - Mirai
- Is that intentional? – “follow the money”

Compromised CMSes

ICC International Cybersecurity Congress

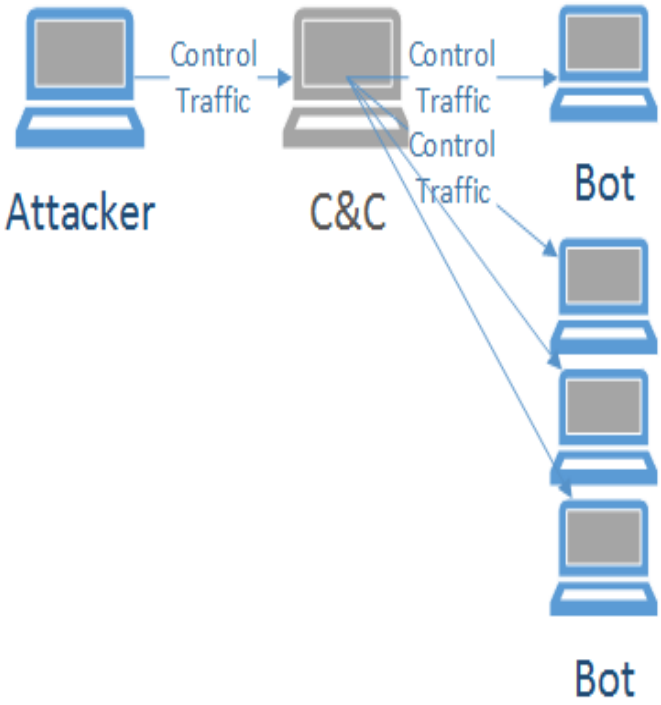
- Most targeted Content Management Systems:
  - WordPress
  - Joomla
- Started in early 2013 - notably around the attacks against US financial institutions
- Now it is an easy way to build a botnet and other groups abuse it as well

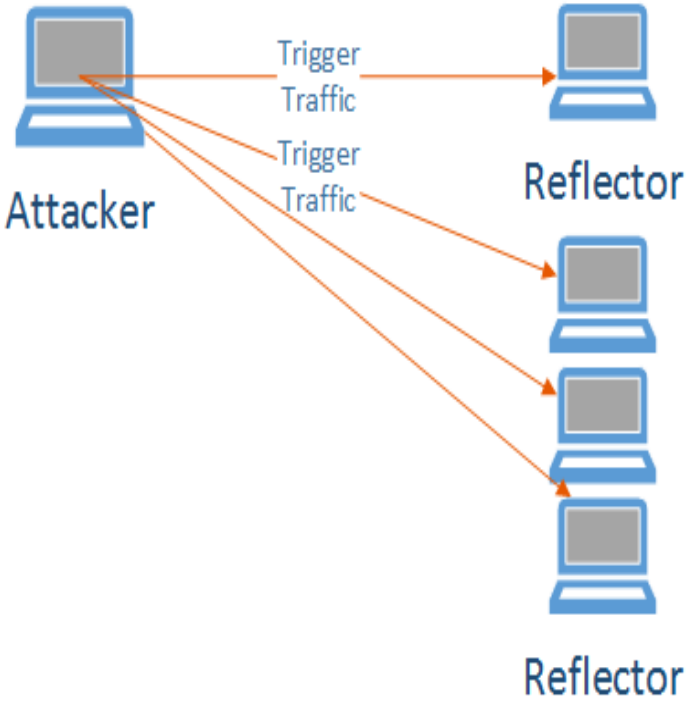
Booters/Stressors

ICC International Cybersecurity Congress

- Inexpensive
- Popular among gamers
- Tools are sold for cheap on the black market (forums)
- Range 5-10 Gbps and up to 40GBps
- Usually short duration

Low cost thanks to reflection





ICC
International
Cybersecurity
Congress

Questions?

The Adversary

Overview

ICC International Cybersecurity Congress

- Who are they
- Motivation
- Skill level
- Booters
- Tools

Adversary

ICC International Cybersecurity Congress

- Wide range of attackers
  - Gamers – on the rise!!! ☺
  - Professional DDoS operators and booters/stressors
  - Some of the attacks have been attributed to nation states
  - Hacktivists – though not recently

…and more

Motivation

ICC International Cybersecurity Congress

- Wide range of motivating factors as well
  - Financial gain
    - extortion (DD4BC/Armada Collective/copy cats)
    - taking the competition offline during high-gain events
      (online betting, superbowl, etc).
  - Political statement
  - Divert attention (seen in cases with **data exfiltration** or financial fraud)
  - Disable firewalls (WAF)
  - Immature behavior

Skill level

ICC International Cybersecurity Congress

- Wide range of skills
  - Depending on the role in the underground community
  - Mostly segmented between operators and tool-smiths
  - Tool-smiths are not that sophisticated (at this point) and there is a large reuse of code and services
  - This leads to clear signatures for some of the tools

- Increasing complexity
  - DirtJumper
  - xnote.1
  - Mirai

Software

ICC International Cybersecurity Congress

- Individual attack scripts – pastebin, hackfroums, etc.
- booter scripts – basic, sometimes control panel
- More advanced - C&C server and separate agent for the drones
  - dirt jumper
  - black energy (general RAT)
- Most kits are in the $100-600 range (if not free)
- Open source

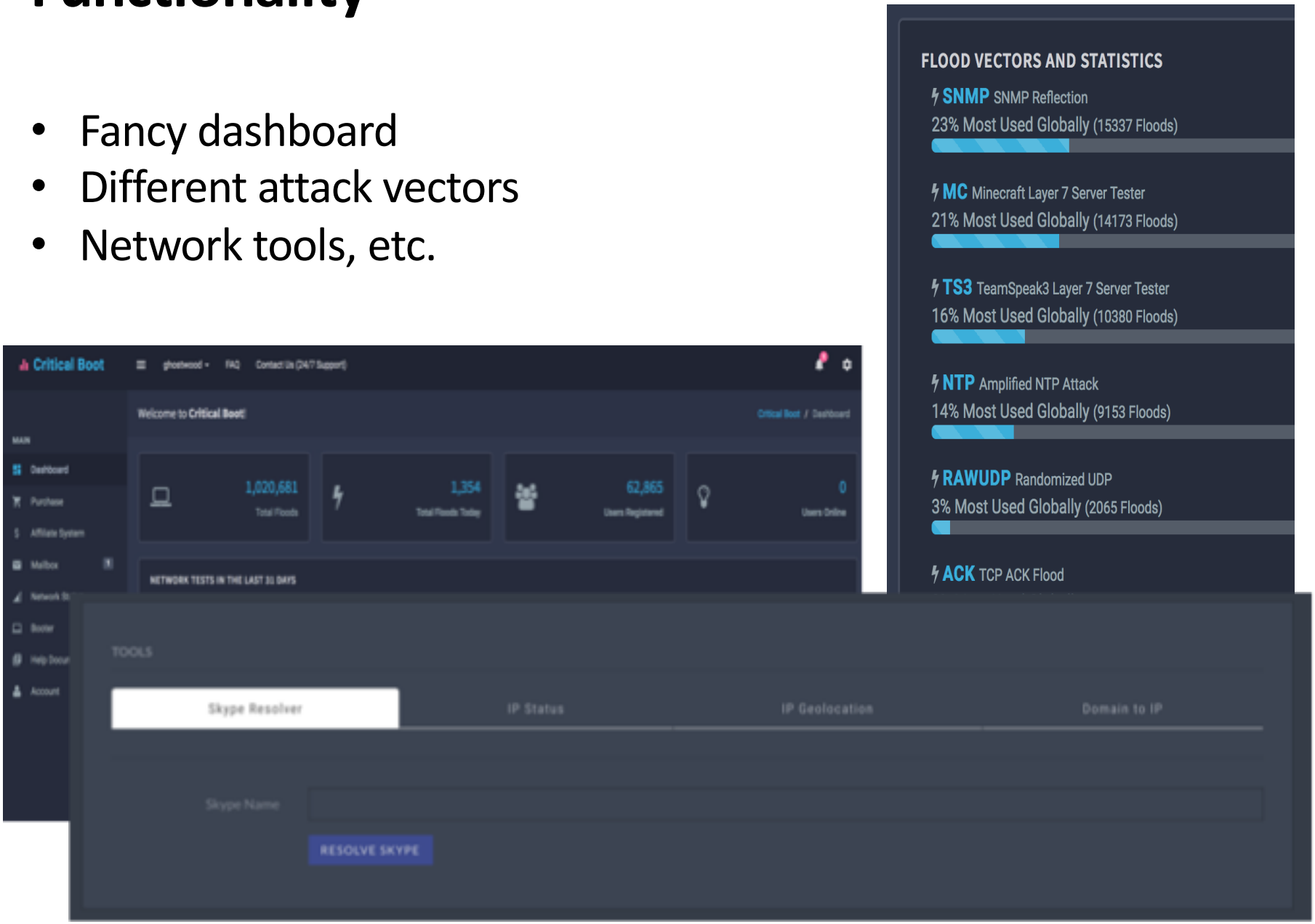
Booters

Booters

- Booter services
- Gained popularity over the past 4 years
- Mostly reflected attack (no need for additional infrastructure)
- Mostly computer gaming industry related
- - Short, bursty attacks
- - Use rudimentary scripts
- Fairly inexpensive

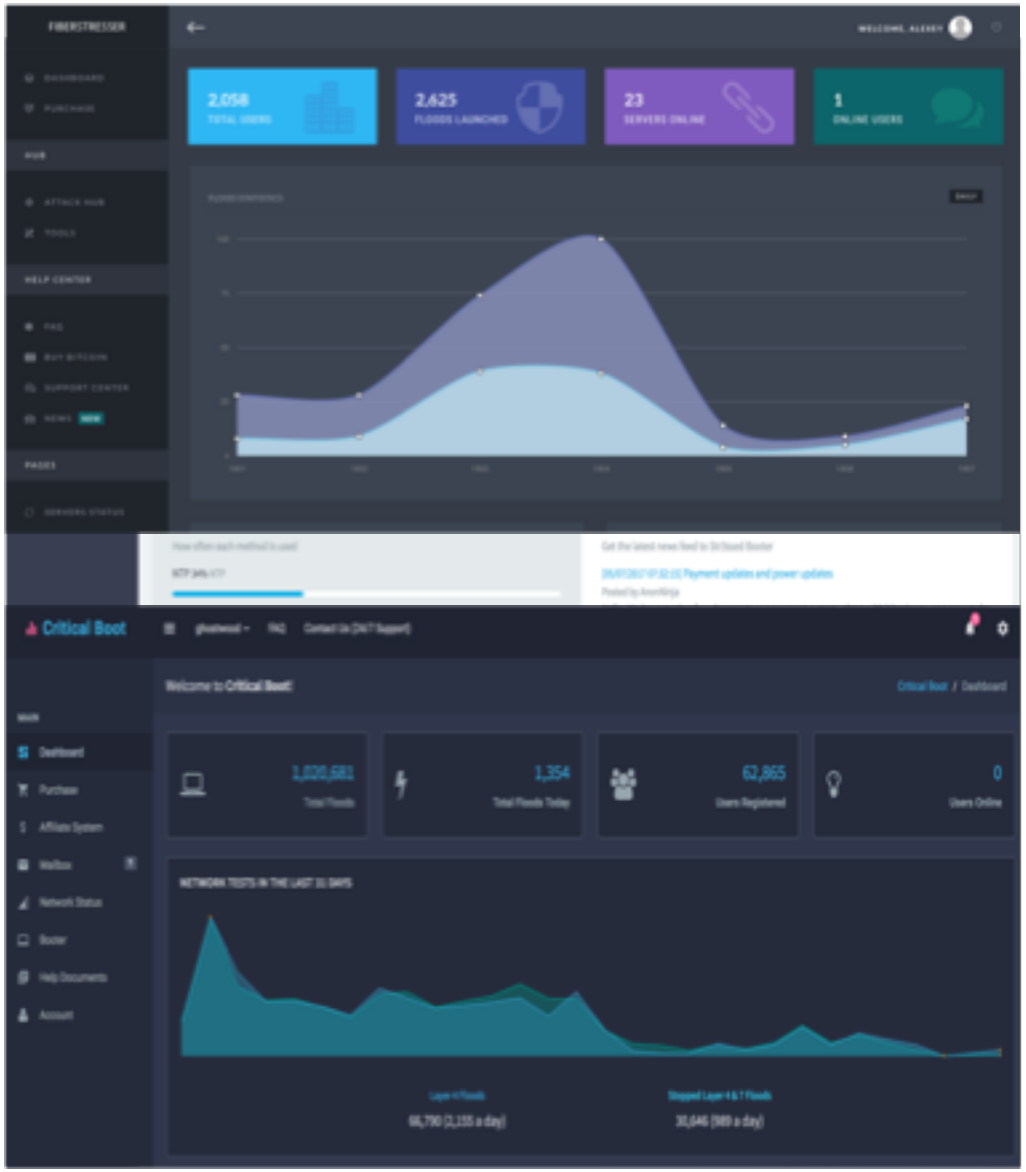
Functionality

- Fancy dashboard
- Different attack vectors
- Network tools, etc.

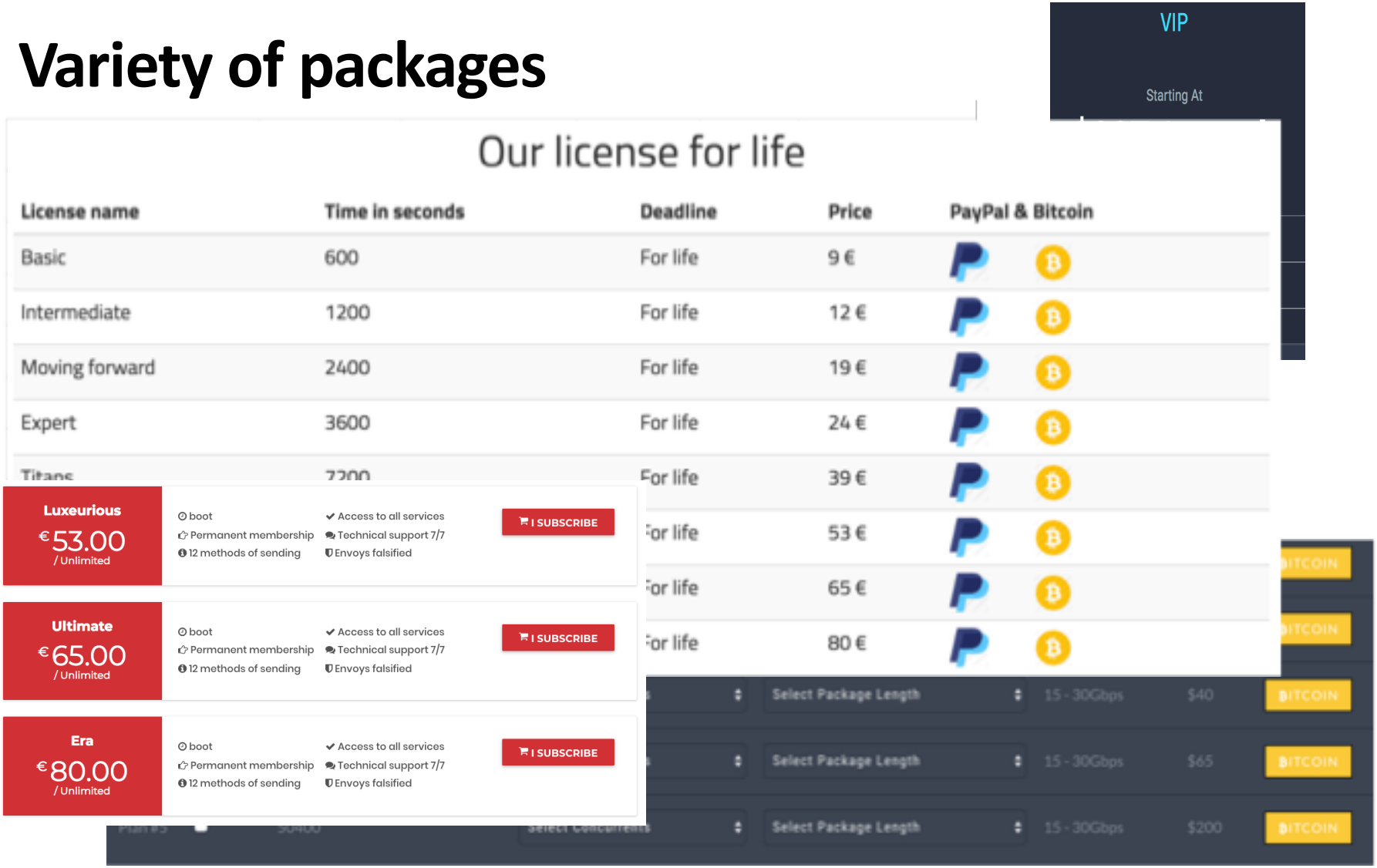


Code reuse

- Individual attack scripts reused widely
- Limited set of kits (control panel)
- Also some operators set multiple fronts



Variety of packages



Bottom line

ICC International Cybersecurity Congress

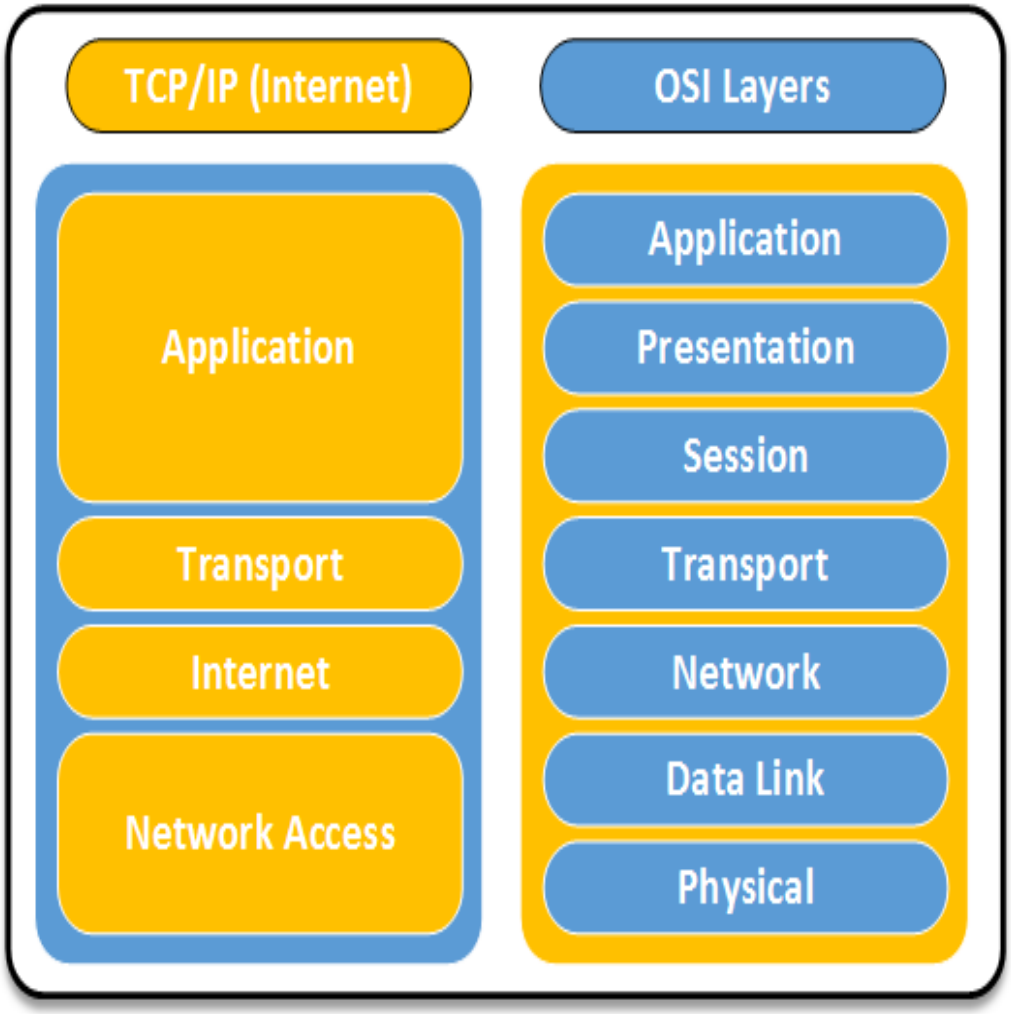
Service:

- $15-250/month

Do-it-yourself (DIY):

- Kit - $100-600 (one time)
- Hosting - $100-250/month
- Time spent on forums

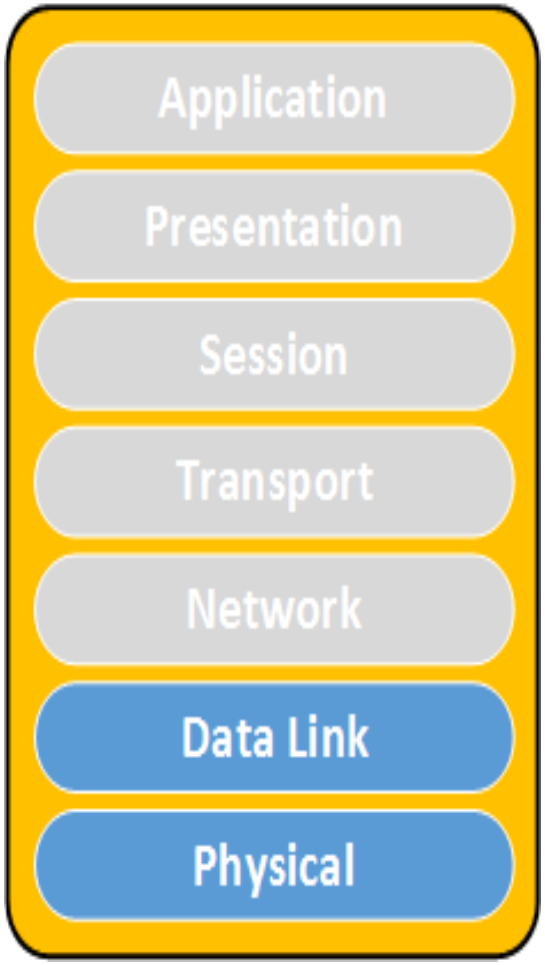
Network Layers – OSI vs Internet Model



Physical and Data-link Layers

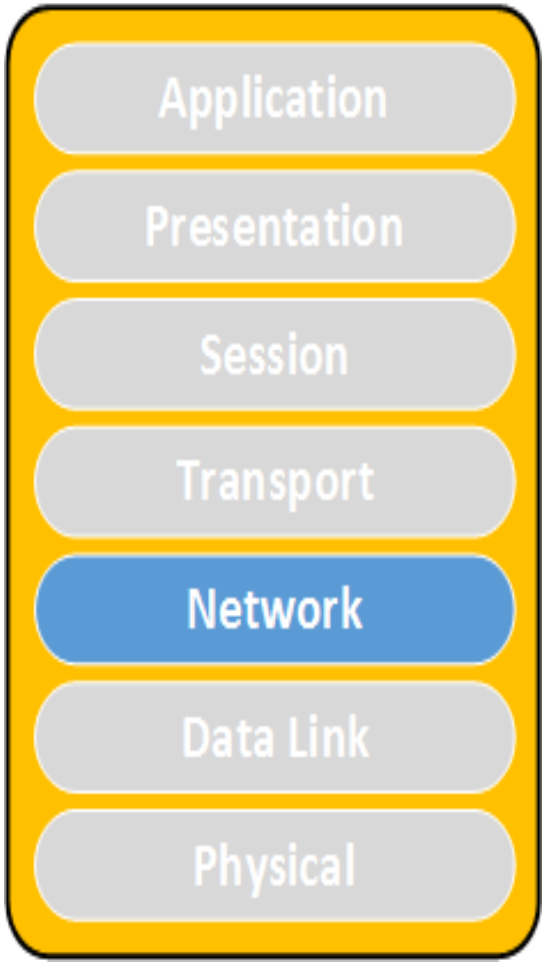
- Cut cables
- Jamming
- Power surge
- EMP

- MAC Spoofing
- MAC flood



Network Layer

- Floods (ICMP)
- Teardrop
  (overlapping IP segments)

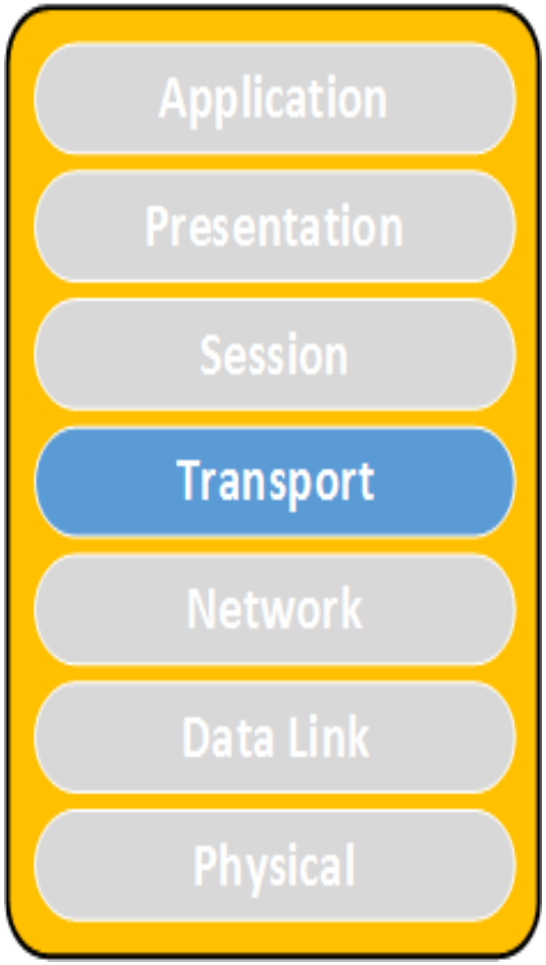


Transport Layer

ICC International Cybersecurity Congress

- SYN Flood
- RST Flood
- FIN Flood
- You name it…

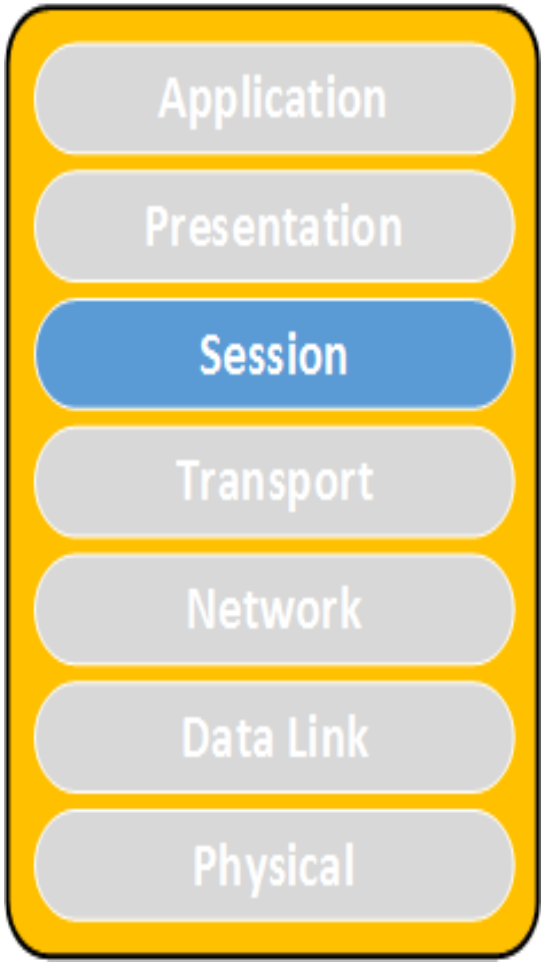
- Window size 0 (looks like Slowloris)
- Connect attack
- LAND (same IP as src/dst)



Session Layer

ICC International Cybersecurity Congress

- Slowloris
- Sending data to a port with no BR/NL in it (long headers, long request lines)

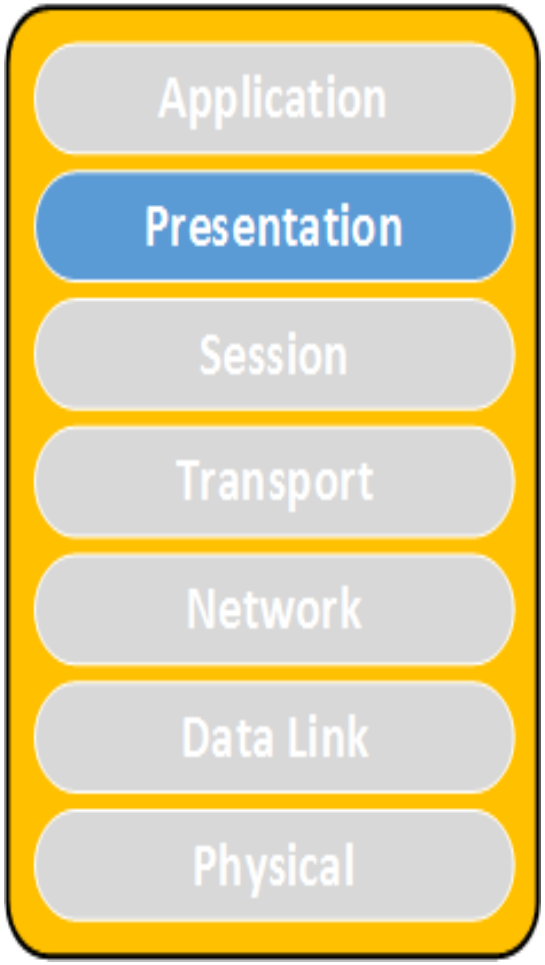


Presentation Layer

ICC International Cybersecurity Congress

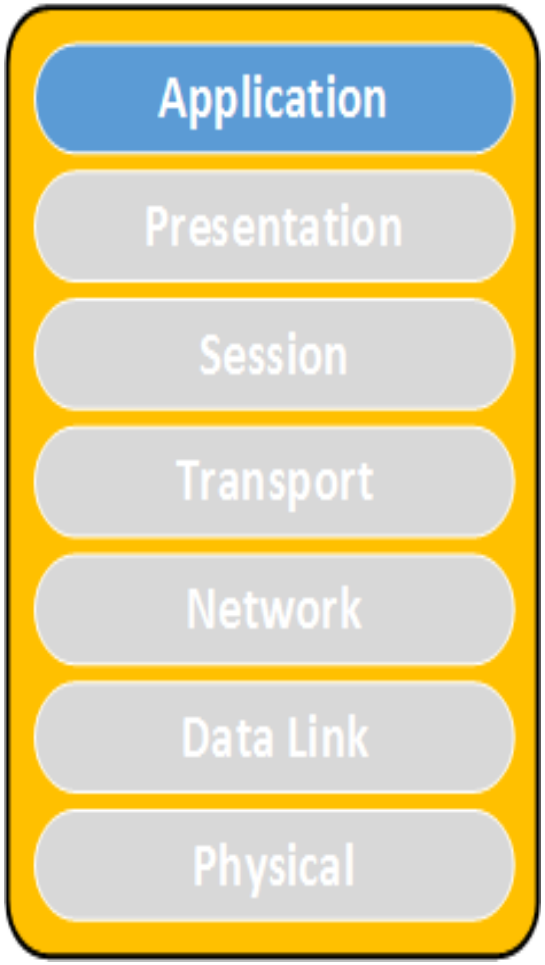
- Expensive queries (repeated many times)
- XML Attacks

```
<!DOCTYPE lolz
[
<!ENTITY lol1 "&lol2;">
<!ENTITY lol2 "&lol1;">
 ]>
<lolz>&lol1;</lolz>
```

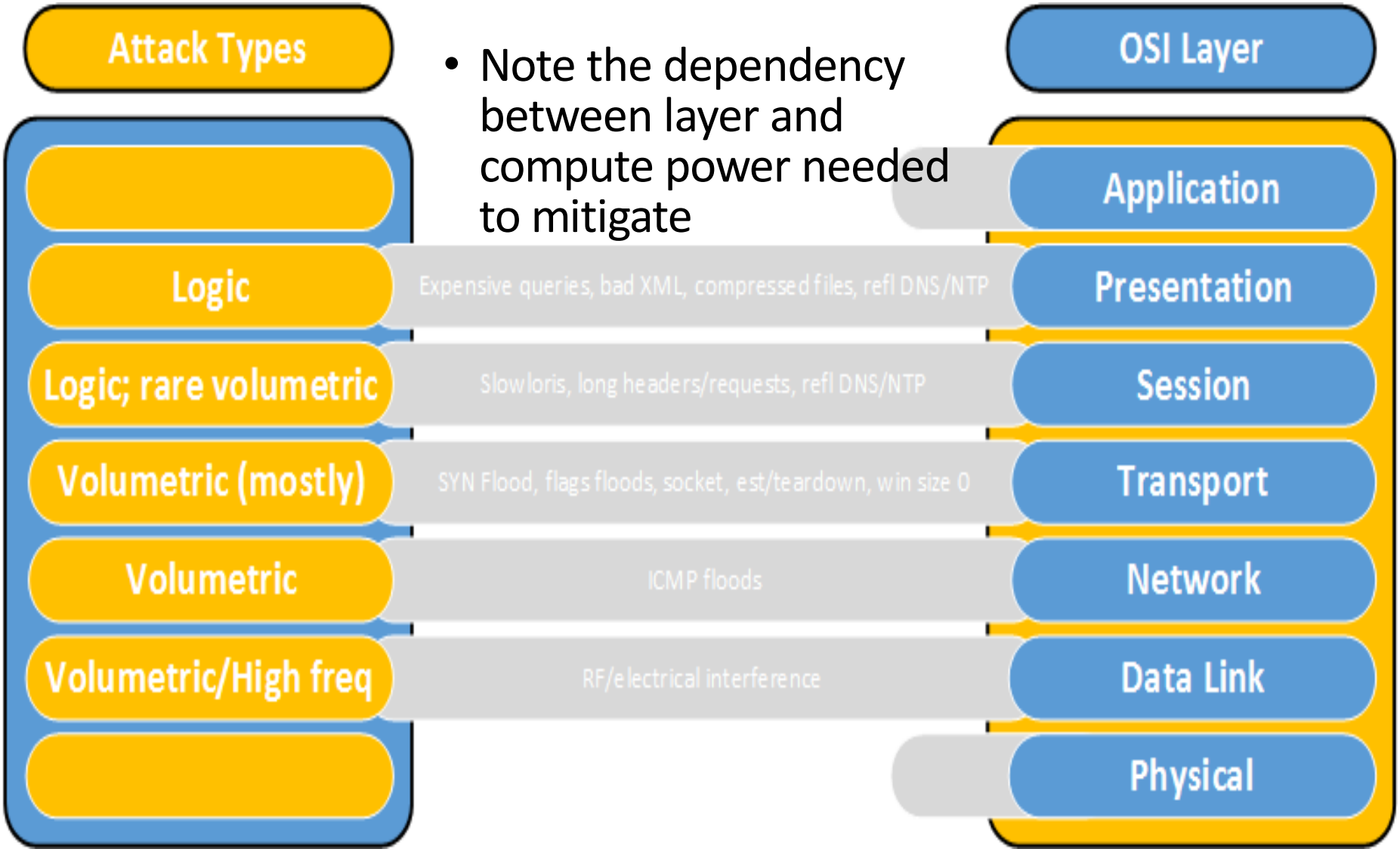


Application Layer

- Depends on the application
- Black fax



Attack summary by layer



- Note the dependency between layer and compute power needed to mitigate

Sockets

Sockets

ICC International Cybersecurity Congress

- Socket is an abstraction allowing an application to bind to a transport layer address (aka network port)
- It is described by a state machine
- Throughout its life time it goes through a number of states

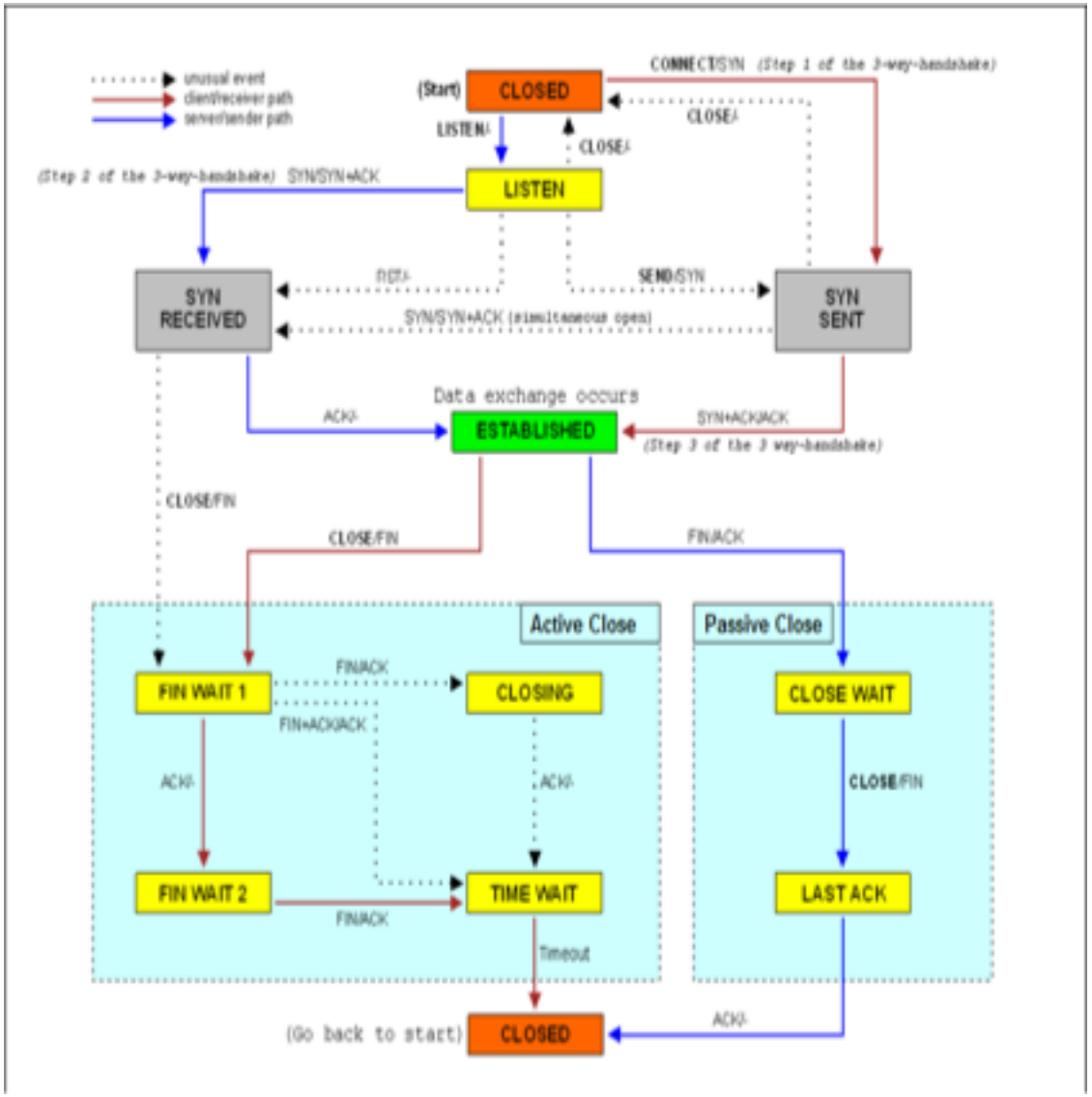
Socket States

ICC International Cybersecurity Congress

- Here are some of the socket states of importance:
  - CLOSED – start state
  - LISTEN – waiting for a connection request
  - SYN_SENT – initiated a connection
  - SYN_RECV – received request still negotiating
  - ESTABLISHED – connection working OK
  - CLOSE_WAIT – waiting for the application to wrap up
  - FIN-WAIT1/2, CLOSING, LAST_ACK – one side closed the connection
  - TIME-WAIT – waiting for 2 x MSL

Socket State Diagram

ICC International Cybersecurity Congress

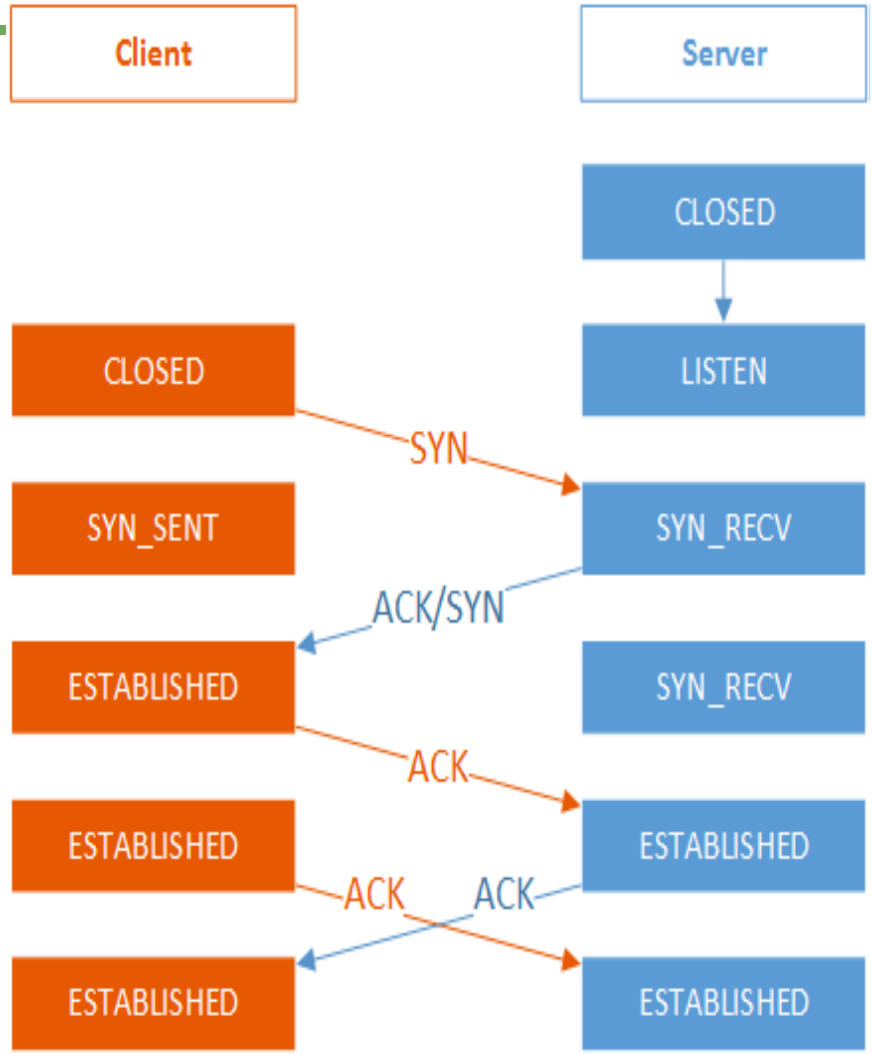


Source: Wikipedia

Opening a TCP connection

Let's review the sequence for opening a connection

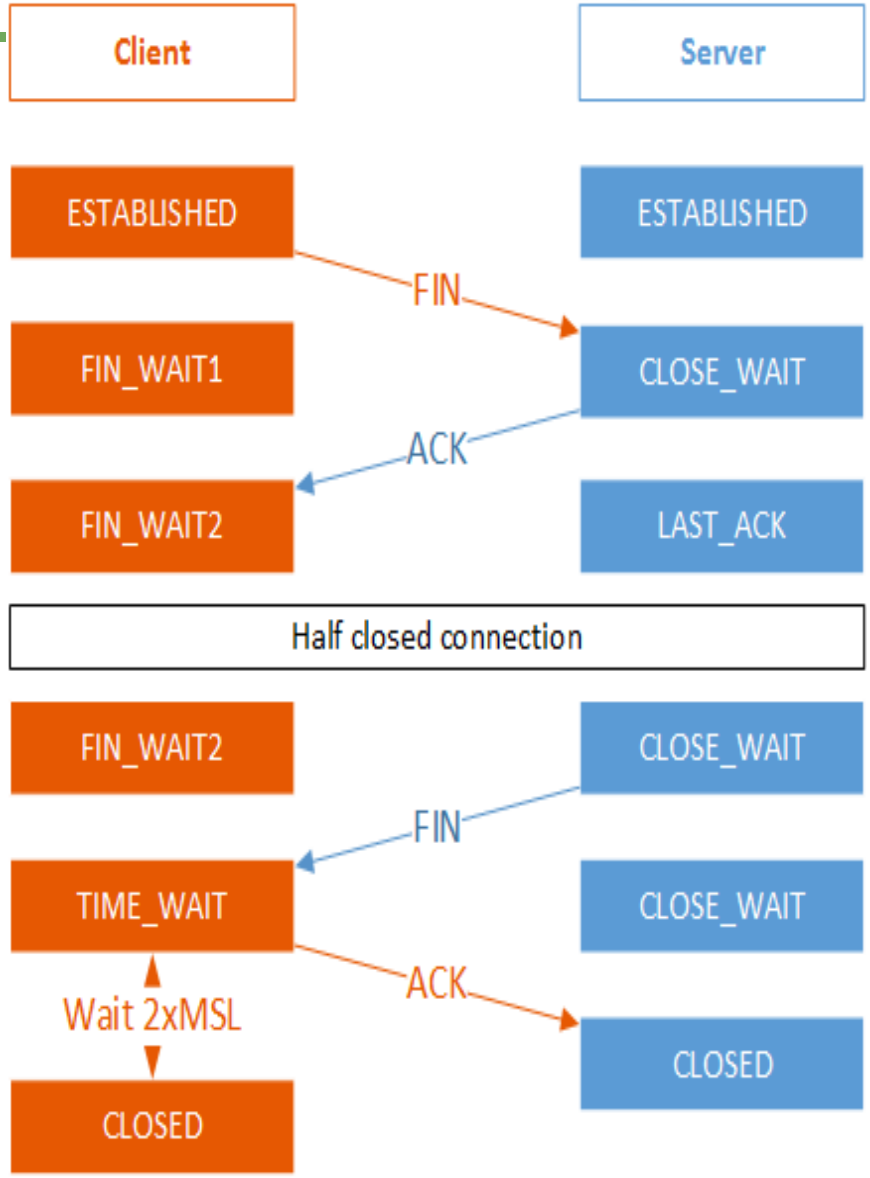
- Server side opens a port by changing to LISTEN state
- Client sends a SYN packet and changes state to SYN_SENT
- Server responds with SYN/ACK and changes state to SYN_RECV. For the client this is ESTABLISHED connection
- Client has to ACK and this completes the handshake for the server
- Packet exchange continues; both parties are in ESTABLISHED state



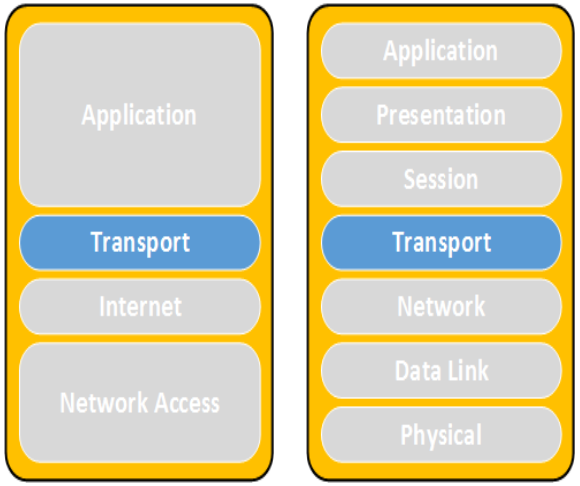
Closing a TCP connection

Sequence for closing a connection

- Both parties are in ESTABLISHED state
- One side initiates closing by sending a FIN packet and changes state to FIN_WAIT1; this changes the other side to CLOSE_WAIT
- It responds with ACK and this closes one side of the connection
- We are observing a half closed connection
- The other side closes the connection by sending FIN
- And the first side ACKs
- The first side goes into a wait for 2 times the MSL time (by default 60 seconds)

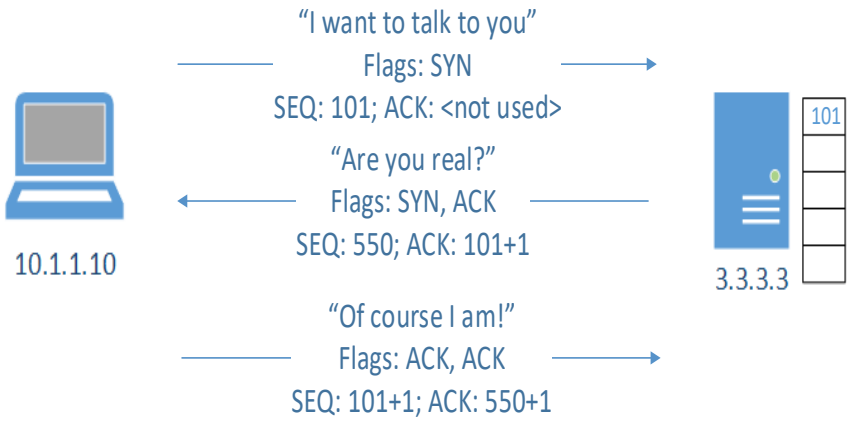


SYN Flood


Application
Transport
Internet
Network Access
Application
Presentation
Session
Transport
Network
Data Link
Physical

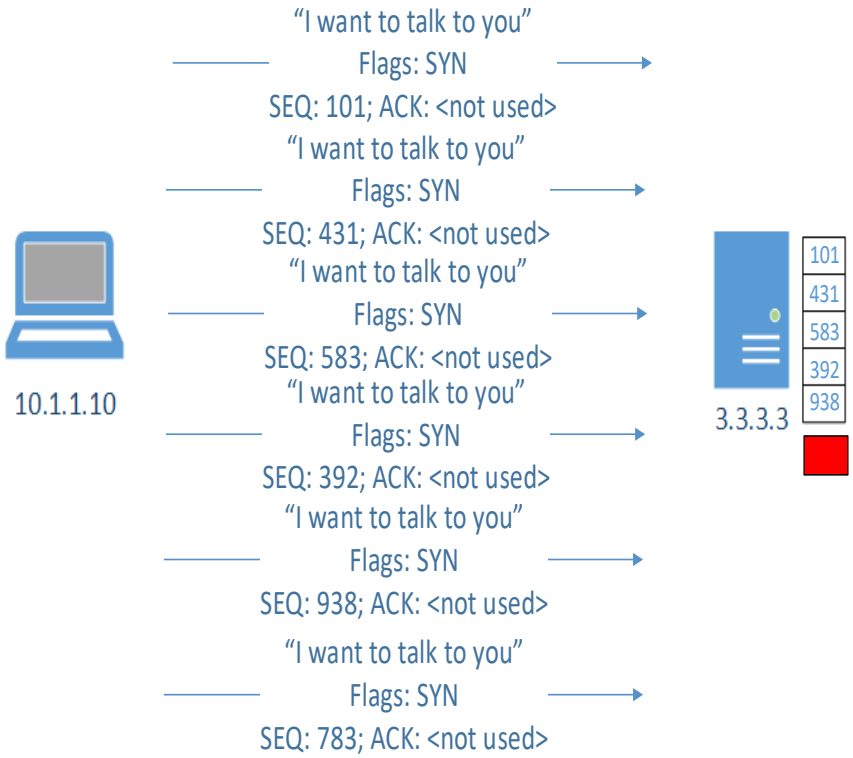
What is a SYN flood?

- What is a 3-way handshake?



SYN flood

- Exploits the limited slots for pending connections
- Overloads them



What is a SYN cookie?

ICC International Cybersecurity Congress

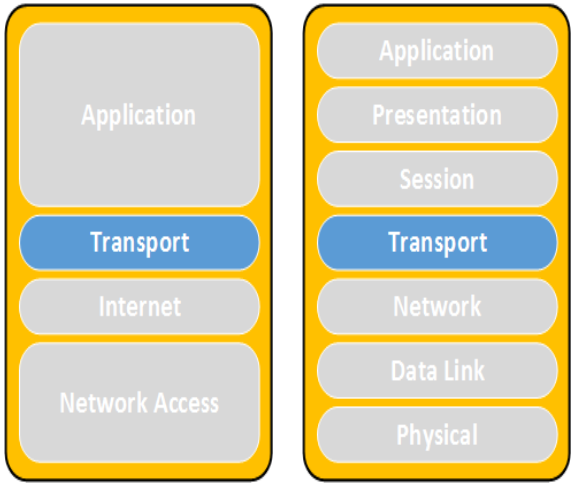
- Hiding information in ISN (initial sequence number)

- SYN Cookie:

  Timestamp % 32 + MSS + 24-bit hash

- Components of 24-bit hash:
  - server IP address
  - server port number
  - client IP address
  - client port
  - timestamp >> 6 (64 sec resolution)

Slowloris


Application
Transport
Internet
Network Access
Application
Presentation
Session
Transport
Network
Data Link
Physical

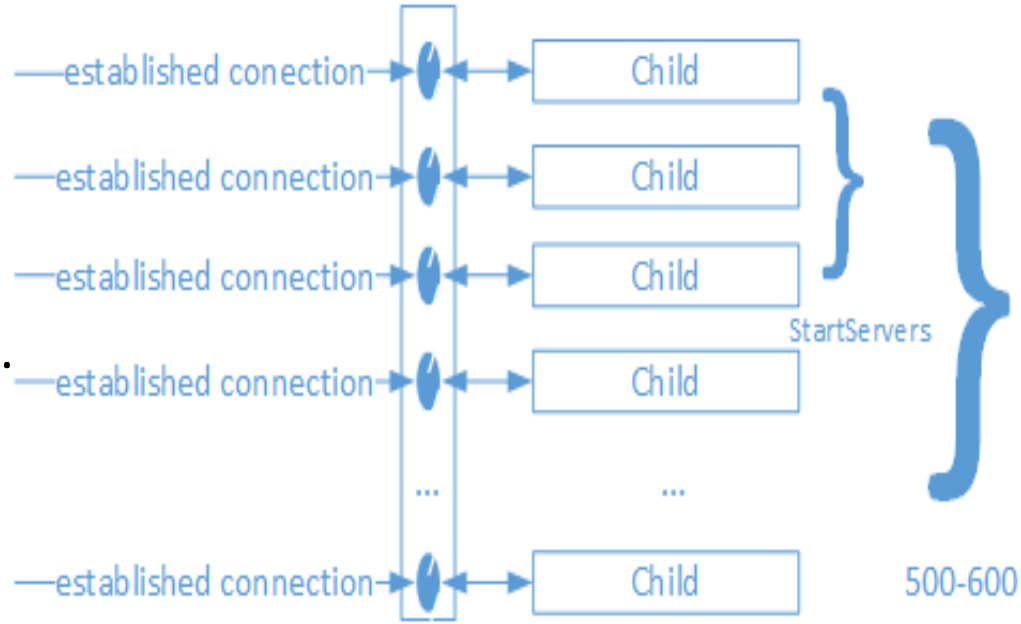
Connection handling architectures

ICC International Cybersecurity Congress

- Process based connection handling?
  - Think “Apache”
- Event based connection handling?
  - Think “nginx”

Apache web server (simplified)

- Few child processes listen on a socket
- A new connection comes in…
- …and one of them takes it
- Another new connection comes in…
- …and the next one takes it.
- Pool is exhausted; new processes are spawned (forked)
- …and so on…
- Up to about 500-600
- The initial set is defined by StartServers



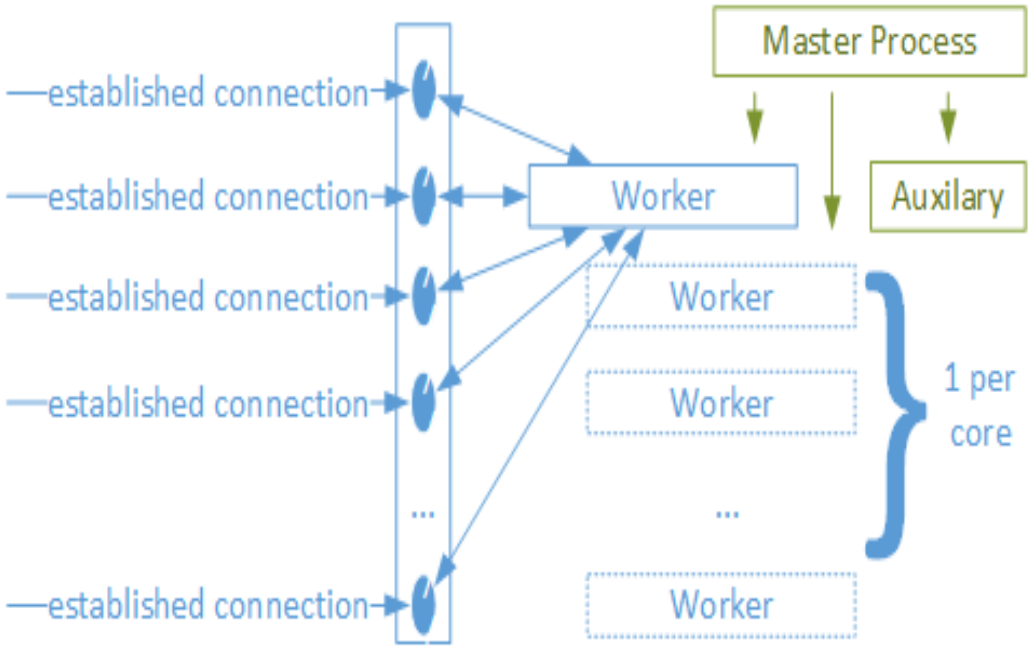
Nginx (simplified)

ICC International Cybersecurity Congress

- Master Process controls logistics
- Support processes (cache management)
- Worker processes process connections
- One or more…

  …one per core
- Each worker can handle many sockets concurrently
- A new connection comes in

  …and is established; no dup()
- …and so on…



Slowloris

ICC International Cybersecurity Congress

- Exploits the process based model but opening a number of concurrent connections and holds them open for as long as possible with the least amount of bandwidth possible

Slowloris request

ICC International Cybersecurity Congress

Request:

send: GET /pki/crl/products/WinPCA.crl HTTP/1.1

wait...

send: Cache-Control: max-age = 900

wait...

send: Connection: Keep-Alive

wait...

send: Accept: */*

wait...

send: If-Modified-Since: Thu, 06 Aug 2015 05:00:26 GMT

wait...

send: User-Agent: Microsoft-CryptoAPI/6.1

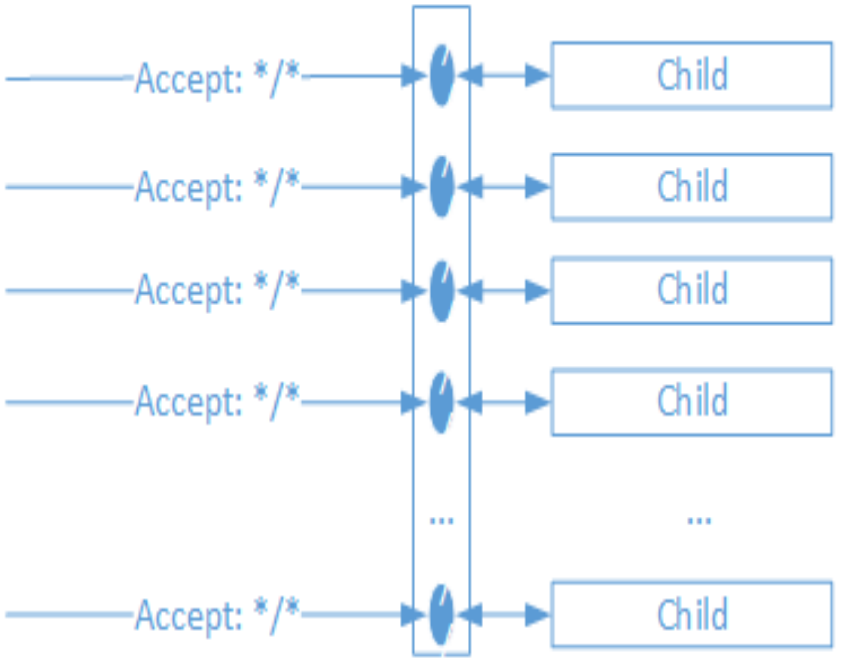
wait...

send: Host: crl.microsoft.com

Slowloris illustrated

ICC International Cybersecurity Congress

- The client opens a connection and sends a request…
- …then another…
- …and another…
- …and so on.



- …and waits some time…
- …and sends the next header
- …and so for each connection
- …and so on…

Slowloris mitigation

ICC International Cybersecurity Congress

- Change of the software architecture
- Use of event driven reverse proxy to protect the server (like nginx)
- Dedicated hardware devices

Reflection and amplification attacks

Two different terms

- Reflection
  using an intermediary to deliver the attack traffic
- Amplification
  ability to deliver larger response than the query traffic

Reflection

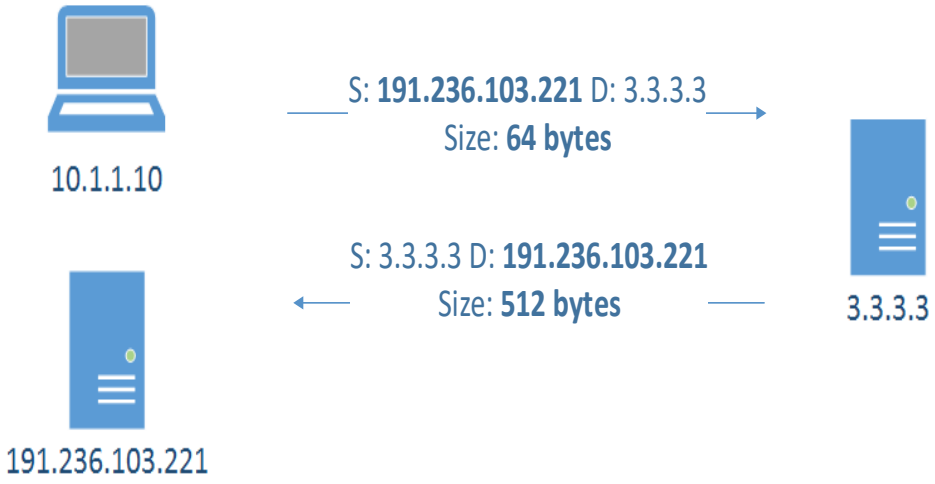
Reflective attacks

ICC International Cybersecurity Congress

- Attacks where the an unwilling intermediary is used to deliver the attack traffic
- The attacker would normally send a packet with a forged source IP address to the intermediary. The forget address is going to be the one of the target. The intermediary will deliver a response which will go to the target instead of the attacker

What is reflection(ed) attack

- Attacks where the an unwilling intermediary is used to deliver the attack traffic
- Attacker sends a packet with a spoofed source IP set to the victim's
- Reflectors respond to the victim



Reflector types

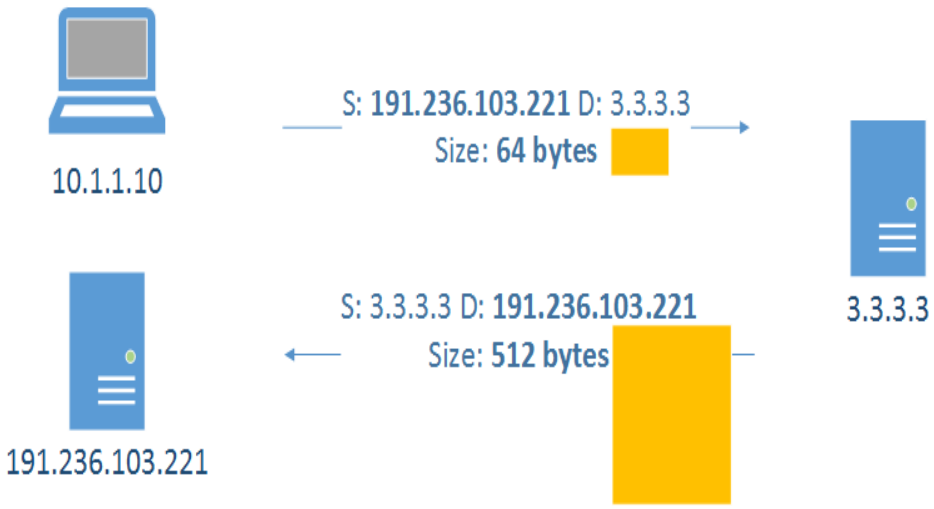
The ones that are of interest are:

- DNS
- NTP
- SSDP
- SNMP
- RPC (reported lately but not really large)

Amplification

What is amplification attack?

- Asymmetric attack where response is much larger than the original query



Amplifiers types

- The ones that are of interest and provide amplifications are:
  - DNS
  - SSDP
  - NTP
  - SNMP

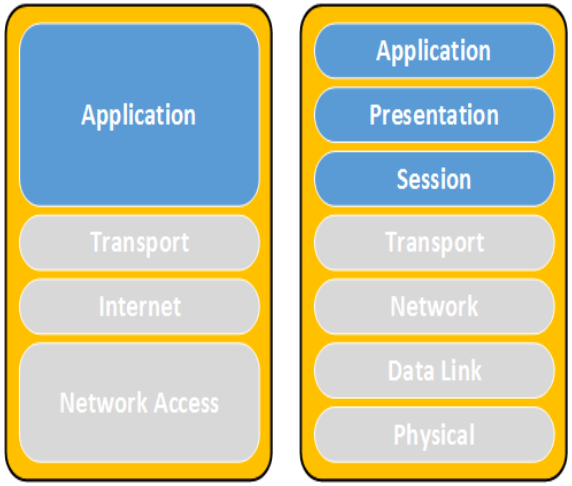
- Amplification factors:
  https://www.us-cert.gov/ncas/alerts/TA14-017A

Amplification quotients

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	Multiple
NTP	556.9	Multiple
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange

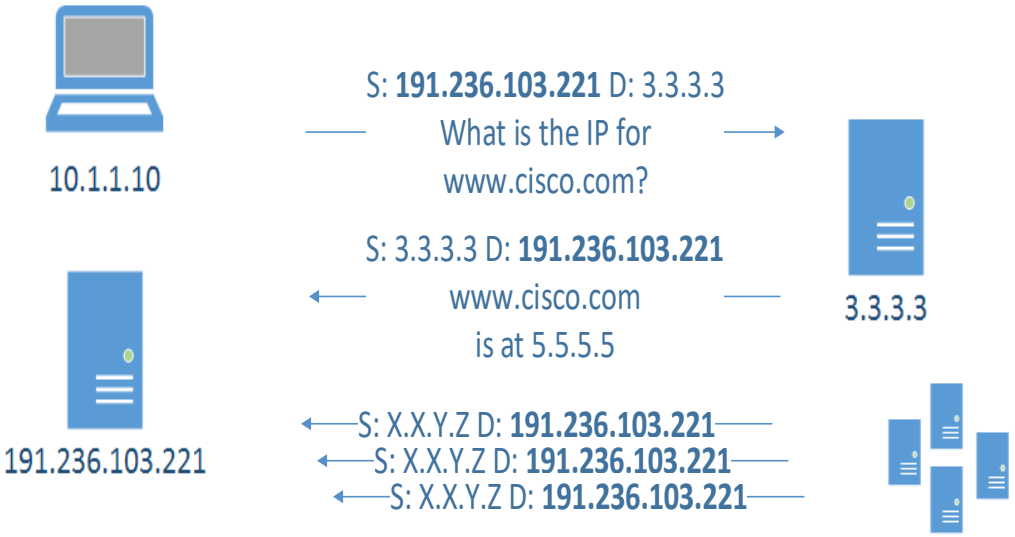
- Source: US-CERT: https://www.us-cert.gov/ncas/alerts/TA14-017A

DNS Reflection



What is DNS reflection attack?

- What happens if an attacker forges the victim address as its source?



...the reflected traffic goes to the target server

- ... and what if hundreds of misconfigured open DNS resolvers are used?

Consider this query

ICC International Cybersecurity Congress

- Triggered by something like:

  dig ANY isc.org @3.3.3.3

- Example:

  ~$ dig ANY isc.org @172.20.1.1 # My home lab

- Flip over for answer

Consider this (cont'd)

ICC International Cybersecurity Congress

ghostwood@sgw:~$ dig ANY isc.org @172.20.1.1

;; ANSWER SECTION:

isc.org. 481 IN RRSIG DS 7 2 86400 20130607155725 20130517145725 42353 org. KHMs09DaFMx416/7xXhaD9By0NrqCiQ4kBnqi6oq2VocZRREAbUHHrAY
KydlgKO5vOaw6l1Fy86/oiODkk3yyHspciwdJvjIefu4PktdUnd1IQxW 791q/jWgHBL5iQQigBYv7Z5IfY1ENn+6fPOchAywWqEBYcdqW8pzzOjz zlU=

isc.org. 481 IN DS 12892 5 2 F1E184C0E1D615D20EB3C223ACED3B03C773DD952D5F0EB5C777586D E18DA6B5

isc.org. 481 IN DS 12892 5 1 982113D08B4C6A1D9F6AEE1E2237AEF69F3F9759

isc.org. 5725 IN RRSIG A 5 2 7200 20130620134150 20130521134150 50012 isc.org. iCBy1Jj9P6mXVYjaSc62JClrZW+hvYAUGHo7WwRmxGRaipS8I9+LCvRl
2erglomkBP79m9ahnFOxWEAaueA6TIHClGxOkgrk3hBtMFjUB9rhvkIm uxO2D8gc1DJDLl5egfpJCF2fITFhEvWzeMt6QGNwicWMxBsFHCxM7Fms D8I=

isc.org. 5725 IN A 149.20.64.42

isc.org. 5725 IN RRSIG DNSKEY 5 2 7200 20130620130130 20130521130130 12892 isc.org. dfxTGA/f6vdhuIqojp+Konkdt8c4y3WiU+Vs5TjznvhdEyH14qPh/cHh
+y1vA6+gAwTHl4X+GpzctNxiElwaSwVu3m9NocniwI/AZQoL/SyDgEsI bJM/X+ZXY5qrgQrV2grOcKAAA91Bus3behYQZTsdaH2TStAKjKINEgvm

yQ5xWEo6zE3p0ygtPq4eMNO4fRT9UQDhTRD3v3ztxFlNXKvBsQWZGBH0 5tQcbC6xnGyn1bBptJEEGhCBG01ncJt1MCyEf98VGHKJFeowORiirDQ3
cjJRFPTCCkA8n4j8vnsimIUP/TGl+Mg4ufAZpE96jJnvFBsdcC/iOo6i XkQVIA==

isc.org. 5725 IN RRSIG DNSKEY 5 2 7200 20130620130130 20130521130130 50012 isc.org. o18F3KIFkYedFRw1e5MP4qDo3wSg0XK9l5WCYD75aGhs9Rl5eyc/6KEW
Se4lZXRhf6d77xXlerMYCrsfh/GHdjPRoE1xL/nzH/hTBJAI9XDbC5I/ EUpFlGVLVdQy43XKtywm0j2nyc5MdGa2VeLKo+hHTmH3St3pGRVJp2IK 5Z0=

isc.org. 5725 IN DNSKEY 257 3 5 BEAAAAOhHQDBrhQbtphgq2wQUpEQ5t4DtUHxoMVFu2hWLDMvoOMRXjGr hhCeFvAZih7yJHf8ZGfW6hd38hXG/xylYCO6Krpbdojwx8YMXLA5/kA+
u50WIL8ZR1R6KTbsYVMf/Qx5RiNbPClw+vT+U8eXEJmO20jIS1ULgqy3 47cBB1zMnnz/4LJpA0da9CbKj3A254T515sNIMcwsB8/2+2E63/zZrQz
Bkj0BrN/9Bexjpiks3jRhZatEsXn3dTy47R09Uix5WcJt+xzqZ7+ysyL KOOedS39Z7SDmsn2eA0FKtQpwA6LXeG2w+jxmw3oA8lVUgEf/rzeC/bB yBNsO70aEFTd

isc.org. 5725 IN DNSKEY 256 3 5 BQEAAAABwuHz9Cem0BJ0JQTO7C/a3McR6hMaufljs1dfG/inaJpYv7vH XTrAOm/MeKp+/x6eT4QLru0KoZkvZJnqTI8JyaFTw2OM/ItBfh/hL2lm
Cft2O7n3MfeqYtvjPnY7dWghYW4sVfH7VVEGm958o9nfi79532Qeklxh x8pXWdeAaRU=

a.root-servers.net. 297269 IN A 198.41.0.4

a.root-servers.net. 415890 IN AAAA 2001:503:ba3e::2:30

b.root-servers.net. 298007 IN A 192.228.79.201

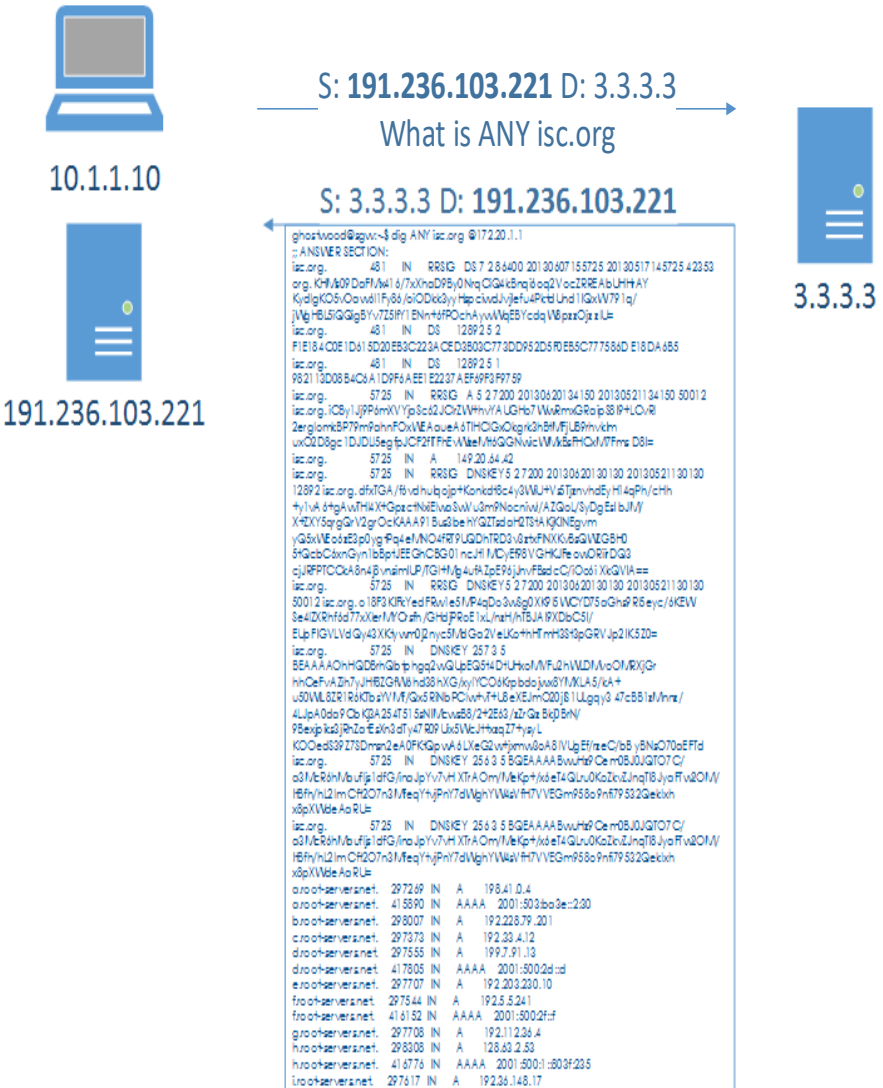
c.root-servers.net. 297373 IN A 192.33.4.12

d.root-servers.net. 297555 IN A 199.7.91.13

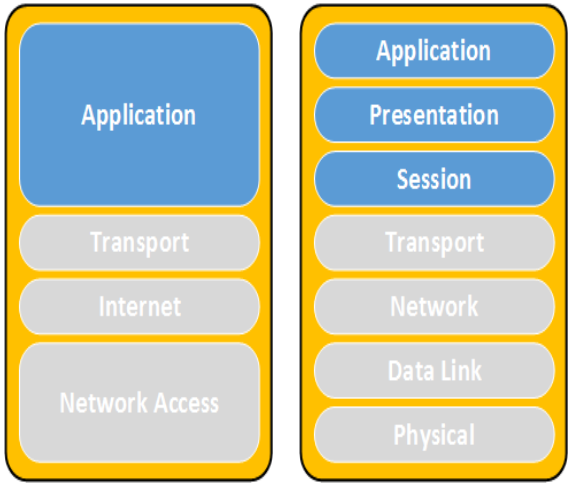
d.root-servers.net. 417805 IN AAAA 2001:500:2d::d

e.root-servers.net. 297707 IN A 192.203.230.10

Reflection and Amplification

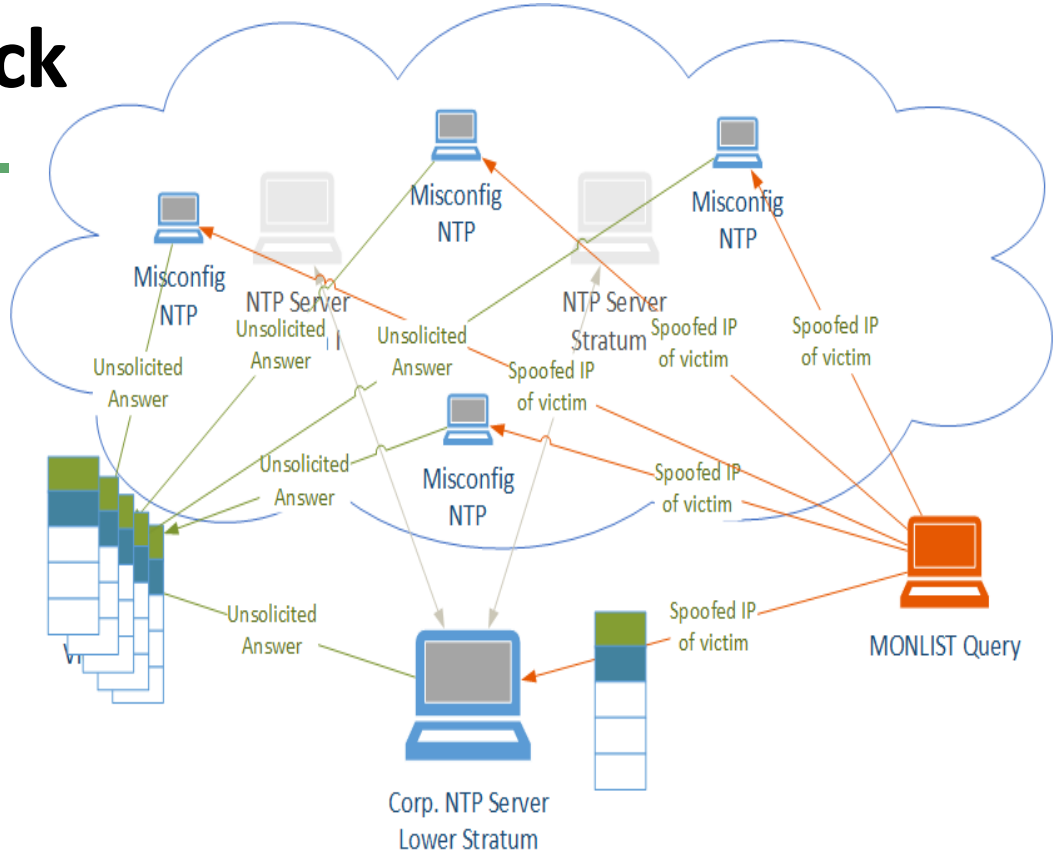


Network Time Protocol (NTP)



NTP reflection attack

- Stratum servers
- NTP queries



- MONLIST command
  - provides
    a list of clients that have
    time readings

NTP server configuration

ICC International Cybersecurity Congress

- Access lists
- NTP authentication
- Disable the MONLIST command
- Useful hints: http://www.team-cymru.org/secure-ntp-template.html
- List of open NTP reflectors: http://openntpproject.org/

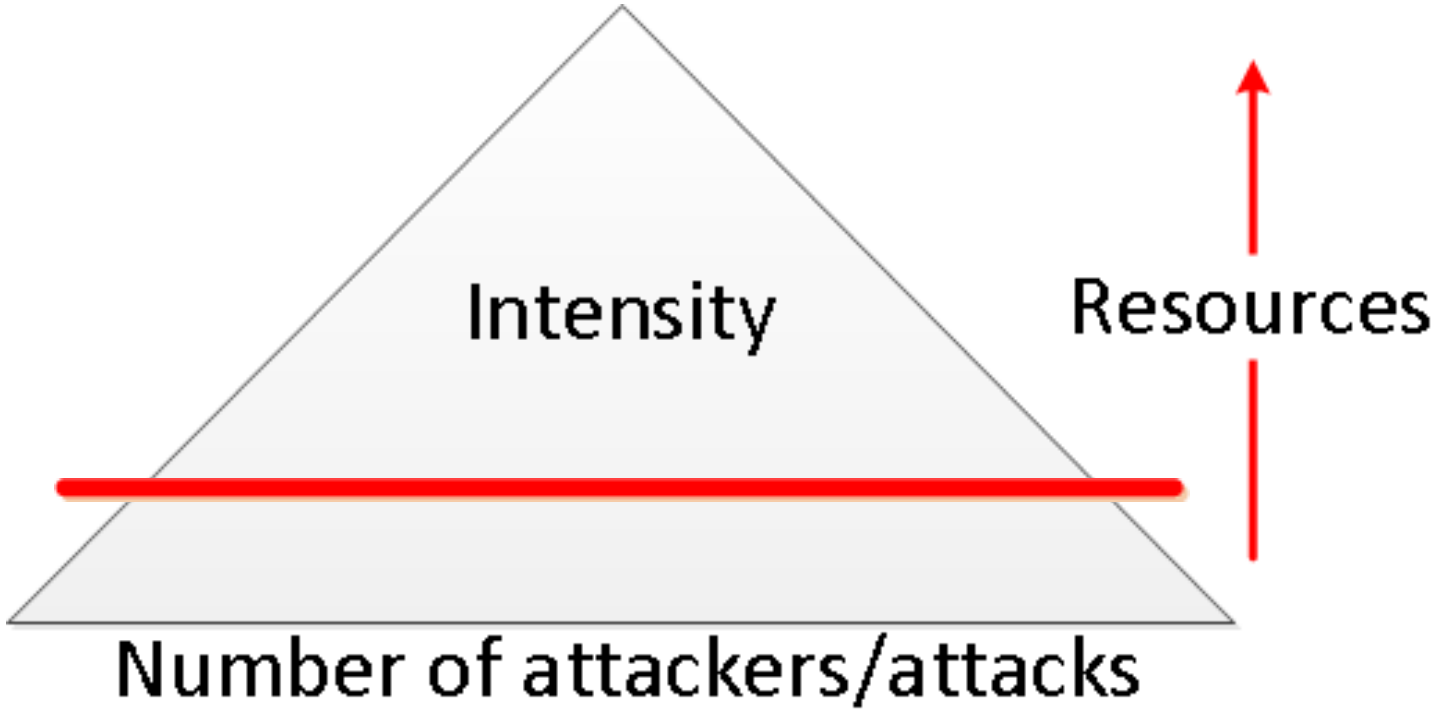
Mitigation Strategies

Overview

ICC International Cybersecurity Congress

- Risk pyramid
- Value of being online/Outage costs
- Mitigation strategies

Risk Pyramid



The cost of a minute?

ICC International Cybersecurity Congress

- How much does a minute of outage cost to your business?
- Are there other costs associated with it? Reputation?
- Are you in a risk category?
- How much is executive management willing to spend to stay up?

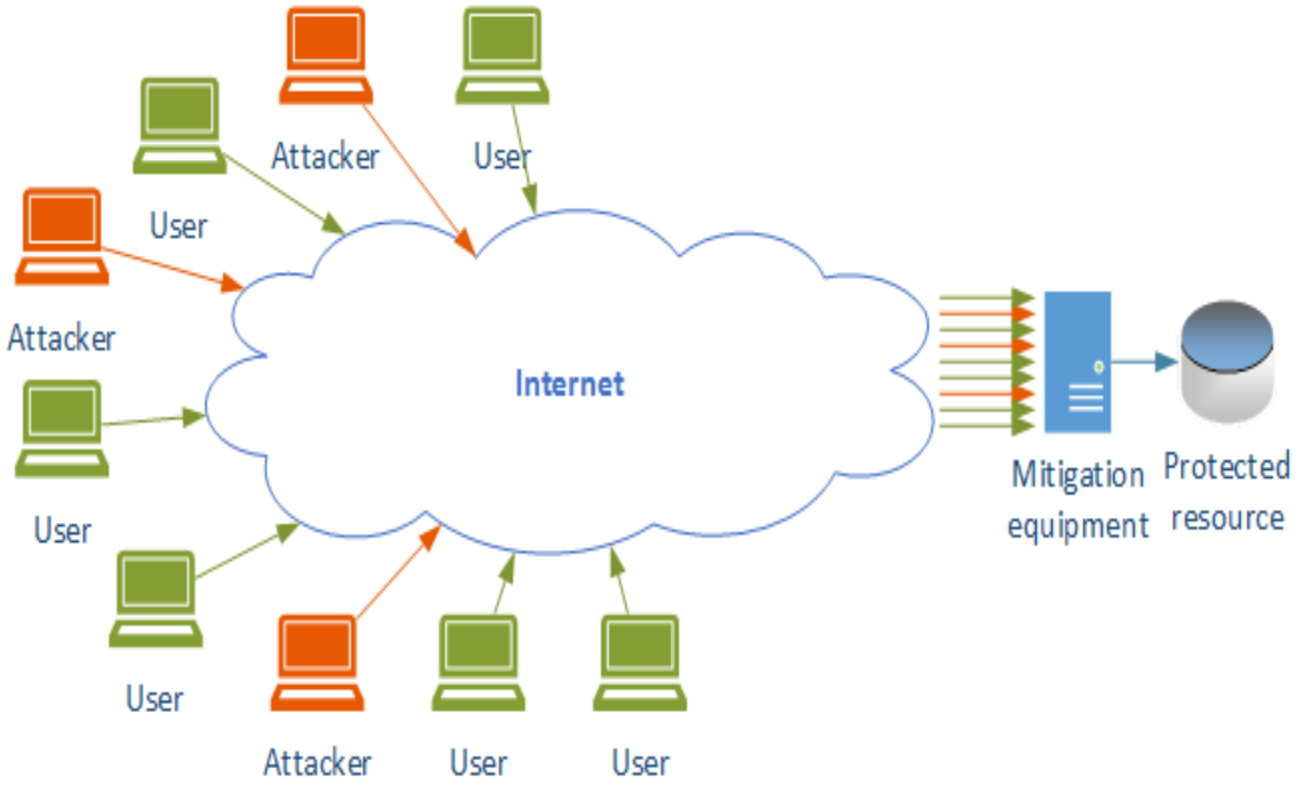
- Are there reasons you need to mitigate on-site vs offsite? Latency?

Mitigation

Different approaches:

- Do it yourself (DIY)
- Outsource/service
  - On demand
  - Always on
- Hybrid

Do it Yourself (On Premise)



DIY: Considerationss

- Network capacity: bandwidth
- Hardware capacity: packet rates, inspecting headers and content?
- One time cost (refresh every 3-4 years)
- Depending on attacks size can be in $100,000s

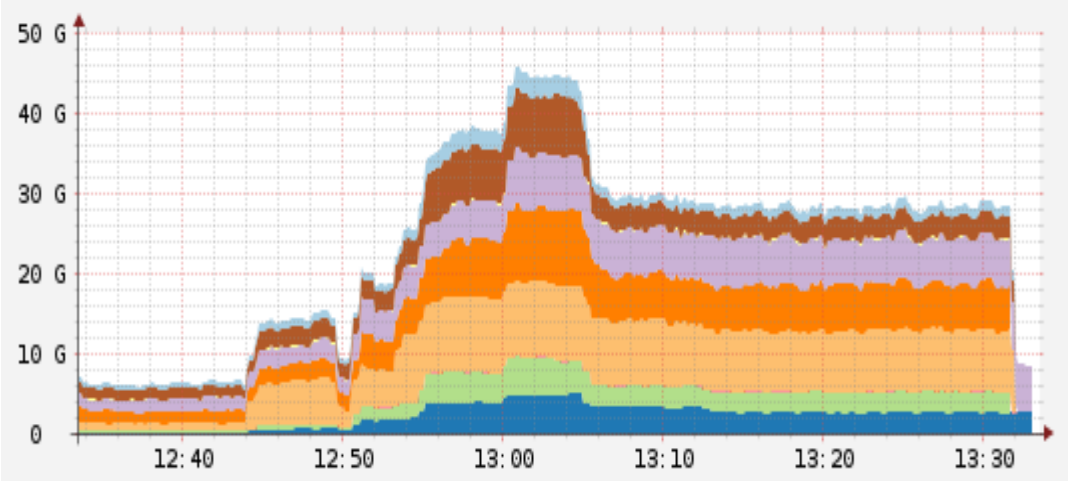
DIY: Benefits

ICC International Cybersecurity Congress

- Very low latency
- Can be application specific (non-http, gaming industry)
- Better control of the mitigation
- If inspecting TLS traffic keeps the keys in the company

DIY: Drawbacks

- Network capacity:
- Fluctuates
- How much do you over provision?
  Double, triple, ten times?



- Need to procure
  - bandwidth - monthly recurring - expensive, adds up
  - compute and network hardware
  - qualified personnel – hard to find; expensive; hard to retain

DIY: Bottom line

- traffic – 10GBps = $2,000/mo (NA)
- colocation space - $400/mo
- power – depends on equipment and location
- equipment – min $20,000 per 10GBps port
- personnel – go figure… ☺

…and you need them in many locations, with multiple per location

DIY: Conclusions

ICC International Cybersecurity Congress

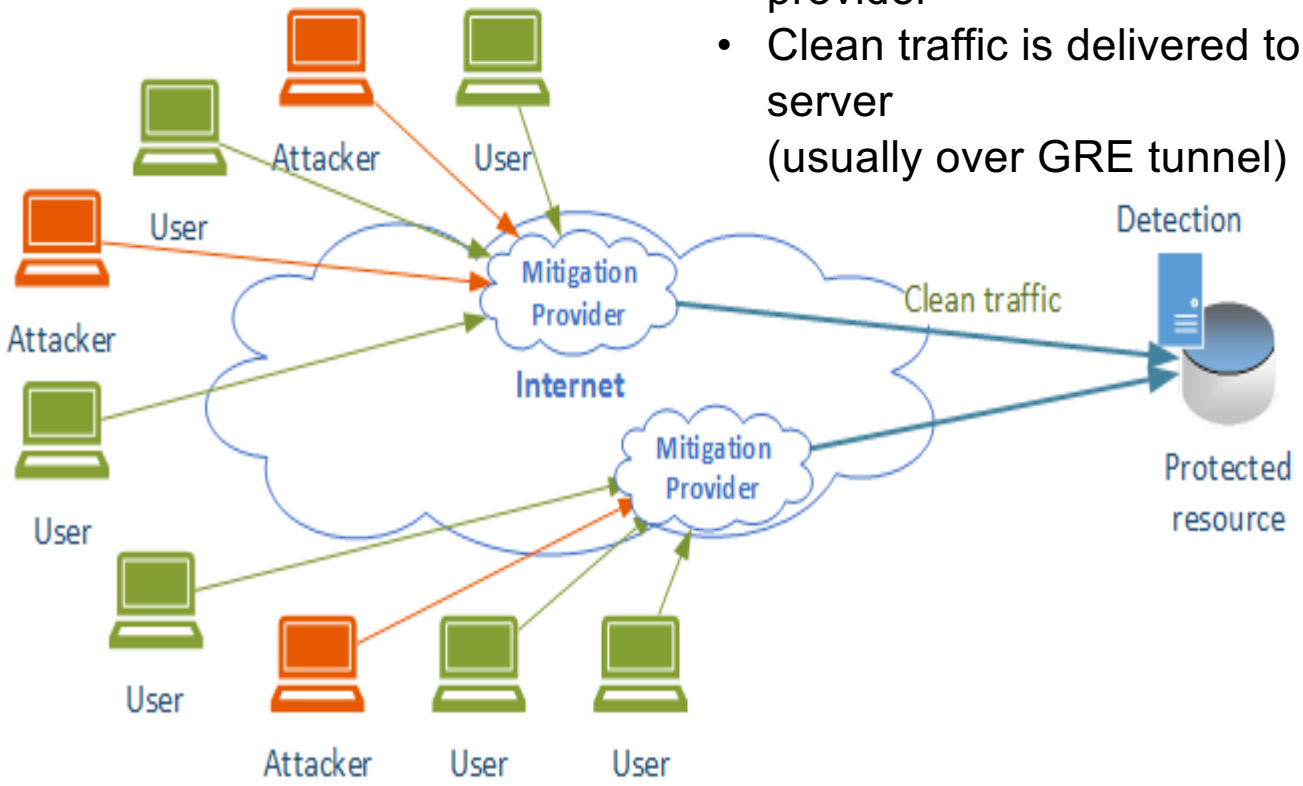
- At present DDoS attacks are at a very large scale but DIY is not easy to scale for small and medium networks
- Leverages economy of scale – requires a large infrastructure
- Infrastructure is very expensive to build and maintain
- Requires significant amount of know-how
- Unless hosting a very large site it’s better left to the professionals

External service

- DDoS mitigation service providers and CDNs
- Pricing:
  - based on size of attack
  - based on clean traffic
- Operating model:
  - on demand
  - always on

On Demand DDoS

- Target: detect and signal the mitigation provider
- Mitigation provider: Inject BGP routes
- Traffic is redirected to the mitigation provider
- Clean traffic is delivered to the origin server
  (usually over GRE tunnel)



On Demand Mitigation - benefits

ICC International Cybersecurity Congress

- Scales up very easily
- Since most applications are HTTP/S based, it is compatible with them
- Easier to deploy
- May leave the target vulnerable to bypass

On Demand Mitigation - drawbacks

ICC International Cybersecurity Congress

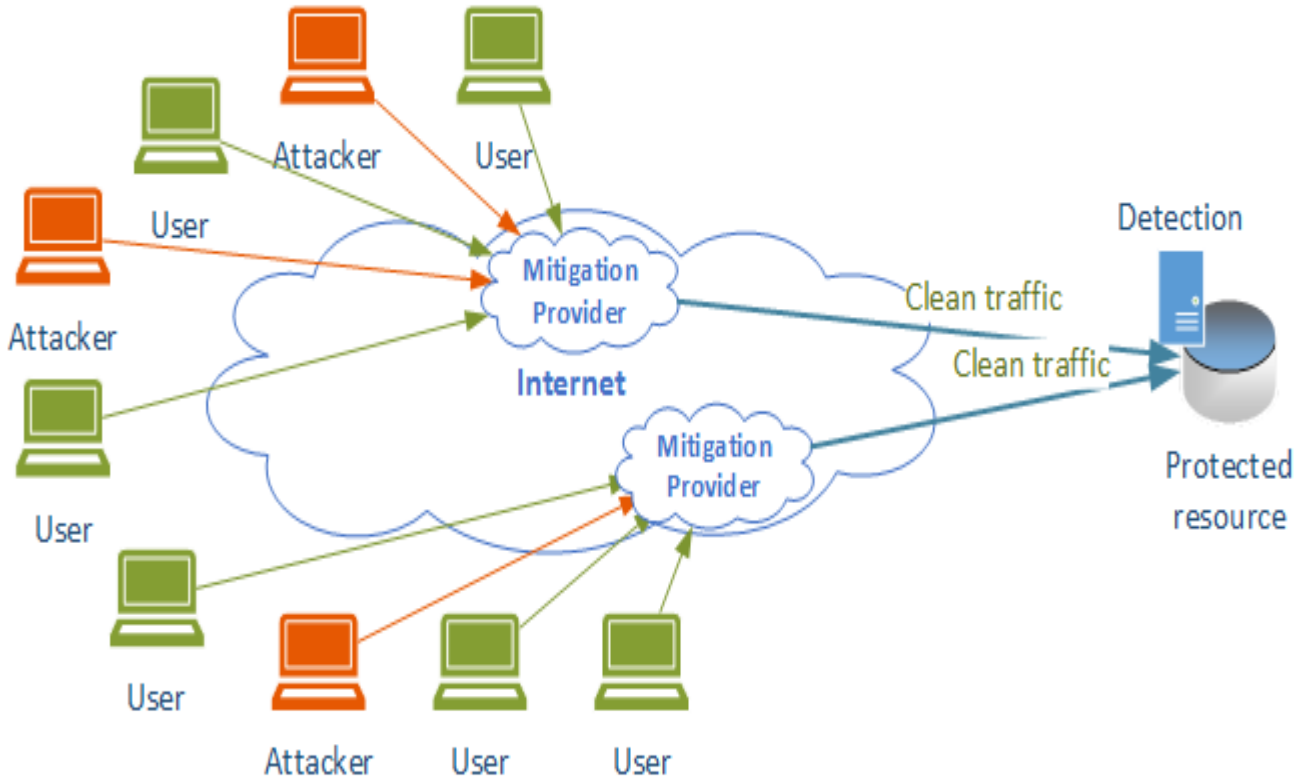
- Takes time between the site being attacked until it switches to the service provider
- Potential outages
- Difficult to establish TLS
- May have increased latency
- Target may still be exposed
- Detection is not Application Aware
- GRE Tunnels create complexity

Always On Mitigation

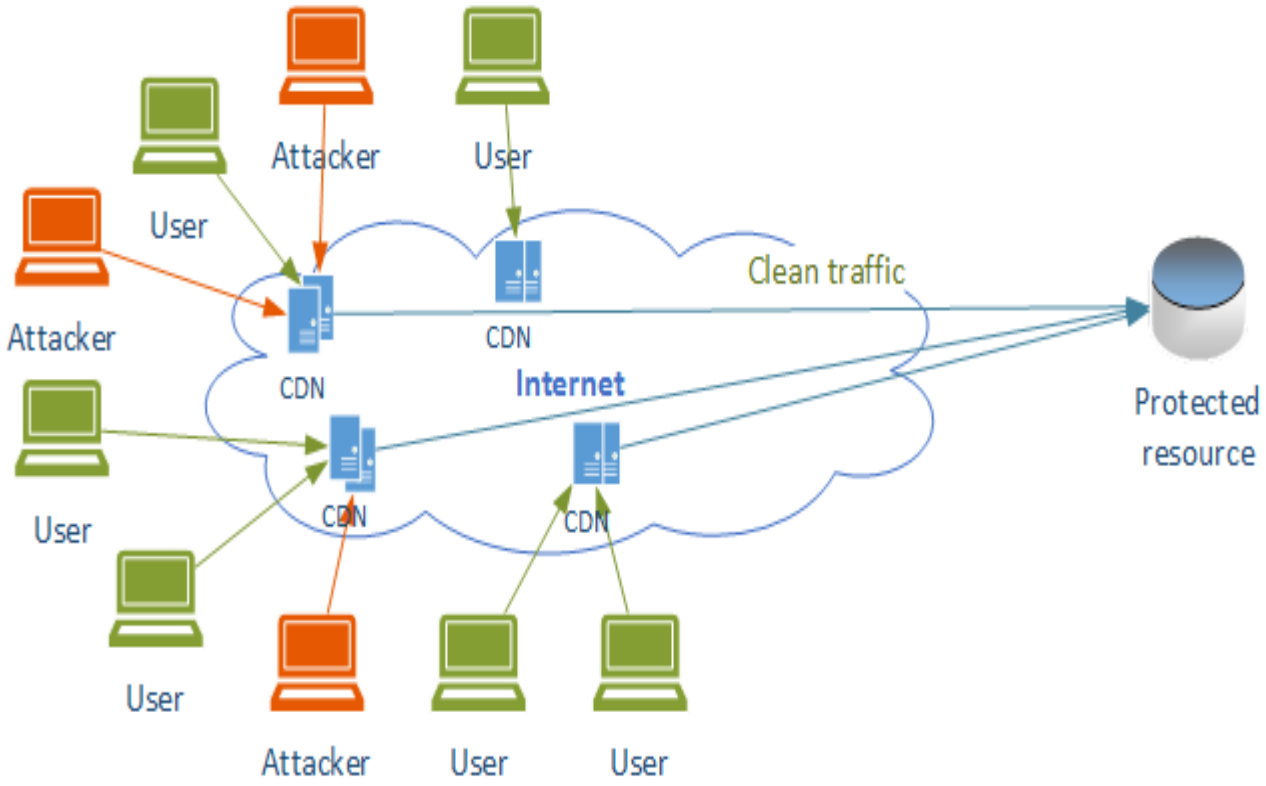
ICC International Cybersecurity Congress

- Permanently serve the customer space
  - Advertise IP address space
  - Use shared delivery infrastructure (CDN)
- Traffic is always flowing through the mitigation systems
- Usually combined with services like CDN, which further increases website performance (even during peace time)

Always On DDoS Mitigation (advertise IP space)



Always On DDoS Mitigation (CDN)



Always On Mitigation - benefits

ICC International Cybersecurity Congress

- Scales up very well during volumetric attacks
- Mitigation can be virtually instantaneous
  - No moving parts during the attack
- Can protect most applications
- Once it’s on there are no moving parts
- Very hard to bypass
- (proxy/caching) If deployed properly, it may improve website performance
- Cost depends on the website traffic (not the attack)

Always On Mitigation - drawbacks

ICC International Cybersecurity Congress

- Can increase latency
- Challenges around TLS
- Stale caches
- May be much more expensive

Hybrid

- Combination of DIY and service providers
- Helps customers manage their risk profile in a more flexible way

Benefits:

- Provides protection against large scale events without the added service cost
- Allows for escalating response postures and risk/finance management
- Overall most of the benefits of On Demand

Drawbacks:

- Increased complexity
- Requires skilled personnel
- May have interoperability issues

DDoS mitigation service providers

ICC International Cybersecurity Congress

- It is an ongoing expense
- Depending on the business model it can be big or small
- Hides the complexities of managing the problem
- May introduce latencies, but also may accelerate content if used properly

DDoS mitigation svc providers – bottom line

ICC International Cybersecurity Congress

- Depends on the exact setup
  - in CDN cases may depend on the size of the size more than the size of the attack
  - varied: $50/month – thousands…

DDoS mitigation service providers

ICC International Cybersecurity Congress

- Pros
- Hides the complexities of managing the problem
- May accelerate content delivery
- May be much cheaper, especially as attack sizes grow but are not common
- Cost: much, much lower than DIY

- Cons
- May not be applicable to all applications - gaming
- May increase latency
- May end up expensive
- Third party sees the users (and maybe the content) - privacy, security
- Issues with stale cache

The other side

- How much does it cost to launch a DDoS?
- What do you need to launch one?

Considerations

ICC International Cybersecurity Congress

- Capacity
  - Hardware (compute, network)
    - drones, reflectors
    - C&C
  - Network (bandwidth)
    - “borrow” ;)
- Software
  - scripts that execute the attacks; C&C

The same dichotomy

ICC International Cybersecurity Congress

Two ways to go about it:

- DIY
- DDoS Service (booters/stressers)

Software

ICC International Cybersecurity Congress

- Individual attack scripts – pastebin, hackfroums, etc.
- booter scripts – basic, sometimes control panel
- More advanced - C&C server and separate agent for the drones
  - dirt jumper
  - black energy (general RAT)
- Most kits are in the $100-600 range (if not free)
- Open source

Capacity

Drones

- Need infected systems
  - purchase – cents per install, depends on geo location, in batches of 1,000
- Infect them – much more work, need to use additional software – EK, spam, etc.

Reflectors

- use a list – easily available in the underground
- scan – $50-60/month to scan freely

Do-it-yourself (DYI)

Benefits:

- Complete control of the attack traffic
- Custom attacks
- Can easily resell

Drawbacks:

- Maintain infrastructure
- Requires some skills
- Requires a lot of personal time to research and build infrastructure

Bottom line

ICC International Cybersecurity Congress

Service:

- $15-250/month

DIY:

- Kit - $100-600 (one time)
- Hosting - $100-250/month
- Spent time on forums

Summary and conclusions

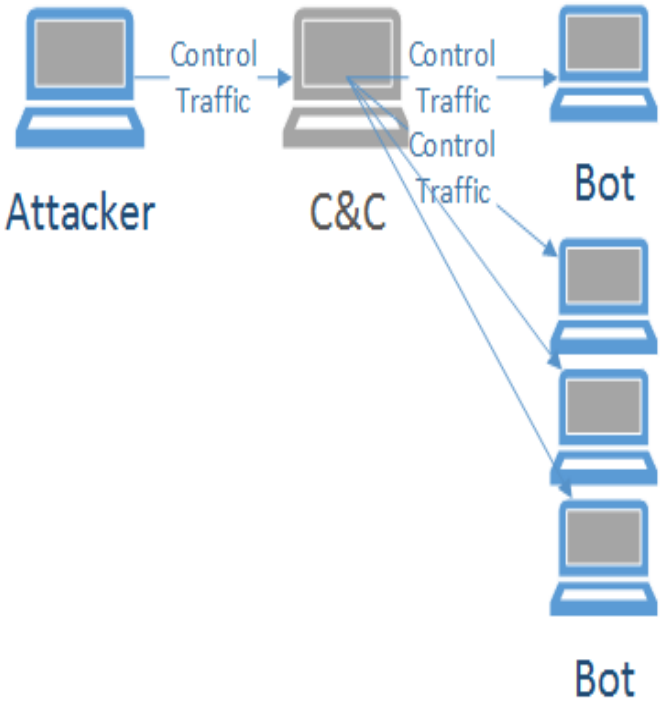
ICC International Cybersecurity Congress

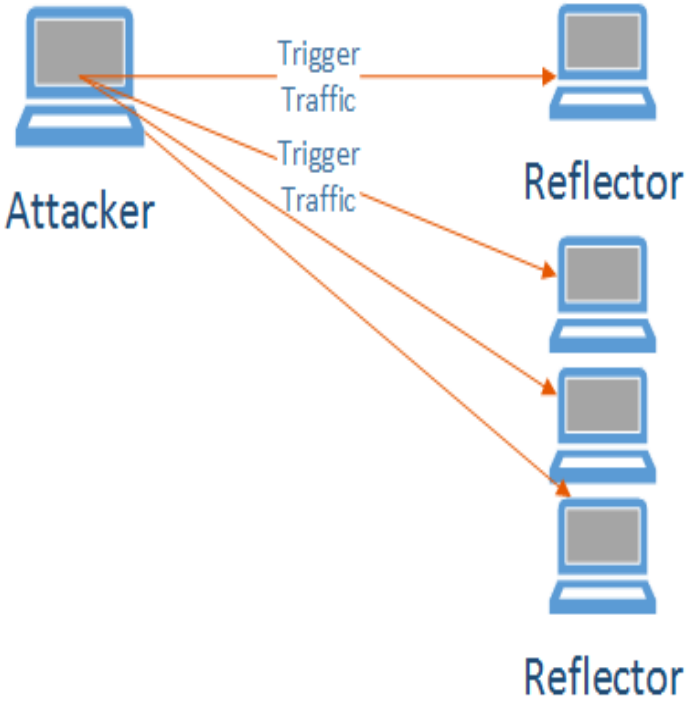
- What can we do about it?

Contributing factors

- Reflected attacks
- **Hosting providers allowing IP address spoofing**
- Hosting providers not cleaning up abuse effectively
- Network providers not providing trace-backs
- Network providers not being incentivized to clean up the traffic.

Low cost thanks to reflection





Network providers

ICC International Cybersecurity Congress

- Most are not willing to provide trace-backs
- In many cases they are bit incentivized, they are moving traffic, no need to spend additional resources
- Even if willing, it's usually done manually which introduces delays
- There are no common protocols for requesting this type of information

Hosting providers

ICC International Cybersecurity Congress

- Fail to deal with abuse complaints
- Fail to enforce abuse complaints
- Fail to cooperate with LE on DDoS issues

Conclusions

ICC International Cybersecurity Congress

- It is much cheaper to execute and attack than defend from it (by at least two orders of magnitude)
- Attack cost will continue to decrease
- Attackers are not disincentivised in any way
- Law enforcement efforts are not matching the scale of the problem
- We need to increase the cost of doing business
- Network providers not being incentivized to clean up the traffic.

The way forward

ICC International Cybersecurity Congress

- Anti-spoofing, potential government regulation

  BCP38, uRPF

- Depeering chronically pathologic providers
- Software updates
- Tracebacks, potential government regulation

In the end…

ICC International Cybersecurity Congress

- It takes many thousands of dollars to defend from DoS and it is fairly inexpensive to execute one
- In both cases economy of scale is important
- A lot of the issues are caused by bad Internet hygiene – no outbound filtering (BCP38)
- The service providers need to start cracking down on abuse

Copyright

Are you noticing the imbalance?

Defend yourself

- Anycast (DNS)
- Some form of IPS/DDoS mitigation gear

- **Lots of money**

Defend the Internet

- Rate-limiting
- BCP38/140 (outbound filtering) source address validation
- Securely configured authoritative DNS servers
- No open resolvers

- **Somewhat cheap**