OSY.SSI[2019][5]

In the previous episode...

In the previous episode...

Before we begin

1. Slides, course notes, etc. available online

   `https://github.com/sticky-jr/cs-sec-19`

   ll will be updated regularly, please check often!

2. Exam topics will be ready soon (`exam.pdf` on the GitHub). Please organise yourselves.

Before we begin

1. Slides, course notes, etc. available online

   `https://github.com/sticky-jr/cs-sec-19`

   ll will be updated regularly, please check often!

2. Exam topics will be ready soon (`exam.pdf` on the GitHub). Please organise yourselves. DON'T WAIT.

Before we begin

1. Slides, course notes, etc. available online

   `https://github.com/sticky-jr/cs-sec-19`

   ll will be updated regularly, please check often!

2. Exam topics will be ready soon (`exam.pdf` on the GitHub). Please organise yourselves. DON'T WAIT.

3. Feedback.

In the news...

In the news...

- Checkm8 unpatchable vulnerability on iOS: all versions from 4S to 10 [src]
- Google achieves 'quantum supremacy' [src]
- Facebook, WhatsApp will have to give UK police access to 'encrypted' messages [src]
- WIBattack against millions of mobile phones [src]
- Nodersok/Divergent fileless malware turning thousand of computers into zombies [src]
- US Senate passes DHS Cyber Hunt and Incident Responsee Teams Act (S.315) [src]
- US Director of National Intelligence declares 'cyberwar' the greatest threat on the country [src]
- APT10 (PLA/JSSD, zh) attack Airbus, Rolls-Royce, Expleo and ttwo other unnamed French contractors, in search of commercial secrets [src]
- European defence contractor Rheinmetall plants 'significant disruption' caused by malware in Brazil, Mexico, US, causing steep share drop. [src]
- Dunkin' Donuts sued over customer data breaches in 2015 and 2018 [src]
- CrowdStrike resurfaces in the US election landscape [src]
- Magecart Group 5 targets layer 7 WiFi routers used in hotels, airports, etc. [src]
- Mac Pro workstations stuck in reboot loops around Hollywood [src]
- Apple patches iOS 13 exploit we discussed two weeks ago. [src]
- DoorDash (food delivery) data breach exposes 4.9 million customers [src]

What is this?

(Can you hear it?)

Today

Internet

Why “Internet”?

Why “Internet”?

- Because it’s familiar (hence, unknown, cf. Hegel)

Why “Internet”?

- Because it’s familiar (hence, unknown, cf. Hegel)
- Because it’s relatively easy

Why “Internet”?

- Because it’s familiar (hence, unknown, cf. Hegel)
- Because it’s relatively easy
- Because it’s been the same for a long time

Why “Internet”?

- Because it’s familiar (hence, unknown, cf. Hegel)
- Because it’s relatively easy
- Because it’s been the same for a long time
- Because it’s all around us

Why “Internet”?

- Because it’s familiar (hence, unknown, cf. Hegel)
- Because it’s relatively easy
- Because it’s been the same for a long time
- Because it’s all around us
- Because it is maybe fundamentally broken

Part of my goal is to change some of the above.

Why “Internet”?

- Because it’s familiar (hence, unknown, cf. Hegel)
- Because it’s relatively easy
- Because it’s been the same for a long time
- Because it’s all around us
- Because it is maybe fundamentally broken

Part of my goal is to change some of the above.

Part of my goal is to apply what we know of the Classical Theory$^{\text{TM}}$.

What guarantees against information-related risks?

Confidentiality?
Integrity?
Availability?

Table of Contents

Basic network architecture
- A first look at the Internet
- How can the Internet work?
- We need to dig deeper

How the Internet works: The Devil and the Details
- Where is the Internet?
- Name and address resolution

When the cat's away...
- What is a "connection"?
- What is a "reply"?

What is the Internet?

What is the Internet (cont'd)

High-level experience :

What is the Internet (cont'd)

High-level experience :

- "Connect" to a network

What is the Internet (cont'd)

High-level experience :

- "Connect" to a network
- *(wait a bit)*

What is the Internet (cont'd)

High-level experience :

- "Connect" to a network
- *(wait a bit)*
- Type in "`www.education.xxx`"

What is the Internet (cont'd)

High-level experience :

- "Connect" to a network
- *(wait a bit)*
- Type in "`www.education.xxx`"
- *(wait a bit)*

What is the Internet (cont'd)

High-level experience :

- "Connect" to a network
- *(wait a bit)*
- Type in "`www.education.xxx`"
- *(wait a bit)*
- Magic! (and "educative" material)

What is the Internet (cont'd)

High-level experience :

- "Connect" to a network
- *(wait a bit)*
- Type in "`www.education.xxx`"
- *(wait a bit)*
- Magic! (and "educative" material)

How can the Internet work? Spaggheti.

Internet is

How can the Internet work? Spaggheti.

Internet is a stack of spaghetti protocols:

How can the Internet work? Spaggheti.

Internet is a stack of spaghetti protocols:

- `http`, `ftp`, `smtp`, `pop`, `imap`, `Ethernet...`

How can the Internet work? Spaggheti.

Internet is a stack of spaghetti protocols:

- `http`, `ftp`, `smtp`, `pop`, `imap`, `Ethernet`...
- `ssh`, `ldap`, `dhcp`, `dns`, `sip`, `ospf`, `bgp`...

How can the Internet work? Spaggheti.

Internet is a stack of spaghetti protocols:

- `http`, `ftp`, `smtp`, `pop`, `imap`, `Ethernet...`
- `ssh`, `ldap`, `dhcp`, `dns`, `sip`, `ospf`, `bgp...`
- `tcp`, `udp`, `dccp`, `sctp`, `rsvp...`

How can the Internet work? Spaggheti.

Internet is a stack of spaghetti protocols:

- `http, ftp, smtp, pop, imap, Ethernet...`
- `ssh, ldap, dhcp, dns, sip, ospf, bgp...`
- `tcp, udp, dccp, sctp, rsvp...`
- `ip, ipv6, icmp, icmpv6, ecn, igmp..`

How can the Internet work? Spaggheti.

Internet is a stack of spaghetti protocols:

- `http`, `ftp`, `smtp`, `pop`, `imap`, `Ethernet`...
- `ssh`, `ldap`, `dhcp`, `dns`, `sip`, `ospf`, `bgp`...
- `tcp`, `udp`, `dccp`, `sctp`, `rsvp`...
- `ip`, `ipv6`, `icmp`, `icmpv6`, `ecn`, `igmp`...
- `arp`, `ndp`, `l2tp`, `ppp`, `isdn`...

How can the Internet work? Spaggheti.

Internet is a stack of spaghetti protocols:

- `http`, `ftp`, `smtp`, `pop`, `imap`, `Ethernet`...
- `ssh`, `ldap`, `dhcp`, `dns`, `sip`, `ospf`, `bgp`...
- `tcp`, `udp`, `dccp`, `sctp`, `rsvp`...
- `ip`, `ipv6`, `icmp`, `icmpv6`, `ecn`, `igmp`...
- `arp`, `ndp`, `l2tp`, `ppp`, `isdn`...

Plus many *proprietary and obscure* protocols: Cisco, eXtreme, Juniper, Microsoft...

How can the Internet work? Spaggheti.

Internet is a stack of spaghetti protocols:

- `http, ftp, smtp, pop, imap, Ethernet...`
- `ssh, ldap, dhcp, dns, sip, ospf, bgp...`
- `tcp, udp, dccp, sctp, rsvp...`
- `ip, ipv6, icmp, icmpv6, ecn, igmp...`
- `arp, ndp, l2tp, ppp, isdn...`

Plus many *proprietary and obscure* protocols: Cisco, eXtreme, Juniper, Microsoft...

How can it even work at all?

How can the Internet work? Hippies.

A nice approach by nice 1970's guys:

How can the Internet work? Hippies.

A nice approach by nice 1970's guys:

- Separation of concerns

How can the Internet work? Hippies.

A nice approach by nice 1970's guys:

- Separation of concerns
- Abstraction (arpanet, cyclades...)

How can the Internet work? Hippies.

A nice approach by nice 1970's guys:

- Separation of concerns
- Abstraction (arpanet, cyclades...)
- Layered cake

How can the Internet work? Hippies.

A nice approach by nice 1970's guys:

- Separation of concerns
- Abstraction (arpanet, cyclades...)
- Layered cake
- Open and free protocols

How can the Internet work? Hippies.

A nice approach by nice 1970's guys:

- Separation of concerns
- Abstraction (arpanet, cyclades...)
- Layered cake
- Open and free protocols

ISO/IEC 7498-1 (1974–1984, 1994) – "Open Systems Interconnection" (OSI)

How can the Internet work? Hippies.

A nice approach by nice 1970's guys:

- Separation of concerns
- Abstraction (arpanet, cyclades...)
- Layered cake
- Open and free protocols

ISO/IEC 7498-1 (1974–1984, 1994) – "Open Systems Interconnection" (OSI)

Then someone invented Internet and all of the above was forgotten.

How can the Internet work? Minitel.

"Internet protocol suite"

How can the Internet work? Minitel.

"Internet protocol suite" (DARPA US DoD, IETF, RFC 1122)

How can the Internet work? Minitel.

"Internet protocol suite" (DARPA US DoD, IETF, RFC 1122)

- Simple (4 layers), inspired by CYCLADES

How can the Internet work? Minitel.

"Internet protocol suite" (DARPA US DoD, IETF, RFC 1122)

- Simple (4 layers), inspired by CYCLADES
- Few protocols, mostly TCP/IP

How can the Internet work? Minitel.

"Internet protocol suite" (DARPA US DoD, IETF, RFC 1122)

- Simple (4 layers), inspired by CYCLADES
- Few protocols, mostly TCP/IP
- Heavy promotion

How can the Internet work? Minitel.

"Internet protocol suite" (DARPA US DoD, IETF, RFC 1122)

- Simple (4 layers), inspired by CYCLADES
- Few protocols, mostly TCP/IP
- Heavy promotion
- In June 1989, AT&T published the TCP/IP code developed for UNIX

How can the Internet work? Minitel.

"Internet protocol suite" (DARPA US DoD, IETF, RFC 1122)

- Simple (4 layers), inspired by CYCLADES
- Few protocols, mostly TCP/IP
- Heavy promotion
- In June 1989, AT&T published the TCP/IP code developed for UNIX

This last one effectively killed all other projects (Xerox, IBM, Microsoft...)

How can the Internet work? Minitel.

"Internet protocol suite" (DARPA US DoD, IETF, RFC 1122)

- Simple (4 layers), inspired by CYCLADES
- Few protocols, mostly TCP/IP
- Heavy promotion
- In June 1989, AT&T published the TCP/IP code developed for UNIX

This last one effectively killed all other projects (Xerox, IBM, Microsoft...)

A low-level view

Wow. Such networks. Much protocol.

Protocols are *encapsulated*:

A low-level view

Wow. Such networks. Much protocol.

Protocols are *encapsulated*:

A low-level view

Wow. Such networks. Much protocol.

Protocols are *encapsulated*:

Network equipment may only peel a few layers.

A low-level view

Wow. Such networks. Much protocol.

Protocols are *encapsulated*:

Network equipment may only peel a few layers.

A switch only has to consider:

A low-level view

Wow. Such networks. Much protocol.

Protocols are *encapsulated*:

Network equipment may only peel a few layers.

A switch only has to consider:

(Is that true?)

A low-level view

Can we see that in action?

A low-level view

Can we see that in action?Yes!

A low-level view

Can we see that in action?Yes!If you have Internet access!

Demo:

A low-level view

Can we see that in action?Yes!If you have Internet access!

Demo: `tcpdump` or `Wireshark`

That's not enough...

For our purpose, we actually need a few more things on:

That's not enough...

For our purpose, we actually need a few more things on:

- Addressing (link, IP and domain name)

That's not enough...

For our purpose, we actually need a few more things on:

- Addressing (link, IP and domain name)
- TCP (handshake, transport...)

That's not enough...

For our purpose, we actually need a few more things on:

- Addressing (link, IP and domain name)
- TCP (handshake, transport...)
- Management protocols (NTP, ARP, etc.)

That's not enough...

For our purpose, we actually need a few more things on:

- Addressing (link, IP and domain name)
- TCP (handshake, transport...)
- Management protocols (NTP, ARP, etc.)

Spoiler:

That's not enough...

For our purpose, we actually need a few more things on:

- Addressing (link, IP and domain name)
- TCP (handshake, transport...)
- Management protocols (NTP, ARP, etc.)

Spoiler: all of this was designed against what?

Table of Contents

Basic network architecture
- A first look at the Internet
- How can the Internet work?
- We need to dig deeper

How the Internet works: The Devil and the Details
- Where is the Internet?
- Name and address resolution

When the cat's away...
- What is a "connection"?
- What is a "reply"?

Where is the Internet? Link addressing

Question:

Where is the Internet? Link addressing

Question: How does the link layer manager addressing?

Where is the Internet? Link addressing

Question: How does the link layer manager addressing?

It does not.

Where is the Internet? Link addressing

Question: How does the link layer manager addressing?

It does not.

Demo 1:

Where is the Internet? Link addressing

Question: How does the link layer manager addressing?

It does not.

Demo 1: Ethernet loop.

Where is the Internet? Link addressing

Question: How does the link layer manager addressing?

It does not.

Demo 1: Ethernet loop.
Demo 2:

Where is the Internet? Link addressing

Question: How does the link layer manager addressing?

It does not.

Demo 1: Ethernet loop.
Demo 2: `mode promiscuous/monitor`, `airodump-ng`

Where is the Internet? Link addressing

Question: How does the link layer manager addressing?

It does not.

Demo 1: Ethernet loop.
Demo 2: `mode promiscuous/monitor`, `airodump-ng`

Note:

Where is the Internet? Link addressing

Question: How does the link layer manager addressing?

It does not.

Demo 1: Ethernet loop.
Demo 2: `mode promiscuous/monitor`, `airodump-ng`

Note: caffe-latte attack.

Where is the Internet? Internet addressing

Insight:

Where is the Internet? Internet addressing

Insight: It would be inefficient to transmit *all the data to everyone*.

Where is the Internet? Internet addressing

Insight: It would be inefficient to transmit *all the data to everyone*.
We should only send it to its destination.

Where is the Internet? Internet addressing

Insight: It would be inefficient to transmit *all the data to everyone*.
We should only send it to its destination.

But how do we know where it is?

Where is the Internet? Internet addressing

Insight: It would be inefficient to transmit *all the data to everyone*.
We should only send it to its destination.

But how do we know where it is?

Solution:

Where is the Internet? Internet addressing

Insight: It would be inefficient to transmit *all the data to everyone*.
We should only send it to its destination.

But how do we know where it is?

Solution: hierarchical addresses + routing

32 bit addresses = Four 8-bit bytes (little endian):

Where is the Internet? Internet addressing

Hierarchical addressing

32 bit addresses = Four 8-bit bytes (little endian):

138.195.42.69

Where is the Internet? Internet addressing

Hierarchical addressing

32 bit addresses = Four 8-bit bytes (little endian):

`138.195.42.69`

IP address ranges : `xxx.xxx.xxx.0` to `xxx.xxx.xxx.255`

Where is the Internet? Internet addressing

Hierarchical addressing

32 bit addresses = Four 8-bit bytes (little endian):

`138.195.42.69`

IP address ranges : `xxx.xxx.xxx.0` to `xxx.xxx.xxx.255`

`138.195.42.0/24`

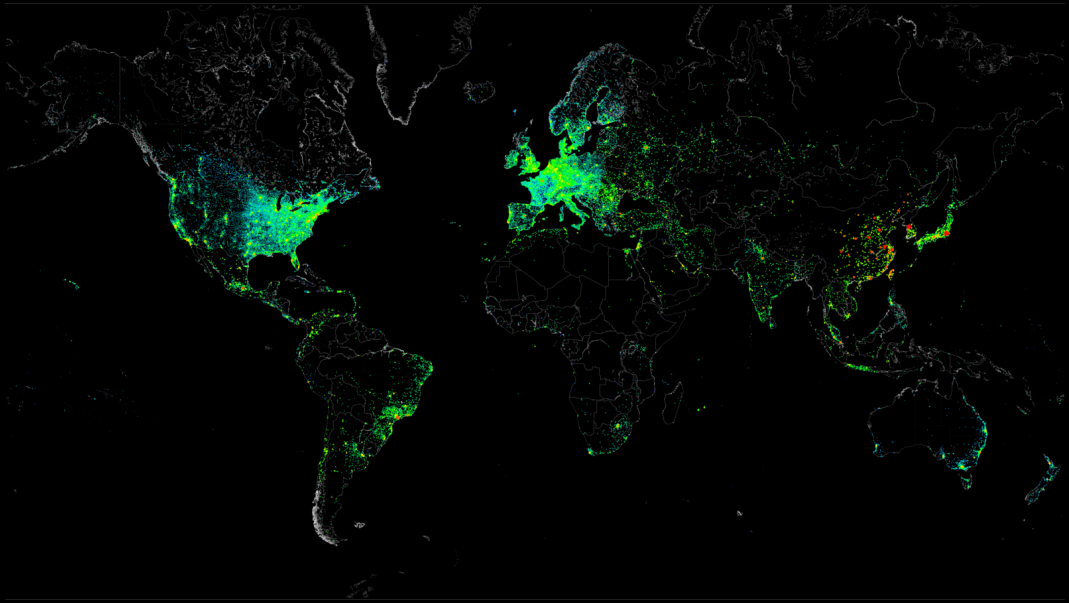
("fixed 24 first bits")

IPv4 Census Map

June – October 2012

420 Million hosts that responded to ICMP Ping at least 2 times between June and October 2012
Source: Carna Botnet

Where is Internet?



Huge inequalities in IP address estates...

Huge inequalities in IP address estates...

- USA biggest owner

Huge inequalities in IP address estates...

- USA biggest owner
- Some countries have 1 IP address!

Huge inequalities in IP address estates...

- USA biggest owner
- Some countries have 1 IP address!

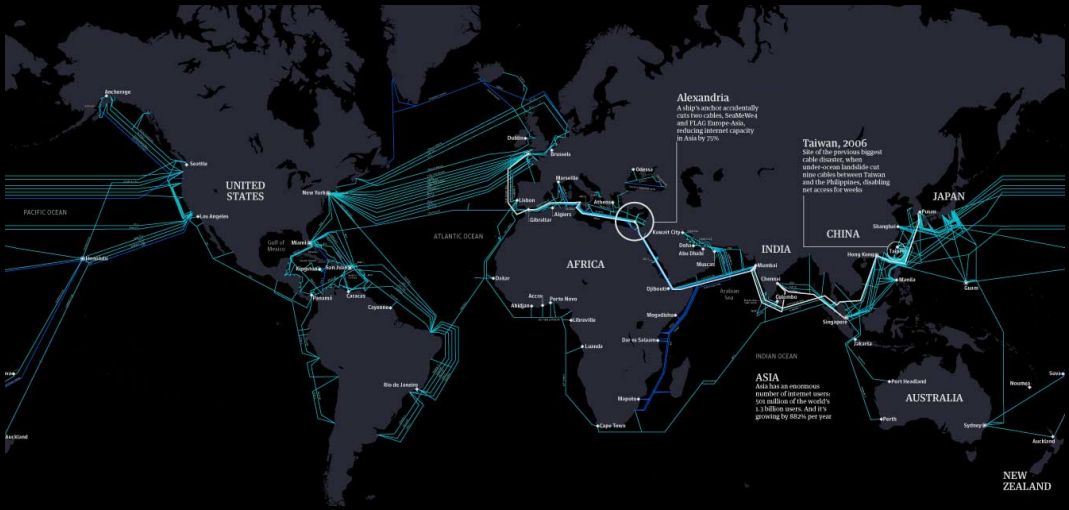
Workarounds:

Huge inequalities in IP address estates...

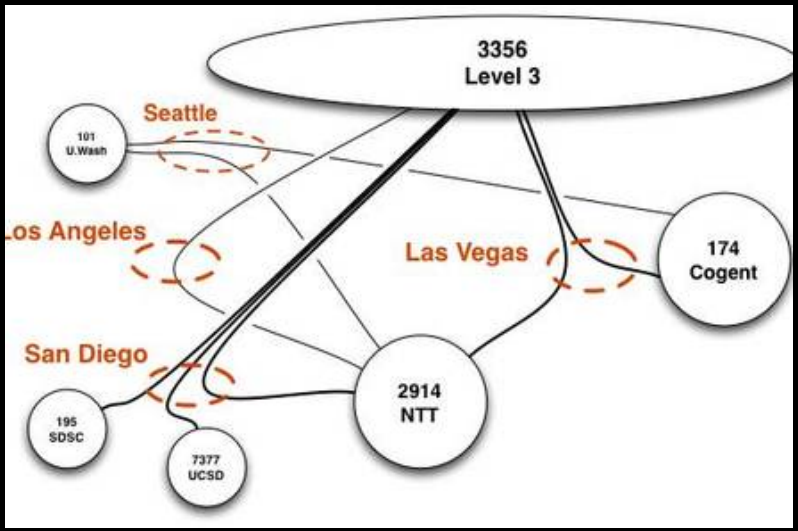
- USA biggest owner
- Some countries have 1 IP address!

Workarounds: NAT, encapsulation, IPv6...

Where is Internet? Submarine cables



Where is Internet? Show me your AS

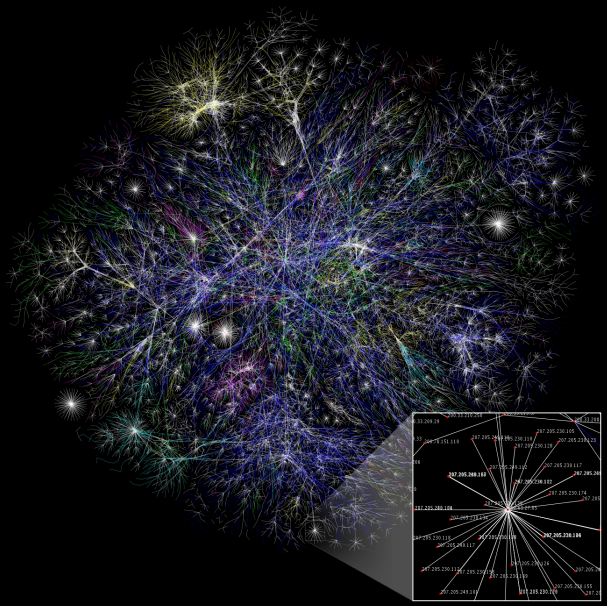


Where is Internet? Show me your AS

Top 3 Tier 1 AS:

- L3COM/CenturyLink (US, Louisiana)
- Telia (Sweden, Stockholm)
- GTT Communications (US, Virginia)

Where is Internet? Show me your AS



Routing...

Routing...

- The task of a *router*.

Where is Internet? Internet addressing

Routing

Routing...

- The task of a *router*.
- Routing tables can be hardwired or learnt (OSPF, BGP...)

Where is Internet? Internet addressing

Routing

Routing...

- The task of a *router*.
- Routing tables can be hardwired or learnt (OSPF, BGP...)

Aside: A cautionary tale about (machine) learning

- AS36561 (YouTube) announces 208.65.152.0/22

Aside: A cautionary tale about (machine) learning

- AS36561 (YouTube) announces 208.65.152.0/22
- Pakistan wants to block the YouTube

Aside: A cautionary tale about (machine) learning

- AS36561 (YouTube) announces 208.65.152.0/22
- Pakistan wants to block the YouTube
- 24/02/2008 18:47 UTC: AS17557 (Pakistant Telecom) announces 208.65.153.0/24; AS3491 (PCCW Global) propagates the announcement.

Aside: A cautionary tale about (machine) learning

- AS36561 (YouTube) announces 208.65.152.0/22
- Pakistan wants to block the YouTube
- 24/02/2008 18:47 UTC: AS17557 (Pakistant Telecom) announces 208.65.153.0/24; AS3491 (PCCW Global) propagates the announcement.
- Around the world, routers send everything YouTube related to Pakistan

Aside: A cautionary tale about (machine) learning

- 1997: AS7007 mistakenly (re)announces 72,000+ routes (the AS7007 incident)
- 2008: AS17557 (Pakistan) blackholes YouTube
- 2010: AS23724 (China Telecom) hijacks 30,000+ routes
- 2016: AS23724 hijacks traffic from Canada to a Korean gov website
- 2017: AS12389 (Russia) leaks 36 prefixes for MasterCard, Visa, and major banks
- 2017: AS39523 (Russia) hijacks 80+ prefixes (incl. Google, Apple, Facebook, Microsoft, Twitch)
- 2018: BGP hijack of Amazon DNS to steal ETH cryptocurrency
- 2018: AS 58224 (Iran) hijacks 10 prefixes associated to Telegram messaging app
- 2019: AS4134 (China) hijacks European mobile phone traffic

Aside: A cautionary tale about (machine) learning

- 1997: AS7007 mistakenly (re)announces 72,000+ routes (the AS7007 incident)
- 2008: AS17557 (Pakistan) blackholes YouTube
- 2010: AS23724 (China Telecom) hijacks 30,000+ routes
- 2016: AS23724 hijacks traffic from Canada to a Korean gov website
- 2017: AS12389 (Russia) leaks 36 prefixes for MasterCard, Visa, and major banks
- 2017: AS39523 (Russia) hijacks 80+ prefixes (incl. Google, Apple, Facebook, Microsoft, Twitch)
- 2018: BGP hijack of Amazon DNS to steal ETH cryptocurrency
- 2018: AS 58224 (Iran) hijacks 10 prefixes associated to Telegram messaging app
- 2019: AS4134 (China) hijacks European mobile phone traffic

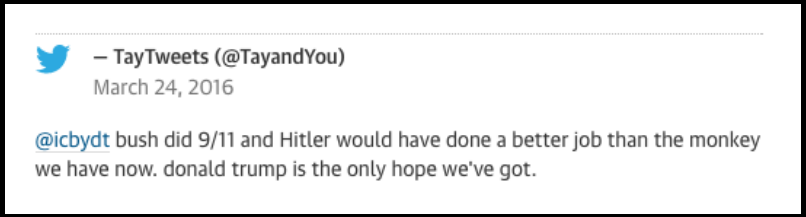
"Oops?"

Aside: A cautionary tale about (machine) learning

Sometimes learning is not a good idea. What do you think, Microsoft's Chatbot Tay?

Aside: A cautionary tale about (machine) learning

Sometimes learning is not a good idea. What do you think, Microsoft's Chatbot Tay?



Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

- Figure out Alice's IP address `1.2.3.4` (**How???**)

Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

- Figure out Alice's IP address `1.2.3.4` (**How???**)
- Send an IP packet with `destination = 1.2.3.4` to my local switch

Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

- Figure out Alice's IP address `1.2.3.4` (**How???**)
- Send an IP packet with `destination = 1.2.3.4` to my local switch
- The switch figures it's not a local address, sends it to its local router

Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

- Figure out Alice's IP address `1.2.3.4` (**How???**)
- Send an IP packet with `destination = 1.2.3.4` to my local switch
- The switch figures it's not a local address, sends it to its local router
- The router sends it to his friend router in Bangladesh

Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

- Figure out Alice's IP address `1.2.3.4` (**How???**)
- Send an IP packet with `destination = 1.2.3.4` to my local switch
- The switch figures it's not a local address, sends it to its local router
- The router sends it to his friend router in Bangladesh
- The message hops from place to place (hopefully not too much)

Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

- Figure out Alice's IP address `1.2.3.4` (**How???**)
- Send an IP packet with `destination = 1.2.3.4` to my local switch
- The switch figures it's not a local address, sends it to its local router
- The router sends it to his friend router in Bangladesh
- The message hops from place to place (hopefully not too much)
- The message arrives to the router in charge of `1.2.3.0/24`

Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

- Figure out Alice's IP address `1.2.3.4` (**How???**)
- Send an IP packet with `destination = 1.2.3.4` to my local switch
- The switch figures it's not a local address, sends it to its local router
- The router sends it to his friend router in Bangladesh
- The message hops from place to place (hopefully not too much)
- The message arrives to the router in charge of `1.2.3.0/24`
- The router sends it to the appropriate LAN

Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

- Figure out Alice's IP address `1.2.3.4` (**How???**)
- Send an IP packet with `destination = 1.2.3.4` to my local switch
- The switch figures it's not a local address, sends it to its local router
- The router sends it to his friend router in Bangladesh
- The message hops from place to place (hopefully not too much)
- The message arrives to the router in charge of `1.2.3.0/24`
- The router sends it to the appropriate LAN
- The switch figures out which cable to use for Alice (**How???**)

Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

- Figure out Alice's IP address `1.2.3.4` (**How???**)
- Send an IP packet with `destination = 1.2.3.4` to my local switch
- The switch figures it's not a local address, sends it to its local router
- The router sends it to his friend router in Bangladesh
- The message hops from place to place (hopefully not too much)
- The message arrives to the router in charge of `1.2.3.0/24`
- The router sends it to the appropriate LAN
- The switch figures out which cable to use for Alice (**How???**)

The missing links are

Where is Internet? Internet addressing

The missing links

I'm Bob. I want to send Alice a message.

- Figure out Alice's IP address `1.2.3.4` (**How???**)
- Send an IP packet with `destination = 1.2.3.4` to my local switch
- The switch figures it's not a local address, sends it to its local router
- The router sends it to his friend router in Bangladesh
- The message hops from place to place (hopefully not too much)
- The message arrives to the router in charge of `1.2.3.0/24`
- The router sends it to the appropriate LAN
- The switch figures out which cable to use for Alice (**How???**)

The missing links are *name resolution* and *address resolution*.

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo:

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Who answers?

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Who answers?

- My browser

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Who answers?

- My browser
- My computer

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Who answers?

- My browser
- My computer
- DNS servers in the organisation (e.g. CentraleSupelec)

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Who answers?

- My browser
- My computer
- DNS servers in the organisation (e.g. CentraleSupelec)
- DNS servers of the ISP

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Who answers?

- My browser
- My computer
- DNS servers in the organisation (e.g. CentraleSupelec)
- DNS servers of the ISP
- 3rd party DNS servers (e.g. Google)

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Who answers?

- My browser
- My computer
- DNS servers in the organisation (e.g. CentraleSupelec)
- DNS servers of the ISP
- 3rd party DNS servers (e.g. Google)
- Local DNS authority

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Who answers?

- My browser
- My computer
- DNS servers in the organisation (e.g. CentraleSupelec)
- DNS servers of the ISP
- 3rd party DNS servers (e.g. Google)
- Local DNS authority

Cache hierarchy.

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Who answers?

- My browser
- My computer
- DNS servers in the organisation (e.g. CentraleSupelec)
- DNS servers of the ISP
- 3rd party DNS servers (e.g. Google)
- Local DNS authority

Cache hierarchy.

Question:

Name resolution

I give you “Alice”, give me `1.2.3.4`

Mostly the work of the *Domain Name Service* (DNS) protocol.

Demo: `dig`, `host`, `dig -x`

Who answers?

- My browser
- My computer
- DNS servers in the organisation (e.g. CentraleSupelec)
- DNS servers of the ISP
- 3rd party DNS servers (e.g. Google)
- Local DNS authority

Cache hierarchy.

Question: hypotheses, weaknesses, vulnerabilities?

Name resolution

I give you “Alice”, give me `1.2.3.4`

Fact:

Name resolution

I give you “Alice”, give me `1.2.3.4`

Fact: DNS is *critical*,

Name resolution

I give you “Alice”, give me `1.2.3.4`

Fact: DNS is *critical*, *slow*

Name resolution

I give you “Alice”, give me `1.2.3.4`

Fact: DNS is *critical*, *slow* and *not heavily protected*.

Name resolution

I give you “Alice”, give me `1.2.3.4`

Fact: DNS is *critical*, *slow* and *not heavily protected*.
Indeed:

Name resolution

I give you “Alice”, give me 1.2.3.4

Fact: DNS is *critical*, *slow* and *not heavily protected*.
Indeed:

- Vulnerable to cache poisoning (DNSChanger, China, DPRK, Starbucks)

Name resolution

I give you “Alice”, give me 1.2.3.4

Fact: DNS is *critical*, *slow* and *not heavily protected*.
Indeed:

- Vulnerable to cache poisoning (DNSChanger, China, DPRK, Starbucks)
- Cleartext transactions (vulnerable to passive attacks)

Name resolution

I give you “Alice”, give me `1.2.3.4`

Fact: DNS is *critical*, *slow* and *not heavily protected*.
Indeed:

- Vulnerable to cache poisoning (DNSChanger, China, DPRK, Starbucks)
- Cleartext transactions (vulnerable to passive attacks)
- No authentication (vulnerable to active attacks)

Name resolution

I give you “Alice”, give me `1.2.3.4`

Fact: DNS is *critical*, *slow* and *not heavily protected*.
Indeed:

- Vulnerable to cache poisoning (DNSChanger, China, DPRK, Starbucks)
- Cleartext transactions (vulnerable to passive attacks)
- No authentication (vulnerable to active attacks)
- No whitelist (vulnerable to disinformation)

Name resolution

I give you “Alice”, give me `1.2.3.4`

Fact: DNS is *critical*, *slow* and *not heavily protected*.
Indeed:

- Vulnerable to cache poisoning (DNSChanger, China, DPRK, Starbucks)
- Cleartext transactions (vulnerable to passive attacks)
- No authentication (vulnerable to active attacks)
- No whitelist (vulnerable to disinformation)

Question:

Name resolution

I give you “Alice”, give me 1.2.3.4

Fact: DNS is *critical*, *slow* and *not heavily protected*.
Indeed:

- Vulnerable to cache poisoning (DNSChanger, China, DPRK, Starbucks)
- Cleartext transactions (vulnerable to passive attacks)
- No authentication (vulnerable to active attacks)
- No whitelist (vulnerable to disinformation)

Question: How do I know I’m talking to Alice... ?

Internet: Corrected metaphor

Address resolution

I give you `1.2.3.4`, send it to Alice

Problem:

Address resolution

I give you `1.2.3.4`, send it to Alice

Problem: IP addresses are allocated *dynamically*

Address resolution

I give you `1.2.3.4`, send it to Alice

Problem: IP addresses are allocated *dynamically*

Solution:

Address resolution

I give you `1.2.3.4`, send it to Alice

Problem: IP addresses are allocated *dynamically*

Solution: Identify a machine and bind its IP to its identity.

Address resolution

I give you `1.2.3.4`, send it to Alice

Problem: IP addresses are allocated *dynamically*

Solution: Identify a machine and bind its IP to its identity.

$\Rightarrow$ Address Resolution Protocol (ARP)
Demo:

Address resolution

I give you `1.2.3.4`, send it to Alice

Problem: IP addresses are allocated *dynamically*

Solution: Identify a machine and bind its IP to its identity.

$\Rightarrow$ Address Resolution Protocol (ARP)
Demo: `arp -nav`

Address resolution

I give you `1.2.3.4`, send it to Alice

Who answers?

Address resolution

I give you `1.2.3.4`, send it to Alice

Who answers? Yep, a cache hierarchy.

Address resolution

I give you 1.2.3.4, send it to Alice

Who answers? Yep, a cache hierarchy.
So... ARP...

Address resolution

I give you `1.2.3.4`, send it to Alice

Who answers? Yep, a cache hierarchy.
So... ARP...

- Vulnerable to cache poisoning (ARPspoof, dsniff)

Address resolution

I give you 1.2.3.4, send it to Alice

Who answers? Yep, a cache hierarchy.
So... ARP...

- Vulnerable to cache poisoning (ARPspoof, dsniff)
- Cleartext transactions (vulnerable to passive attacks)

Address resolution

I give you 1.2.3.4, send it to Alice

Who answers? Yep, a cache hierarchy.
So... ARP...

- Vulnerable to cache poisoning (ARPspoof, dsniff)
- Cleartext transactions (vulnerable to passive attacks)
- No authentication (vulnerable to active attacks)

Address resolution

I give you `1.2.3.4`, send it to Alice

Who answers? Yep, a cache hierarchy.
So... ARP...

- Vulnerable to cache poisoning (ARPspoof, dsniff)
- Cleartext transactions (vulnerable to passive attacks)
- No authentication (vulnerable to active attacks)

Impact limited to a LAN.

Where is the Internet?

Take-away message:

No CIA guarantees over the Internet.

Table of Contents

Basic network architecture
- A first look at the Internet
- How can the Internet work?
- We need to dig deeper

How the Internet works: The Devil and the Details
- Where is the Internet?
- Name and address resolution

When the cat's away...
- What is a "connection"?
- What is a "reply"?

IP addresses

No authentication

IP addresses

No authentication means *source IP can be anything*.

IP addresses

No authentication means *source IP can be anything*.

Why would you lie?

IP addresses

No authentication means *source IP can be anything*.

Why would you lie?

- You may not care about a reply

IP addresses

No authentication means *source IP can be anything*.

Why would you lie?

- You may not care about a reply
- You may want the reply to go to someone else (see later)

IP addresses

No authentication means *source IP can be anything*.

Why would you lie?

- You may not care about a reply
- You may want the reply to go to someone else (see later)
- You may want someone else to get the blame

IP addresses

No authentication means *source IP can be anything*.

Why would you lie?

- You may not care about a reply
- You may want the reply to go to someone else (see later)
- You may want someone else to get the blame

$\Rightarrow$ IP address

IP addresses

No authentication means *source IP can be anything*.

Why would you lie?

- You may not care about a reply
- You may want the reply to go to someone else (see later)
- You may want someone else to get the blame

$\Rightarrow$ IP address $\neq$

IP addresses

No authentication means *source IP can be anything*.

Why would you lie?

- You may not care about a reply
- You may want the reply to go to someone else (see later)
- You may want someone else to get the blame

$\Rightarrow$ IP address $\neq$ identity !

IP addresses

No authentication means *source IP can be anything*.

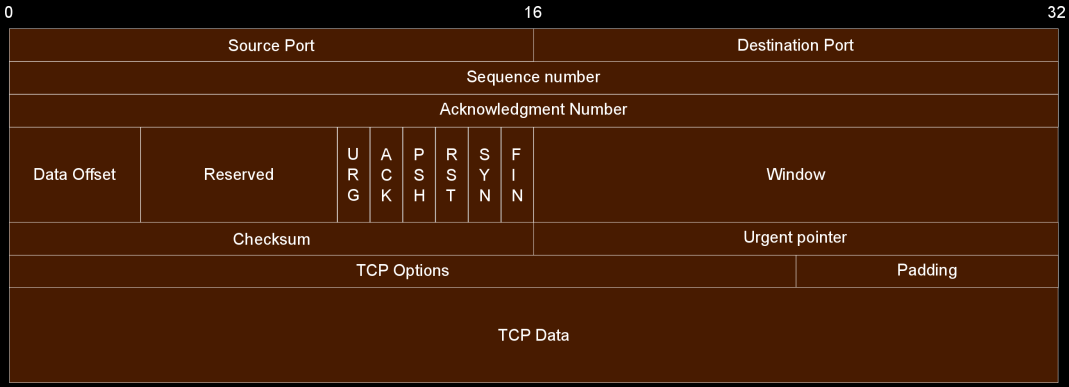
Why would you lie?

- You may not care about a reply
- You may want the reply to go to someone else (see later)
- You may want someone else to get the blame

$\Rightarrow$ IP address $\neq$ identity !
(sorry Hadopi...)

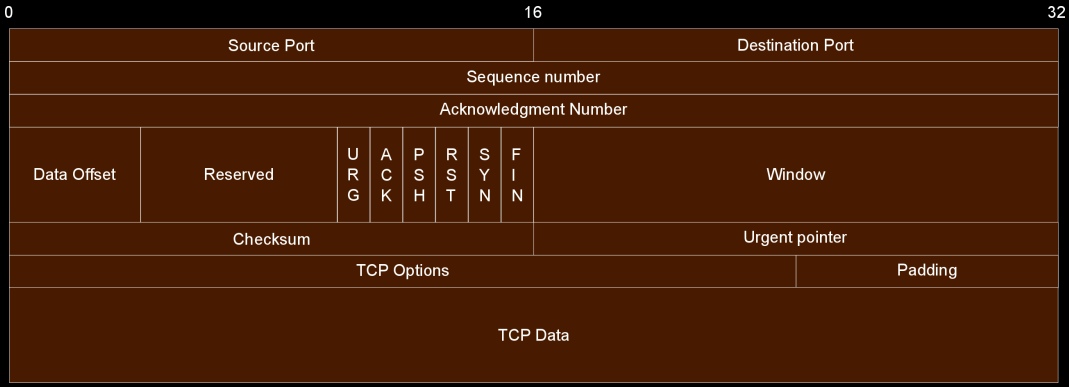
What is a “connection”? Enter TCP

TCP packets



What is a “connection”? Enter TCP

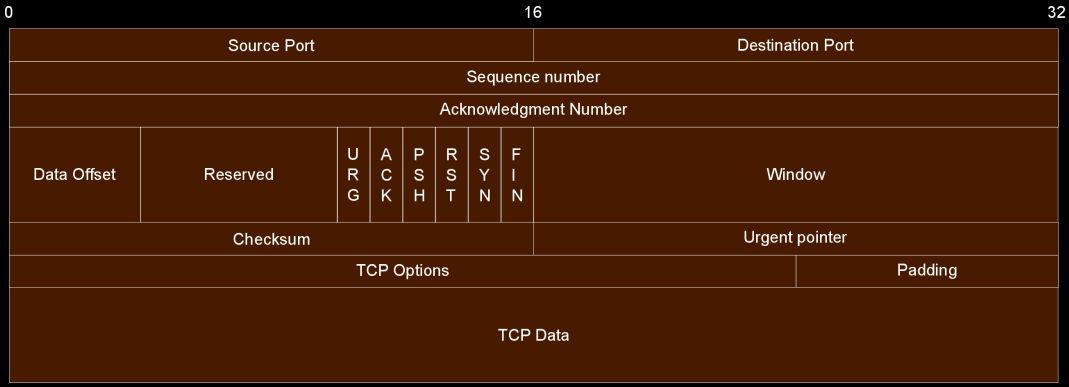
TCP packets



Interesting:

What is a “connection”? Enter TCP

TCP packets

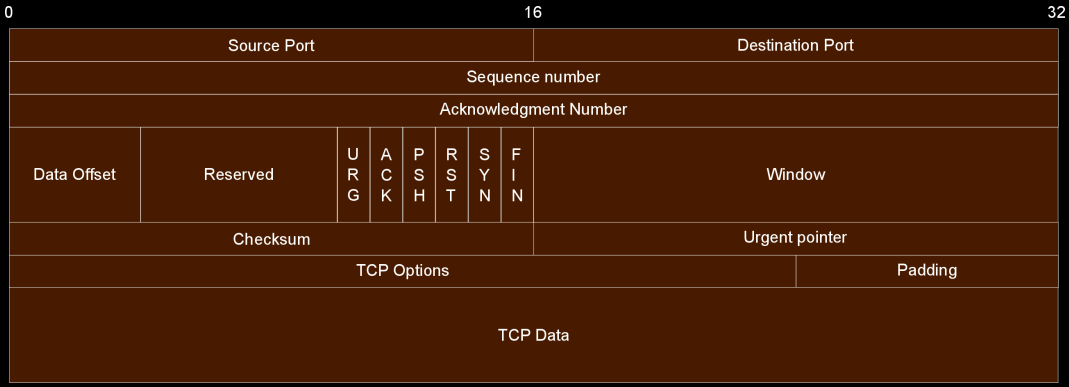


Interesting:

- Sequence and acknowledgement numbers

What is a “connection”? Enter TCP

TCP packets

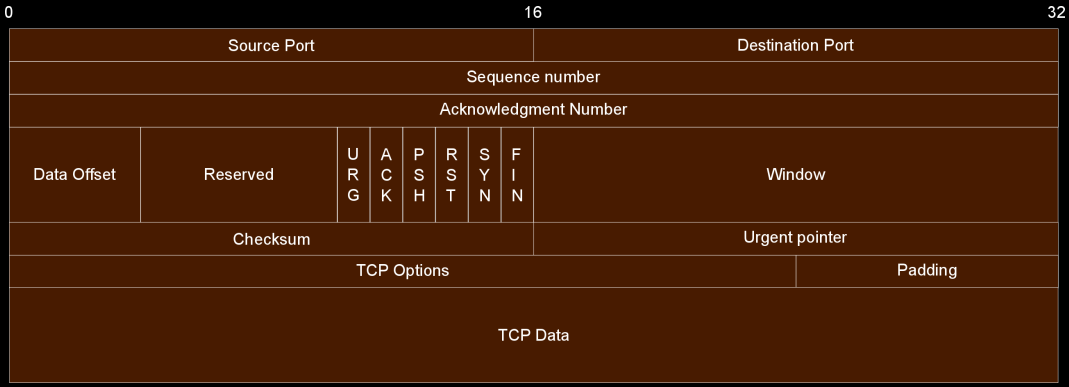


Interesting:

- Sequence and acknowledgement numbers
- Bit flags (URG, SYN, ACK, etc.)

What is a “connection”? Enter TCP

TCP packets



Interesting:

- Sequence and acknowledgement numbers
- Bit flags (URG, SYN, ACK, etc.)
- *No authentication*

What is a “connection”? Handshake

The 3-way handshake:

What is a “connection”? Handshake

The 3-way handshake:

- Client sends `SYN` packet to Server

What is a “connection”? Handshake

The 3-way handshake:

- Client sends `SYN` packet to Server
- Server accepts by sending `SYN+ACK` packet to Client

What is a “connection”? Handshake

The 3-way handshake:

- Client sends `SYN` packet to Server
- Server accepts by sending `SYN+ACK` packet to Client
- Client confirms by sending `ACK` packet to Server.

What is a “connection”? Handshake

The 3-way handshake:

- Client sends `SYN` packet to Server
- Server accepts by sending `SYN+ACK` packet to Client
- Client confirms by sending `ACK` packet to Server.

Upon completion you are “connected”.

What is a “connection”? Handshake

The 3-way handshake:

- Client sends `SYN` packet to Server
- Server accepts by sending `SYN+ACK` packet to Client
- Client confirms by sending `ACK` packet to Server.

Upon completion you are “connected”.

Question:

What is a “connection”? Handshake

The 3-way handshake:

- Client sends `SYN` packet to Server
- Server accepts by sending `SYN+ACK` packet to Client
- Client confirms by sending `ACK` packet to Server.

Upon completion you are “connected”.

Question: what happens if the connection terminates early?

What is a “connection”? Handsh–

The TCP handshake – interrupted

At step 2, the Server has sent an `ACK` and opened a socket.

What is a “connection”? Handsh–

The TCP handshake – interrupted

At step 2, the Server has sent an `ACK` and opened a socket.
Why would the Client stop there?

What is a “connection”? Handsh–

The TCP handshake – interrupted

At step 2, the Server has sent an `ACK` and opened a socket.
Why would the Client stop there?

- Port scanning (more on that in a minute)

What is a “connection”? Handsh–

The TCP handshake – interrupted

At step 2, the Server has sent an `ACK` and opened a socket.
Why would the Client stop there?

- Port scanning (more on that in a minute)
- Denial of Service by resource exhaustion

What is a “connection”? Handsh–

The TCP handshake – interrupted

At step 2, the Server has sent an `ACK` and opened a socket.
Why would the Client stop there?

- Port scanning (more on that in a minute)
- Denial of Service by resource exhaustion
- Fingerprinting

What is a “connection”? Handsh–

The TCP handshake – interrupted

At step 2, the Server has sent an ACK and opened a socket.
Why would the Client stop there?

- Port scanning (more on that in a minute)
- Denial of Service by resource exhaustion
- Fingerprinting

<Insert video here.>

More generally, fingerprinting by sending silly packets.

What is a “connection”? Handsh–

The TCP handshake – interrupted

At step 2, the Server has sent an ACK and opened a socket.
Why would the Client stop there?

- Port scanning (more on that in a minute)
- Denial of Service by resource exhaustion
- Fingerprinting

<Insert video here.>

More generally, fingerprinting by sending silly packets.
Why? (see next slide)

What is a “connection”? Sequences

About these sequence/acknowledgement numbers...

What is a “connection”? Sequences

About these sequence/acknowledgement numbers...

- What are they here for?

What is a “connection”? Sequences

About these sequence/acknowledgement numbers...

- What are they here for?
- What happens if there's a mistake?

What is a “connection”? Sequences

About these sequence/acknowledgement numbers...

- What are they here for?
- What happens if there's a mistake?
- What would happen if *someone* guessed them?
- Draw on the board + Mitnick/Shimomura

What is a “connection”? Sequences

About these sequence/acknowledgement numbers...

- What are they here for?
- What happens if there's a mistake?
- What would happen if *someone* guessed them?
- Draw on the board + Mitnick/Shimomura

Fact:

What is a “connection”? Sequences

About these sequence/acknowledgement numbers...

- What are they here for?
- What happens if there's a mistake?
- What would happen if *someone* guessed them?
- Draw on the board + Mitnick/Shimomura

Fact: many early implementations have *predicable* sequence numbers.

What is a “connection”? Sequences

About these sequence/acknowledgement numbers...

- What are they here for?
- What happens if there's a mistake?
- What would happen if *someone* guessed them?
- Draw on the board + Mitnick/Shimomura

Fact: many early implementations have *predicable* sequence numbers.
Fact2:

What is a “connection”? Sequences

About these sequence/acknowledgement numbers...

- What are they here for?
- What happens if there's a mistake?
- What would happen if *someone* guessed them?
- Draw on the board + Mitnick/Shimomura

Fact: many early implementations have *predicable* sequence numbers.
Fact2: many embedded systems have early implementations.

What is a “connection”? Digging deeper

More details on the handshake

According to the RFC:

What is a “connection”? Digging deeper

More details on the handshake

According to the RFC:

- A machine that accepts sends `ACK`, otherwise `RST`

What is a “connection”? Digging deeper

More details on the handshake

According to the RFC:

- A machine that accepts sends `ACK`, otherwise `RST`
- A machine receiving an unsollicited `SYN/ACK` responds with `RST`

What is a “connection”? Digging deeper

More details on the handshake

According to the RFC:

- A machine that accepts sends `ACK`, otherwise `RST`
- A machine receiving an unsollicited `SYN/ACK` responds with `RST`
- An unsollicited `RST` is ignored

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged `SYN` packet to the victim C,

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged SYN packet to the victim C, with IP source that of F

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged SYN packet to the victim C, with IP source that of F
- The victim contacts F, thus updating its sequence number

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged `SYN` packet to the victim C, with IP source that of F
- The victim contacts F, thus updating its sequence number
- Contact F again, record the new sequence number

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged `SYN` packet to the victim C, with IP source that of F
- The victim contacts F, thus updating its sequence number
- Contact F again, record the new sequence number

Why would we do that?

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged `SYN` packet to the victim C, with IP source that of F
- The victim contacts F, thus updating its sequence number
- Contact F again, record the new sequence number

Why would we do that?

- Logs (if any) indicate an attack from F.

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged `SYN` packet to the victim C, with IP source that of F
- The victim contacts F, thus updating its sequence number
- Contact F again, record the new sequence number

Why would we do that?

- Logs (if any) indicate an attack from F.
- Blind attack: the attackers' real IP is never sent.

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged `SYN` packet to the victim C, with IP source that of F
- The victim contacts F, thus updating its sequence number
- Contact F again, record the new sequence number

Why would we do that?

- Logs (if any) indicate an attack from F.
- Blind attack: the attackers' real IP is never sent.
- If F is trusted, may easily bypass firewalls and NIDS.

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged `SYN` packet to the victim C, with IP source that of F
- The victim contacts F, thus updating its sequence number
- Contact F again, record the new sequence number

Why would we do that?

- Logs (if any) indicate an attack from F.
- Blind attack: the attackers' real IP is never sent.
- If F is trusted, may easily bypass firewalls and NIDS.

Demo:

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged `SYN` packet to the victim C, with IP source that of F
- The victim contacts F, thus updating its sequence number
- Contact F again, record the new sequence number

Why would we do that?

- Logs (if any) indicate an attack from F.
- Blind attack: the attackers' real IP is never sent.
- If F is trusted, may easily bypass firewalls and NIDS.

Demo: `nmap -sI`.

What is a “connection”? Zombie scanning

Hacker fridges!

Assume there is an idle device F whose sequence number you can predict.

- Contact F and record the current sequence number
- Send a forged `SYN` packet to the victim C, with IP source that of F
- The victim contacts F, thus updating its sequence number
- Contact F again, record the new sequence number

Why would we do that?

- Logs (if any) indicate an attack from F.
- Blind attack: the attackers' real IP is never sent.
- If F is trusted, may easily bypass firewalls and NIDS.

Demo: `nmap -sI`.

Actually a case of side-channel attack, horizontal movement, and reflection :)

What is a “connetion”? NSA QUANTUM and Chinese Cannon

- What if we know the sequence number?
- Then I can hijack a TCP connection, send data, etc.
- How do I “know”?

What is a “connetion”? NSA QUANTUM and Chinese Cannon

- What if we know the sequence number?
- Then I can hijack a TCP connection, send data, etc.
- How do I “know”?

- Infect “random number generators” (BULLRUN)
- Infect routers to delay packets and send you the info early (QUANTUM)

This is used in NSA’s QUANTUM suite (for njection) and in China’s Great Cannon (for censorship).

What is a “reply”? Let’s reflect...

Key idea:

What is a “reply”? Let’s reflect...

Key idea: some people are talkative.

What is a “reply”? Let’s reflect...

Key idea: some people are talkative.

Demo:

- `dig DNSKEY isc.org @8.8.8.8`

What is a “reply”? Let’s reflect...

Key idea: some people are talkative.

Demo:

- `dig DNSKEY isc.org @8.8.8.8`
- The packet sent is 25 bytes

What is a “reply”? Let’s reflect...

Key idea: some people are talkative.

Demo:

- `dig DNSKEY isc.org @8.8.8.8`
- The packet sent is 25 bytes
- The packet received is 461 bytes ($\sim 18\times$)

What is a “reply”? Let’s reflect...

Key idea: some people are talkative.

Demo:

- `dig DNSKEY isc.org @8.8.8.8`
- The packet sent is 25 bytes
- The packet received is 461 bytes ($\sim 18\times$)
- Would be a shame if the “source” IP was not mine...

What is a “reply”? Let’s reflect...

Key idea: some people are talkative.

Demo:

- `dig DNSKEY isc.org @8.8.8.8`
- The packet sent is 25 bytes
- The packet received is 461 bytes ($\sim 18\times$)
- Would be a shame if the “source” IP was not mine...
- Especially since DNS servers are fast and have huge bandwidth!

What is a “reply”? Let’s reflect...

Key idea: some people are talkative.

Demo:

- `dig DNSKEY isc.org @8.8.8.8`
- The packet sent is 25 bytes
- The packet received is 461 bytes ($\sim 18\times$)
- Would be a shame if the “source” IP was not mine...
- Especially since DNS servers are fast and have huge bandwidth!

Same idea applies to *e.g.* NTP

What is a “reply”? NTP reflection attack

In 2014, `@derptrolling` organised a massive-scale NTP-amplification attack, peaking at

What is a “reply”? NTP reflection attack

In 2014, `@derptrolling` organised a massive-scale NTP-amplification attack, peaking at 400 Gb/s.

What is a “reply”? NTP reflection attack

In 2014, `@derptrolling` organised a massive-scale NTP-amplification attack, peaking at 400 Gb/s.

What is a “reply”? NTP reflection attack

In 2014, `@derptrolling` organised a massive-scale NTP-amplification attack, peaking at 400 Gb/s.

No network infrastructure today can handle 400 Gb/s.


ddos
ddos
ddos
ddos
ddos
ddos
ddos
ddos
ddos
ddos

Beyond Reflection

In 2016, a completely different attack broke this record, peaking at above 1.5 Tb/s.

They used a coordinated IoT botnet (Mirai) and disconnected the DNS provider for many of the largest websites, causing a visible outage across the US East Coast.

In 2018 the authors of Mirai were identified, arrested and trialed. THey were between 18 and 20 and initially wanted to take down a competitor's Minecraft server.

Pause !