University of BRISTOL

Systems Security

COMSM1500

University of BRISTOL

Before we get started…

Questions about the coursework?

(non-technical)

Citation and Latex

- I strongly suggest to use Latex
- How to:
  - – http://www-h.eng.cam.ac.uk/help/tpl/textprocessing/bibliographies.html
- Citations do not count in page count (so do cite properly)
- If you are not sure how to cite, please, do get in touch

University of BRISTOL

Network Security

bristol.ac.uk

Plan

- OSI Model
- TCP/IP Model
- Type of attacks
  - Traffic Analysis
  - Message Disclosure
  - Masquerade
  - Message Modification
  - Replay
  - Topology Disclosure
  - Unauthorized Access
  - Denial of Service
- TCP Syn related attacks
- DNS poisoning
- Slow Loris attack

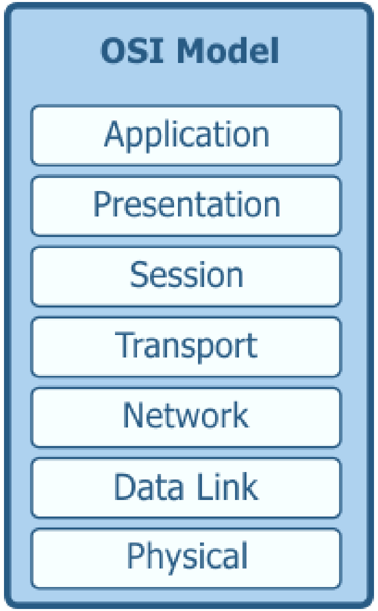
OSI Model

Layer	Description
Application Layer	High-level APIs. e.g. resource sharing, remote file access etc…
Presentation Layer	Translates data between the application and the network service. e.g. compression, encryption/decryption
Session Layer	Manages transmissions between two nodes across multiple messages.
Transport Layer	Supports and organises data transfer between nodes. e.g. segmentation, acknowledgment, multiplexing etc…
Network Layer	Handles addressing, routing and traffic control.
Data Link layer	Handles reliable data transmissions between two nodes connected by a physical layer.
Physical Layer	Transmission and reception of raw bits over a physical medium.

OSI Model

- This is just a model
- It does not quite fit reality
- … but it is a good mental model

OSI Model vs TCP/IP Model



OSI Model

Application

Presentation

Session

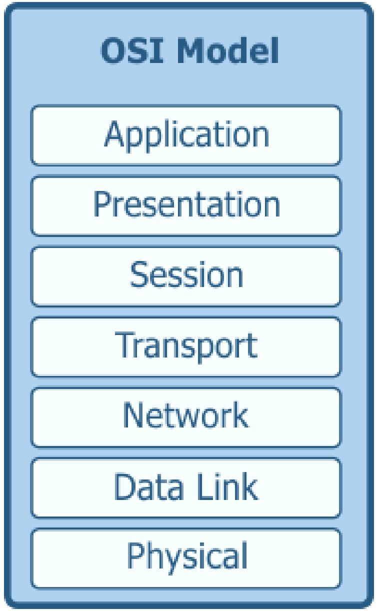
Transport

Network

Data Link

Physical

OSI Model vs TCP/IP Model



OSI Model

Application

Presentation

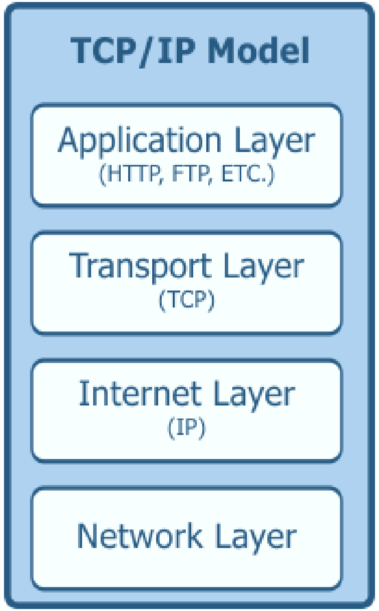
Session

Transport

Network

Data Link

Physical



TCP/IP Model

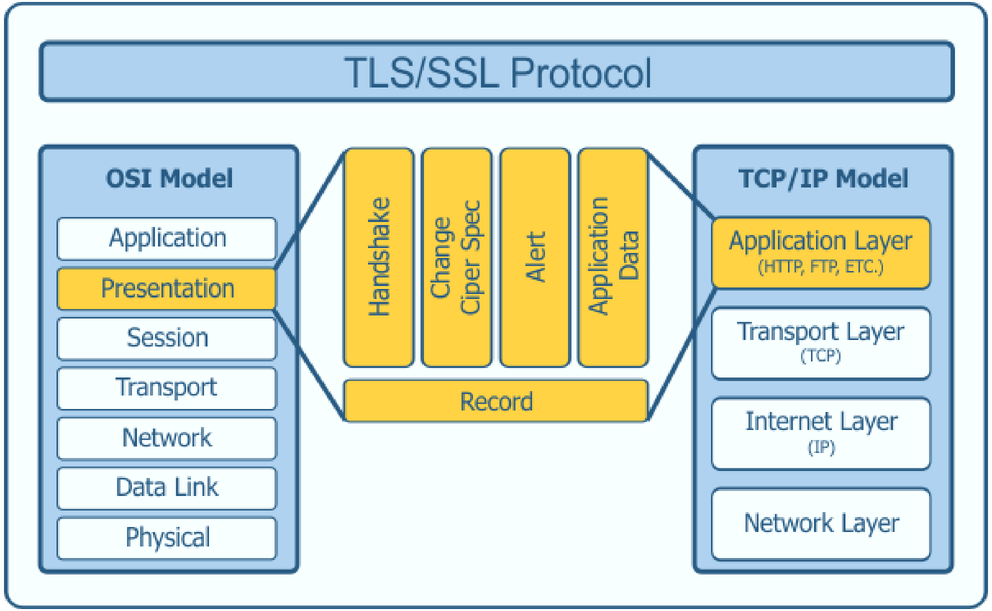
Application Layer
(HTTP, FTP, ETC.)

Transport Layer
(TCP)

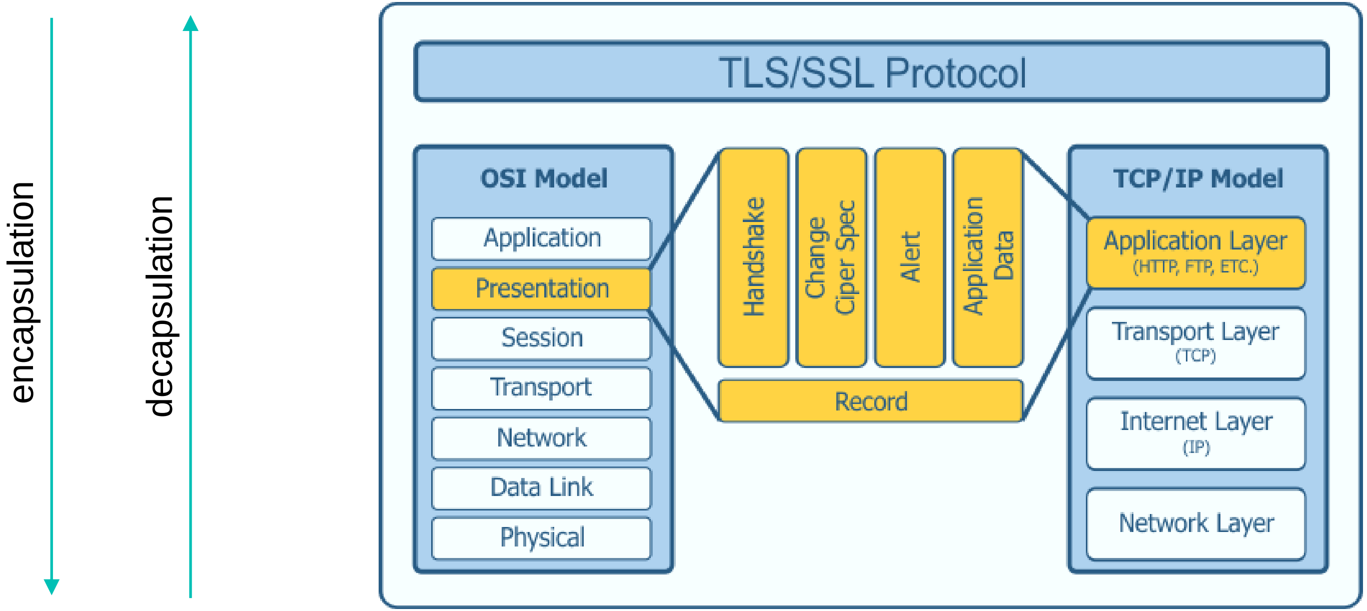
Internet Layer
(IP)

Network Layer

OSI Model vs TCP/IP Model



Encapsulation/Decapsulation



encapsulation

decapsulation

TLS/SSL Protocol

OSI Model

Application

Presentation

Session

Transport

Network

Data Link

Physical

Handshake

Change Ciper Spec

Alert

Application Data

Record

TCP/IP Model

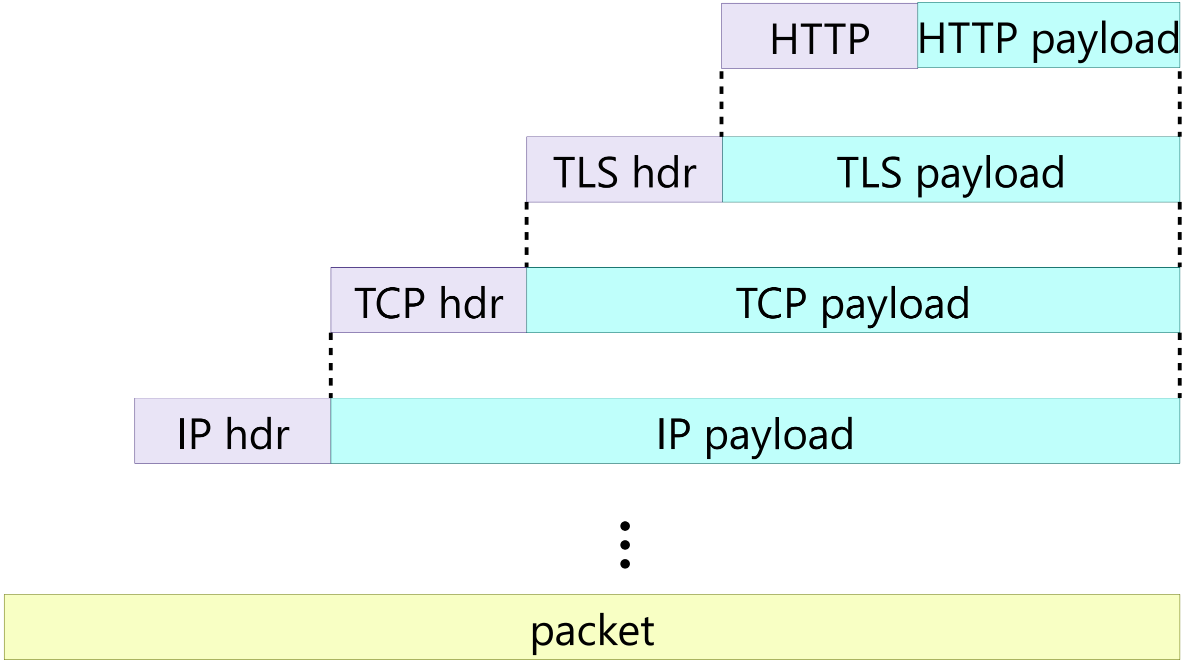
Application Layer (HTTP, FTP, ETC.)

Transport Layer (TCP)

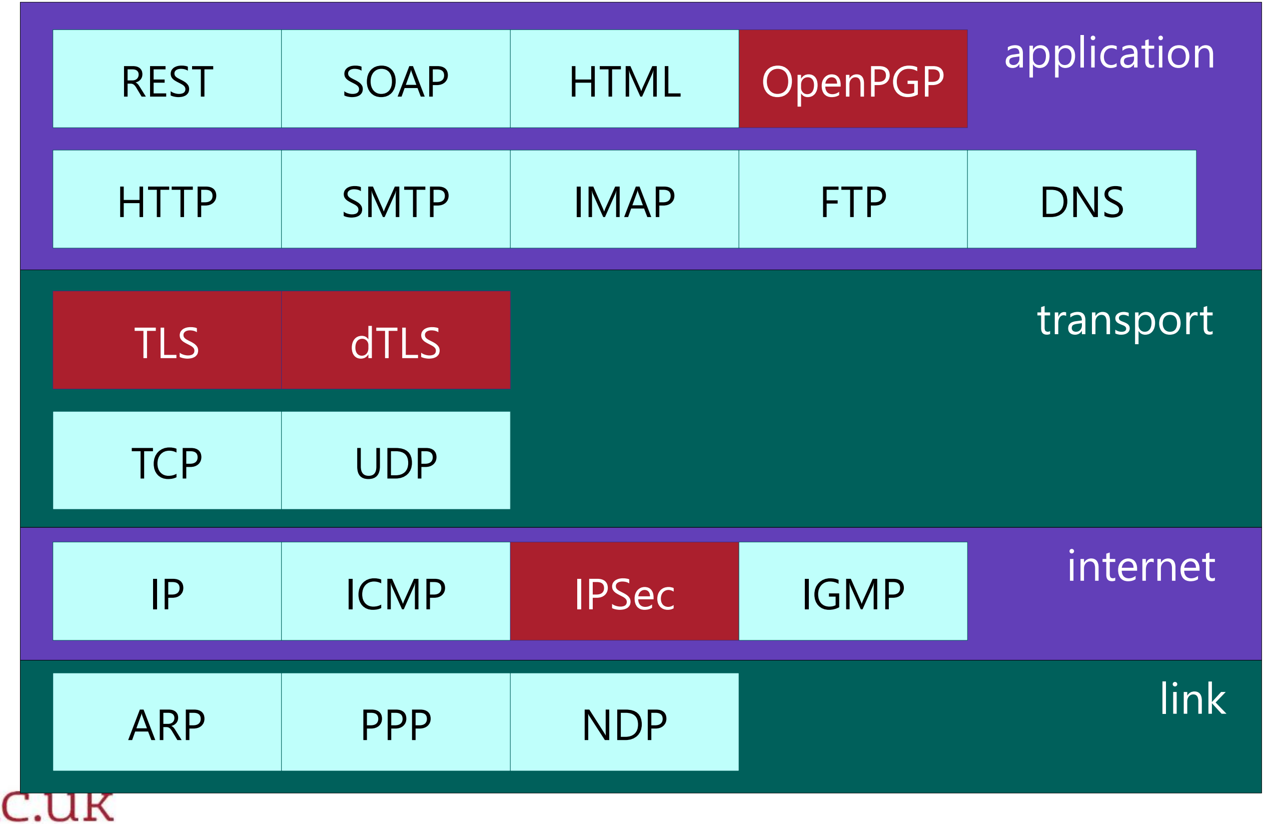
Internet Layer (IP)

Network Layer

Encapsulation/Decapsulation



Security at different layers



application

REST SOAP HTML OpenPGP

HTTP SMTP IMAP FTP DNS

transport

TLS dTLS

TCP UDP

internet

IP ICMP IPSec IGMP

link

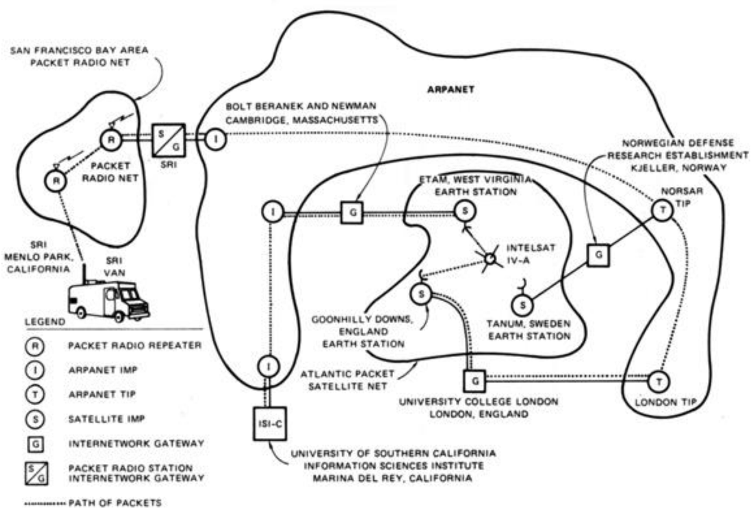
ARP PPP NDP

Problems

- Size of the network have grown exponentially since most of the protocols were designed

Problems

- Size of the network have grown exponentially since most of the protocols were designed
  - e.g. 1975 TCP/IP test between Stanford and UCL


SAN FRANCISCO BAY AREA PACKET RADIO NET
PACKET RADIO NET
R
S G
SRI
I
ARPANET
BOLT BERANEK AND NEWMAN CAMBRIDGE, MASSACHUSETTS
NORWEGIAN DEFENSE RESEARCH ESTABLISHMENT KJELLER, NORWAY
ETAM, WEST VIRGINIA EARTH STATION
NORSAR TIP
T
G
S
INTELSAT IV-A
SRI MENLO PARK, CALIFORNIA
SRI VAN
GOONHILLY DOWNS, ENGLAND EARTH STATION
TANUM, SWEDEN EARTH STATION
ATLANTIC PACKET SATELLITE NET
UNIVERSITY COLLEGE LONDON LONDON, ENGLAND
LONDON TIP
ISI-C
UNIVERSITY OF SOUTHERN CALIFORNIA INFORMATION SCIENCES INSTITUTE MARINA DEL REY, CALIFORNIA
LEGEND
R PACKET RADIO REPEATER
I ARPANET IMP
T ARPANET TIP
S SATELLITE IMP
G INTERNETWORK GATEWAY
S G PACKET RADIO STATION INTERNETWORK GATEWAY
PATH OF PACKETS

Problems

- Size of the network have grown exponentially since most of the protocols were designed
- Moved to a world where we know there is malign element in the network

Problems

- Size of the network have grown exponentially since most of the protocols were designed
- Moved to a world where we know there is malign element in the network
- Issues in implementations
  - We discussed many kind of vulnerabilities so far…

Problems

- Size of the network have grown exponentially since most of the protocols were designed
- Moved to a world where we know there is malign element in the network
- Issues in implementations
  - We discussed many kind of vulnerabilities so far…
- … but also in the protocol themselves

Problems

- Size of the network have grown exponentially since most of the protocols were designed
- Moved to a world where we know there is malign element in the network
- Issues in implementations
- … but also in the protocol themselves
- Need to improve security without disturbing the old
  - Lead to optional extra security, extra layers etc…
  - Takes a lot of time to move forward (e.g. IPv6)

Problems

Homework/potential exam question: Discuss why securing network protocols is proving difficult in practice

- Size of the network have grown exponentially since most of the protocols were designed
- Moved to a world where we know there is malign element in the network
- Issues in implementations
- … but also in the protocol themselves
- Need to improve security without disturbing the old
  - Lead to optional extra security, extra layers etc…
  - Takes a lot of time to move forward (e.g. IPv6)

Type of attacks

Type of attacks

- Traffic Analysis
- Message Disclosure
- Masquerade
- Message Modification
- Replay
- Topology Disclosure
- Unauthorized Access
- Denial of Service

Type of attacks

- Understanding attacks
  - What and How

Type of attacks

- Understanding attacks
  - What and How
- Two targets
  - Network Data
  - Systems Connected to the Network or Within the Network (e.g. switches)

Type of attacks

- Understanding attacks
  - What and How
- Two targets
  - Network Data
  - Systems Connected to the Network or Within the Network (e.g. switches)
- Passive and Active attacks

Type of attacks

	Passive	Active
Network Data	Traffic Analysis Message Disclosure	Masquerade Message Modification Replay
System	Topology disclosure Unauthorized access Denial of Service	

Type of attacks

- Traffic Analysis
  - Attacker can see who is exchanging messages
  - Number, time, pattern
  - e.g. timing analysis (seen in previous lecture, also check SSH timing attack on github)
- Message Disclosure
- Masquerade
- Message Modification
- Replay
- Topology Disclosure
- Unauthorized Access
- Denial of Service

Type of attacks

- Traffic Analysis
- Message Disclosure
  - The attacker can read the content or some content of exchanged message
  - Countermeasure encryption
  - Although size can leak information
- Masquerade
- Message Modification
- Replay
- Topology Disclosure
- Unauthorized Access
- Denial of Service

Type of attacks

- Traffic Analysis
- Message Disclosure
- Masquerade
  - Pretending to be someone else
  - We have seen several examples in past lecture
- Message Modification
- Replay
- Topology Disclosure
- Unauthorized Access
- Denial of Service

Type of attacks

- Traffic Analysis
- Message Disclosure
- Masquerade
- Message Modification
  - Man in the middle
  - Receive message from Alice
  - Modify Message
  - Send it to Bob
  - Need to block traffic between Alice and Bob; and to Masquerade as Alice
  - See example in Browser Security Lecture
- Replay
- Topology Disclosure
- Unauthorized Access
- Denial of Service

Type of attacks

- Traffic Analysis
- Message Disclosure
- Masquerade
- Message Modification
- Replay
  - Data maliciously retransmitted
  - e.g. Send “pay 100$” multiple times
  - We have seen example last week
- Topology Disclosure
- Unauthorized Access
- Denial of Service

Type of attacks

- Traffic Analysis
- Message Disclosure
- Masquerade
- Message Modification
- Replay
- Topology Disclosure
  - Discover nodes connected to a network
  - Discover services running on those nodes
  - Example: port scan discussed several times during lectures (browser security lecture and Morris Worm)
- Unauthorized Access
- Denial of Service

Type of attacks

- Traffic Analysis
- Message Disclosure
- Masquerade
- Message Modification
- Replay
- Topology Disclosure
- Unauthorized Access
  - Attacker try to break in another system
  - Many possible way to do so
  - Social Engineering, Phishing, Brute Force
  - See Lecture on Password
- Denial of Service

Type of attacks

- Traffic Analysis
- Message Disclosure
- Masquerade
- Message Modification
- Replay
- Topology Disclosure
- Unauthorized Access
- Denial of Service
  - Attacker want to block usage of network resources (end nodes, routers etc…)
  - e.g. overload a server with very large number of request

Type of attacks

Homework/potential exam question:
Explain succinctly X type of attack

- Traffic Analysis
- Message Disclosure
- Masquerade
- Message Modification
- Replay
- Topology Disclosure
- Unauthorized Access
- Denial of Service

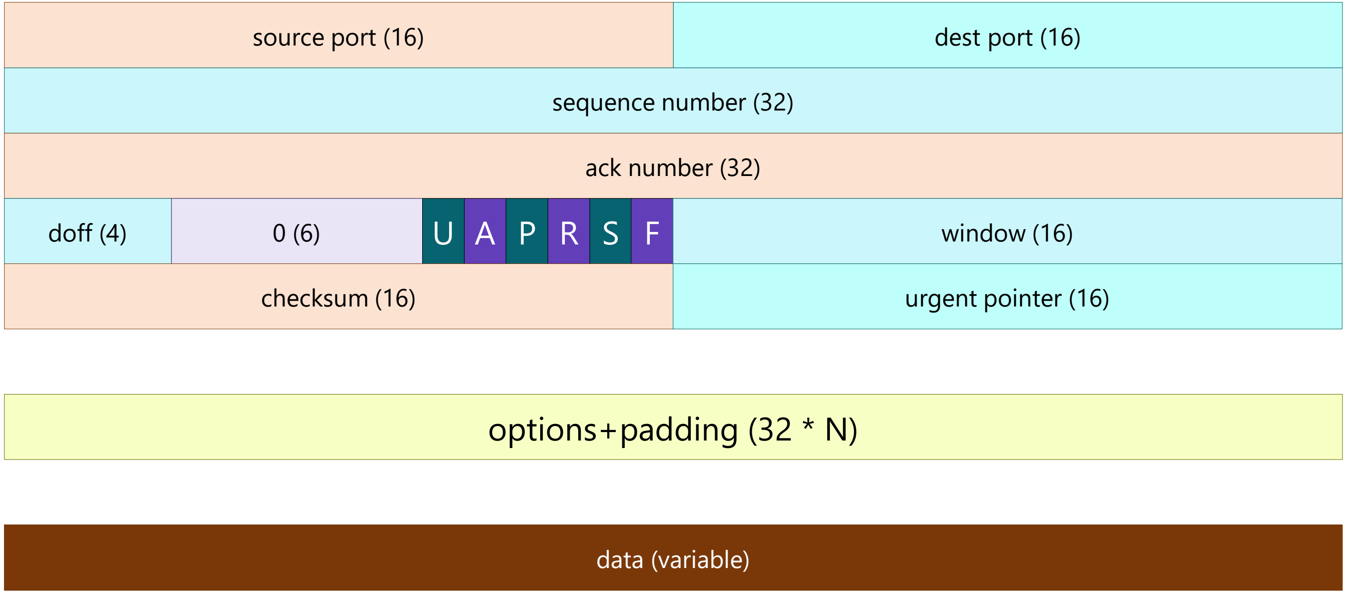
Type of attacks

- Traffic Analysis
  - We will discuss Tor and the like in a future lecture
- Message Disclosure
- Masquerade
- Message Modification
- Replay
- Topology Disclosure
- Unauthorized Access
- Denial of Service

Vulnerability examples

TCP

█ = 1 bit



source port (16)
dest port (16)

sequence number (32)

ack number (32)

doff (4)
0 (6)
U A P R S F
window (16)

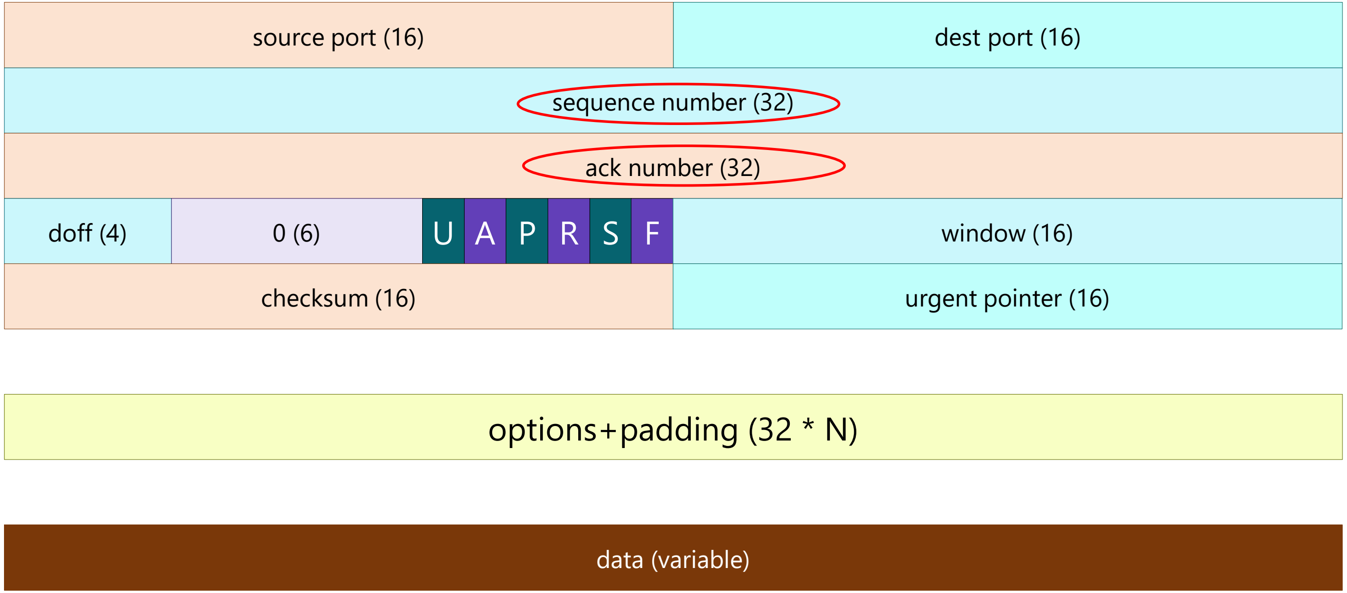
checksum (16)
urgent pointer (16)

options+padding (32 * N)

data (variable)

TCP

▮ = 1 bit



source port (16) | dest port (16)

sequence number (32)

ack number (32)

doff (4) | 0 (6) | U | A | P | R | S | F | window (16)

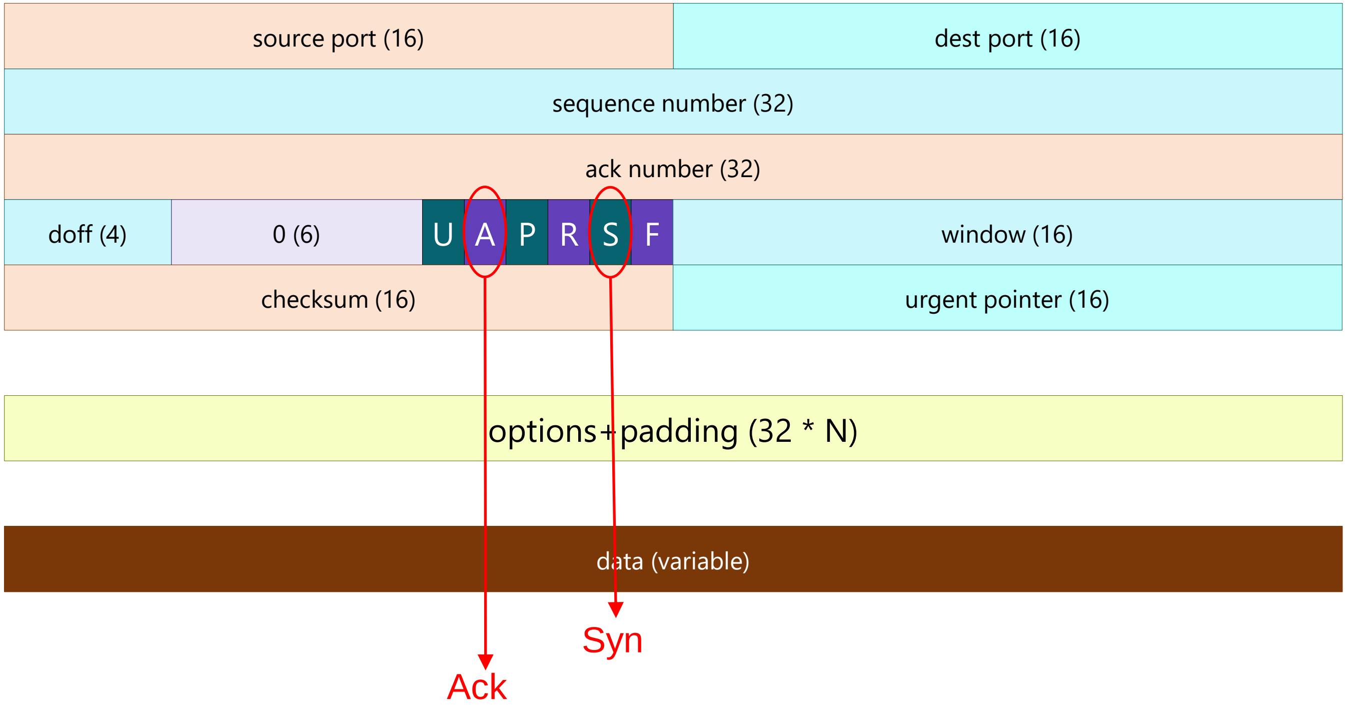
checksum (16) | urgent pointer (16)

options+padding (32 * N)

data (variable)

█ = 1 bit

TCP



source port (16)

dest port (16)

sequence number (32)

ack number (32)

doff (4)

0 (6)

U A P R S F

window (16)

checksum (16)

urgent pointer (16)

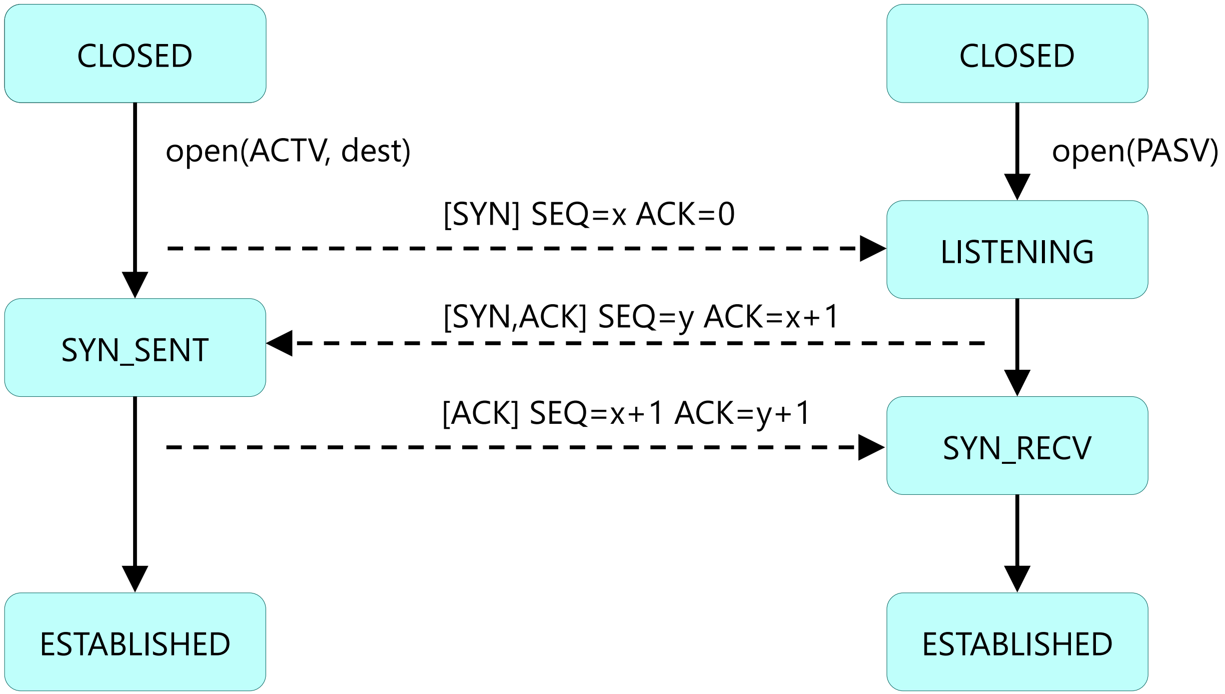
options+padding (32 * N)

data (variable)

Syn

Ack

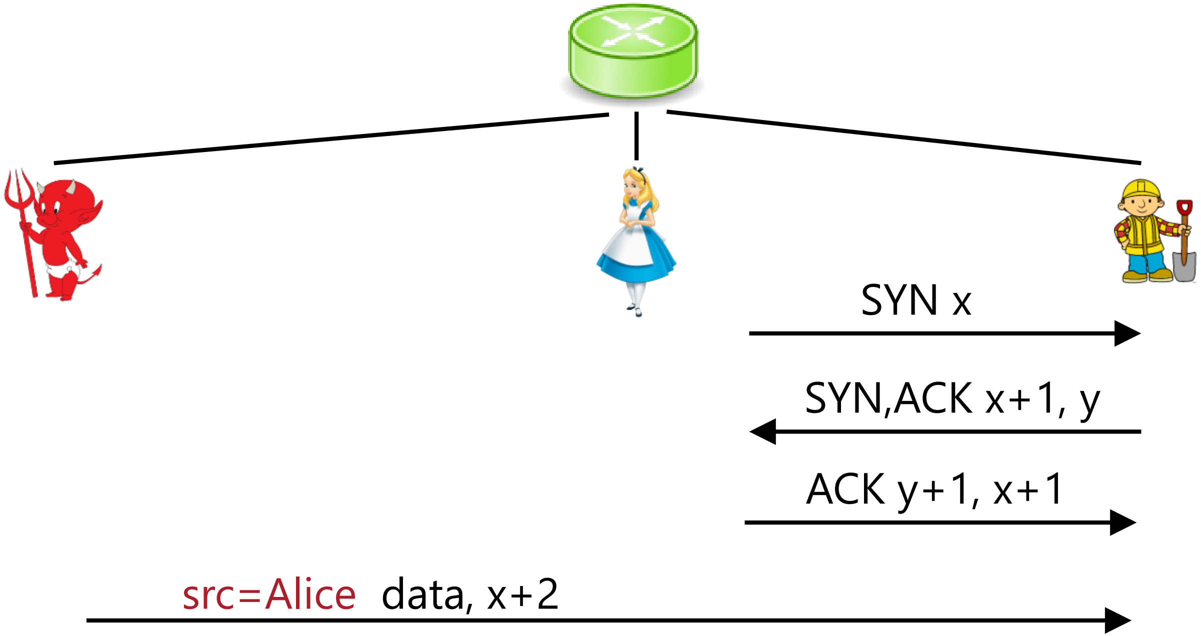
TCP handshake



Problem

- Sequence number are not random
- They were designed to prevent collision
- But things can go wrong
- Attack can guess sequence numbers!

Session Hijacking



SYN x

SYN,ACK x+1, y

ACK y+1, x+1

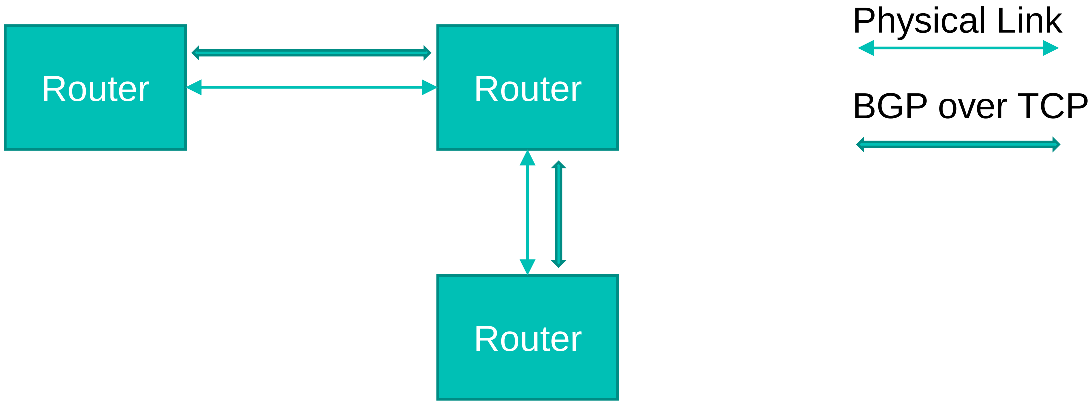
src=Alice data, x+2

Problem

- IP-based authorization (do not this! this is bad!)
  - Masquerade + Unauthorized Access

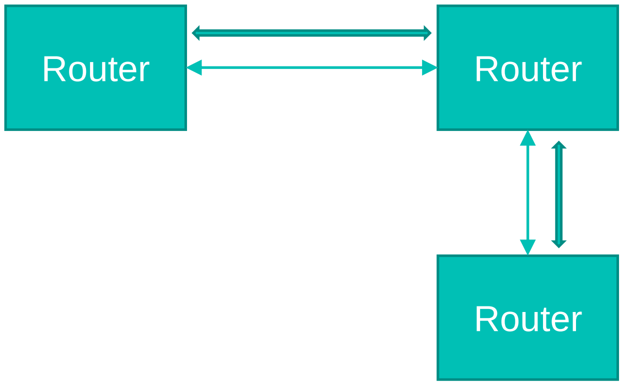
Problem

- IP-based authorization (do not this! this is bad!)
- Reset attack



Problem

- IP-based authorization (do not this! this is bad!)
- Reset attack



Physical Link ⟷

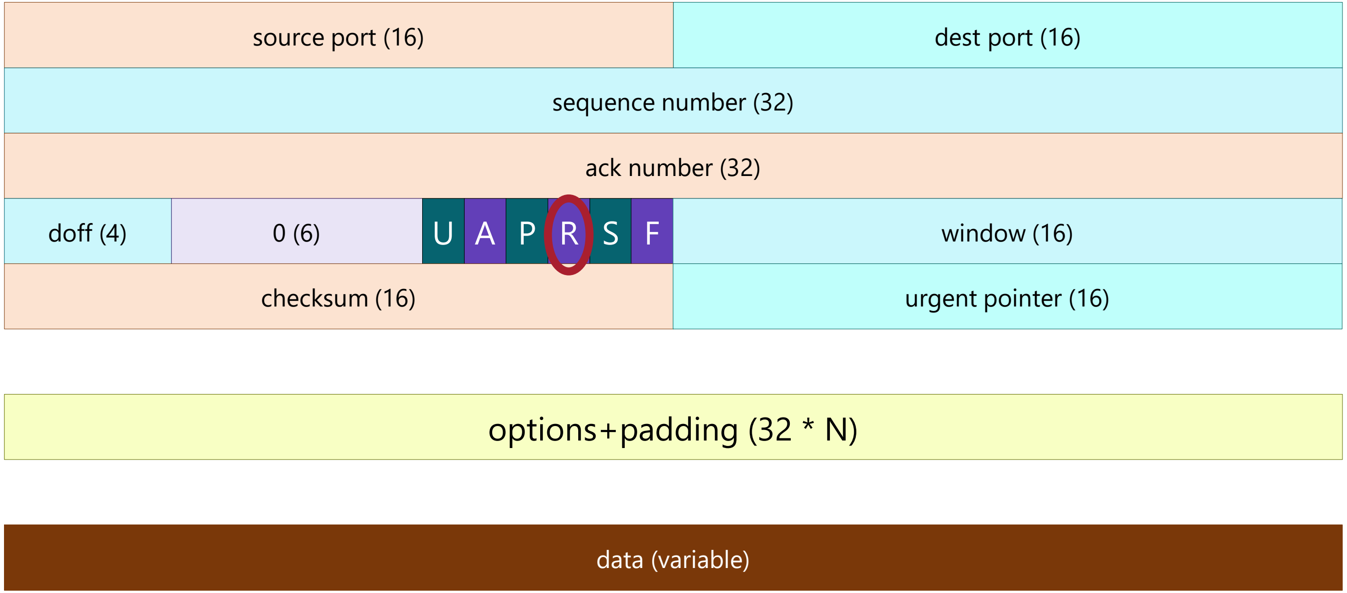
BGP over TCP ⟷

Border Gateway Protocol

- Used to exchange info for packet routing.

TCP

■ = 1 bit



source port (16)

dest port (16)

sequence number (32)

ack number (32)

doff (4)

0 (6)

U A P R S F

window (16)

checksum (16)

urgent pointer (16)

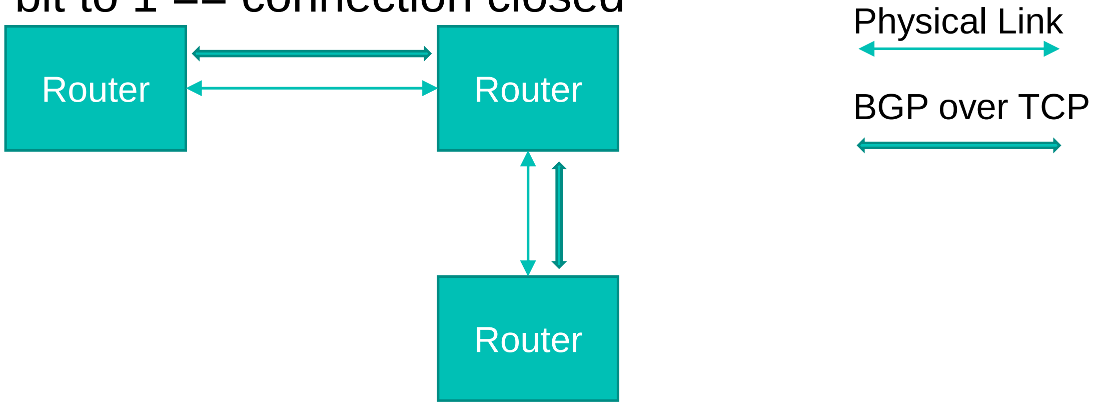
options+padding (32 * N)

data (variable)

bristol.ac.uk

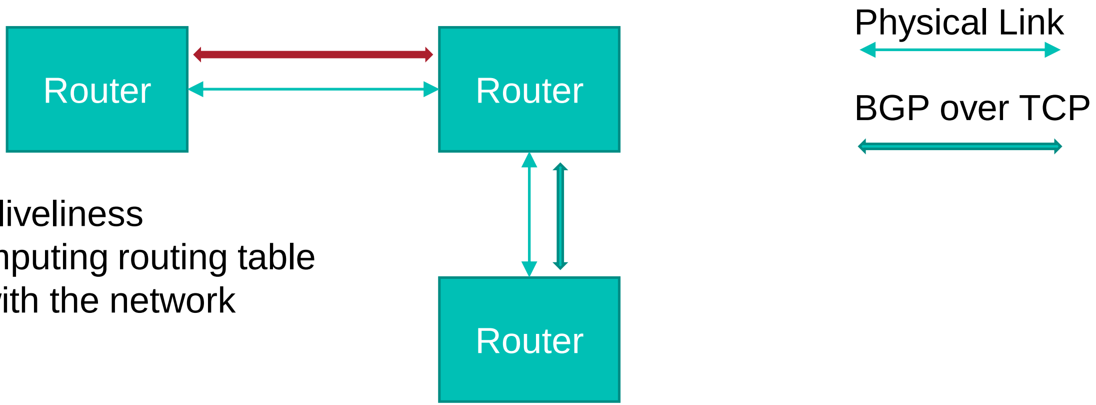
Problem

- IP-based authorization (do not this! this is bad!)
- Reset attack
  - Spoof a tcp message
  - Set RESET bit to 1 == connection closed



Problem

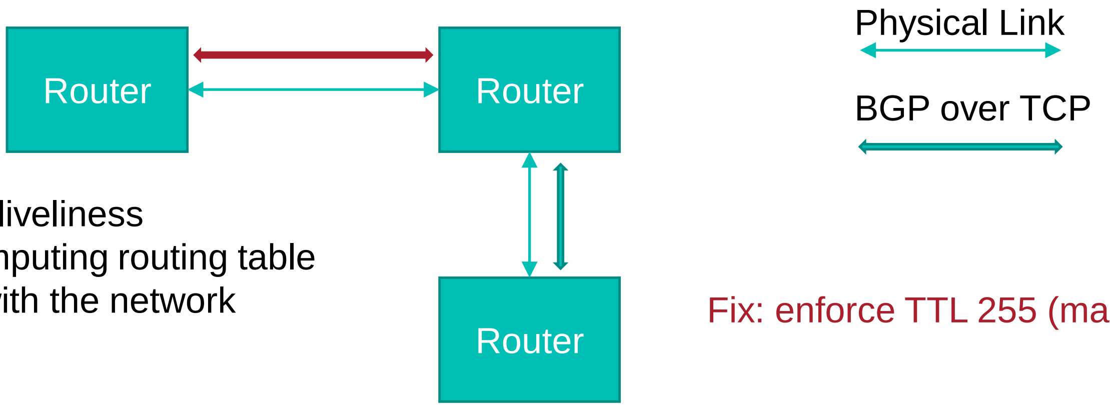
- IP-based authorization (do not this! this is bad!)
- Reset attack



Use connection to infer liveliness
If lost connection, recomputing routing table
Attacker can mess up with the network
Denial of Service

Problem

- IP-based authorization (do not this! this is bad!)
- Reset attack



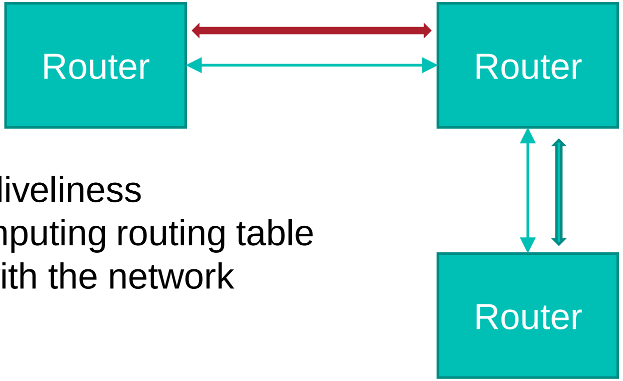
Use connection to infer liveliness
If lost connection, recomputing routing table
Attacker can mess up with the network
Denial of Service

Fix: enforce TTL 255 (max value)

Problem

Homework/potential exam question:
Give an example of DOS attack

- IP-based authorization (do not this! this is bad!)
- Reset attack



Physical Link

BGP over TCP

Use connection to infer liveliness
If lost connection, recomputing routing table
Attacker can mess up with the network
Denial of Service

Fix: enforce TTL 255 (max value)

Problem

- IP-based authorization (do not this! this is bad!)
- Reset attack
  - Break application relying on long-lived connection
- Data injection
  - Wait application level authentication have been achieved
  - Insert packet that will be treated as coming from the users

Problem

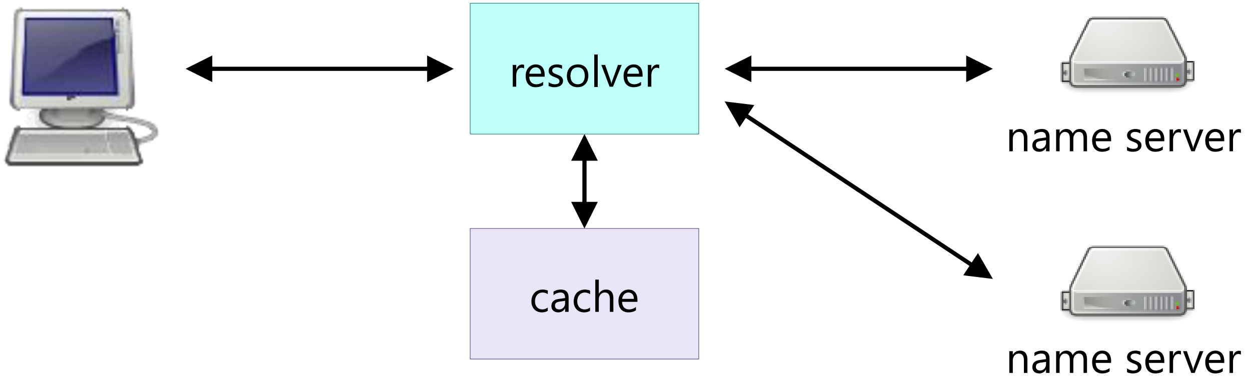
- IP-based authorization (do not this! this is bad!)
- Reset attack
  - Break application relying on long-lived connection
- Data injection
  - Wait application level authentication have been achieved
  - Insert packet that will be treated as coming from the users
  - … DO NOT RELY ON TCP FOR SECURITY
  - Masquerade

Problem

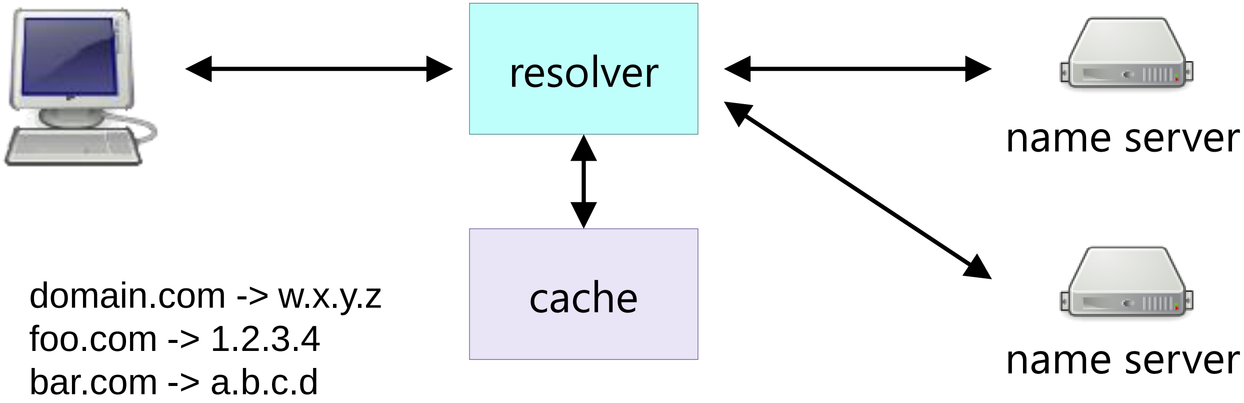
Homework/potential exam question:
Look at SYN flood attack type

- IP-based authorization (do not this! this is bad!)
- Reset attack
  - Break application relying on long-lived connection
- Data injection
  - Wait application level authentication have been achieved
  - Insert packet that will be treated as coming from the users
  - … DO NOT RELY ON TCP FOR SECURITY
  - Masquerade

DNS resolver & cache

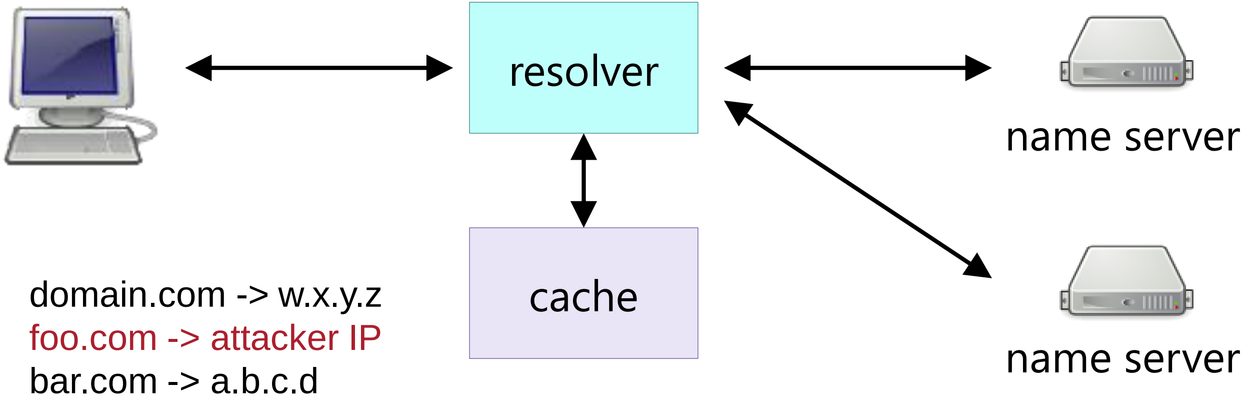


DNS resolver & cache



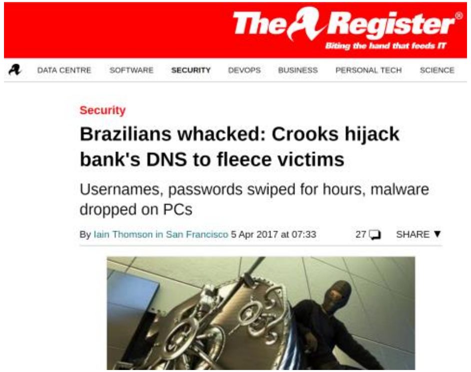
domain.com -> w.x.y.z
foo.com -> 1.2.3.4
bar.com -> a.b.c.d

DNS poisoning



domain.com -> w.x.y.z
foo.com -> attacker IP
bar.com -> a.b.c.d

DNS poisoning



The Register®

Biting the hand that feeds IT

Security

Brazilians whacked: Crooks hijack bank's DNS to fleece victims

Usernames, passwords swiped for hours, malware dropped on PCs

By Iain Thomson in San Francisco 5 Apr 2017 at 07:33

- Exploit vulnerability in the DNS resolver/server
- Man in the middle (send a fake response)
- Modify the client host file (won’t make DNS request then)
- Domain high-jacking (point to a different DNS server for a particular domain)
  - Would require to gain access to a registrar
  - Getting the password (we have seen how)
  - 22/10/2016, attacker gained control of Brazilian bank website for 6h
- Masquerade type attack

Countermeasure: DNSSEC

- Simple idea: sign domain, IP pair with domain owner certificates!
  - We have seen last week:
    - How certificate work
    - How to verify signature
- NSEC: prove subdomain don’t exist
  - sign an entry bar.bristol.ac.uk to foo.bristol.ac.uk
  - there exists no domain (in alpha. order), between bar… and foo…
  - Can someone spot a type of attack we could use this info for?

Countermeasure: DNSSEC

- Simple idea: sign domain, IP pair with domain owner certificates!
  - We have seen last week:
    - How certificate work
    - How to verify signature
- NSEC: prove subdomain don’t exist
  - sign an entry bar.bristol.ac.uk to foo.bristol.ac.uk
  - there exists no domain (in alpha. order), between bar… and foo…
  - Topology Disclosure
    - Start from a.bristol.ac.uk then move the way up until you learn all valide subdomain
    - (It is slightly more complicated in practice)

Countermeasure: DNSSEC

- Simple idea: sign domain, IP pair with domain owner certificates!
  - We have seen last week:
    - How certificate work
    - How to verify signature
- NSEC: prove subdomain don’t exist
  - sign an entry bar.bristol.ac.uk to foo.bristol.ac.uk
  - there exists no domain (in alpha. order), between bar… and foo…
  - Topology Disclosure
    - Start from a.bristol.ac.uk then move the way up until you learn all valide subdomain
    - (It is slightly more complicated in practice)

Countermeasure: DNSSEC

Homework/potential exam question:
Explain how and why DNSSEC

- Simple idea: sign domain, IP pair with domain owner certificates!
  - We have seen last week:
    - How certificate work
    - How to verify signature
- NSEC: prove subdomain don't exist
  - sign an entry bar.bristol.ac.uk to foo.bristol.ac.uk
  - there exists no domain (in alpha. order), between bar… and foo…
  - Topology Disclosure
    - Start from a.bristol.ac.uk then move the way up until you learn all valide subdomain
    - (It is slightly more complicated in practice)

Slow Loris Attack

Slow Loris Attack

- Usual DOS
  - Overload server computing power
  - … or available bandwidth

Slow Loris Attack

- Usual DOS
  - Overload server computing power
  - … or available bandwidth
- Slow Loris is a protocol level attack
  - Require very little computer power from the attacker

Slow Loris Attack

- Usual DOS
  - Overload server computing power
  - … or available bandwidth
- Slow Loris is a protocol level attack
  - Require very little computer power from the attacker
- HTTP request always finished by \n\n

Slow Loris Attack

- Usual DOS
  - Overload server computing power
  - … or available bandwidth
- Slow Loris is a protocol level attack
  - Require very little computer power from the attacker
- HTTP request always finished by \n\n
- Open connection and send data very, very, very slowly
  - Send the request GET XXXX
  - When the server is about to timeout…
  - Send one more character
- Totally normal usage of HTTP protocol

Slow Loris Attack

Homework/potential exam question:
Explain Slow Loris attack

- Usual DOS
  - Overload server computing power
  - … or available bandwidth
- Slow Loris is a protocol level attack
  - Require very little computer power from the attacker
- HTTP request always finished by \n\n
- Open connection and send data very, very, very slowly
  - Send the request GET XXXX
  - When the server is about to timeout…
  - Send one more character
- Totally normal usage of HTTP protocol
- Open multiple connections, until the server ran out of threads (Apache limite #threads)
- DOS done! Very low resource required from attackers!

Plan

- OSI Model
- TCP/IP Model
- Type of attacks
  - Traffic Analysis
  - Message Disclosure
  - Masquerade
  - Message Modification
  - Replay
  - Topology Disclosure
  - Unauthorized Access
  - Denial of Service
- TCP Syn related attacks
- DNS poisoning
- Slow Loris attack

Conclusion

- Protocol have been used in another time and age
- The world changes, protocols change very slowly

Conclusion

- Protocol have been used in another time and age
- The world changes, protocols change very slowly
- Understand guarantees form underlying layers
- Never expect them to do more than this

Conclusion

- Protocol have been used in another time and age
- The world changes, protocols change very slowly
- Understand guarantees form underlying layers
- Never expect them to do more than this
- Always distrust external inputs

Conclusion

- Protocol have been used in another time and age
- The world changes, protocols change very slowly
- Understand guarantees form underlying layers
- Never expect them to do more than this
- Always distrust external inputs
  - Buffer overflow
  - SQL Injection
  - … and network packets!

University of BRISTOL

Thank you, questions?

Office MVB 3.26

bristol.ac.uk