University of BRISTOL

Systems Security

COMSM1500

bristol.ac.uk

Help with lab reports

- Feedback on reflective part
  - Just send me a draft by e-mail
  - I will put notes in the pdf and send it back ASAP
  - If you all send this on the days before the deadline less likely to get it back in time
- Feedback on technical part/extra help
  - Book appointment with your assigned TA
  - Check online for instructions

University of BRISTOL

Anonymous communication

bristol.ac.uk

The problem?

- An attacker could observe network traffic
- Even without access to message data can learn a lot
- Service accessed, usage pattern, etc…

Example: what does your ISP knows

- Internet Service Provider
- Know the domain and IP address you want to visit
- Port (i.e. can infer service), timestamps etc…
- Packet size can leak information about what you do

Example: what does your ISP knows

- Internet Service Provider
- Know the domain and IP address you want to visit
- Port (i.e. can infer service), timestamps etc…
- Packet size can leak information about what you do
- Should I care?

Example: what does your ISP knows

- Internet Service Provider
- Know the domain and IP address you want to visit
- Port (i.e. can infer service), timestamps etc…
- Packet size can leak information about what you do

Example: what does your ISP knows

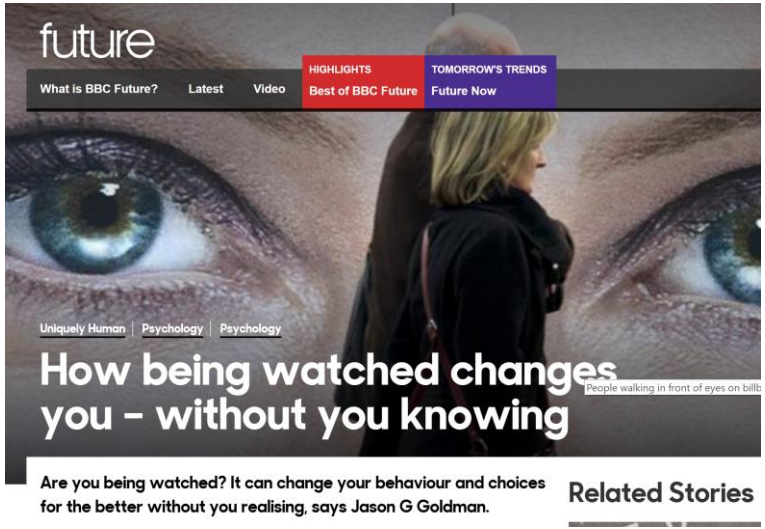
- Internet Service Provider
- Know the domain and IP address you want to visit
- Port (i.e. can infer service), timestamps etc…
- Packet size can leak information about what you do

Example: what does your ISP knows

- Internet Service Provider
- Know the domain and IP address you want to visit
- Port (i.e. can infer service), timestamps etc…
- Packet size can leak information about what you do

Observation is problematic

- Being observed affect your behavior



Observation is problematic Some irony…

- Being observed affect your behavior

Many reason for anonymity

- Means to communicate anonymously in some circumstances
  - Law enforcement to not tip their targets
  - Minority groups
  - Journalists
  - Political militants
  - Lawyers
- There is a few technology to achieve anonymity
- Some usages are less acceptable (more on that later…)

Many reason for anonymity

Homework/exam question:
Discuss why anonymity is important even in a democratic society

- Means to communicate anonymously in some circumstances
  - Law enforcement to not tip their targets
  - Minority groups
  - Journalists
  - Political militants
  - Lawyers
- There is a few technology to achieve anonymity
- Some usages are less acceptable (more on that later…)

Many reason for anonymity

- Means to communicate anonymously in some circumstances
  - Law enforcement to not tip their targets
  - Minority groups
  - Journalists
  - Political militants
  - Lawyers
- There is a few technology to achieve anonymity
- Some usages are less acceptable (more on that later…)
- Also have a look at the news on DNS over HTTPS

Plan

- Anonymity
- Unlinkability
- Unobservability
- VPN
- TOR
- TOR Circuit
- TOR Directory Authority
- TOR vulnerabilities

Anonymity

- Preventing an observer on a network to link a participant to an action

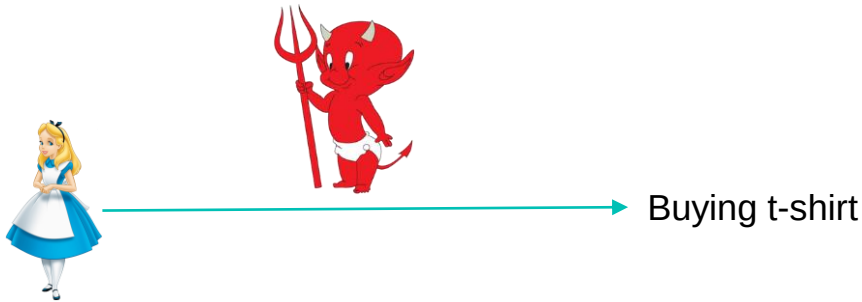
Anonymity

- Preventing an observer on a network to link a participant to an action

- We saw “private browsing” in previous lecture
  - Goal: do not leave trace on your local machine
  - This is not the same
  - You may want both

Anonymity

- Preventing an observer on a network to link a participant to an action



- Observer can now Alice is doing something
- Observer can now someone is buying a t-shirt
- Observer cannot say Alice in particular is buying a t-shirt
  - Absolutely or probabilistically

Other important concepts

- Unlinkability
  - Cannot link Alice to some online identity/profile
- Unobservability
  - Cannot tell Alice is on Internet
  - More realistic cannot tell Alice is using some anonymity tool
- Confidentiality != Anonymity

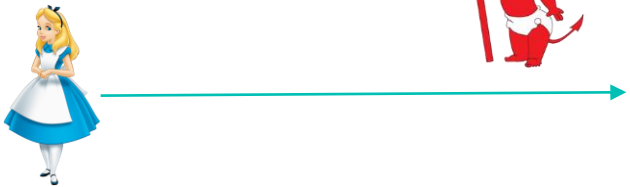
University of BRISTOL

TOR

The Onion Router

bristol.ac.uk

VPN



Buying t-shirt

VPN

Relay

tshirt.com

VPN

Relay

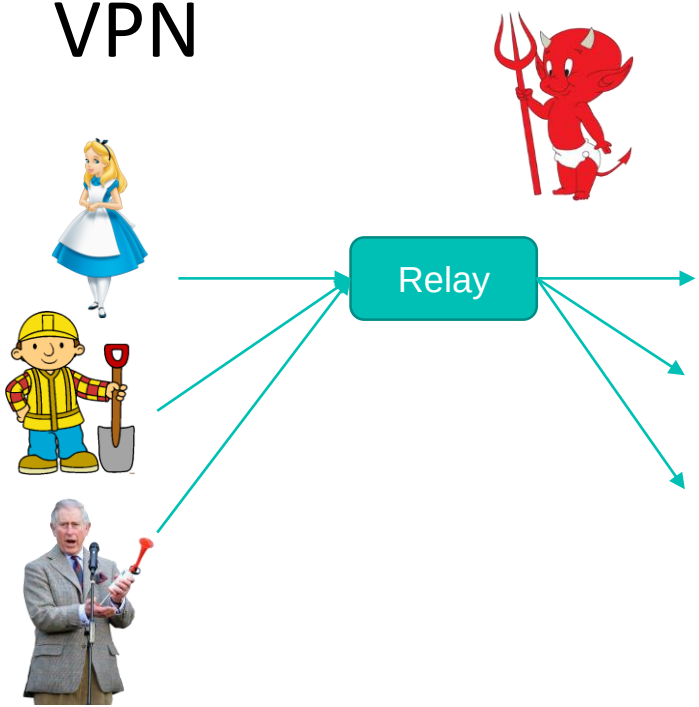
VPN

tshirt.com

books.com

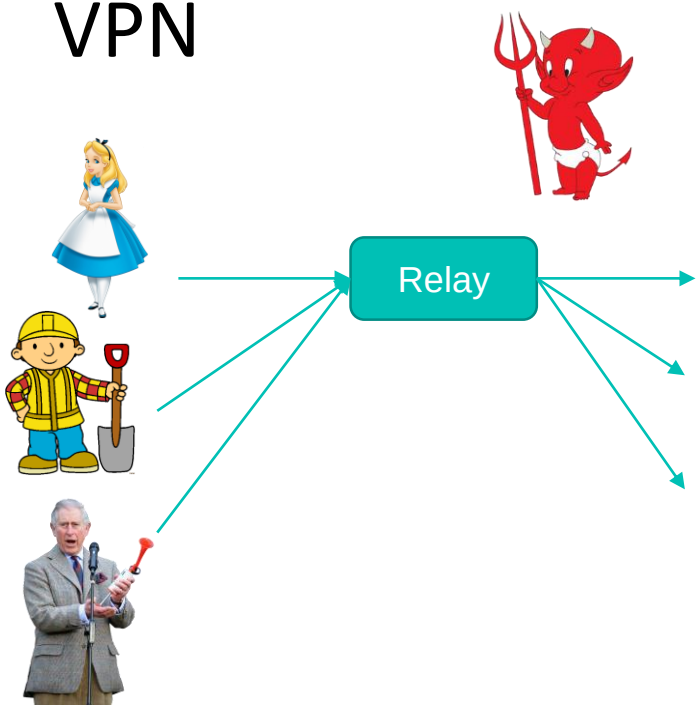
twitter.com

VPN



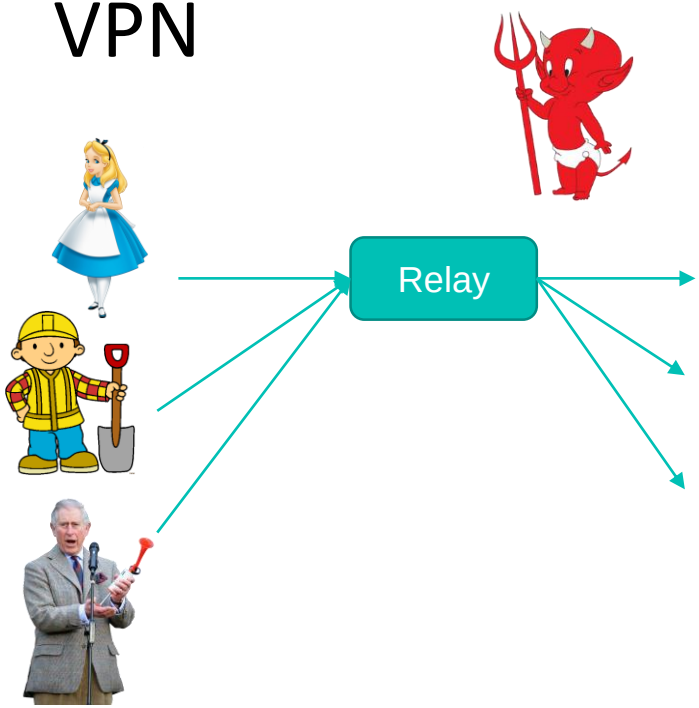
- Harder to know what Alice is doing
  - Observe size
  - Observe timing
- Need to trust the relay

VPN



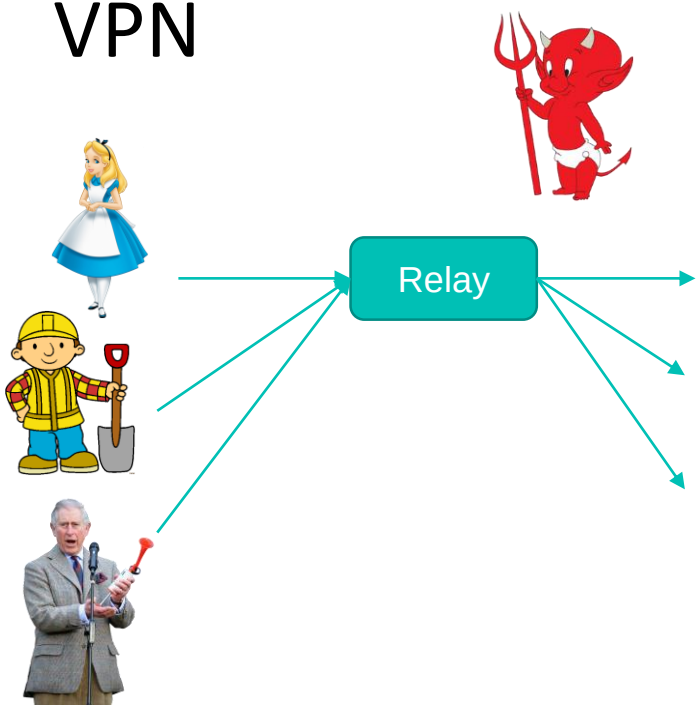
- Harder to know what Alice is doing
  - Observe size
  - Observe timing
- "Mixminion" fix-size request + answer
  - Batch a number of request together
  - Send all at once
  - Problem?
- Need to trust the relay

VPN



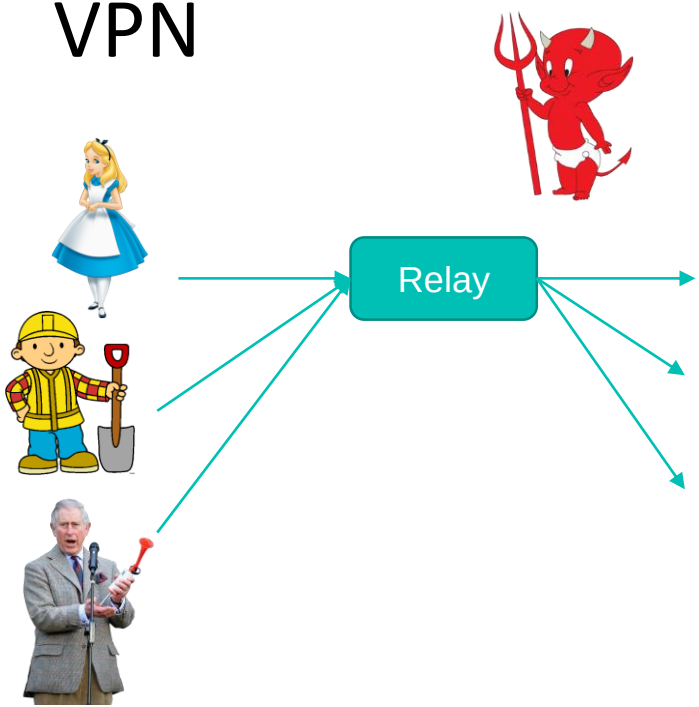
- Harder to know what Alice is doing
  - Observe size
  - Observe timing
- "Mixminion" fix-size request + answer
  - Batch a number of request together
  - Send all at once
  - Problem?
    - Not going to be great to surf online
- Need to trust the relay

VPN



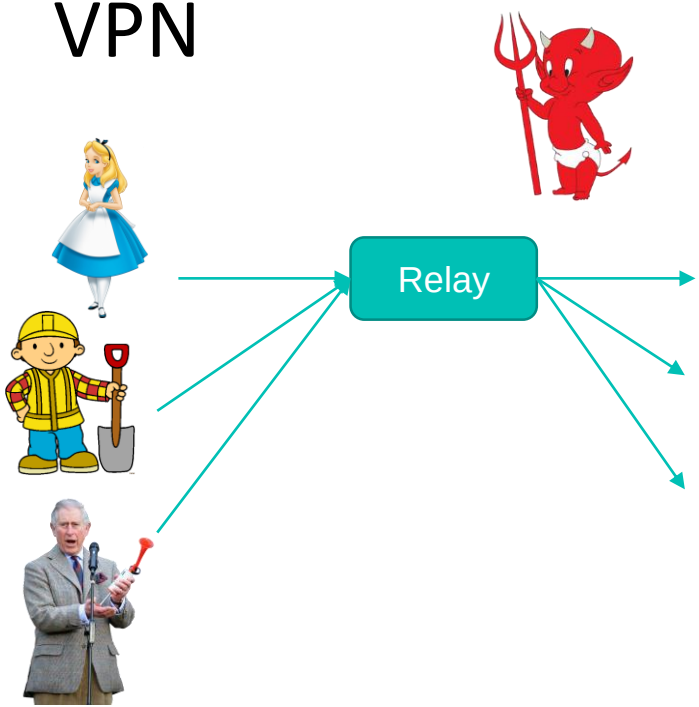
- Harder to know what Alice is doing
- Need to trust the relay

VPN



- Harder to know what Alice is doing
- Need to trust the relay
  - Single relay is obviously a problem
  - If it is compromised no guarantees

VPN



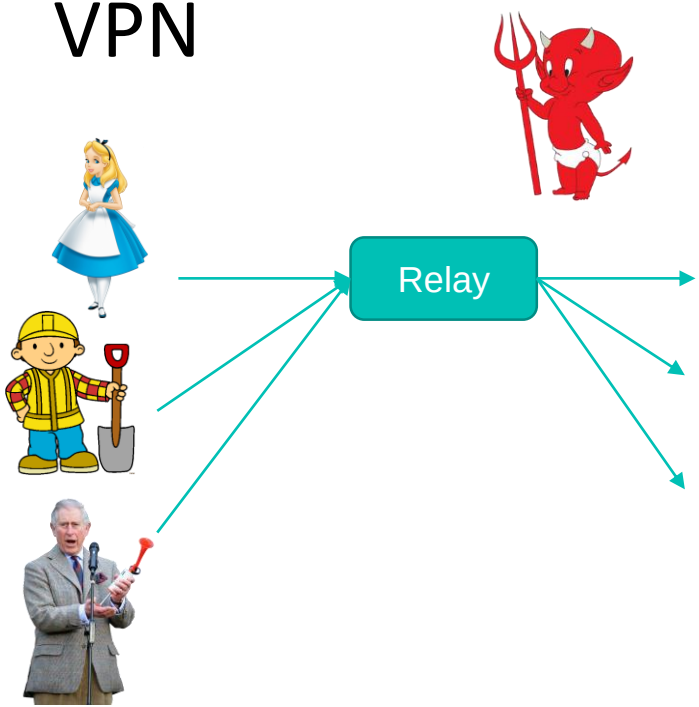
tshirt.com

books.com

twitter.com

- Harder to know what Alice is doing
- Need to trust the relay
  - Single relay is obviously a problem
  - If it is compromised no guarantees
- Trusted VPN are fine
  - e.g. universities run one, if you need to access some info from country that bans some content

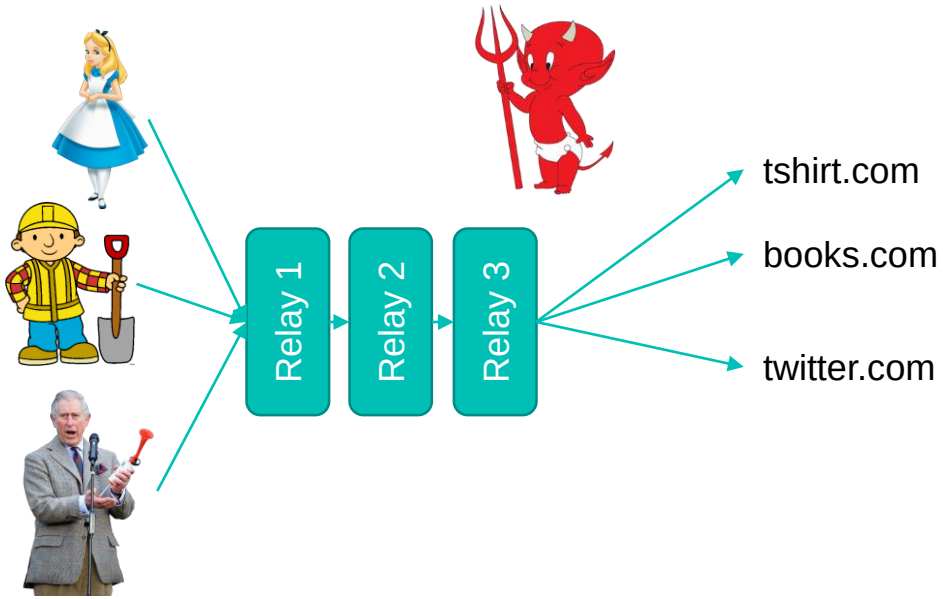
VPN



Homework/potential exam question:
Discuss: Why VPN do not provide good anonymity.

- Harder to know what Alice is doing
- Need to trust the relay
  - Single relay is obviously a problem
  - If it is compromised no guarantees
- Trusted VPN are fine
  - e.g. universities run one, if you need to access some info from country that bans some content

TOR Circuit



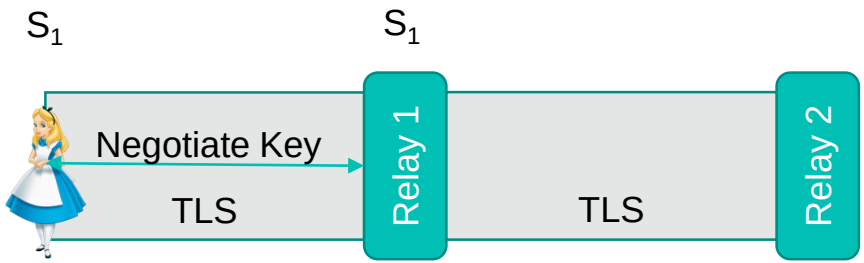
- Harder to know what Alice is doing
- Need to trust the relay
  - Relay 1 now Alice is doing something
  - Relay 3 now some is talking to t-shirt.com
  - Attacker need to control 1 and 3 to be really harmful
  - Hard/Costly to achieve
  - Discussed further later…

TOR Circuit

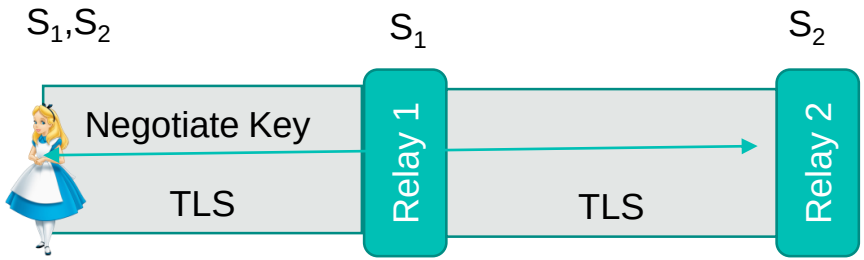
Relay 1

Relay 2

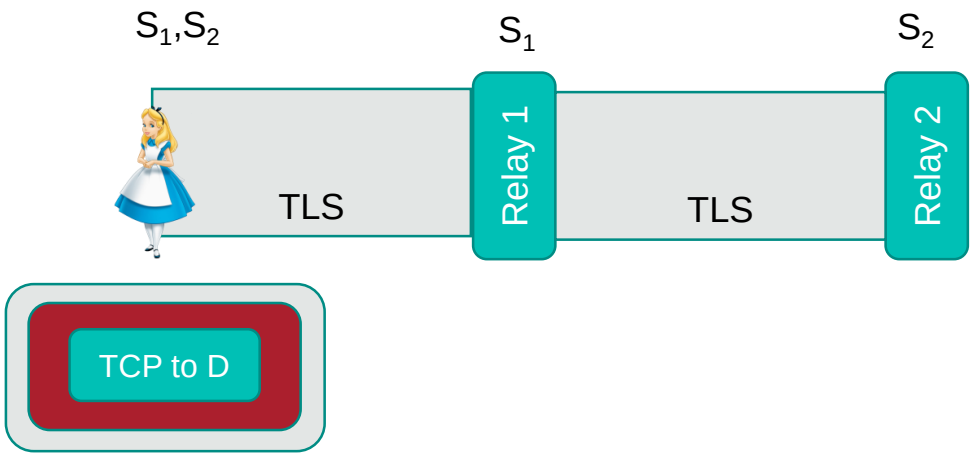
TOR Circuit



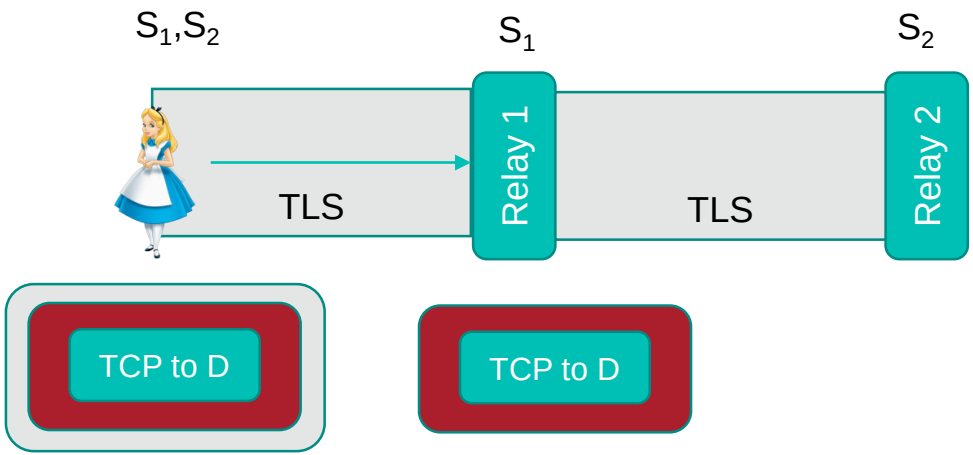
TOR Circuit



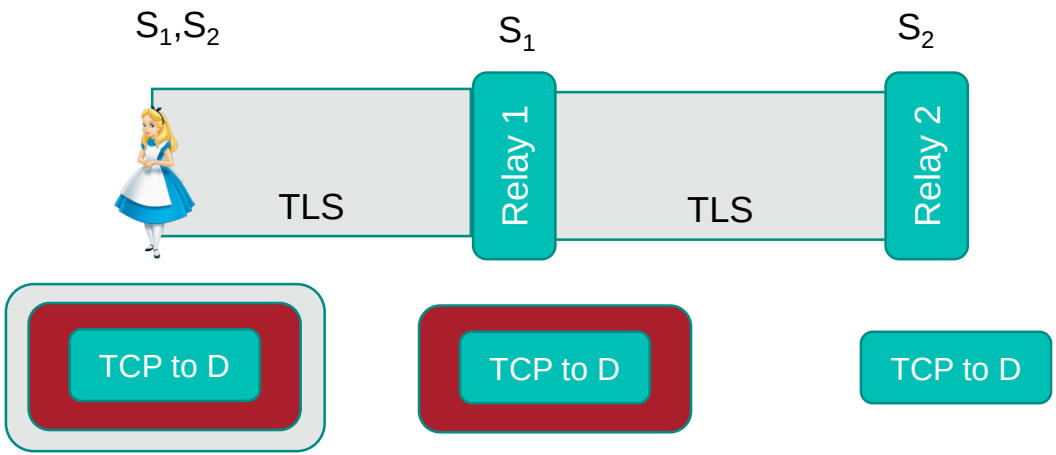
TOR Circuit



TOR Circuit

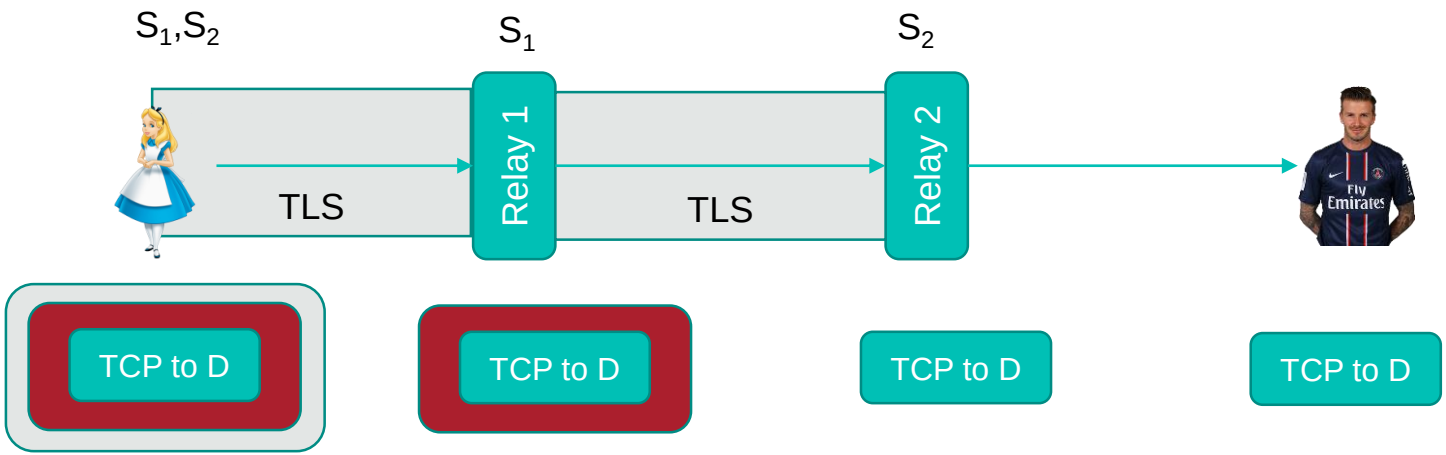


TOR Circuit

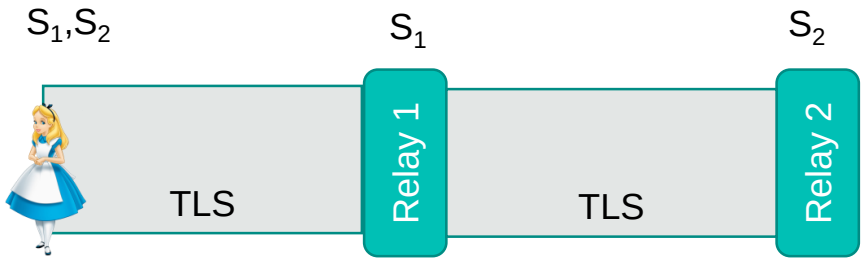

S_1,S_2
S_1
S_2
TLS
Relay 1
TLS
Relay 2
TCP to D
TCP to D
TCP to D


Fly
Emirates

TOR Circuit

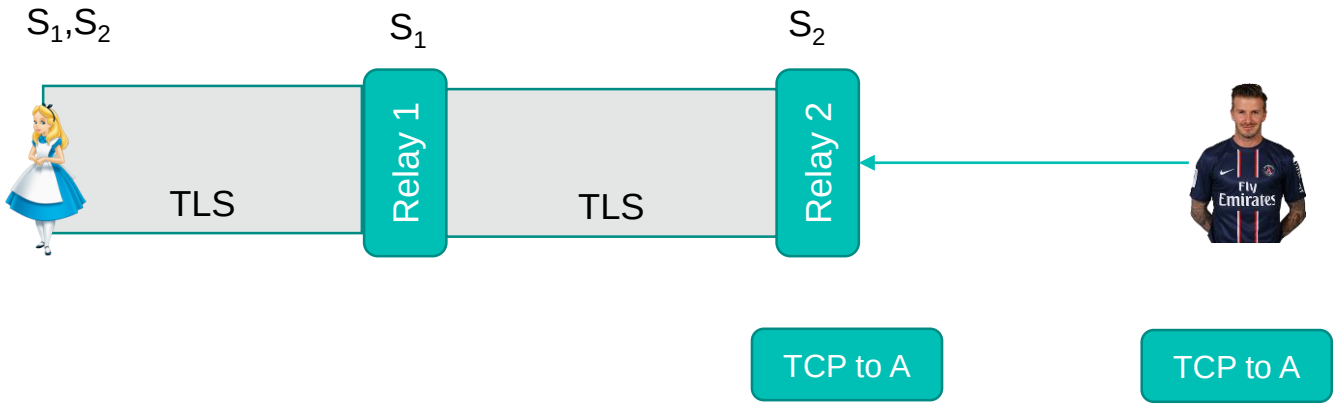

S_1,S_2
S_1
S_2
TLS
Relay 1
TLS
Relay 2
Fly Emirates
TCP to D
TCP to D
TCP to D
TCP to D

TOR Circuit

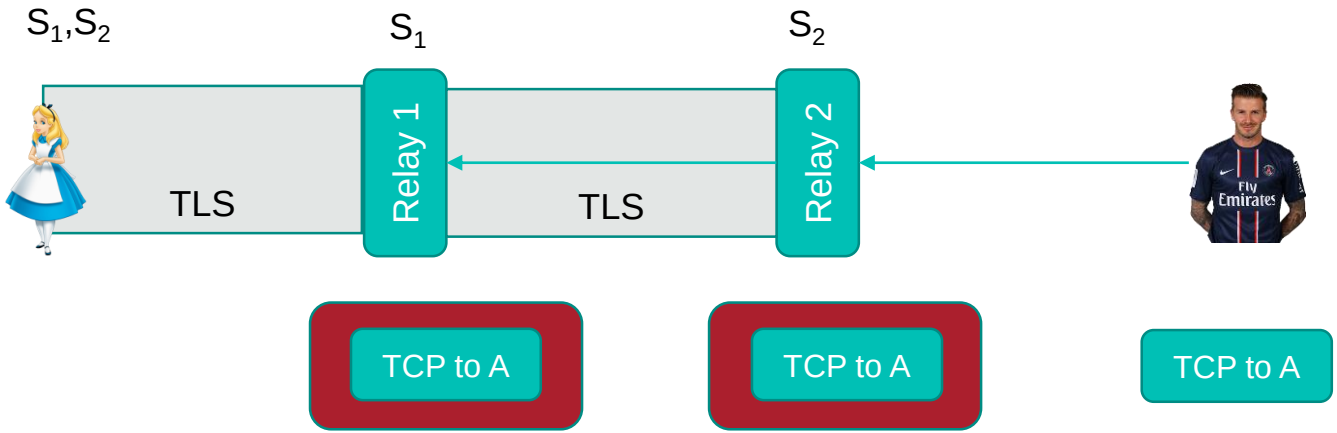


TCP to A

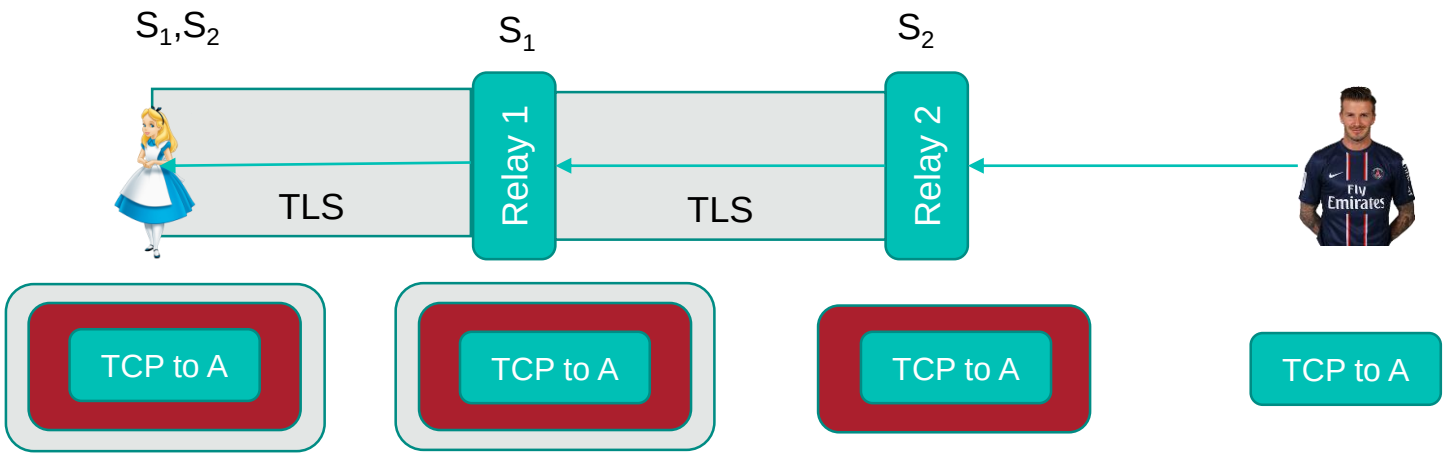
TOR Circuit



TOR Circuit


S_1,S_2
S_1
S_2
TLS
Relay 1
TLS
Relay 2
Fly Emirates
TCP to A
TCP to A
TCP to A

TOR Circuit


S_1,S_2
S_1
S_2
TLS
Relay 1
TLS
Relay 2
Fly Emirates
TCP to A
TCP to A
TCP to A
TCP to A

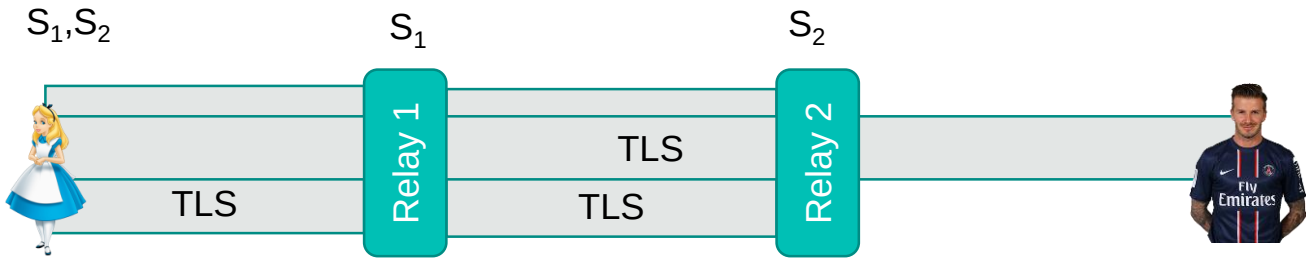
University of BRISTOL

Careful

Messages between end relays and destination is unencrypted!

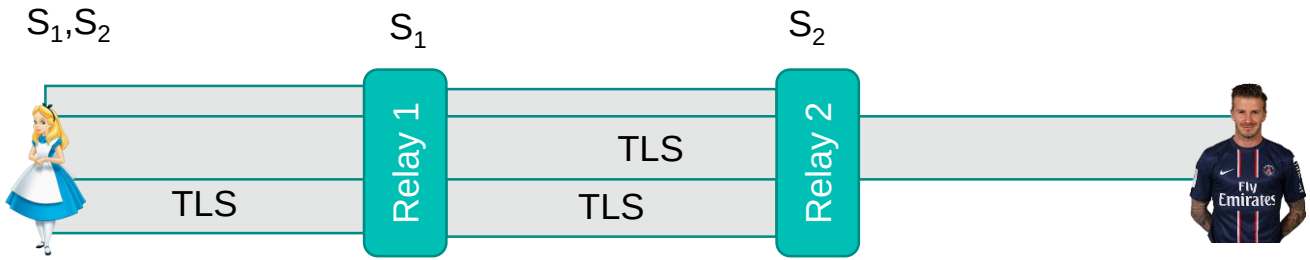
bristol.ac.uk

TOR Circuit



- Carry TCP packets
- Alice can establish an encrypted connection with David over TOR relays
  - e.g. HTTPS/TLS
- None of the relay can see content exchanged between Alice and David
- Relay 1 knows Alice send Data
- Relay 2 knows someone talk to David
- Things we need to be careful about?

TOR Circuit



- Alice can establish an encrypted connection with David over TOR relays
  - e.g. HTTPS/TLS
- None of the relay can see content exchanged between Alice and David
- Relay 1 knows Alice send Data
- Relay 2 knows someone talk to David
- Things we need to be careful about?
  - DNS
  - Certificate verification
  - Need to make sure it goes through TOR

Remember end-service can track you!

- End-servers can track you!
  - Cookies
  - Browser/Machine ID etc…
  - Browser used is important!
- That also include advertisements etc…
- … or leaving information about oneself online

Remember end-service can track you!

- End-servers can track you!
  - Cookies
  - Browser/Machine ID etc…
  - Browser used is important!
- That also include advertisements etc…
- … or leaving information about oneself online

Directory Authorities

- A few of them
- Used to download a list of known relays
- Consensus protocol to decide trusted relays

Directory Authorities

- A few of them
- Used to download a list of known relays
- Consensus protocol to decide trusted relays
- A majority of authorities needs to be trustworthy
  - Classic consensus problem

TOR vulnerabilities

- It is very hard to deanonymize everyone all the time
- … however, definitely possible to deanonymize some person sometimes

TOR vulnerabilities

- Passive attacks
  - Size, timing (the more you can observe the easier)
    - Possible if observe in relay and out relay
    - Either own a lot of relay so you have high change to be picked
    - … or be able to observe the network
  - Service fingerprint
    - Build pattern of size/timing of a service response (e.g. Facebook)
    - Observe entry node and try to match
    - You can learn which users is accessing service you care about

TOR vulnerabilities

Homework/cool project:
Look at fingerprinting as a min to deanonymization.

- Passive attacks
  - Size, timing (the more you can observe the easier)
    - Possible if observe in relay and out relay
    - Either own a lot of relay so you have high change to be picked
    - … or be able to observe the network
  - Service fingerprint
    - Build pattern of size/timing of a service response (e.g. Facebook)
    - Observe entry node and try to match
    - You can learn which users is accessing service you care about

TOR vulnerabilities

Homework/potential exam question:
Discuss: why it is a bad idea to have entry and exit nodes in the same country or owned by the same entity?

- Passive attacks
  - Size, timing (the more you can observe the easier)
    - Possible if observe in relay and out relay
    - Either own a lot of relay so you have high change to be picked
    - … or be able to observe the network
  - Service fingerprint
    - Build pattern of size/timing of a service response (e.g. Facebook)
    - Observe entry node and try to match
    - You can learn which users is accessing service you care about

TOR vulnerabilities

- Active attacks
  - Steal key for TLS encryption between relay
    - High cost attack
    - Rotate keys regularly
  - Iterated compromise
    - i.e. identifying relays one after the other and compromising/coercing them
    - Change circuit regularly
    - Cross border (make coercion harder)
  - Run Relay
    - If attackers control a large number of relays it is likely he could have both ends
    - Need to own a significant portions of relays
    - Cost barrier?

TOR vulnerabilities

- Active attacks
  - Smear attacks
    - Purpose is to force end-nodes to shutdown (e.g. to increase portion of end-nodes controlled by an attacker)
    - Make request to legally questionable service
    - End-nodes need to either have policy to filter this…
    - … or be able to take the heat
    - Running other type of relay is ok
  - DOS on directory authority
    - Could stop the network
  - Run/Compromise directory authority
    - List attacker-controlled relays
    - Consensus is used to decide which relays are used
    - Would need large number of directory servers controlled by the attacker
    - … but see above?

TOR vulnerabilities

Homework/potential exam question:
Discuss: what is the danger of running a TOR exit relay.

- Active attacks
  - Smear attacks
    - Purpose is to force end-nodes to shutdown (e.g. to increase portion of end-nodes controlled by an attacker)
    - Make request to legally questionable service
    - End-nodes need to either have policy to filter this…
    - … or be able to take the heat
    - Running other type of relay is ok
  - DOS on directory authority
    - Could stop the network
  - Run/Compromise directory authority
    - List attacker-controlled relays
    - Consensus is used to decide which relays are used
    - Would need large number of directory servers controlled by the attacker
    - … but see above?

TOR vulnerabilities

- Active attacks
  - Block Relay
    - Everyone can access directory authorities
    - Filter relays IP in traffic
    - China does this
    - Countermeasure: TOR bridge (not advertised)
  - Block bridge
    - Look at SSL traffic
    - Connection to TOR bridge had some recognizable artefact
    - Try to connect to it and see if it is a TOR bridge
    - China did it again
    - Countermeasure: some shared secret between TOR client and Bridge

TOR vulnerabilities

Homework/potential exam question:
Discuss: arm race to prevent access to TOR network.

- Active attacks
  - Block Relay
    - Everyone can access directory authorities
    - Filter relays IP in traffic
    - China does this
    - Countermeasure: TOR bridge (not advertised)
  - Block bridge
    - Look at SSL traffic
    - Connection to TOR bridge had some recognizable artefact
    - Try to connect to it and see if it is a TOR bridge
    - China did it again
    - Countermeasure: some shared secret between TOR client and Bridge

Plan

- Anonymity
- Unlikability
- Unobservability
- VPN
- TOR
- TOR Circuit
- TOR Directory Authority
- TOR vulnerabilities

Conclusion

- Internet anonymity is hard
- Possible to hide from network observation
- Can identify some people sometimes
  - Everyone, all the time is much harder
- Active area of research
  - Check the papers on the github repo
- There is obviously a dark side to TOR-like software
  - Check work by Brian Neil Levine at UMass

University of BRISTOL

Thank you, questions?

Office MVB 3.26

bristol.ac.uk