University of BRISTOL

Systems Security

COMSM1500

Anonymous communication

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

28,748 views | Mar 30, 2017, 08:40am

Now Those Privacy Rules Are Gone, This Is How ISPs Will Actually Sell Your Personal Data

Thomas Brewster Forbes Staff

Security

I cover crime, privacy and security in digital and physical forms.

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

28,748 views | Mar 30, 2017, 08:40am

Now Those Privac
Gone, This Is How
Actually Sell Your

Thomas Brewster Forbes Staff
Security
I cover crime, privacy and security in digita

'Extreme surveillance' becomes UK law with barely a whimper

Investigatory Powers Act legalises range of tools for snooping and hacking by the security services

most viewed

Live Brexit deal: Tusk confirms November summit on 'lose-lose situation' - Politics live

Elton John brings star quality to John Lewis Christmas advert

Theresa May's Brexit plan: a split cabinet, a split party and a split nation

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

28,748 views | Mar 30, 2017, 08:40am

Now Those Privac
Gone, This Is How
Actually Sell Your

Thomas Brewster Forbes Staff
Security
I cover crime, privacy and security in digita

'Extreme surveilla
with barely a whim

Investigatory Powers Act legalises
hacking by the security services

UK has six months to rewrite snooper's charter, high court rules

Judges say Investigatory Powers Act is incompatible with EU law after legal challenge by Liberty

most viewed

Live Brexit deal: Tusk confirms November summit on 'lose-lose situation' - Politics live

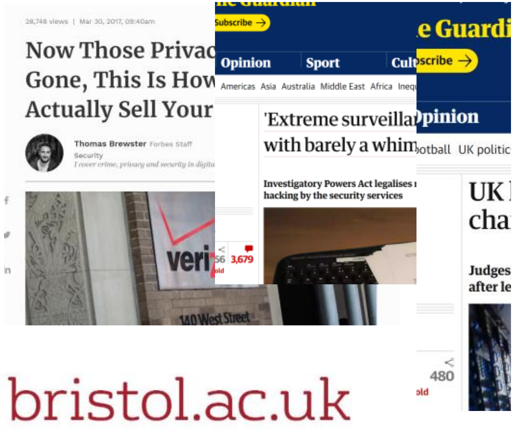
Elton John brings star quality to John Lewis Christmas advert

Brexit deal: key points from the draft withdrawal agreement

Subscribe →
Opinion
Sport
Cult
Americas Asia Australia Middle East Africa Inequ
56
3,679
old
veri
140 West Street
e Guardian
scribe →
Search jobs Dating My account Search UK edition
The Guardian
Opinion Sport Culture Lifestyle More
otball UK politics Environment Education Society Science Tech Global development Cities Obituaries
480
old

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



28,748 views | Mar 30, 2017, 08:40am

Now Those Privac
Gone, This Is How
Actually Sell Your

Thomas Brewster Forbes Staff
Security
I cover crime, privacy and security in digita

140 West Street

Subscribe →
Opinion | Sport | Cult
Americas Asia Australia Middle East Africa Inequ

'Extreme surveilla
with barely a whim

Investigatory Powers Act legalises
hacking by the security services

56 3,679

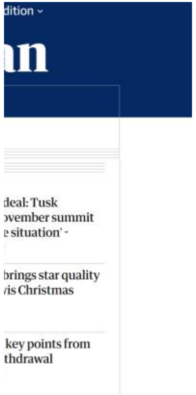
e Guardi
Subscribe →
Opinion
otball UK politic

UK
cha

Judges
after le

480

bristol.ac.uk



dition ⌄

an

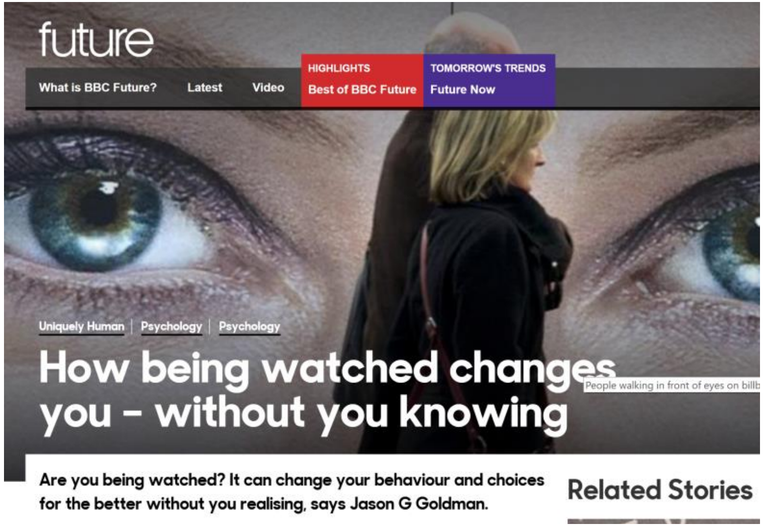
deal: Tusk
ovember summit
e situation' -

brings star quality
is Christmas

key points from
thdrawal

Observation is problematic

- Being observed affect your behavior

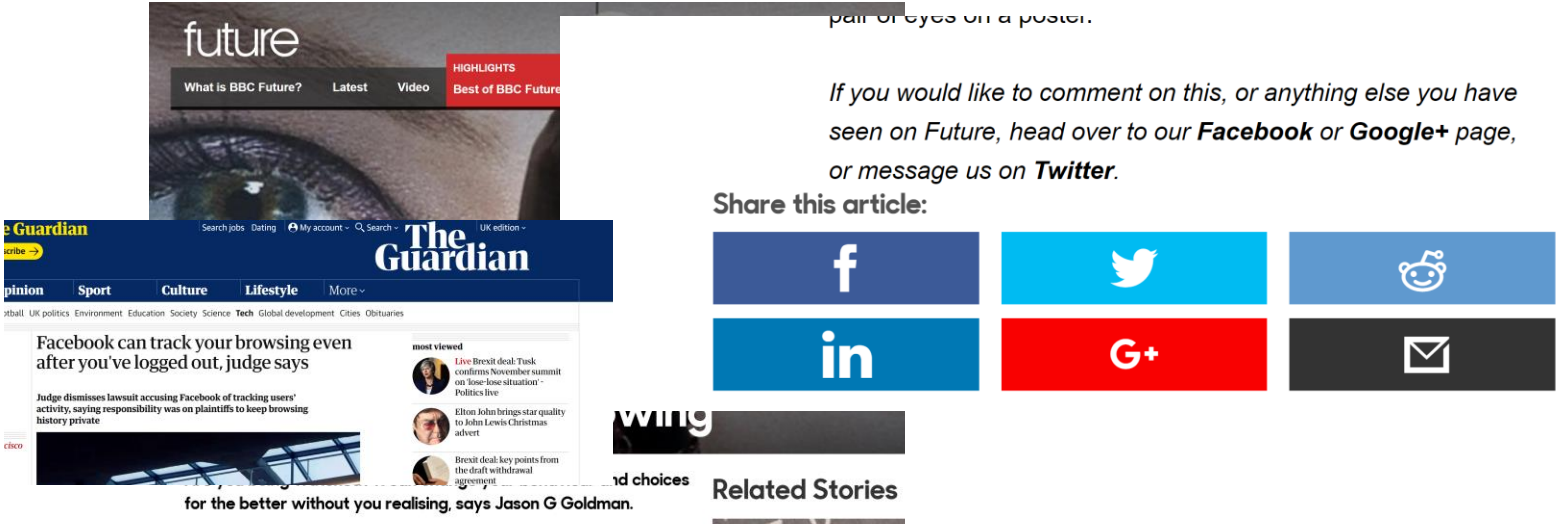


How being watched changes you – without you knowing

Are you being watched? It can change your behaviour and choices for the better without you realising, says Jason G Goldman.

Observation is problematic Some irony…

- Being observed affect your behavior



pair of eyes on a poster.

*If you would like to comment on this, or anything else you have seen on Future, head over to our **Facebook** or **Google+** page, or message us on **Twitter**.*

Facebook can track your browsing even after you've logged out, judge says

Judge dismisses lawsuit accusing Facebook of tracking users' activity, saying responsibility was on plaintiffs to keep browsing history private

Live Brexit deal: Tusk confirms November summit on 'lose-lose situation' - Politics live

Elton John brings star quality to John Lewis Christmas advert

Brexit deal: key points from the draft withdrawal agreement

nd choices for the better without you realising, says Jason G Goldman.

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…)

Plan

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

Anonymity

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

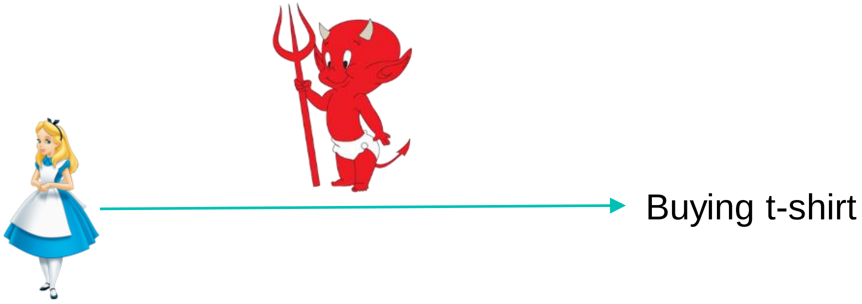
Anonymity

- 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



Buying t-shirt

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

Other important concepts

- Unlikability
  - 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

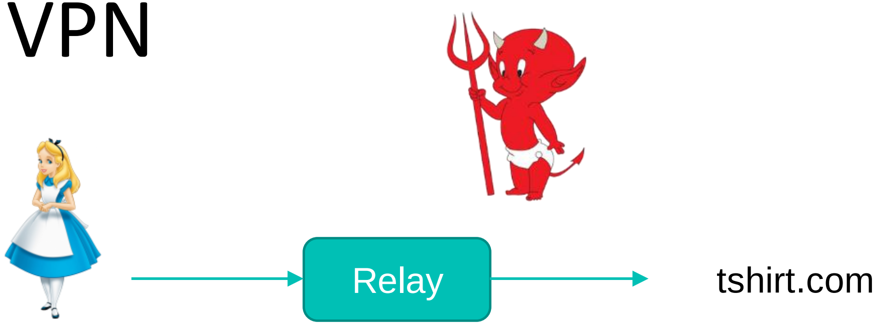
TOR

The Onion Router

VPN

Buying t-shirt

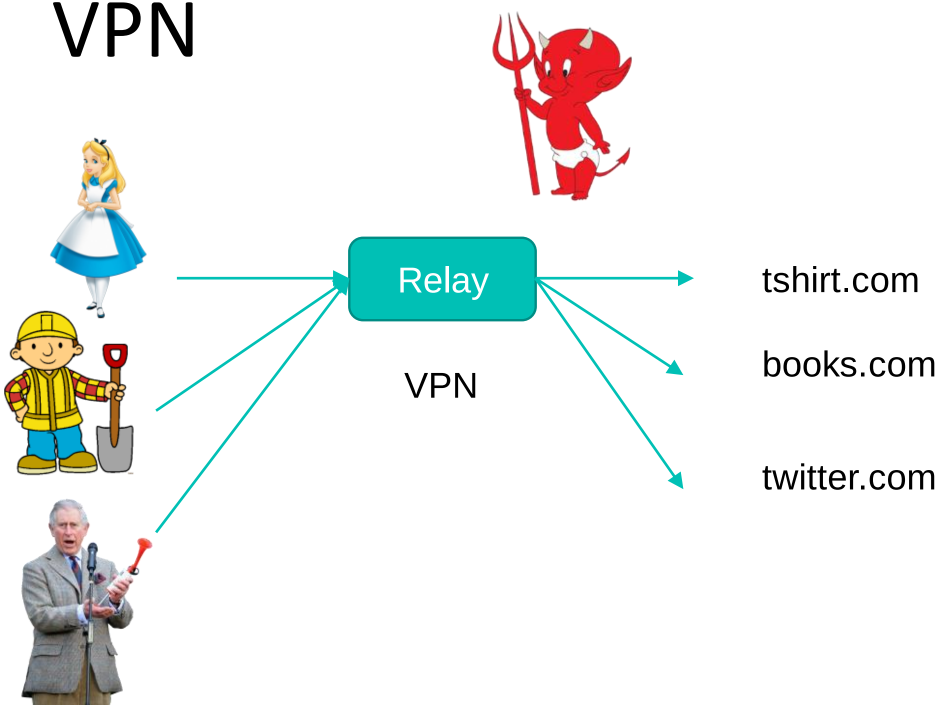
VPN



Relay

tshirt.com

VPN



Relay

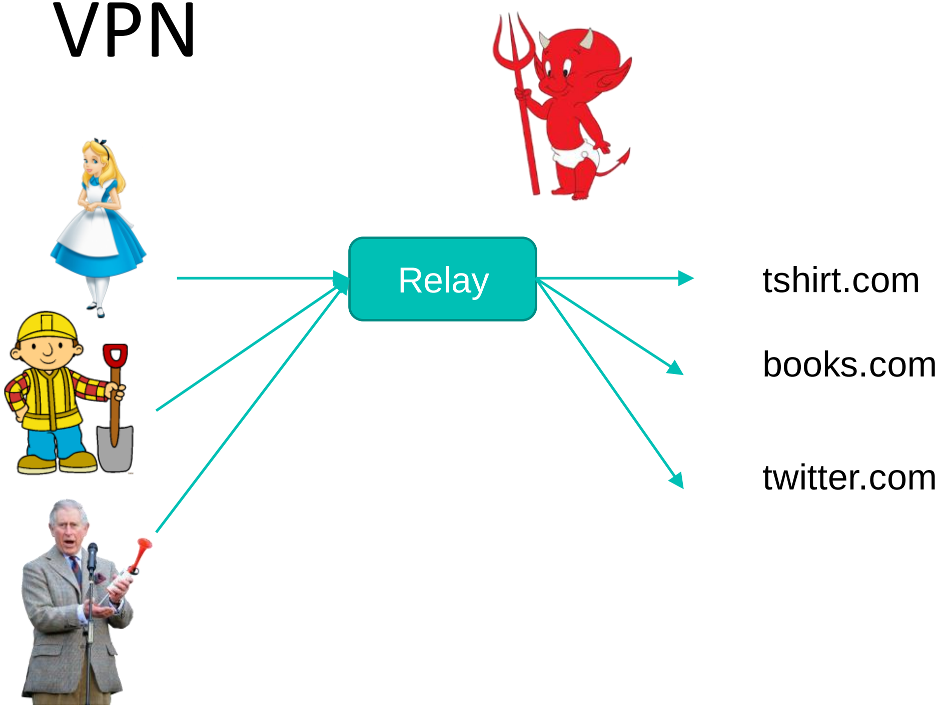
VPN

tshirt.com

books.com

twitter.com

VPN



Relay

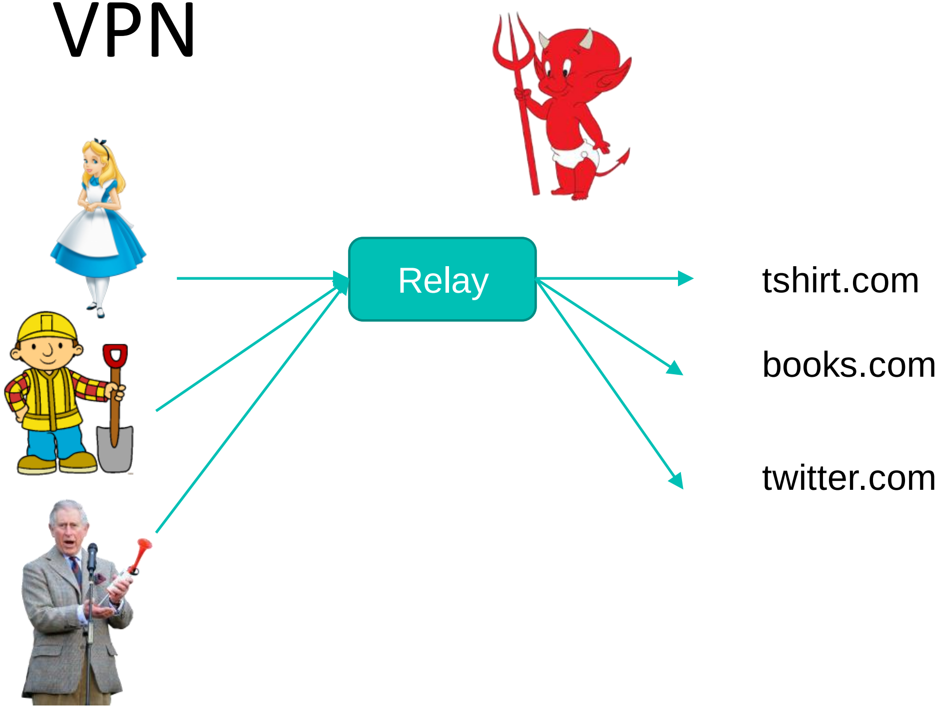
tshirt.com

books.com

twitter.com

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

VPN



Relay

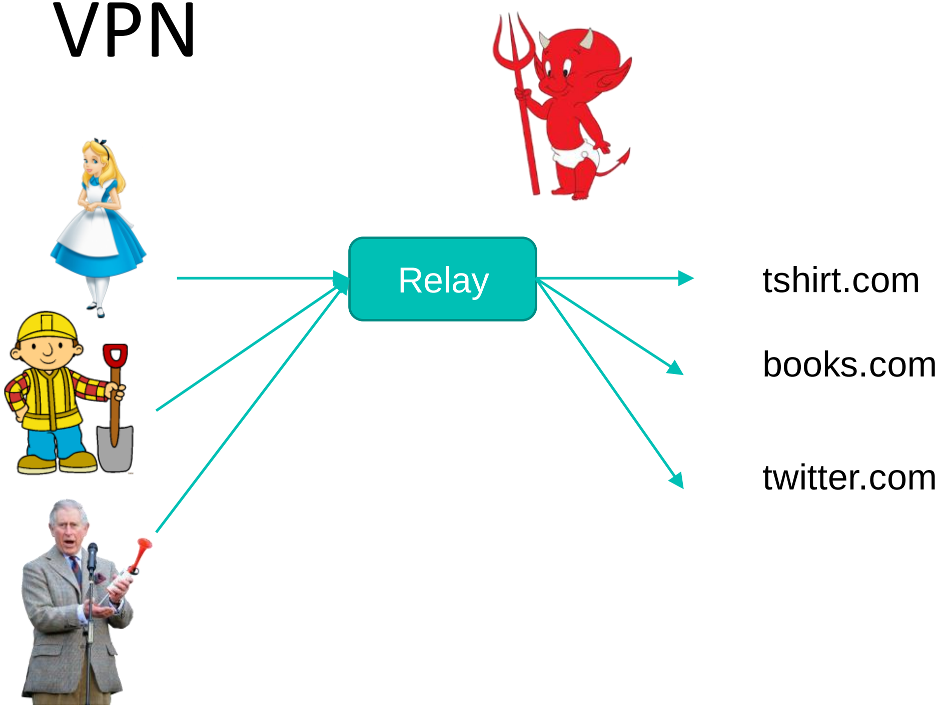
tshirt.com

books.com

twitter.com

- 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



Relay

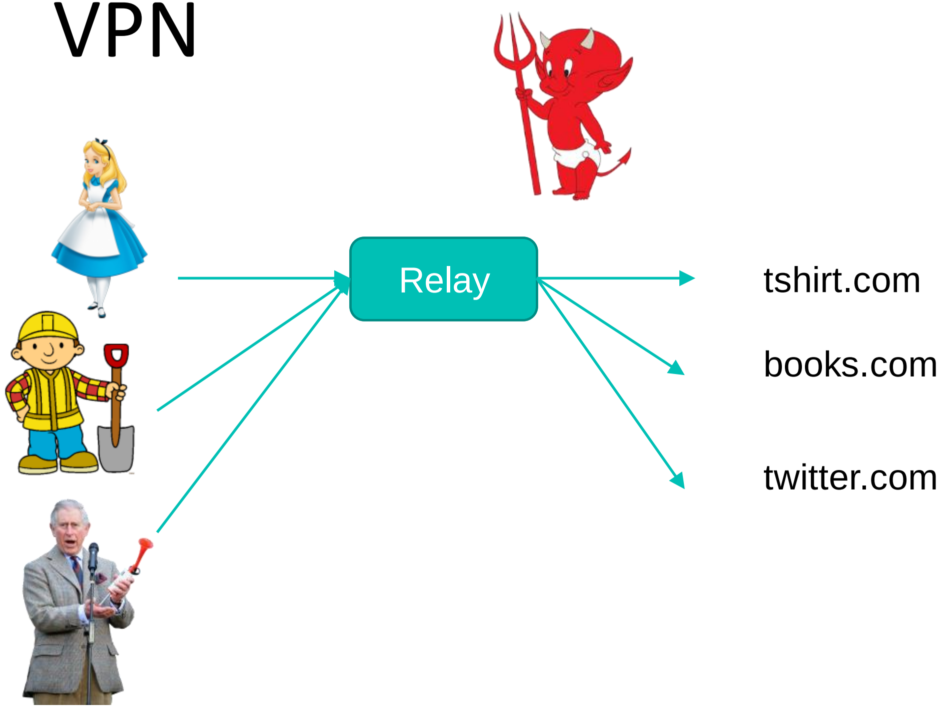
tshirt.com

books.com

twitter.com

- 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



Relay

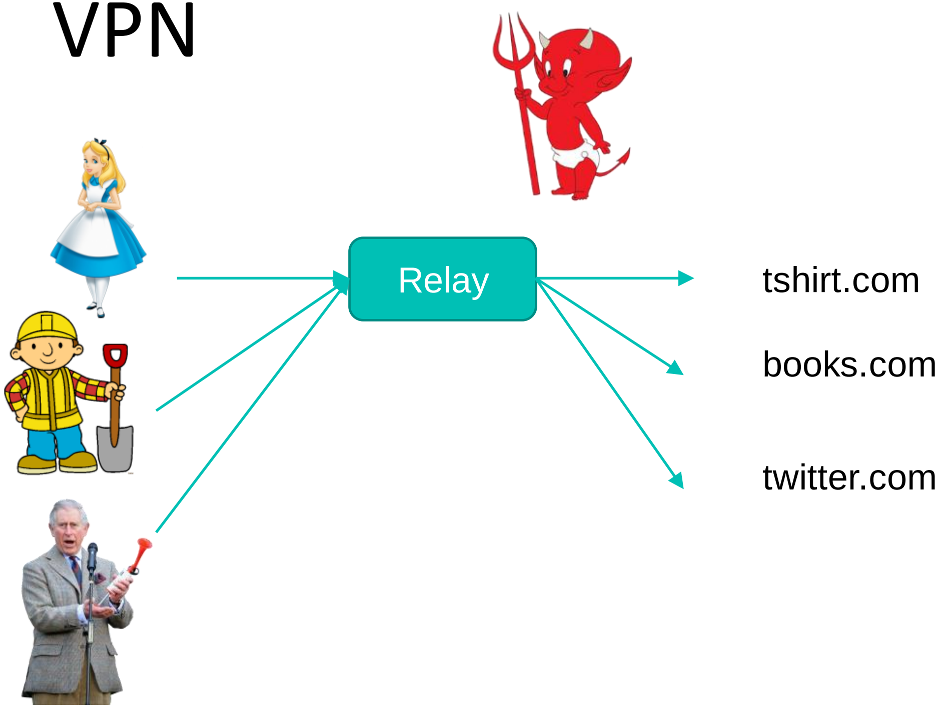
tshirt.com

books.com

twitter.com

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

VPN



Relay

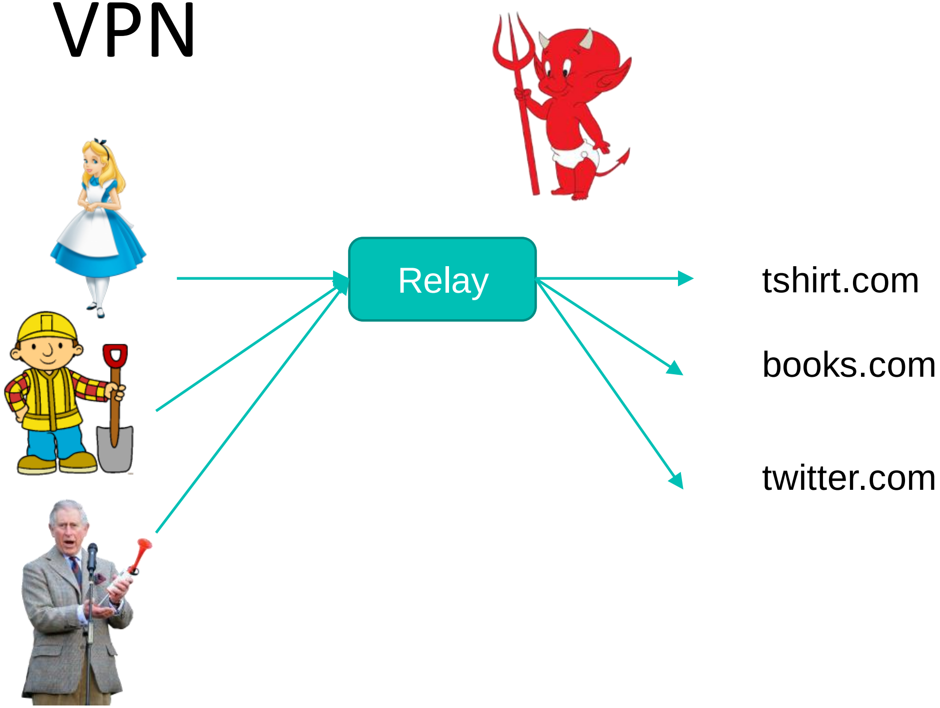
tshirt.com

books.com

twitter.com

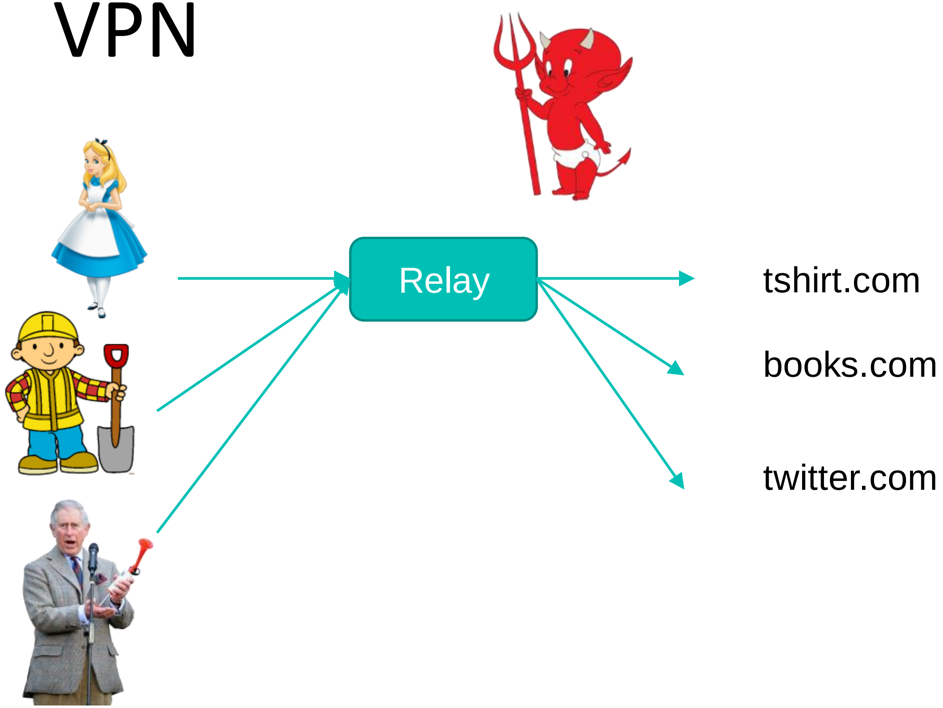
- Harder to know what Alice is doing
- Need to trust the relay
  - Single relay is obviously a problem
  - If it is compromised no guarantees

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
- Trusted VPN are fine
  - e.g. universities run one, if you need to access some info from country that bans some content

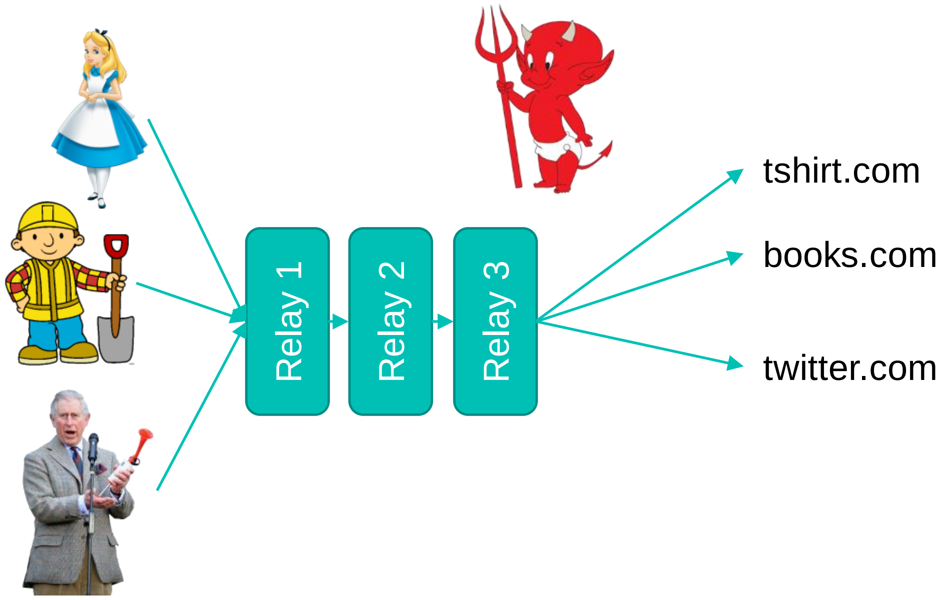
VPN



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

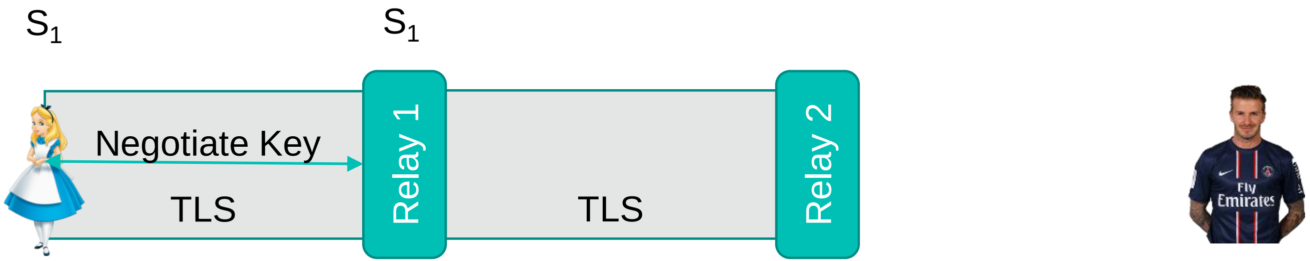


- Harder to know what Alice is doing
- Need to trust the relay
  - Relay 1 now Alice is doing something
  - Relay 3 now some is talking to t-shirt.com
  - Attacker need to control 1 and 3 to be really harmful
  - Hard/Costly to achieve
  - Discussed further later…

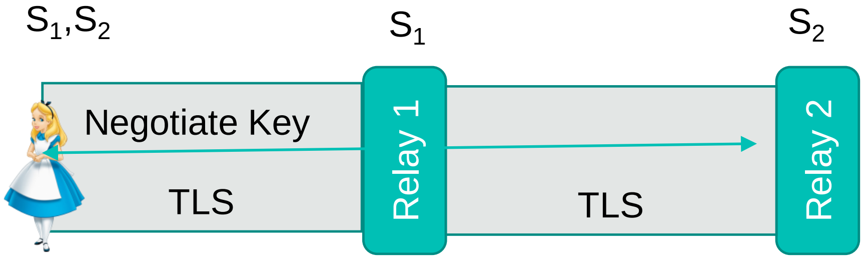
TOR Circuit

Relay 1
Relay 2

TOR Circuit



TOR Circuit



S_1,S_2

S_1

S_2

Negotiate Key

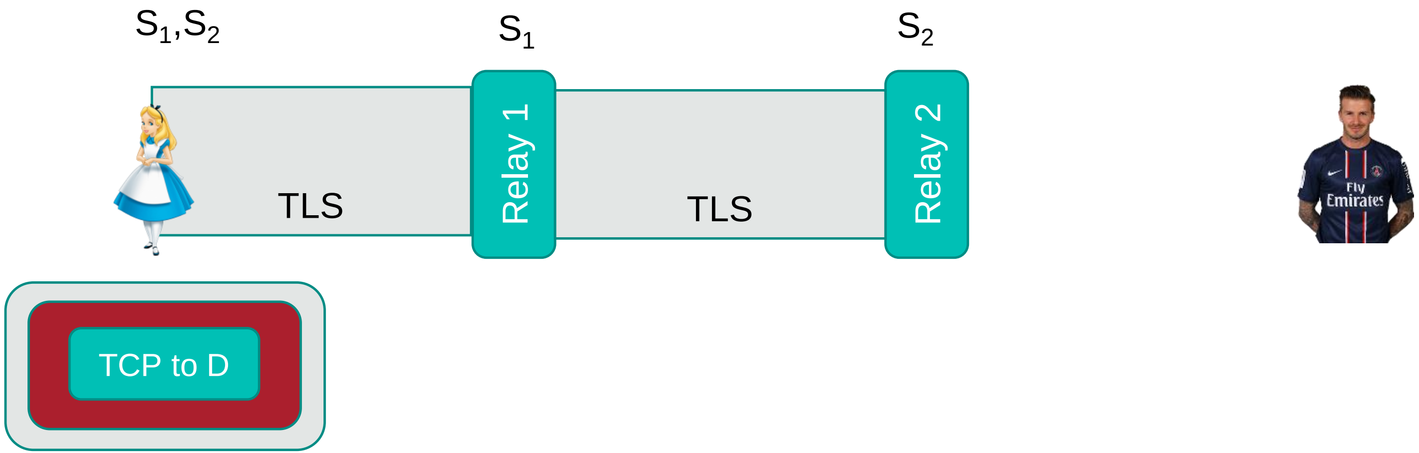
TLS

Relay 1

TLS

Relay 2

TOR Circuit



S_1,S_2

S_1

S_2

TLS

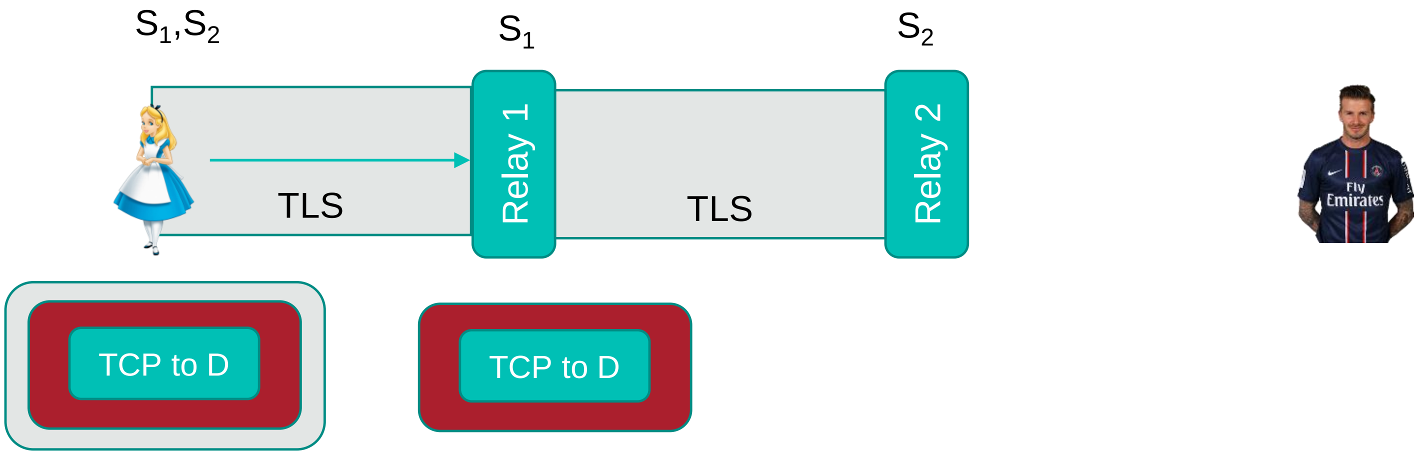
Relay 1

TLS

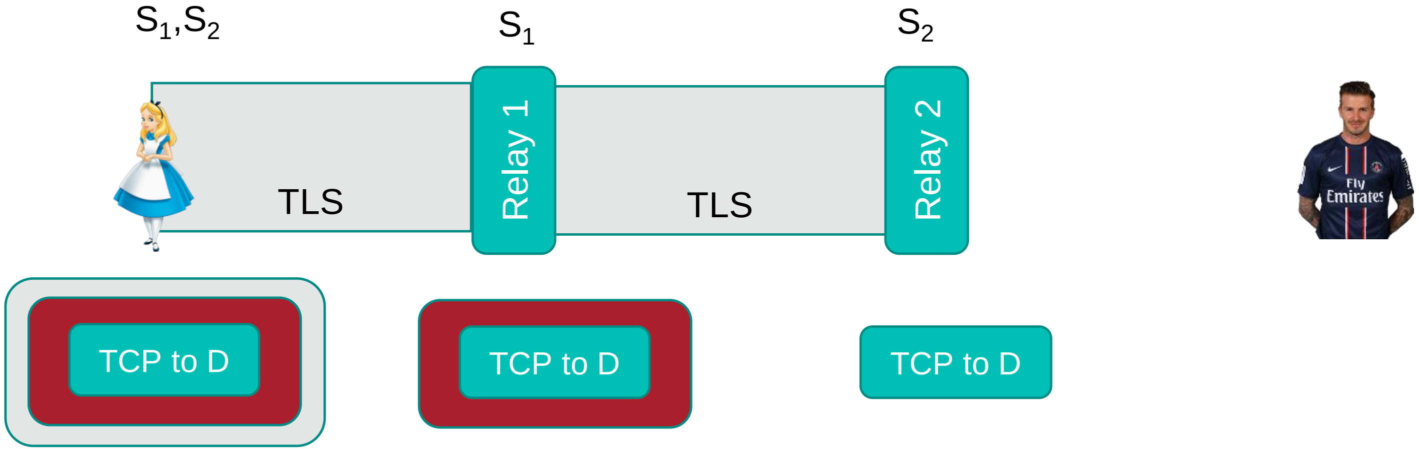
Relay 2

TCP to D

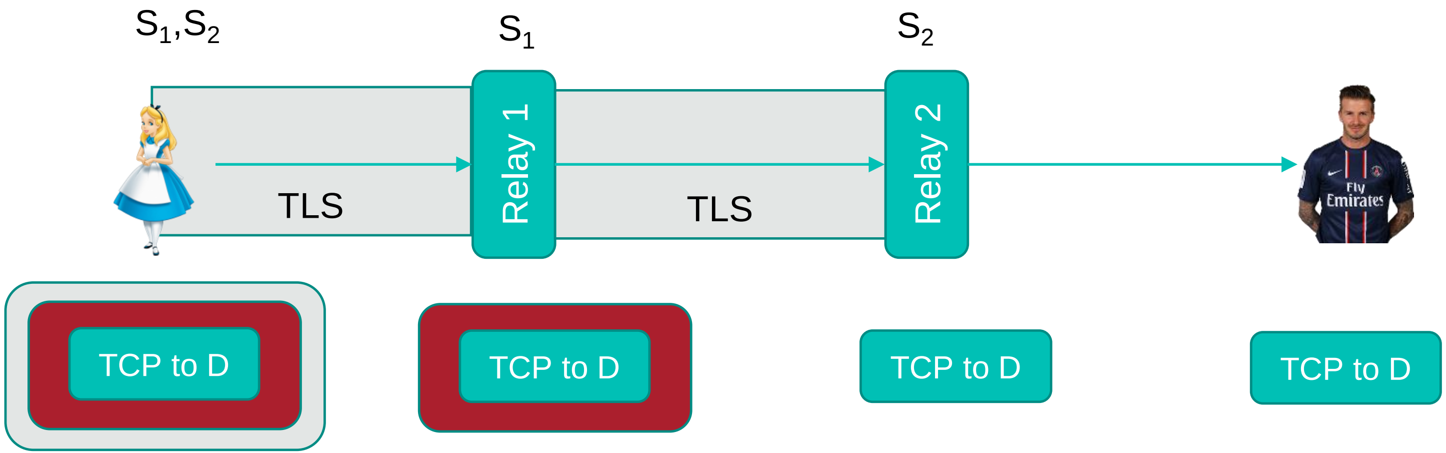
TOR Circuit



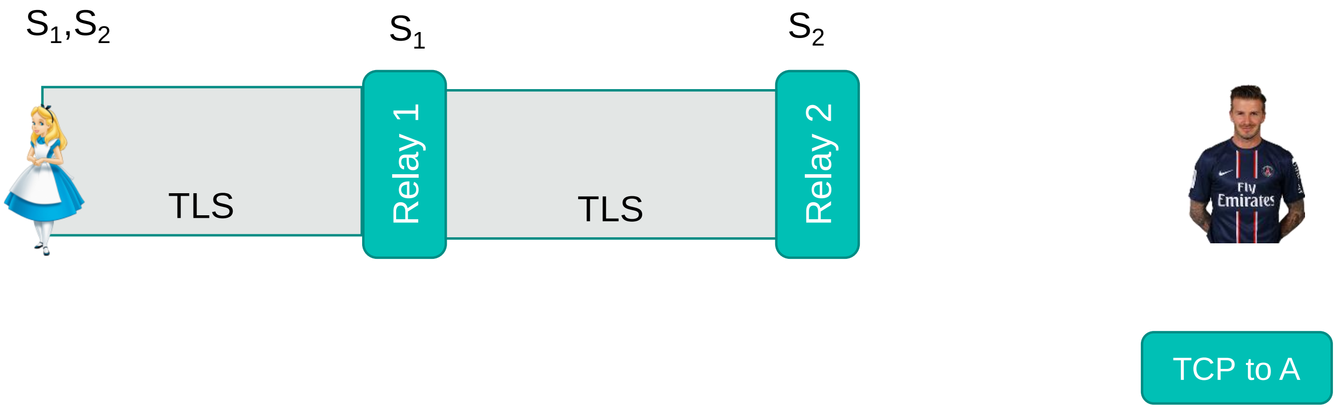
TOR Circuit



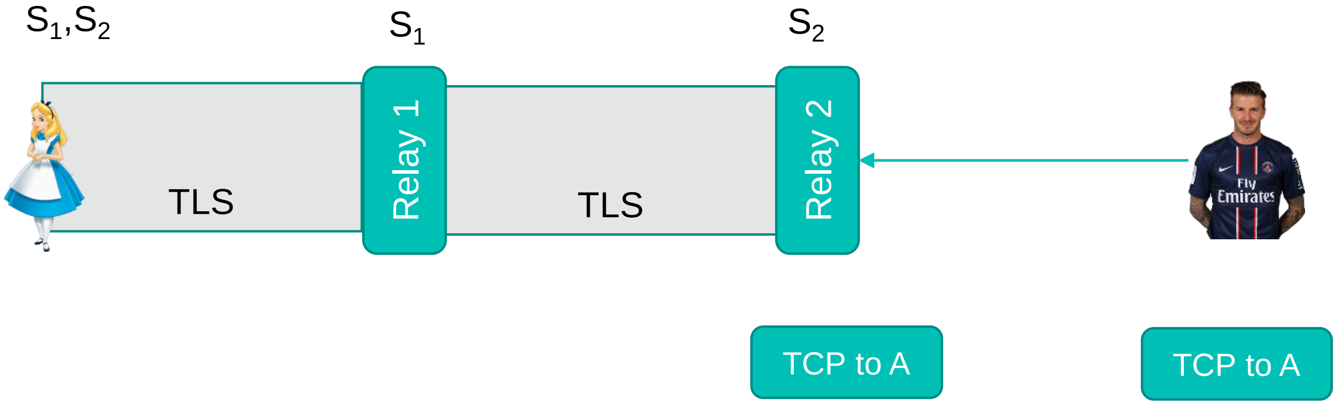
TOR Circuit


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

TOR Circuit



TOR Circuit



S_1,S_2

S_1

S_2

TLS

Relay 1

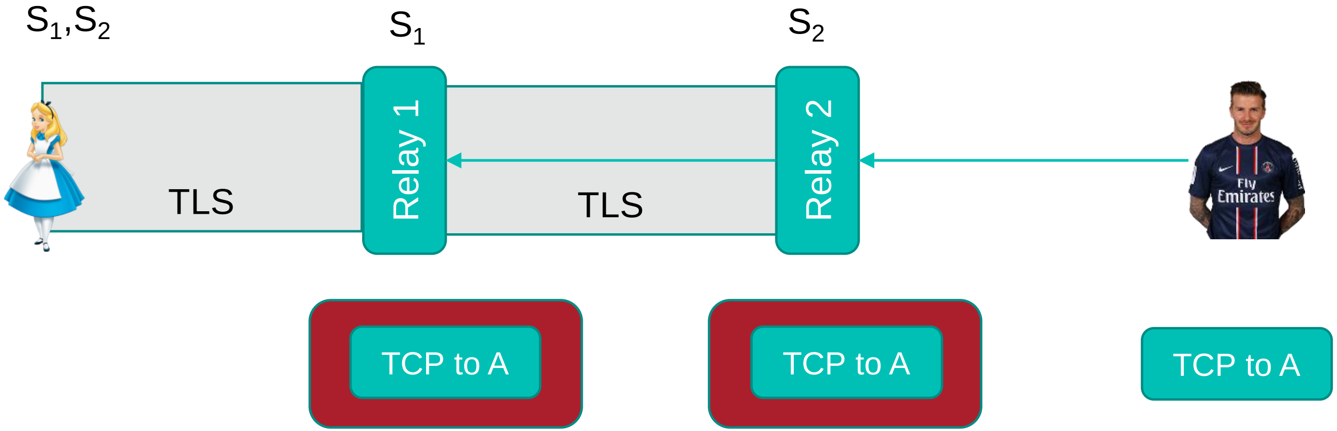
TLS

Relay 2

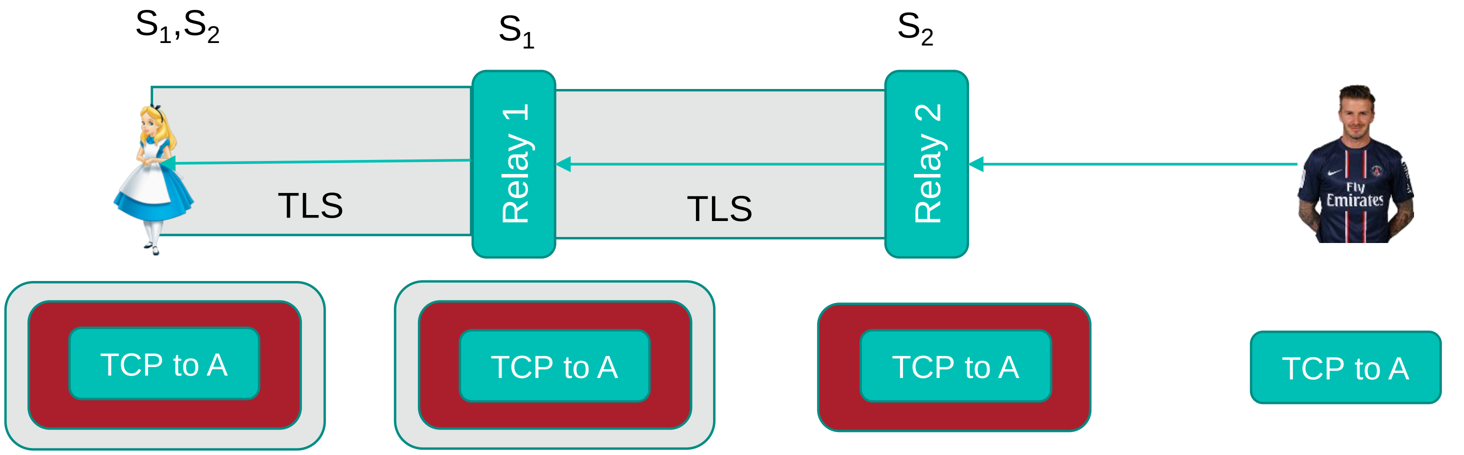
TCP to A

TCP to A

TOR Circuit



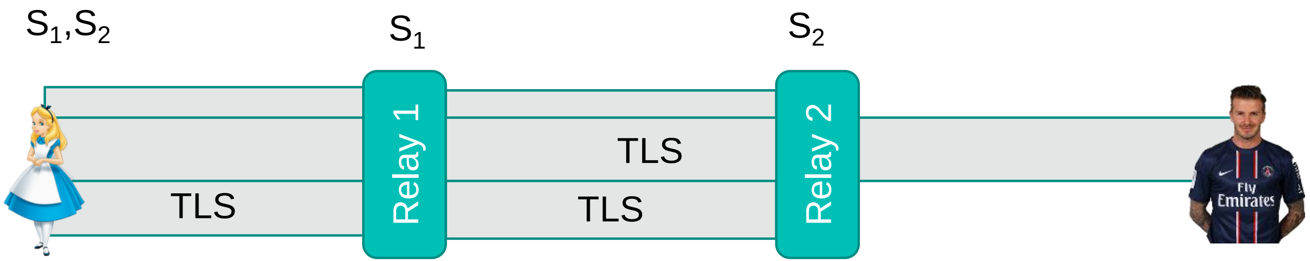
TOR Circuit


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

Careful

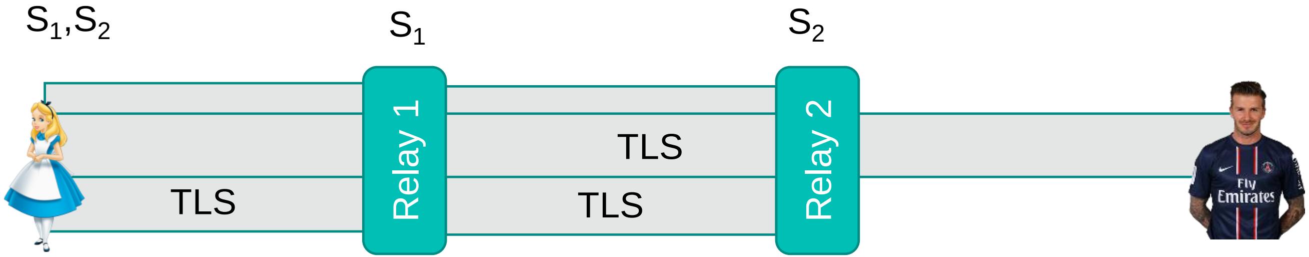
Messages between end relays and destination is unencrypted!

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
- Thins we need to be careful about?

TOR Circuit



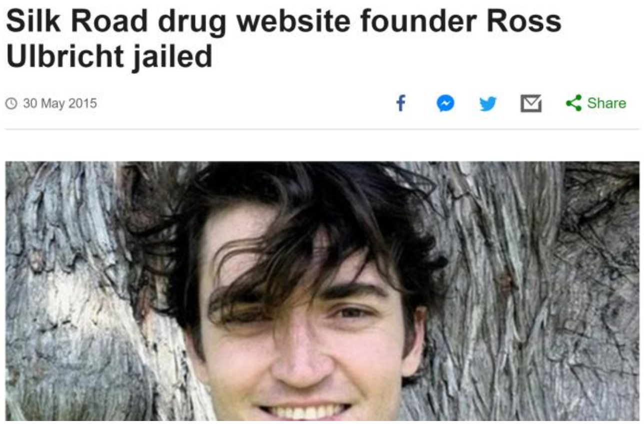
- Alice can establish an encrypted connection with David over TOR relays
    - e.g. HTTPS/TLS
- None of the relay can see content exchanged between Alice and David
- Relay 1 knows Alice send Data
- Relay 2 knows someone talk to David
- Thins we need to be careful about?
    - DNS
    - Certificate verification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



Silk Road drug website founder Ross Ulbricht jailed

30 May 2015

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 chance 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

- 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 controller 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 controller 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 aterfact
    - 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 aterfact
    - 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