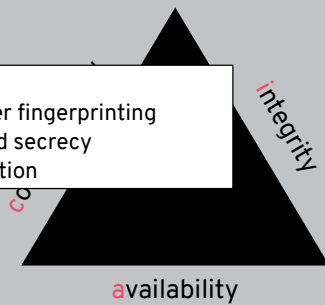


SECURITY (COMP0141): TOR

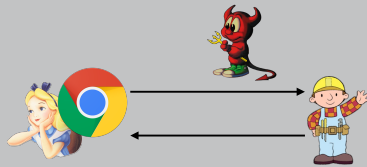


CONFIDENTIALITY, REVISITED

- Tor
- browser fingerprinting
- forward secrecy
- revocation



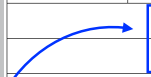
THREAT MODEL



Is there an eavesdropper spying on your web traffic?

3

ENCRYPTED WEB TRAFFIC

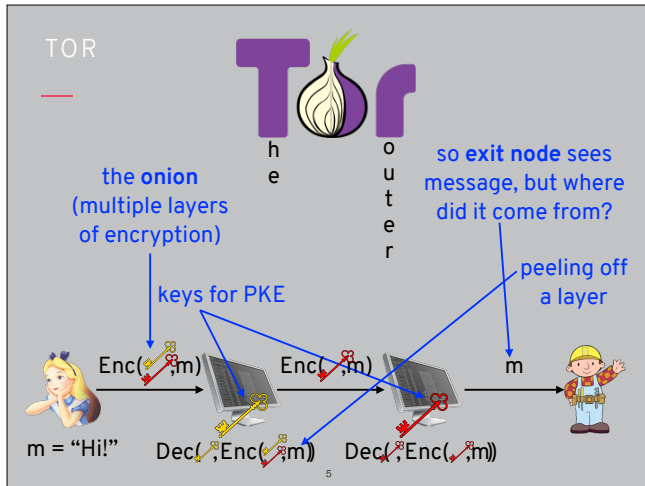
4-bit version	4-bit Header len	8-bit type of service	16-bit total length (in bytes)	
16-bit identification			3-bit flags	13-bit fragment offset
8-bit time to live (TTL)	8-bit protocol		16-bit header checksum	
				
Bob's IP address				
Alice's IP address				
Options (if any)				
Enc(sk, <Content at hi.html (part 1 of N)>)				

HTTPS can hide content...

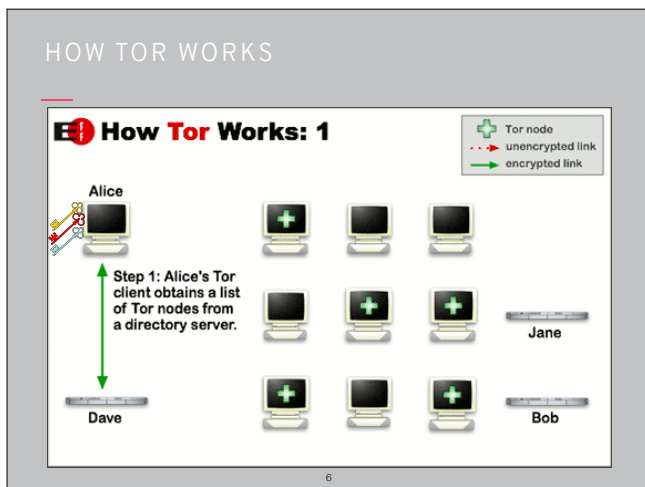
...but this still reveals a lot of information!

4

Remember we saw that encrypted traffic can hide contents from an eavesdropper, but packets act like both an envelope and a letter so we're still revealing who messages are being sent to and from.

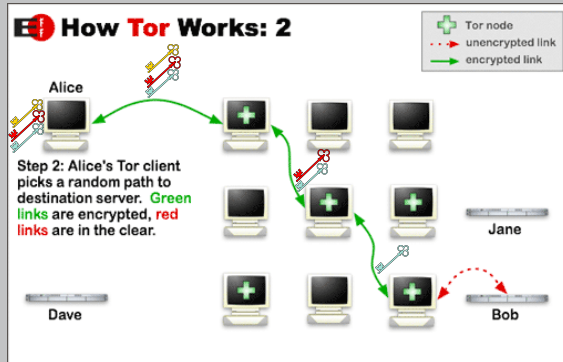


Onion routing hides this information by encrypting the message along the way, and then having an intermediate series of servers decrypt a component (thus “peeling off” a layer of the “onion”). By the time the message is revealed by the exit node, it can’t be linked back to Alice unless all intermediate servers collude. The most common onion router is Tor (https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29)



When Alice first uses Tor, she gets a set of public keys for possible intermediate servers

HOW TOR WORKS

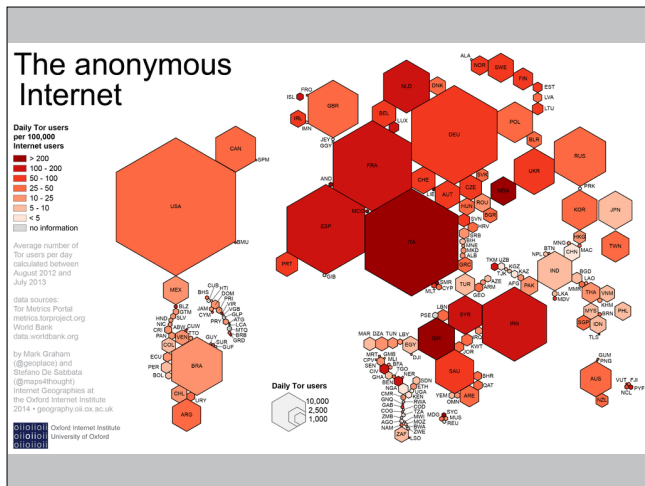


She then chooses a path through the network with three intermediate nodes and uses their keys to form the onion, and more generally to perform onion routing: the next node is revealed to the node peeling off their layer. The link at the end has to be unencrypted because Bob might be a normal site that doesn't deal with ciphertexts

QUESTIONS ABOUT TOR

q: what if I want to ban Tor users from my site?
a: block exit nodes. (Wikipedia, etc. do this.)

Governments block Tor as a form of censorship, you also might want to block Tor for non-censorship reasons, like dealing with graffiti, spam, etc.



QUESTIONS ABOUT TOR

q: what if I want to ban Tor users from my site?

a: block exit nodes. (Wikipedia, etc. do this.)

q: does Tor also hide the content of my web traffic?

a: no! just routing; for content need to use HTTPS.

Tor and HTTPS serve different purposes (hiding envelope vs. hiding letter)

ENCRYPTED WEB TRAFFIC

4-bit version	4-bit Header len	8-bit type of service	16-bit total length (in bytes)	
16-bit identification			3-bit flags	13-bit fragment offset
8-bit time to live (TTL)	8-bit protocol		16-bit header checksum	
<div><div></div><div>Bob's IP address.</div></div>				
<div><div></div><div>Alice's IP address</div></div>				
Options (if any)				
Enc(sk,<Content at hi.html (part 1 of N)>)				

HTTPS can hide content...

...and Tor can hide this.

11

QUESTIONS ABOUT TOR

q: what if I want to ban Tor users from my site?

a: block exit nodes. (Wikipedia, etc. do this.)

q: does Tor also hide the content of my web traffic?

a: no! just routing; for content need to use HTTPS.

q: does Tor just let me visit normal websites anonymously?

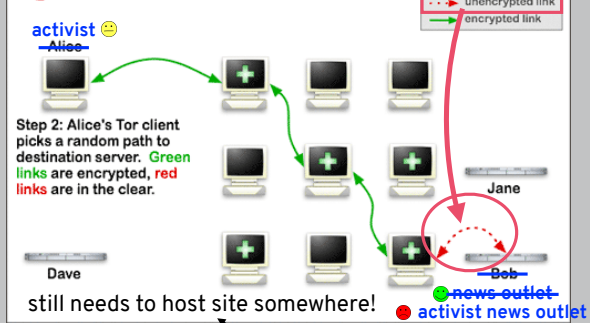
a: no. **Hidden services** exist only within Tor network.

12

Tor hidden services (<https://www.torproject.org/docs/onion-services.html>) do not reveal the IP address of the server

TOR HIDDEN SERVICES

How Tor Works: 2



This is important for people hosting illicit content, such as underground markets like Silk Road, since having an unencrypted link leaves their service vulnerable as their IP address is revealed in the clear

TOR HIDDEN SERVICES



There are also legitimate hidden services; for example, Facebook runs one. Here we could think of using a hidden service kind of like using a VPN in that it allows you to get around something like a firewall

CONFIDENTIALITY, REVISITED

- Tor
- **browser fingerprinting**
- forward secrecy
- revocation

