FIT 1047

Introduction to computer systems, networks and security

Overview for today

- Gaming

- Privacy Enhancing Technologies

- The Dark Net

Gaming hacks

- Obvious target for hackers.

- "Hacking" often does not require any hacking skills at all

- Just install some script/software/plugin/etc.

Gaming hacks

Goals:

- Advantage in games

- Fun

- Annoy others

- Financial

- E-sports success

Virtual Worlds / Virtual Economies

- Virtual items can have real-world value

- Cheat/hack to get more items

- Scams to steal items from other users (e.g. trading in CS:GO)

- Sell items without transferring them.

How to detect/prevent cheating in games

Difficult in large-scale gaming

- Detection using anti-cheating software

- Player reports

- Build secure games (probably impossible: trade-off between usability and security)

Pevent cheating in e-sports

- High motivation

- Situation similar to doping

- Hardware-based solutions might work

- Soluktions to restricted to tournaments with
players physically present

On problem is the lack of publicly available
comprehensive rulsets.....

Privacy issues

- If a product is free you are the product.

- Companies build large collections of user profiles

- Linking this data provides even more information

- One photo might be enough to identify you and link to yohugeur profile
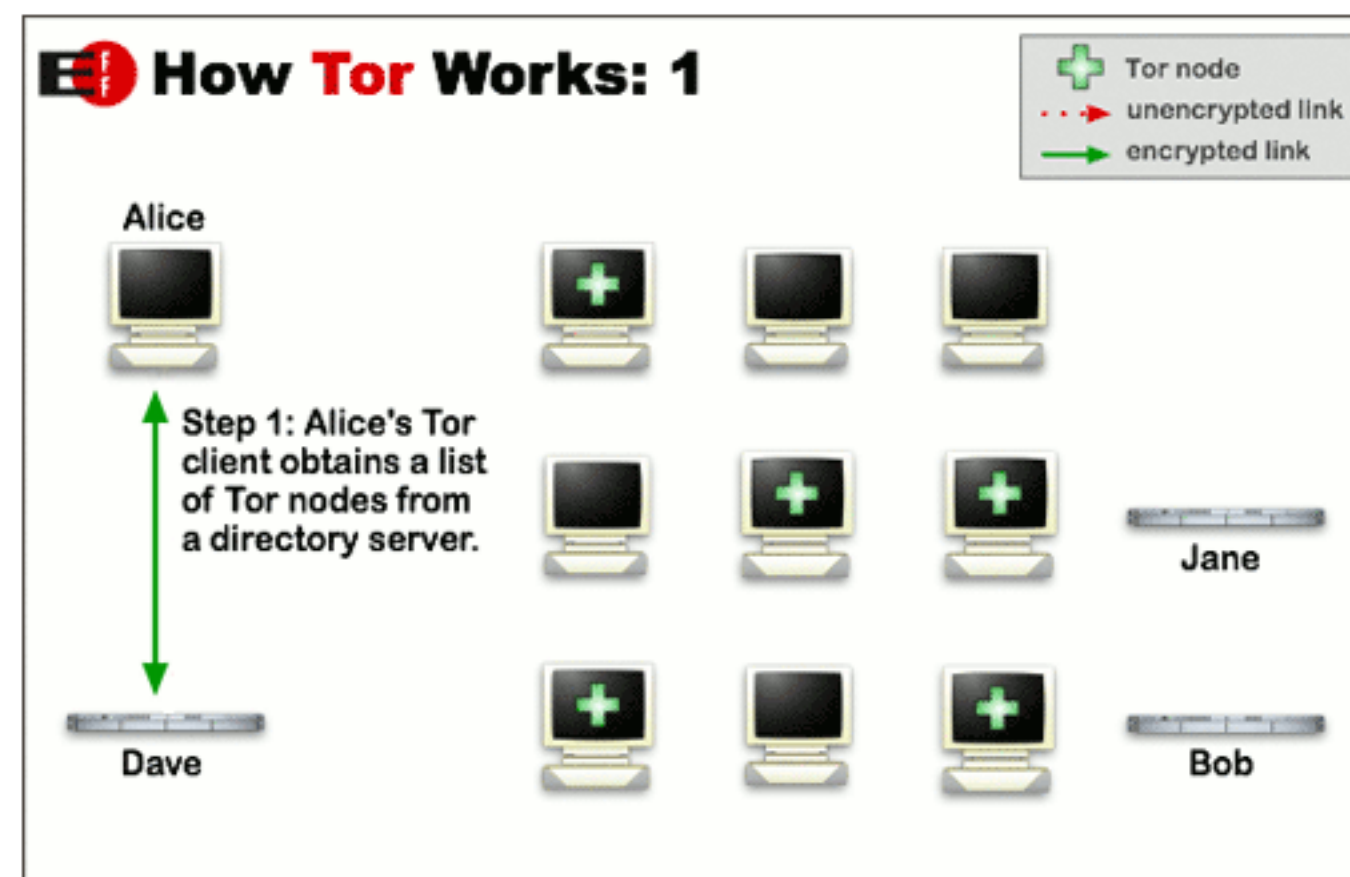
Privacy Enhancing Technologies

- Technologies are available

- They are not used by service providers, but by users

- One example is TOR, The Onion Routing
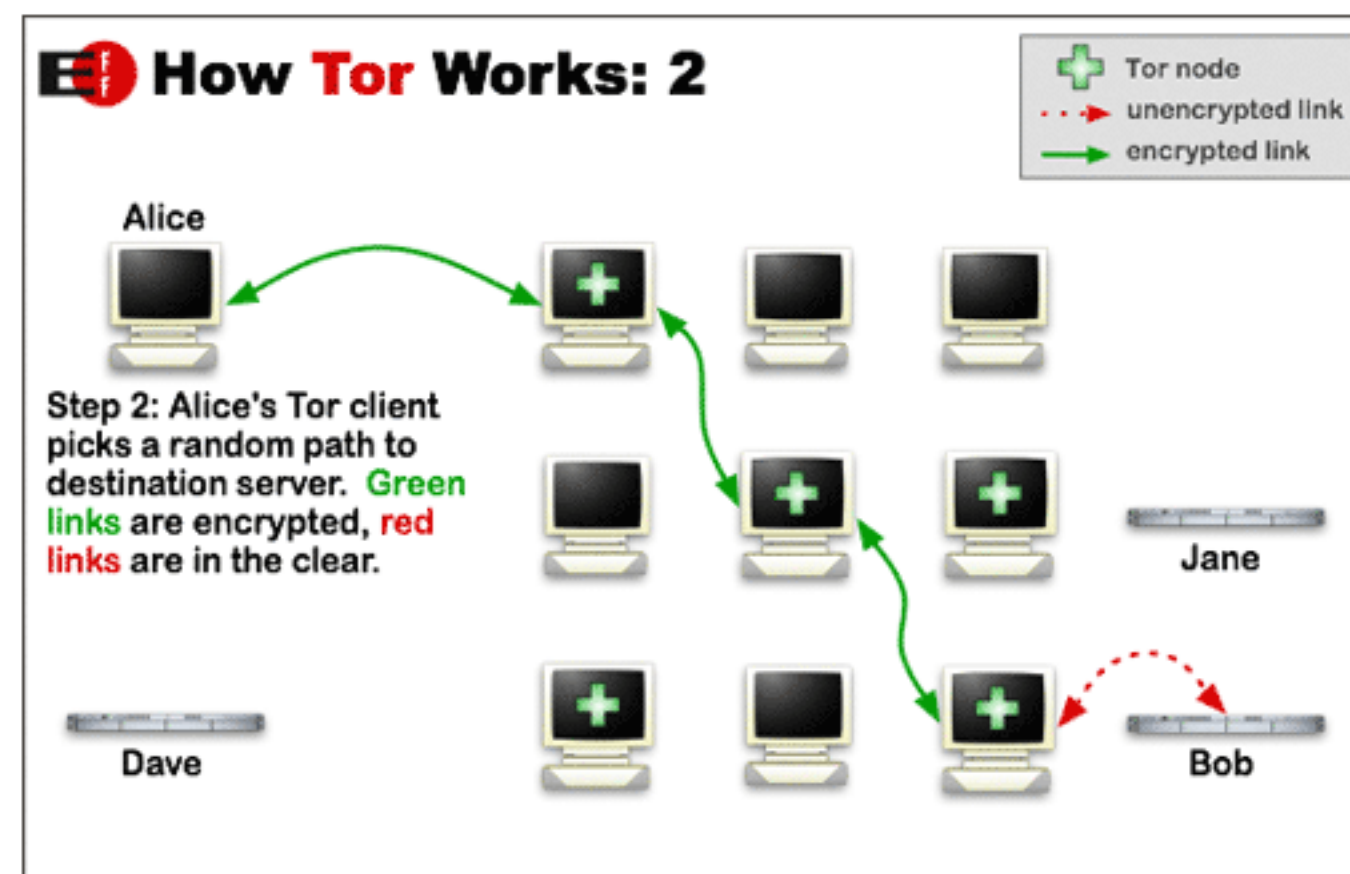
The Onion Router
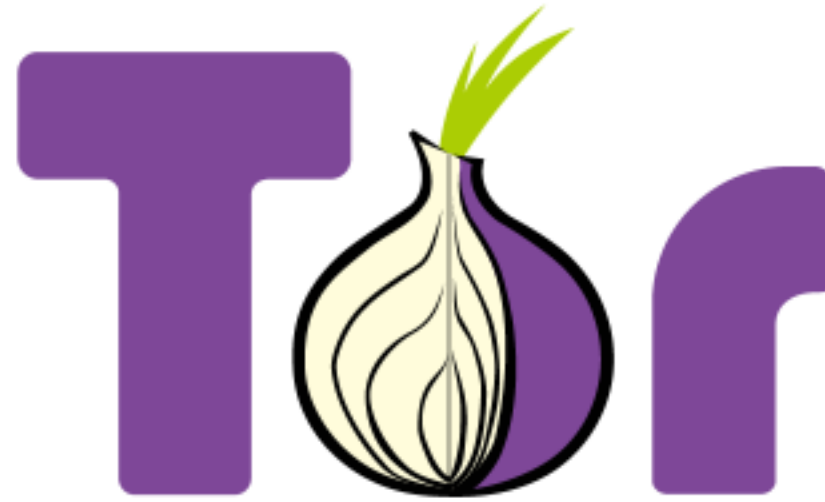
- Developed by US Navy, Protection for secret information

- Useful for:

- Human rights activists, whistleblowers

- For people that just want to have privacy
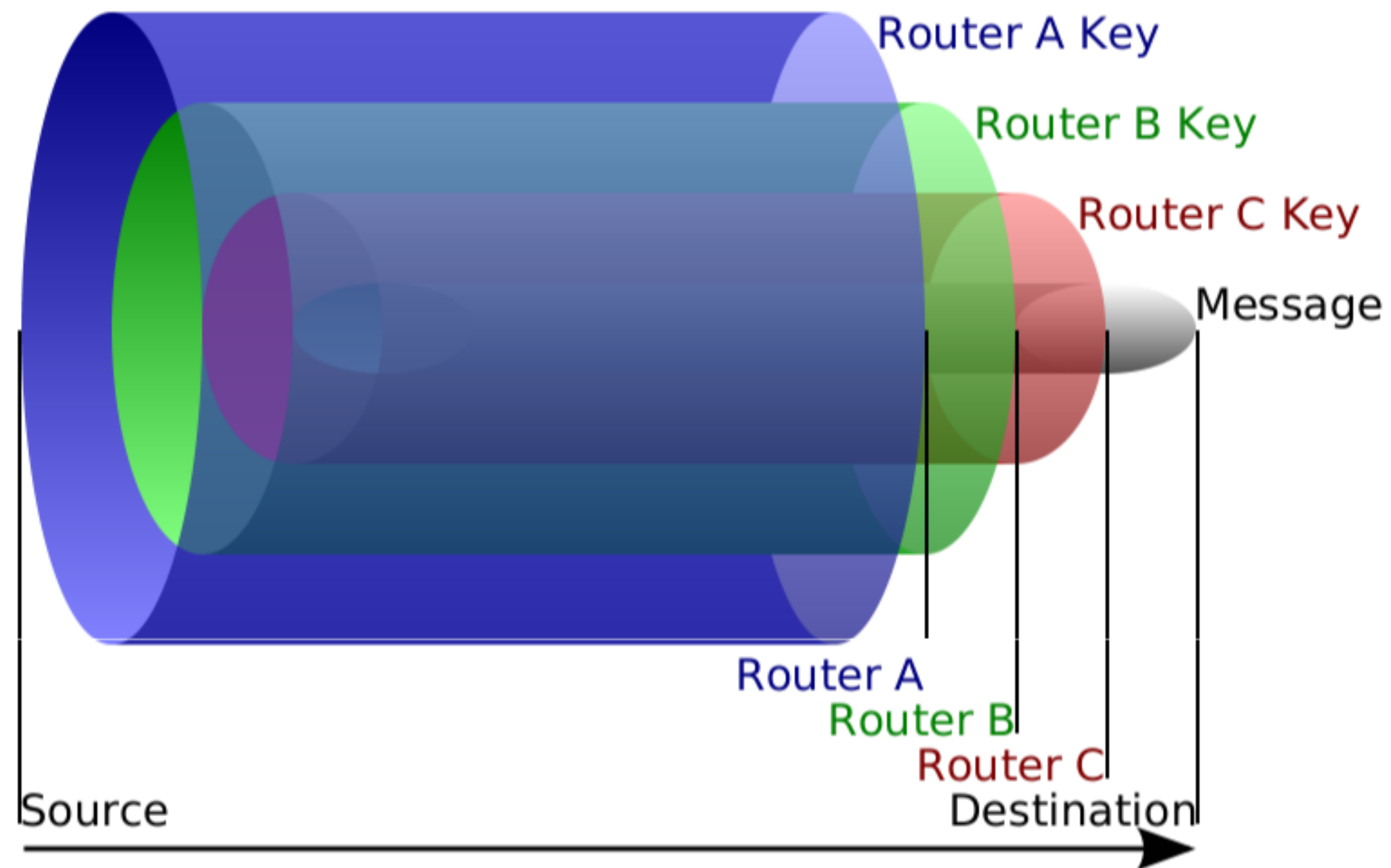
- Also for criminal activities

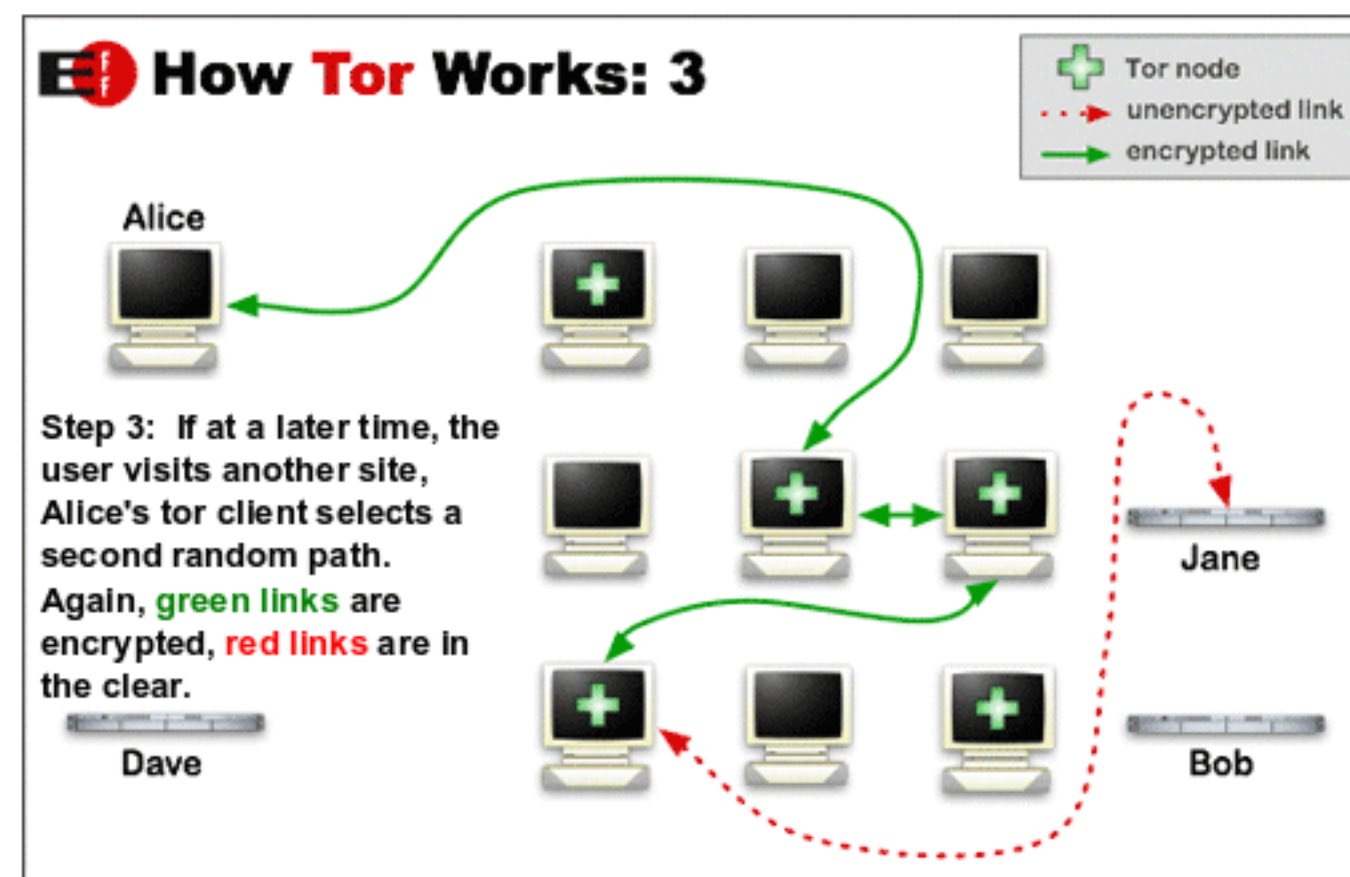# TOR Step 1:

(Electronic Frontier Foundation)

TOR Step 2

(Electronic Frontier Foundation)

TOR The Onion

Router A Key

Router B Key

Router C Key

Message

Router A

Router B

Router C

Source

Destination

(Wikimedia Commons)

TOR Step 3

(Electronic Frontier Foundation)

Deep Web vs Dark Web

Deep Web – All content that is only accessible with known address (might be 99% of all content)

- Cloud Storage

- Private videos

- Data bases

- Other data

Deep Web vs Dark Web

Dark Web – Client and server are hidden (e.g. both sides use TOR)

- Information on weaknesses, exploits, stolen data

- All types of criminal activities

- Lots of things you dont want to see or know about

- But also: Activities of human rights groups

A large part of the dark web is not the evil stuff that tabloid newspapers like to write about.

Risk Assessment

THE ANNUAL DEATH RATE AMONG PEOPLE
WHO KNOW THAT STATISTIC IS ONE IN SIX.

(xkcd.org)

Explanation:

https://www.explainxkcd.com/wiki/index.php/795:_Conditional_Risk