FIT 1047

Introduction to computer systems, networks and security

MONASH University

Overview for today

- Risk management
- Some weaknesses
- Privacy Enhancing Technologies
- The Dark Net

- Risk management basically means to have the right security controls in place
- But: There is a wide range of possible controls:

Risk Assessment; Certification, Accreditation and Security Assessments; System Services and Acquisition; Security Planning; Configuration Management; System and Communications Protection; Personnel Security; Awareness and Training; Physical and Environmental Protection; Media Protection; Contingency Planning; System and Information Integrity; Incident Response; Identification and Authentication; Access Control; and Accountability and Audit

More info at: **https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview/Security-Controls**

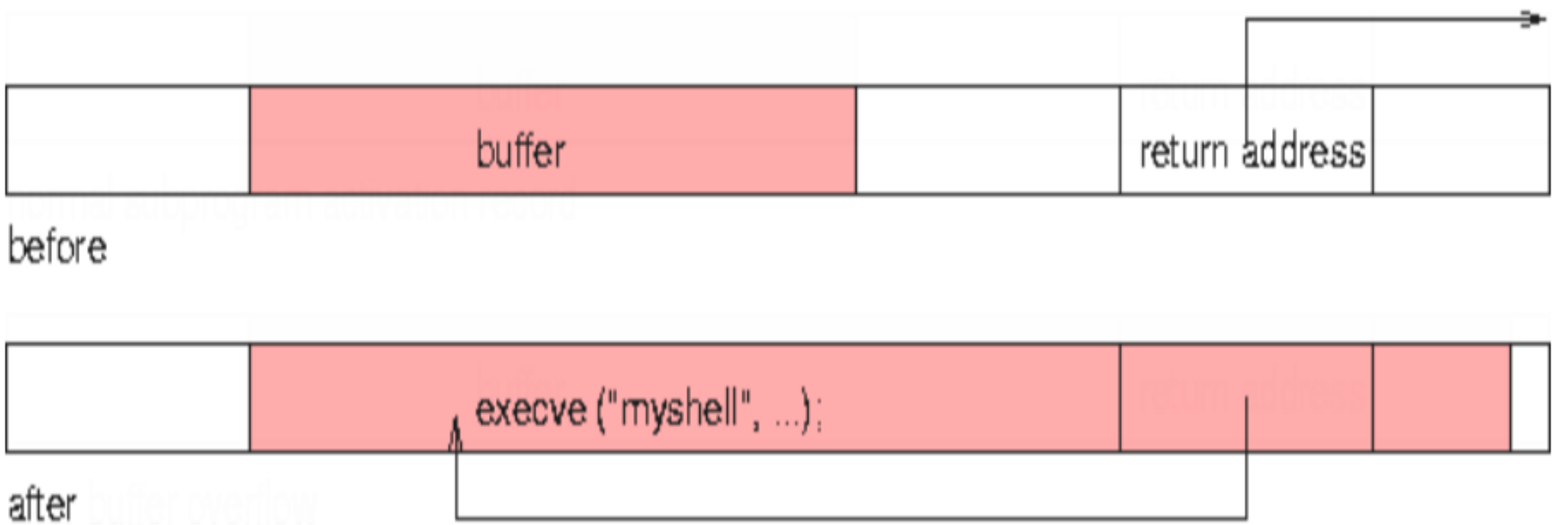
What kind of weaknesses can be exploited?

Some examples:

- Buffer overflow
- Command injection
- Cross-site scripting (XSS)
- SQL Injection

Buffer overflow

Example for an exploit



- Buffer overflow can be possible if input is not properly checked.
- Countermeasures do exist (canary, address randomization,...)

Command Injection

If an application passes on user input to a shell in a bad way, in can be used to execute arbitrary shell commands with the rights of the application process.

Examples at owasp.org (Open Web Applications Security Project):

https://www.owasp.org/index.php/Command_injection

What is Cross-site scripting?

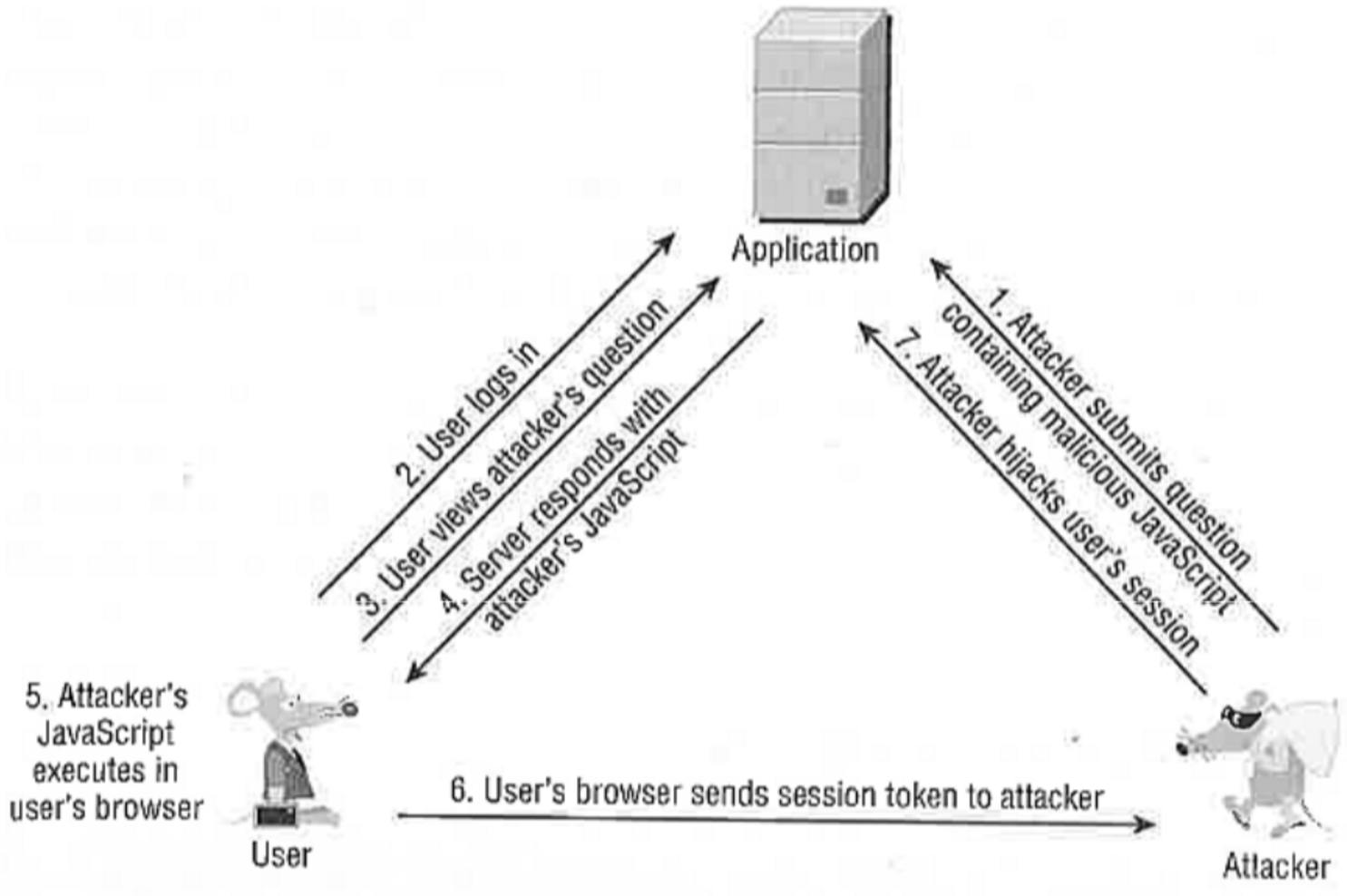
- Usually, browsers don't execute scripts not loaded (directly or indirectly) from the domain of the visited page.
- If an attacker can insert own code to be executed is this cross-site scripting.

How can attacker get script included in the page send from the server?

Let's look at one example:

- Stored XSS attack

Stored XSS attack



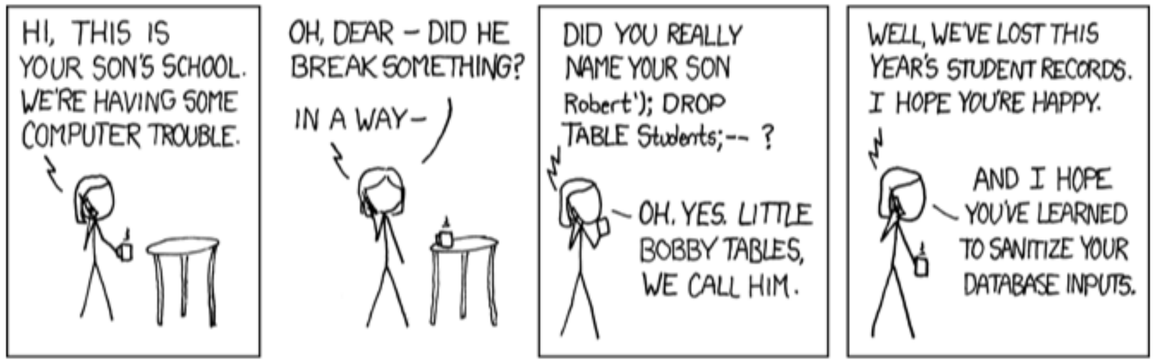
How to prevent XSS?

https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

SQL Injection

This is about attacking SQL databases.

Embed database commands in normal imput



(xkcd.org)

SQL Code that provides # of rows that contain a combination of UserName and password:

```
SELECT Count(*) FROM UsersTable
WHERE UserName= 'Joanne'
AND Password= 'JoannesPassword'
```

Now insert other SQL code and terminate with --

```
SELECT Count(*) FROM UsersTable
WHERE UserName= 'OR 1=1--'
AND Password= "
```

The OR 1=1 always returns TRUE. Thus the query will always return a count greater than zero, resulting in a successful login.

Other attacks

- Attacks via DMA

Direct memory access DMA can potentially be used to read arbitrary parts of memory

Prevention: Don't let anyone just attach devices to your computers.

- Physical (hard-disk access)

With physical (temporary) access, one can directly read from the hard-disk (or write to it) without being logged in.

Prevention: Disk encryption. Self-encrypted disks.

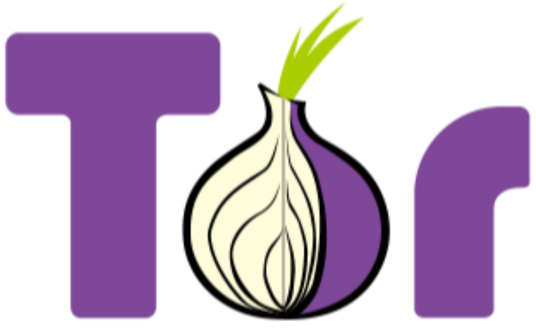
Privacy issues

- 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

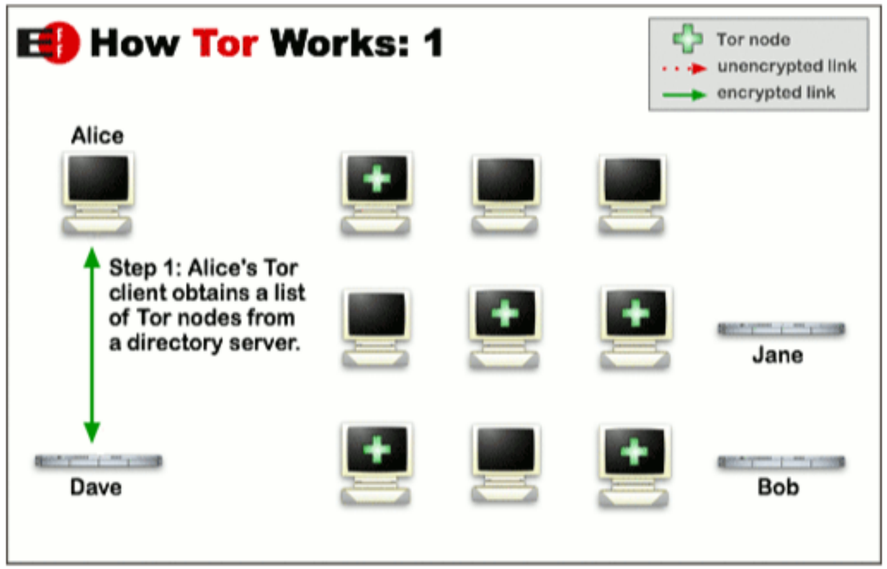
- Technologies are available
- They are not used by service providers, but by users
- One example is TOR, The Onion Routing

The Onion Router



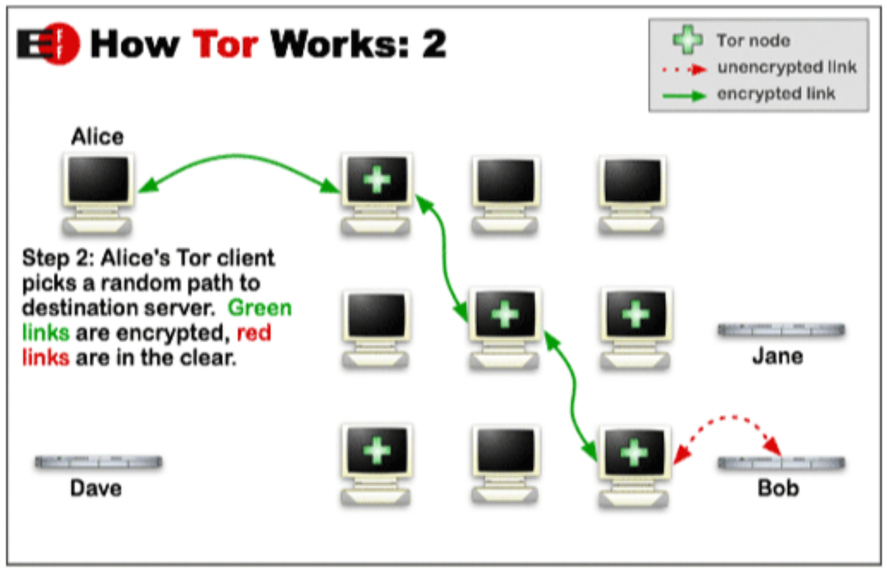
- Developed by US Navy, Protection for secret information
- Useful for:
- Human rights activists, whistleblowers
- For people that just want to have privacy
- Also for criminal activities

TOR Step 1:



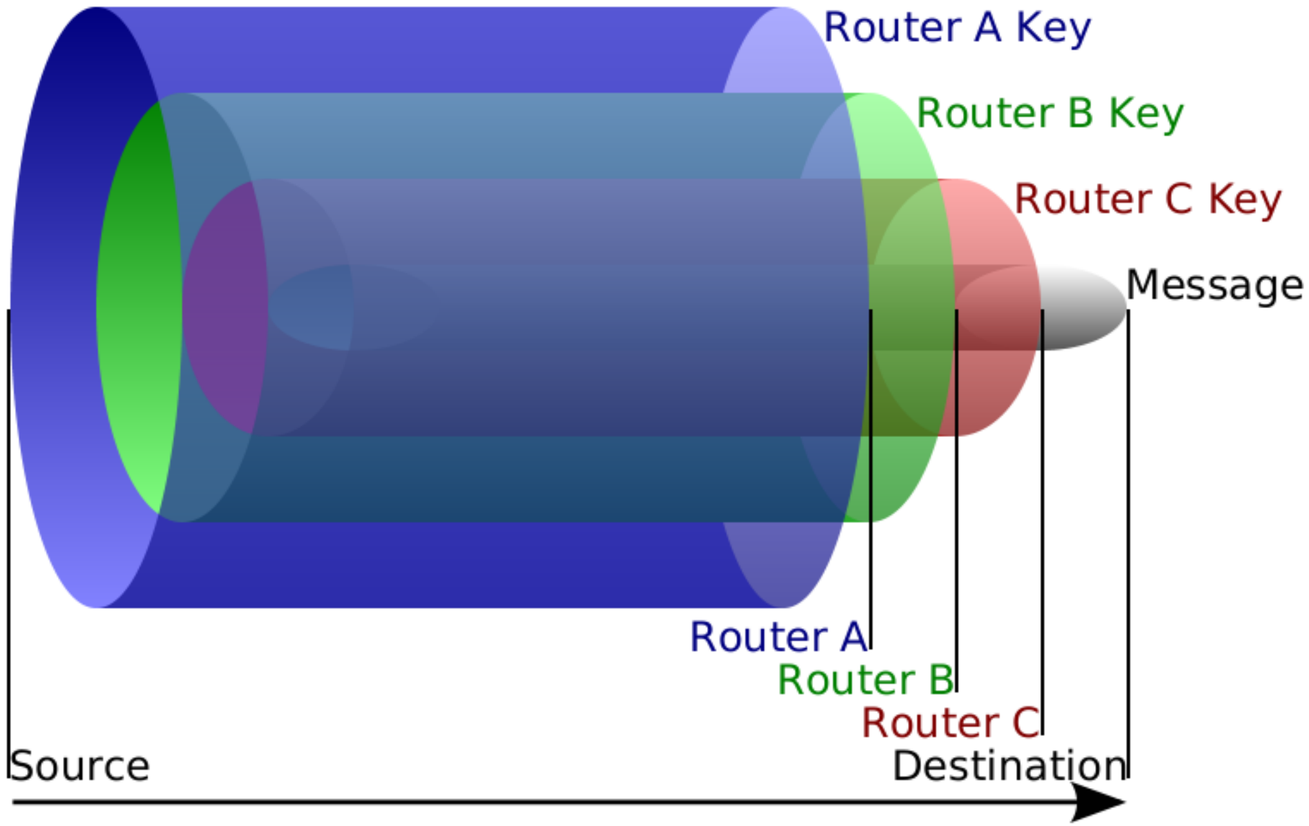
(Electronic Frontier Foundation)

TOR Step 2



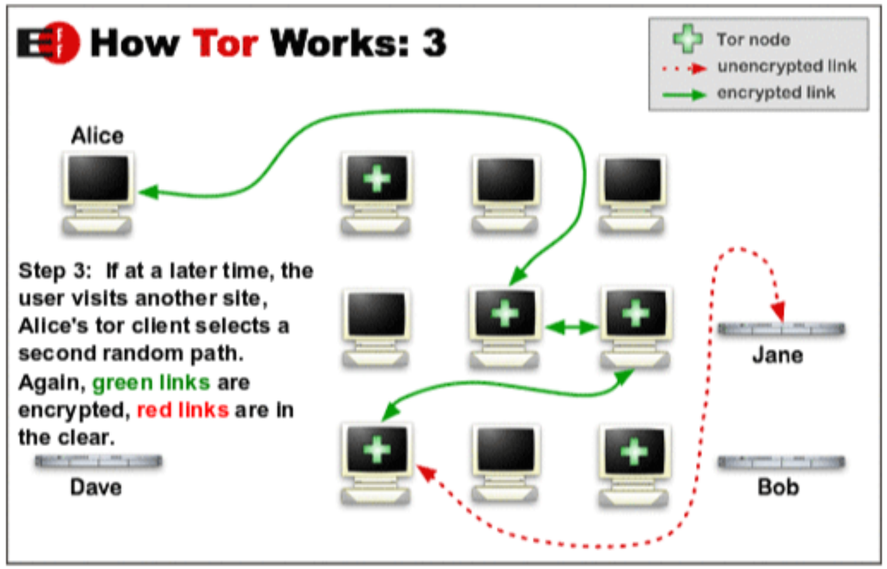
(Electronic Frontier Foundation)

TOR The Onion



(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.

Good Luck with Your Exams

FIT 1047

Introduction to computer systems, networks and security

MONASH University