

# FIT 1047

## Introduction to computer systems, networks and security

**Space**

Forward

**Right, Down, Page  
Down**

Next slide

**Left, Up, Page Up**

Previous slide

**P**



Open presenter  
console

**H**

Toggle this help

# Overview for today

- Some weaknesses
- Privacy Enhancing Technologies
- The Dark Net

## What kind of weaknesses can be exploited?

Some examples:

- |                               |                        |
|-------------------------------|------------------------|
| <b>Space</b>                  | Forward                |
| <b>Right, Down, Page Down</b> | Next slide             |
| <b>Left, Up, Page Up</b>      | Previous slide         |
| <b>P</b>                      | Open presenter console |
| <b>H</b>                      | Toggle this help       |
- Buffer overflow
  - Command injection
  - Cross-site scripting (XSS)
  - SQL Injection

Buffer overflow

# Buffer overflow

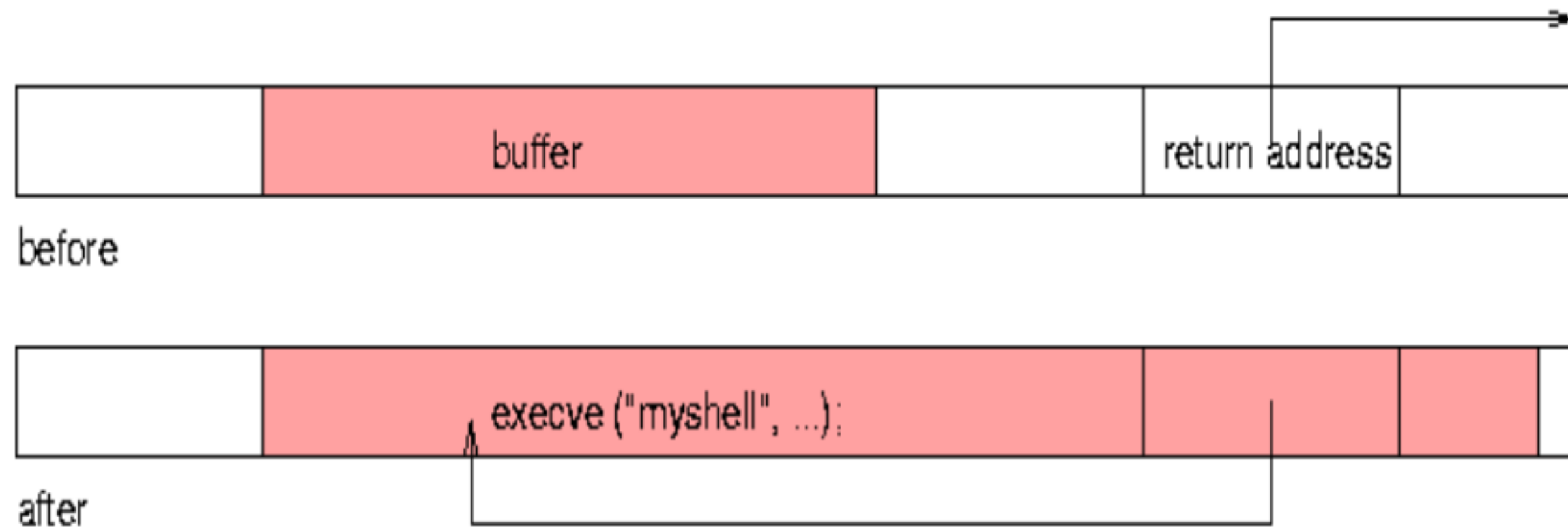


normal subprogram activation record



after 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, it can be used to execute arbitrary shell commands with the rights of the application process.

Examples at [owasp.org](https://www.owasp.org) (Open Web Applications Security Project):

[https://www.owasp.org/index.php/Command\\_injection](https://www.owasp.org/index.php/Command_injection)



# What is Cross-site scripting?

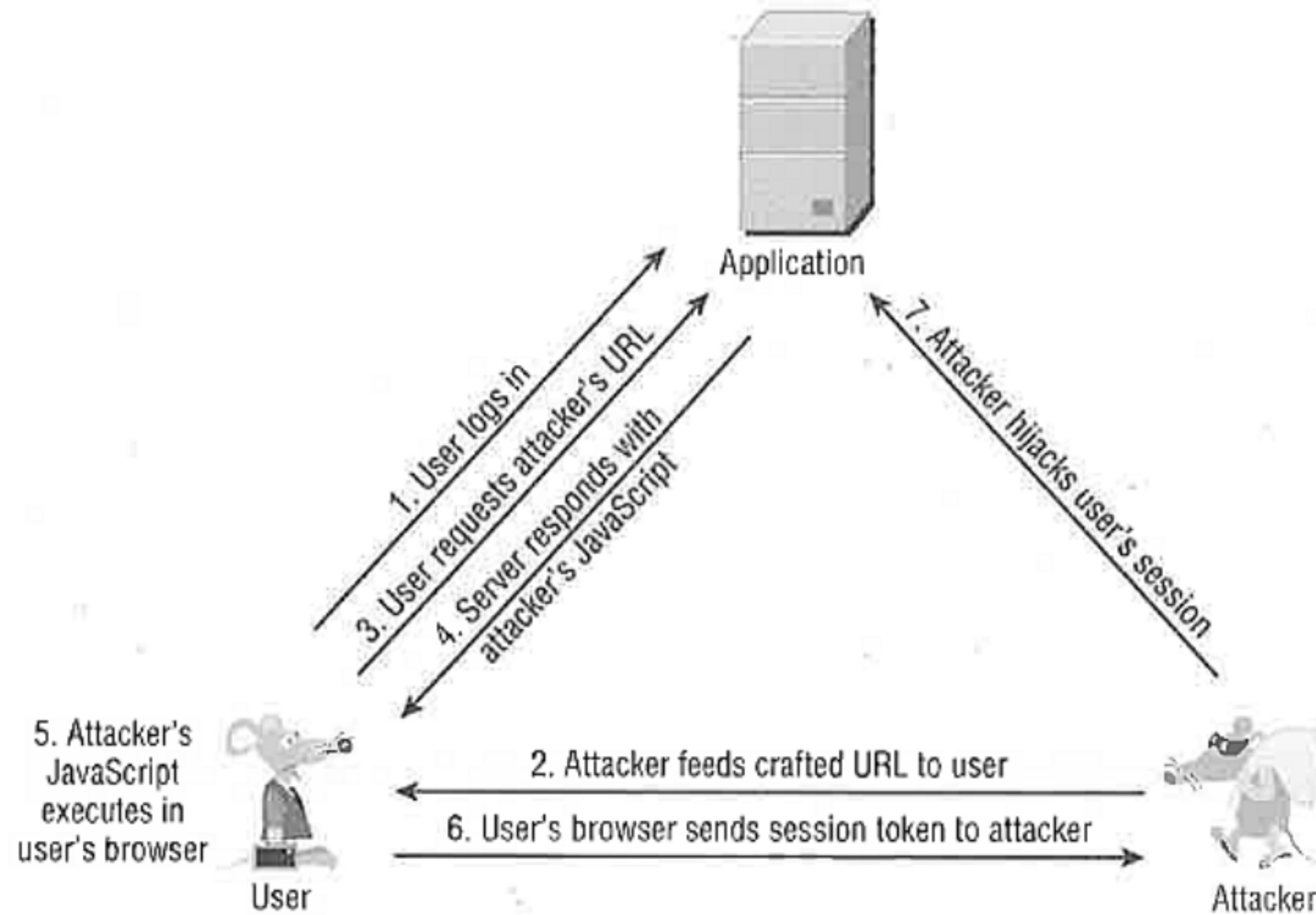
- Usually, browsers don't execute scripts not loaded (directly or indirectly) from the domain of the visited page.
- If attacker can insert own code to be executed is this cross-site.

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

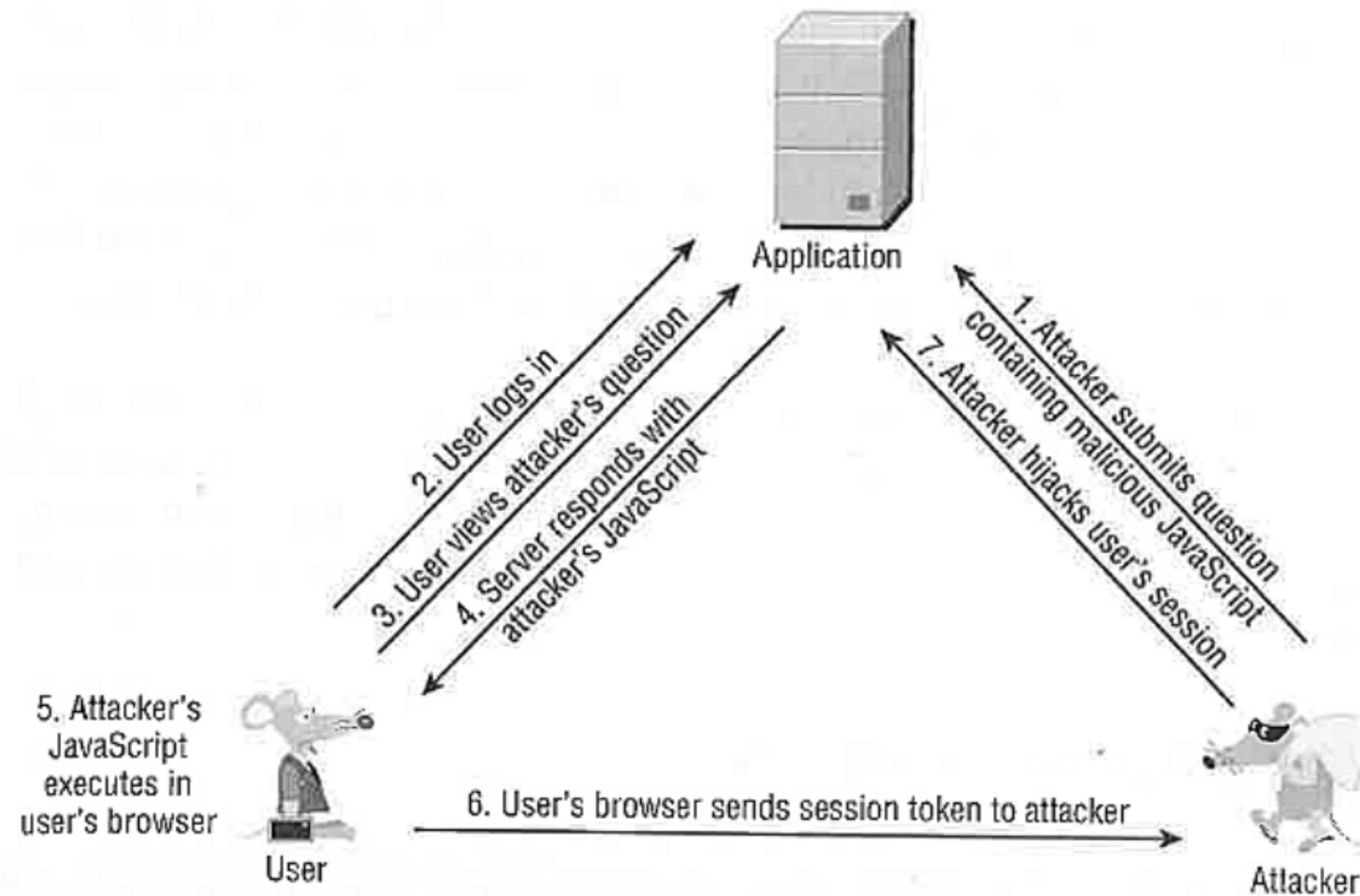
Let's look at two examples:

- Reflected XSS attack
- Stored XSS attack

# Reflected XSS attack



# Stored XSS attack



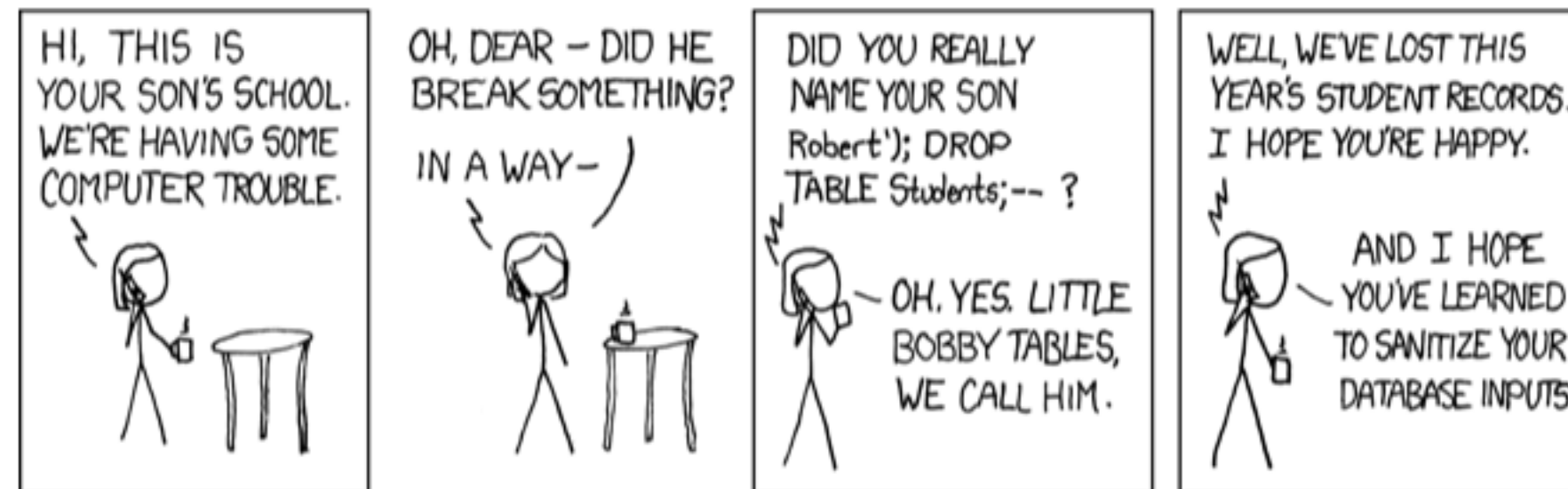
# How to prevent XSS?

[https://www.owasp.org/index.php/XSS\\_\(Cross\\_Site\\_Scripting\)\\_Prevention\\_](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_)

# SQL Injection

This is about attacking SQL databases.

# Embed database commands in normal input



(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

## Example 1/3

- Pod slurping

Attach a storage device (e.g iPod) to a computer and slurp large amounts of data.

Prevention: Don't let anyone just attache devices.

# Other attacks

## Example 2/3

- Attacks via DMA

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

Prevention: Don't let anyone just attach devices.

# Other attacks

## Example 3/3

- 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.

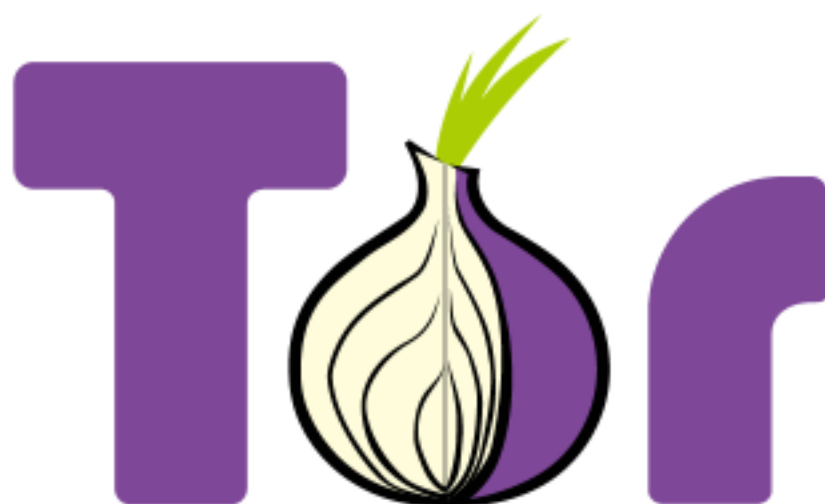
# Privacy issues

- 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

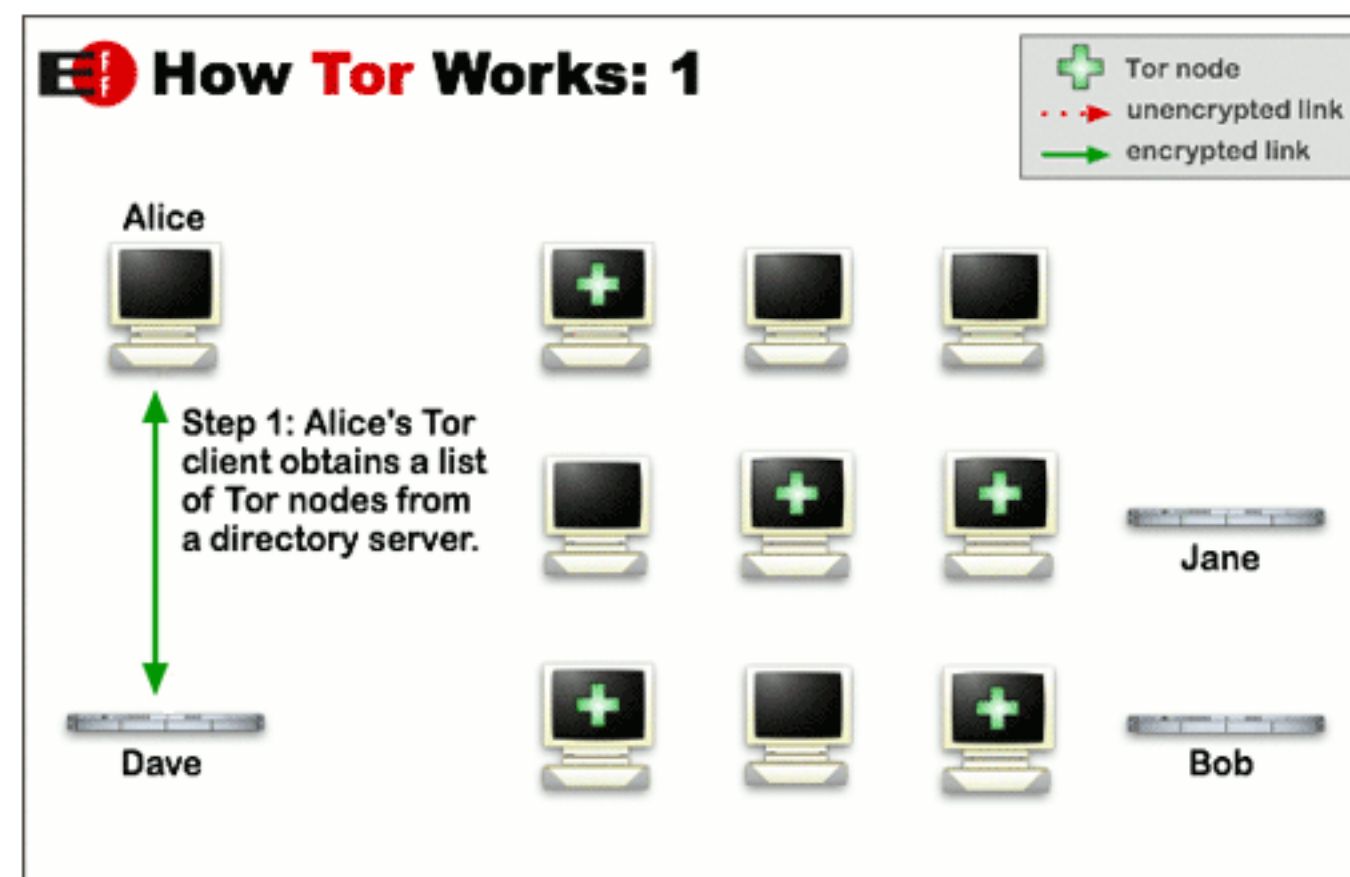
- Technologies are available
- They are not used by service providers, but by users
- One example is TOR, The Onion Routing

# 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

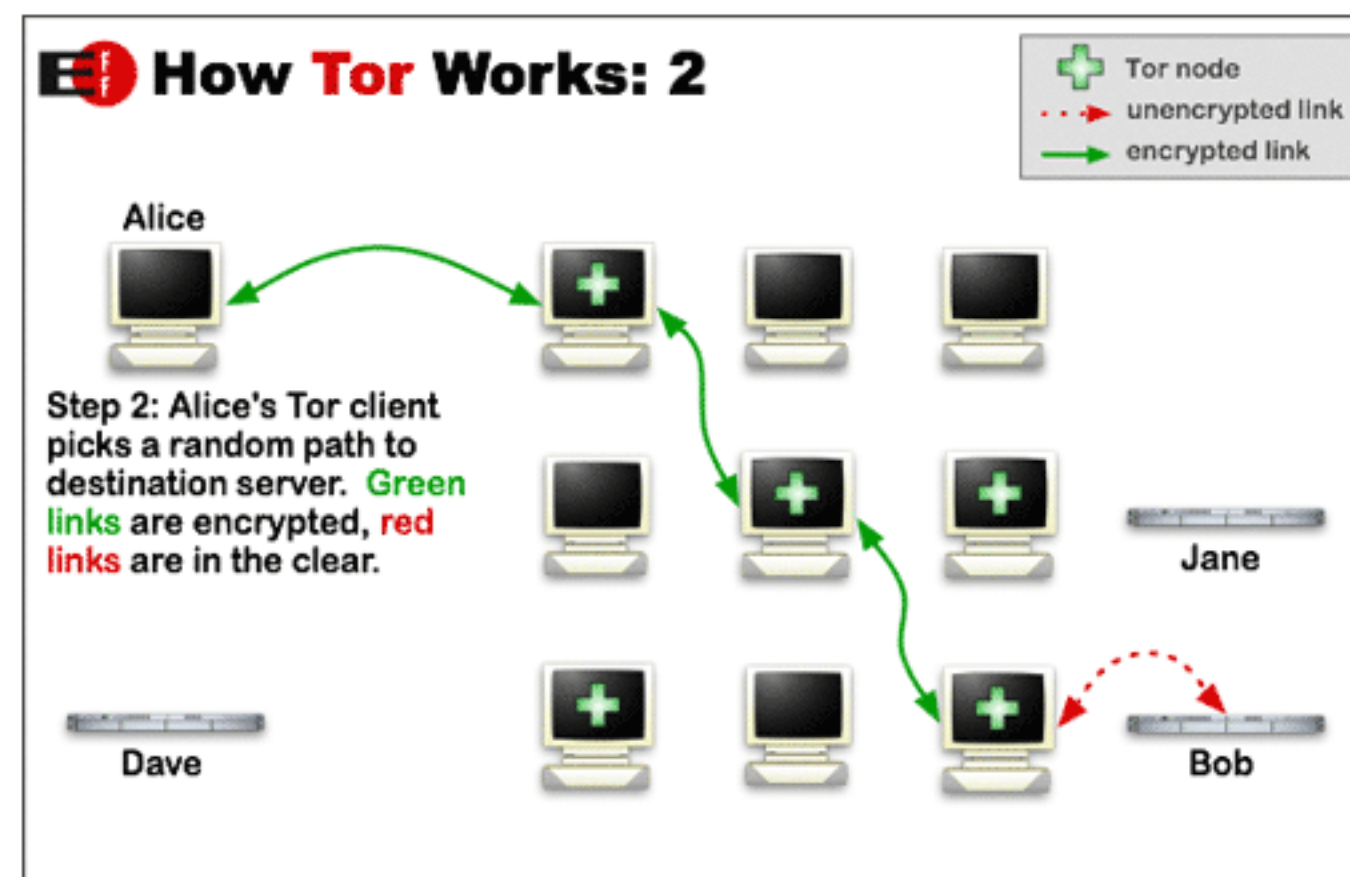
# TOR Step 1:



(Electronic Frontier Foundation)

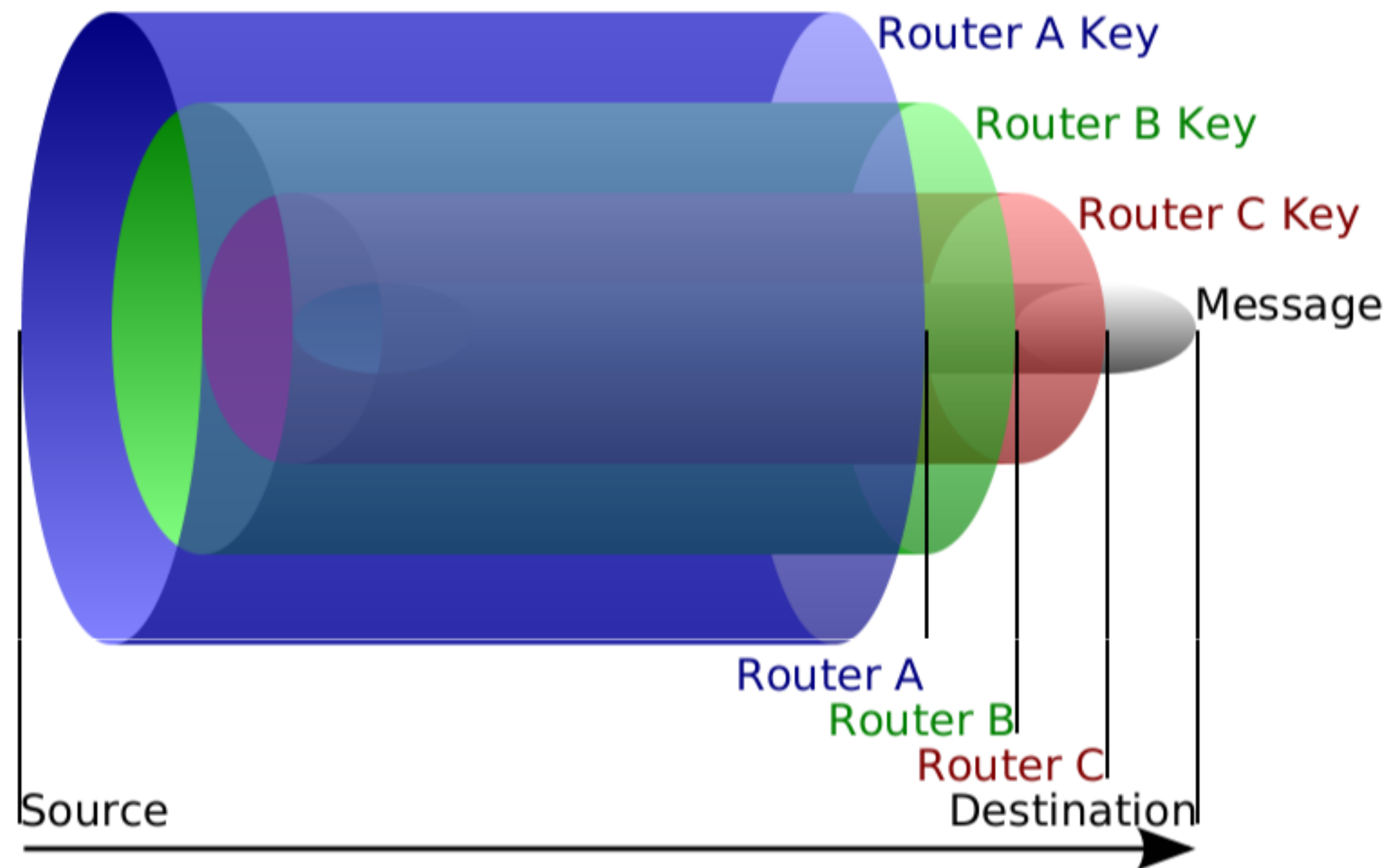


# TOR Step 2



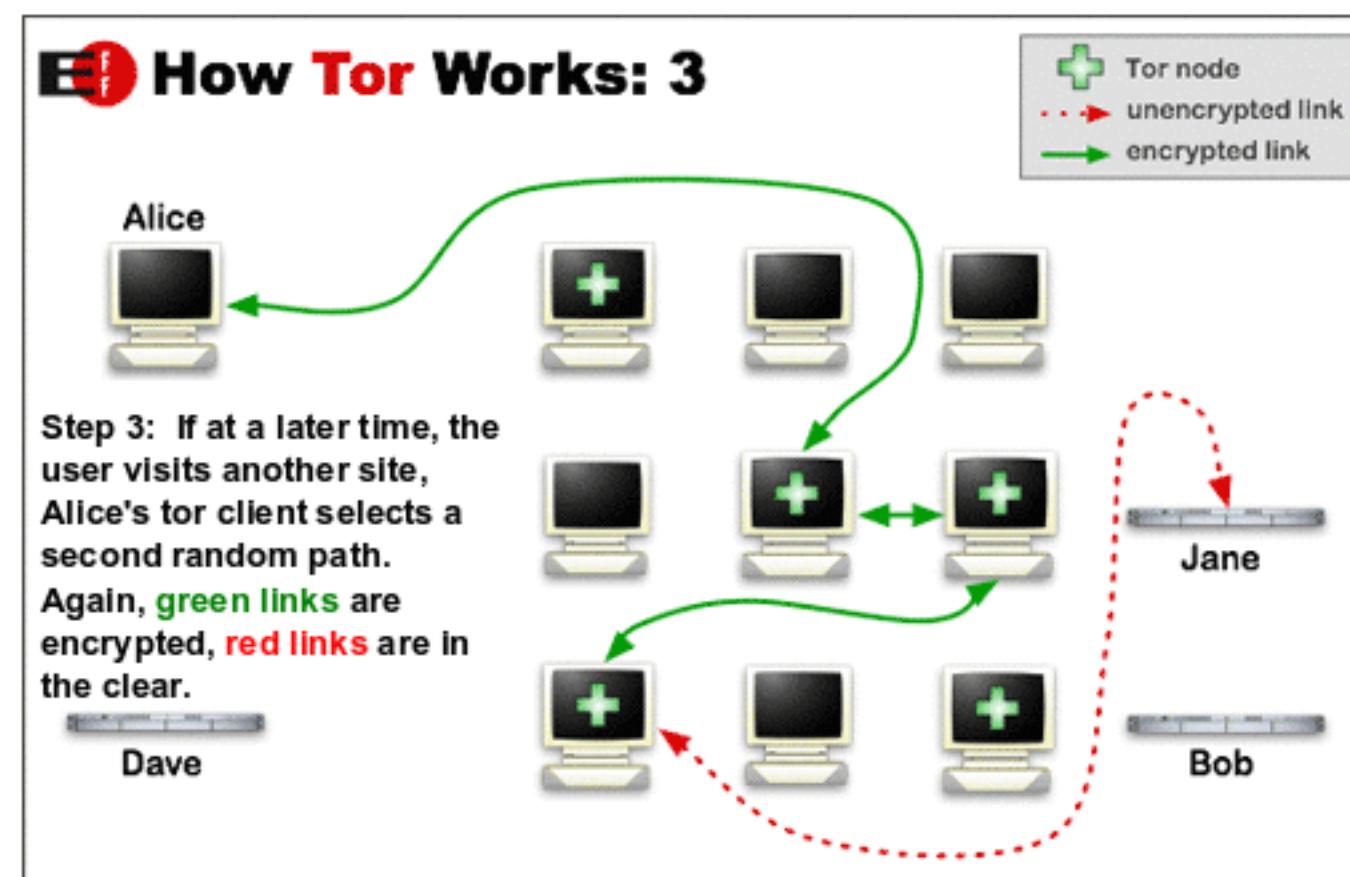
(Electronic Frontier Foundation)

# 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.

Log into mars.mu

Join the feed: 8G407T

Discuss with your neighbours: Is it dangerous to use TOR?

- A. Yes.
- B. No.

Feed: 8G407T

Which security problem/hack have you experienced?

- A. Phishing
- B. Ransomware
- C. Cheating in online games
- D. Credit card fraud
- E. Denial of service
- F. Virus on the computer
- G. More than one of the above

Feed: 8G407T



# Mars Leaderboard

Winner

Roshankumar Ravichandran (31 correct answers)

Second Place

Felix Salim (30 correct answers)

# 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](https://www.explainxkcd.com/wiki/index.php/795:_Conditional_Risk)