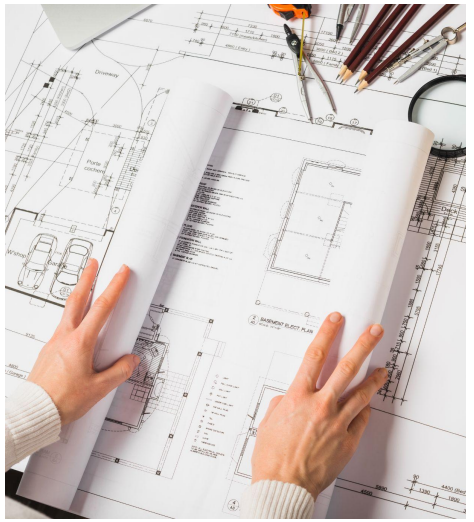
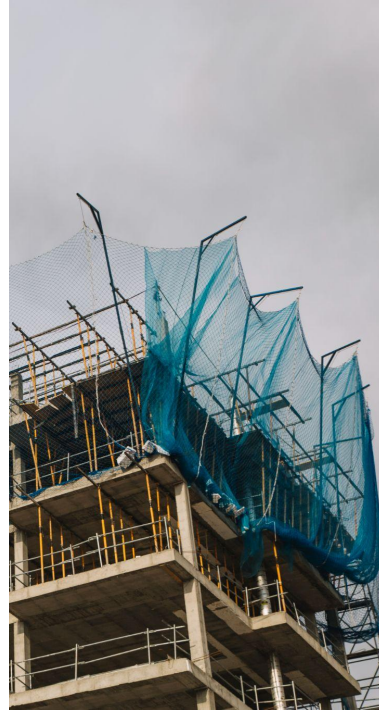
Software Security and Privacy

Software Engineering Course – 9
2024-2025





Security of a Software Product

Figure 7.1 Types of security threat

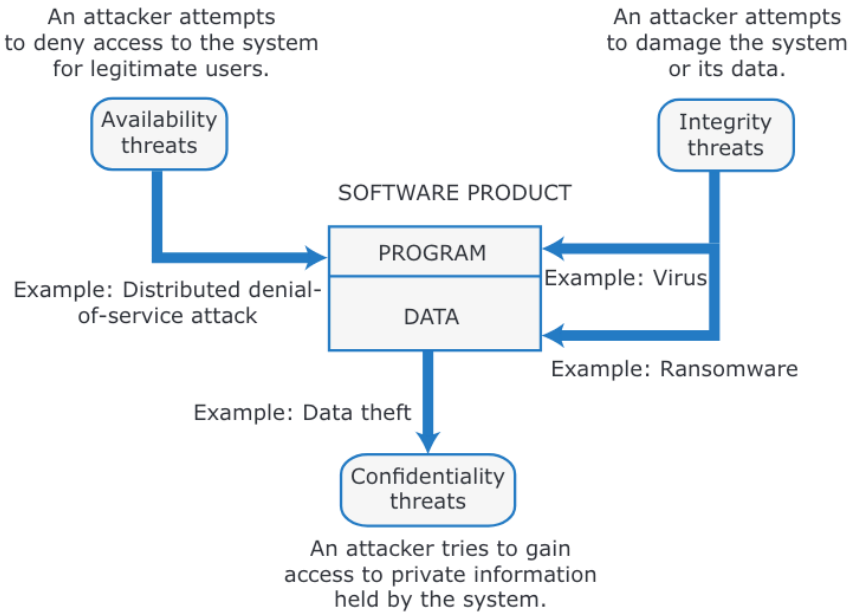
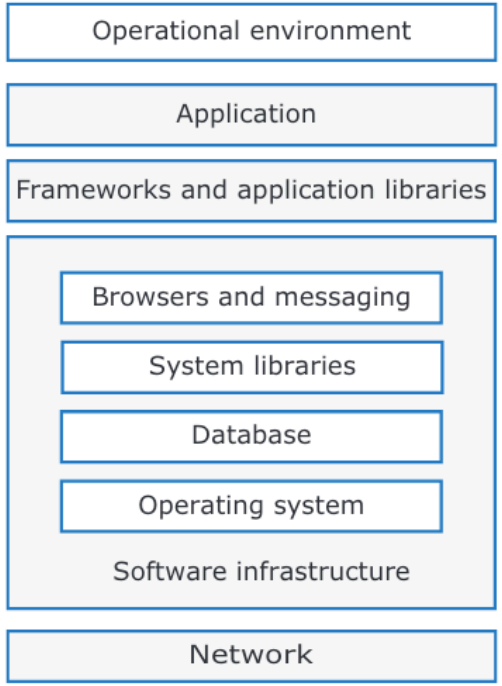


Figure 7.2 System infrastructure stack



Injection attacks

Attacks & Defences

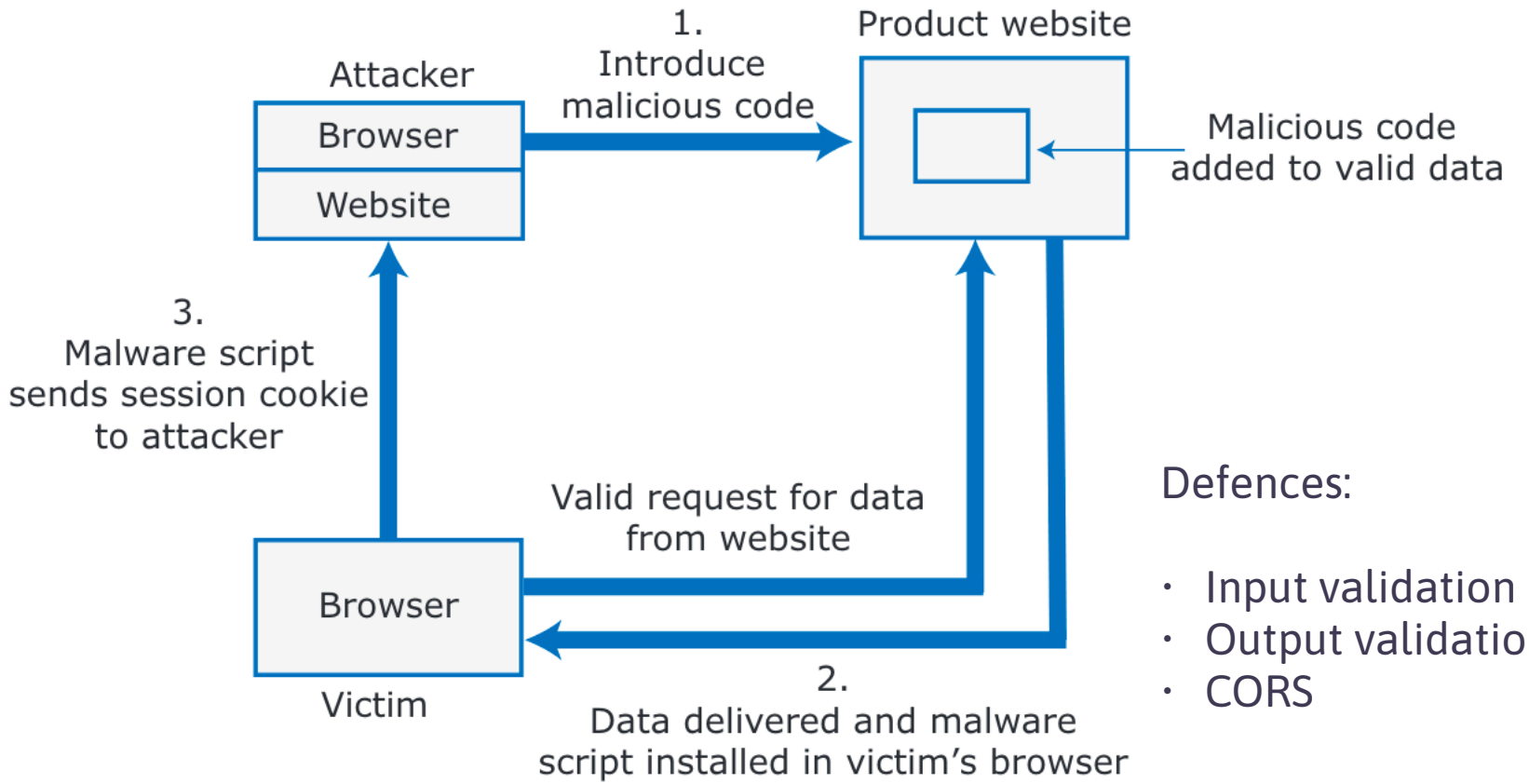
```
accNum = getAccountNumber ()
SQLstat = "SELECT * FROM AccountHolders WHERE accountnumber = '"
+ accNum + "';"
database.execute (SQLstat)
```

```
SELECT * from AccountHolders WHERE accountnumber = ‘10010010’ OR ‘1’ = ‘1’;
```

Cross-site Scripting (XSS)

Attacks & Defences

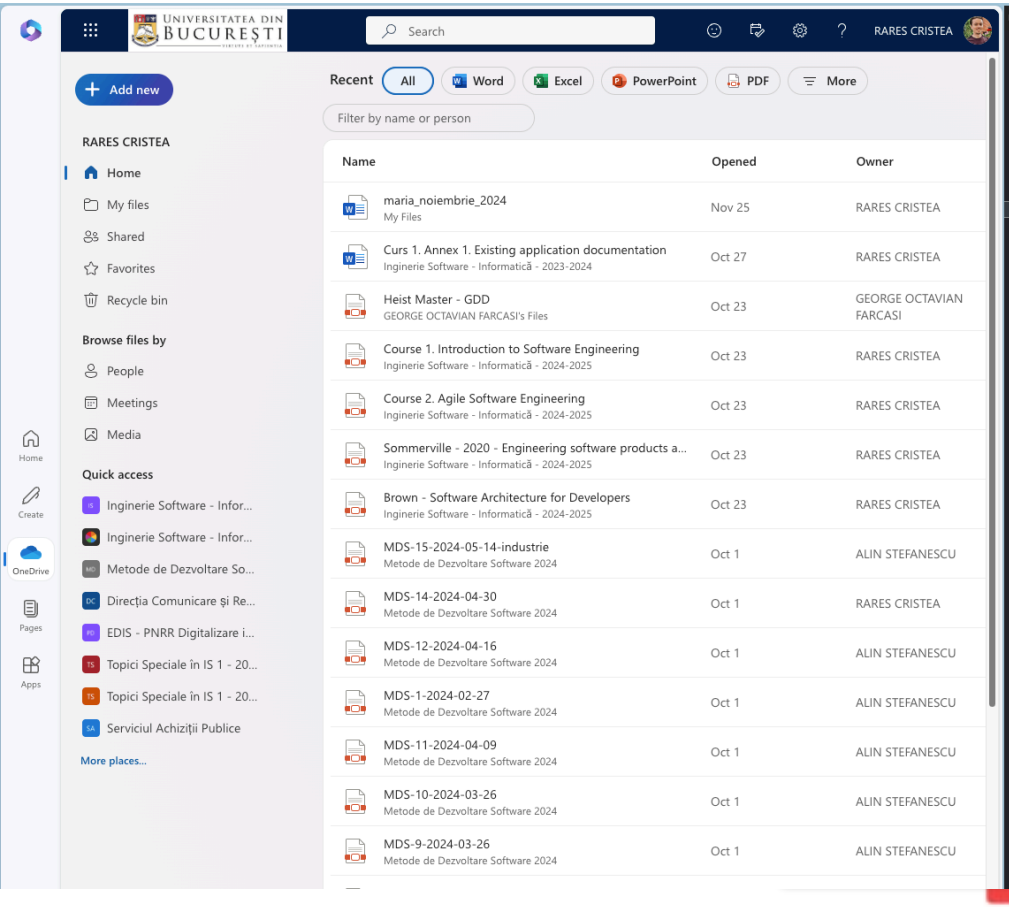
Figure 7.3 Cross-site scripting attack



Defences:

- Input validation
- Output validation
- CORS

Session Hijacking Attack



5. Attacker hijacks the user's session

DDoS

Attacks & Defences

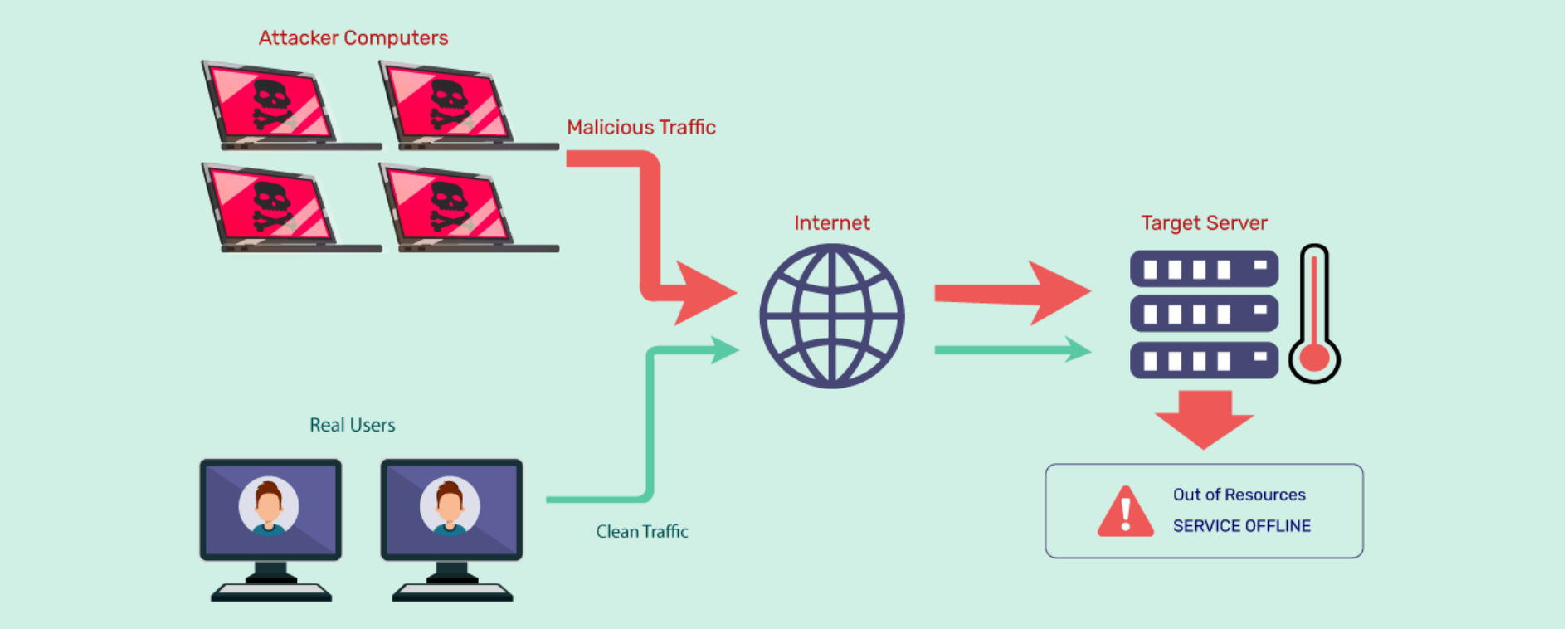
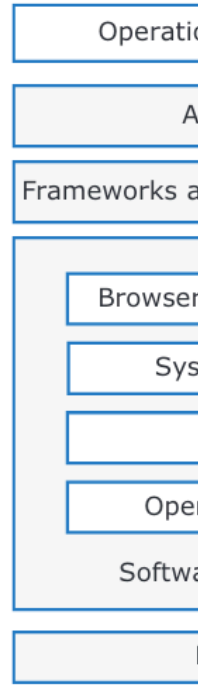


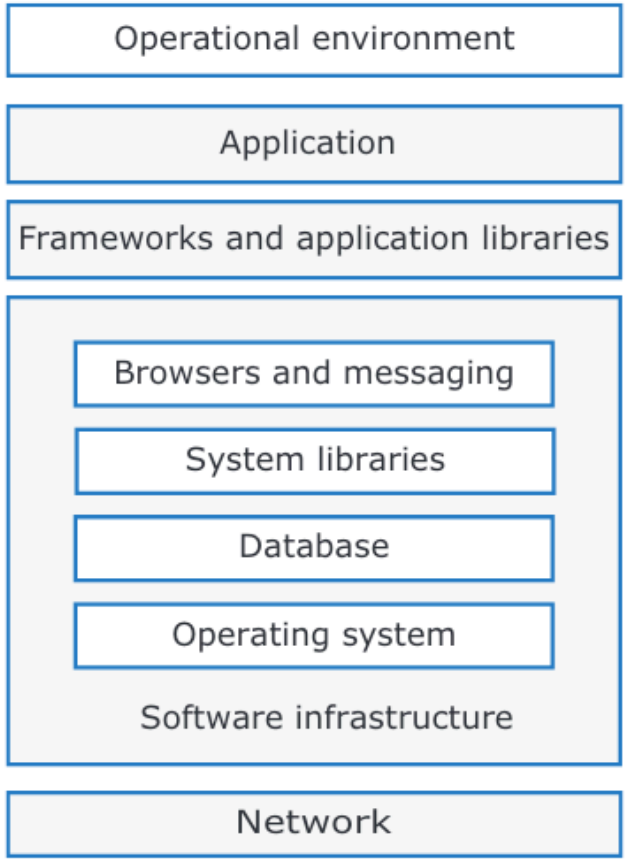
Figure 7.2 System infrastructure stack



DDoS

Attacks & Defences

Figure 7.2 System infrastructure stack



Defences:

- Temporary lockouts
- IP address tracking (and denial)

DDoS

Attacks & Defences

Hackers Flood NPM with Bogus Packages Causing a DoS Attack

Apr 10, 2023 Ravie Lakshmanan Software Security / JavaScript

Threat actors flooded the npm open source package repository for Node.js with bogus packages that briefly even resulted in a denial-of-service (DoS) attack.

"The threat actors create malicious websites and publish empty packages with links to those malicious websites, taking advantage of open-source ecosystems' good reputation on search engines," Checkmarx's Jossef Harush Kadouri said in a report published last week.

"The attacks caused a denial-of-service (DoS) that made NPM unstable with sporadic 'Service Unavailable' errors."

While similar campaigns were recently observed propagating phishing links, the latest wave pushed the number of package versions to 1.42 million, a dramatic uptick from the approximate 800,000 packages released on npm.

The attack technique leverages the fact that open source repositories are ranked higher on search engine results to create rogue websites and upload empty npm modules with links to those sites in the README.md files.

— Trending News

Protecting Tomorrow's World: Shaping the Cyber-Physical Future

Ongoing Phishing and Malware Campaigns in December 2024

SaaS Budget Planning Guide for IT Professionals

Microsoft MFA AuthQuake Flaw Enabled Unlimited Brute-Force Attempts Without Alerts

The Future of Network Security: Automated Internal and External

Dependency Confusion Attack

Attacks & Defences

Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

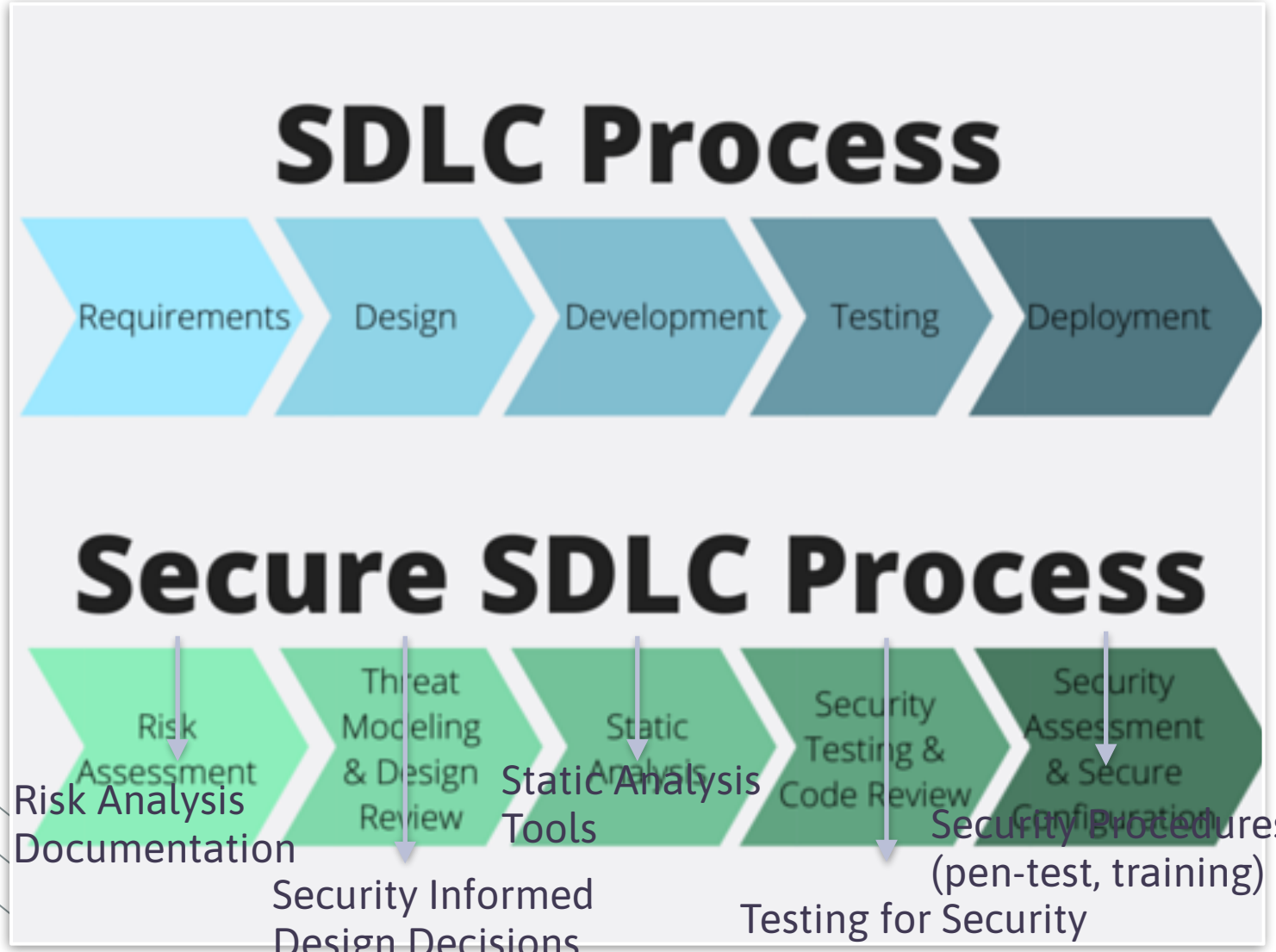
The Story of a Novel Supply Chain Attack

Alex Birsan · Follow

11 min read · Feb 9, 2021

20K 52

Security in the Software Development Lifecycle



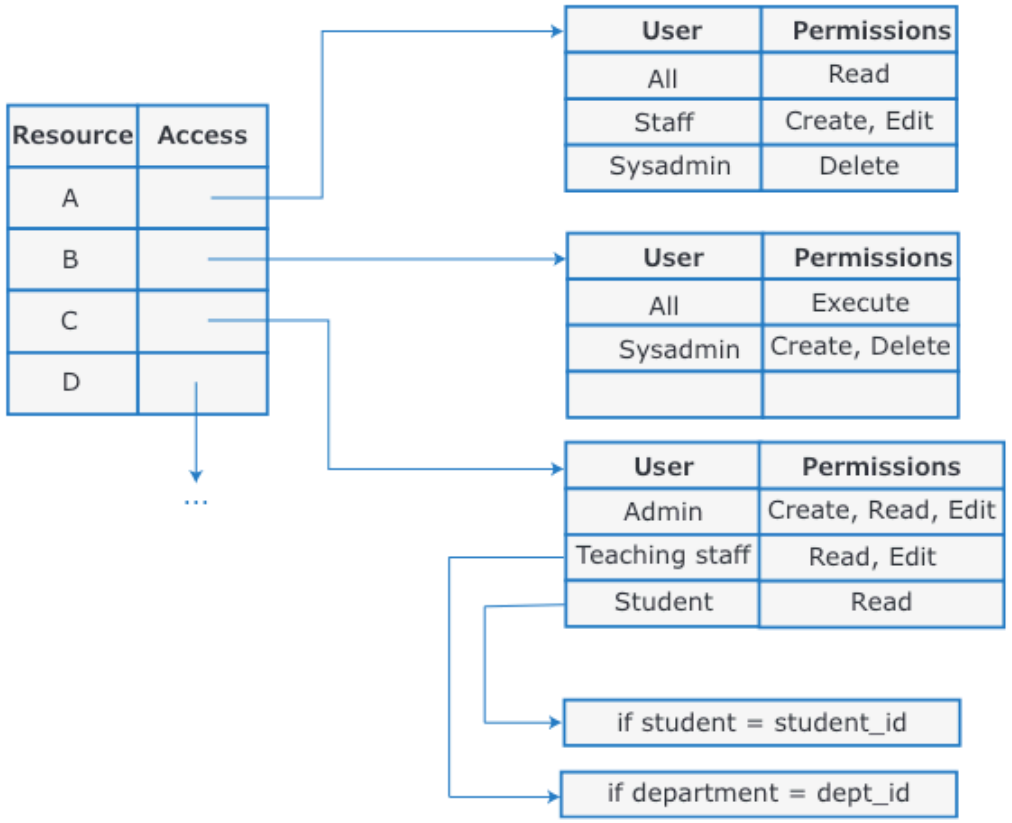
Authentification ...

Table 7.3 Weaknesses of password-based authentication

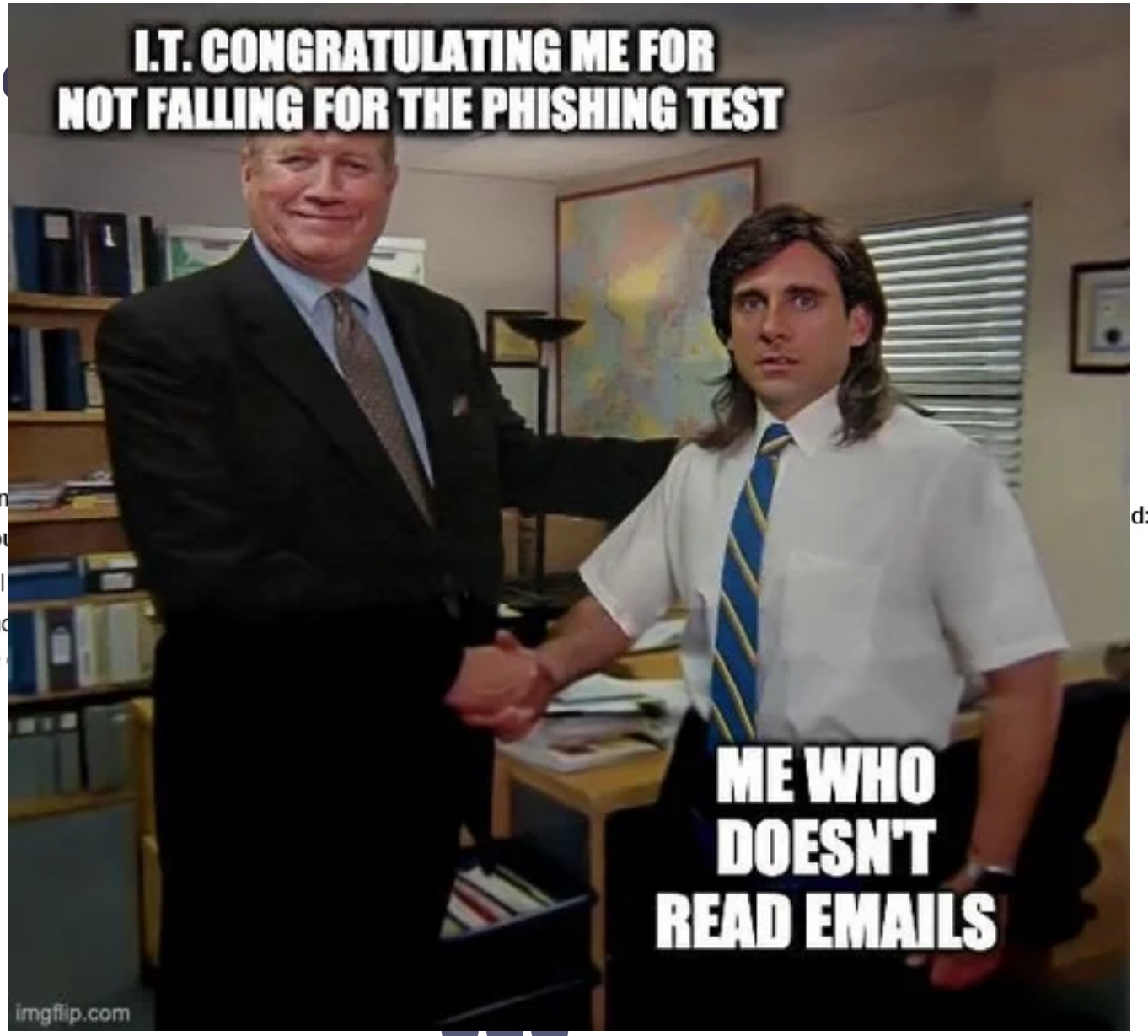
Weakness	Explanation
Insecure passwords	Users choose passwords that are easy to remember. However, it is also easy for attackers to guess or generate these passwords, using either a dictionary or a brute force attack.
Phishing attacks	Users click on an email link that points to a fake site that tries to collect their login and password details.
Password reuse	Users use the same password for several sites. If there is a security breach at one of these sites, attackers then have passwords that they can try on other sites.
Forgotten passwords	Users regularly forget their passwords, so you need to set up a password recovery mechanism to allow these to be reset. This can be a vulnerability if users' credentials have been stolen and attackers use that mechanism to reset their passwords.

… and Authorisation

Figure 7.8 Access control lists



So



Closing the in

ideally withou

- Removing all
- Covering trac
- Bringing the

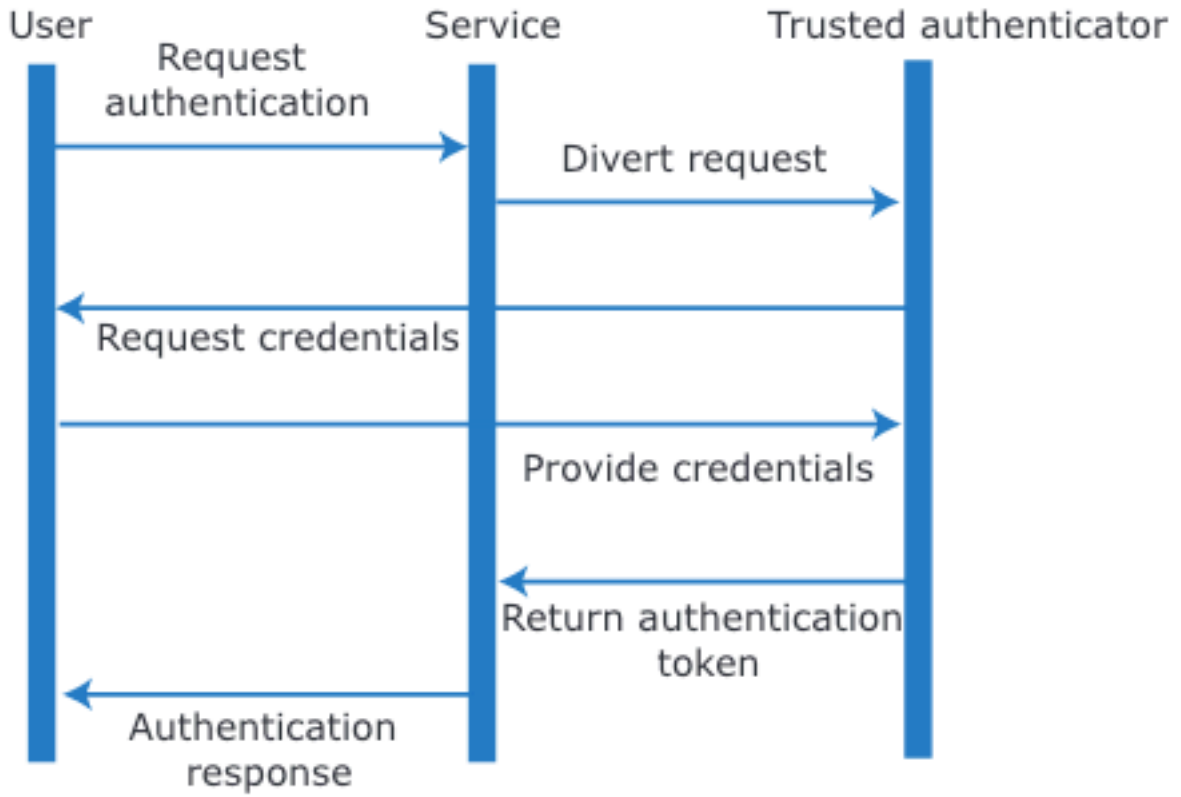
d:

Defences:

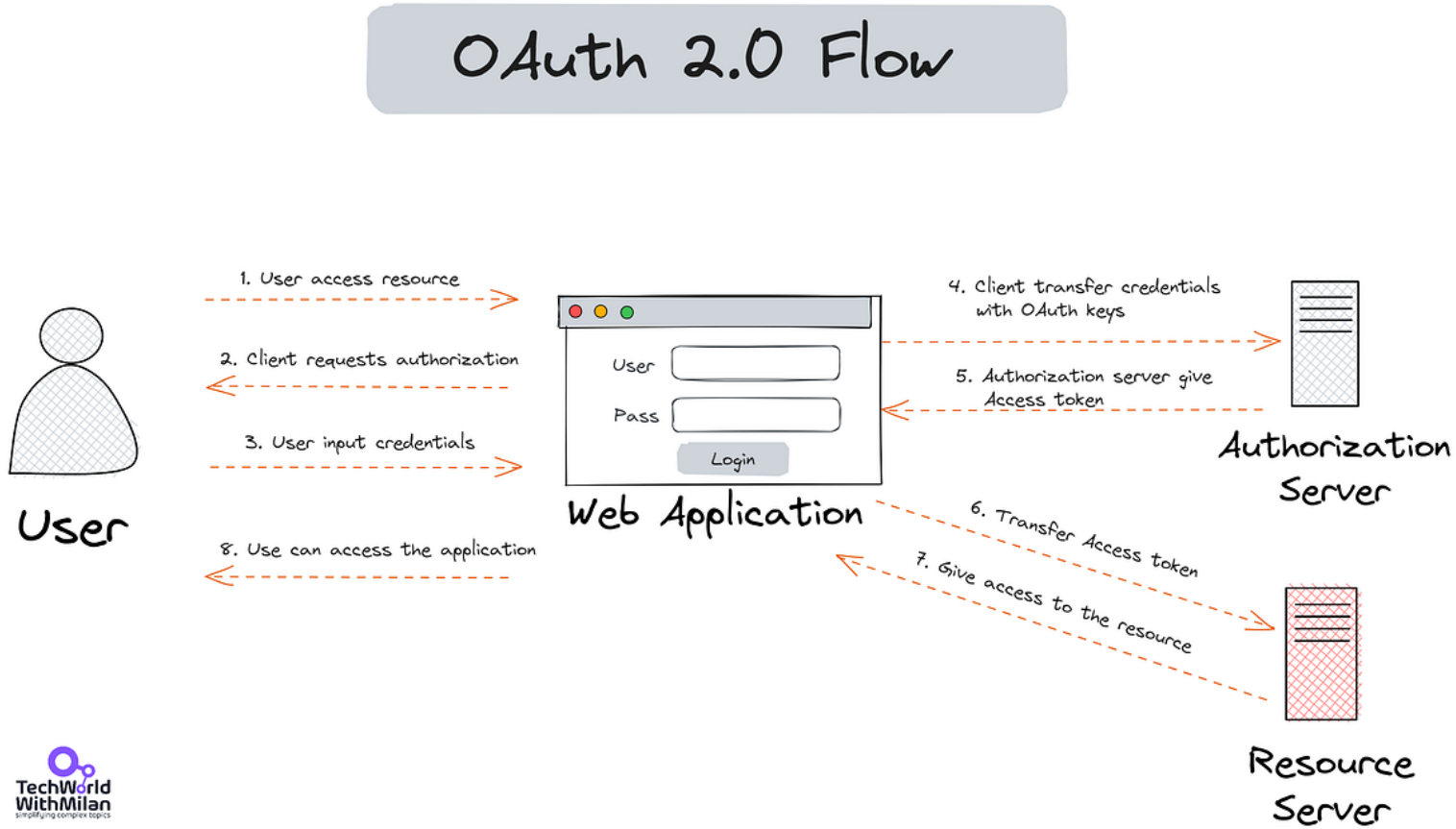
- Training
- MFA
- Antivirus(es)

Federated Identity

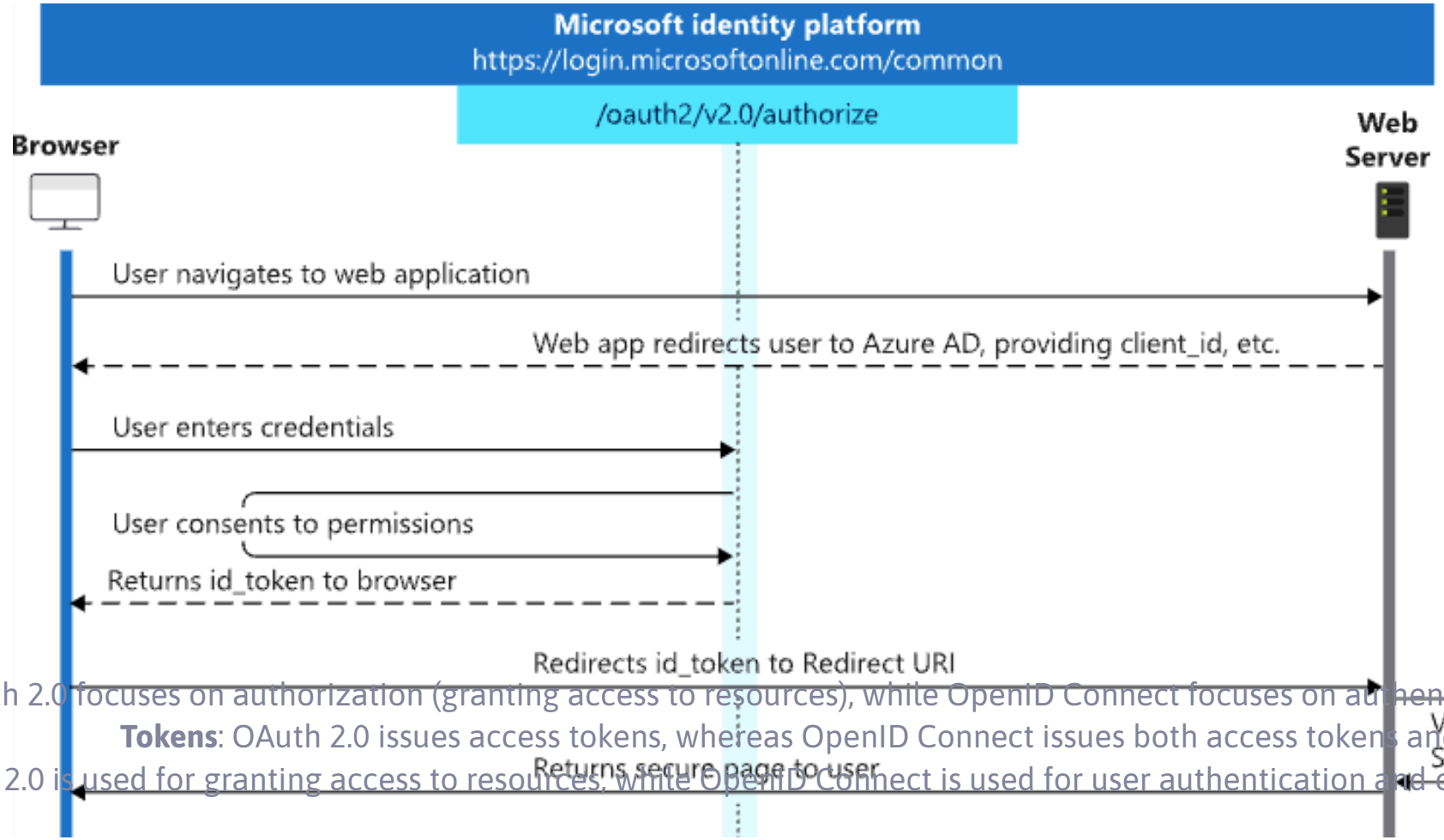
Figure 7.5 Federated identity



Federated Identity



Federated Identity

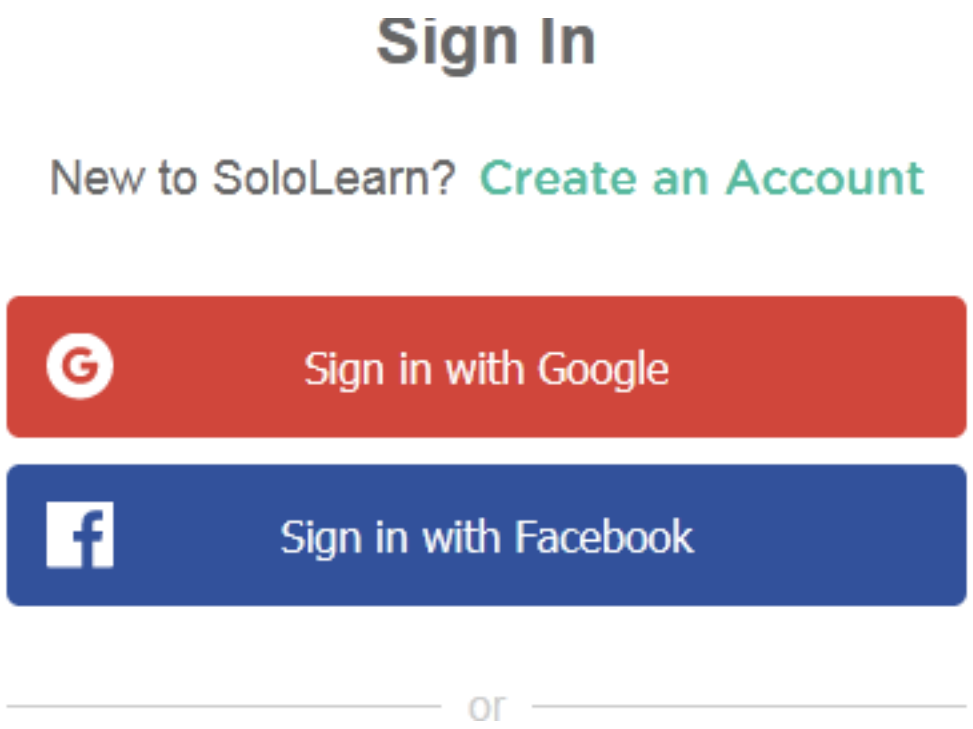


Focus: OAuth 2.0 focuses on authorization (granting access to resources), while OpenID Connect focuses on authentication (verifying user identity).

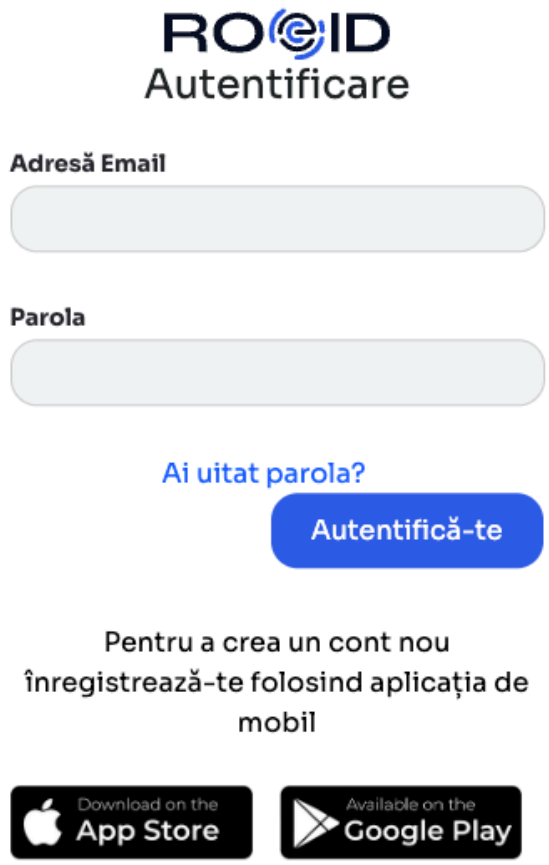
Tokens: OAuth 2.0 issues access tokens, whereas OpenID Connect issues both access tokens and ID tokens.

Scope: OAuth 2.0 is used for granting access to resources, while OpenID Connect is used for user authentication and obtaining user profile information.

Federated Identity



Federated Identity



Privacy

Figure 7.16 Data protection laws

Privacy

Table 7.6 Data protection principles

Data protection principle	Explanation
Awareness and control	Users of your product must be made aware of what data are collected when they are using your product, and must have control over the personal information that you collect from them.
Purpose	You must tell users why data are being collected and you must not use those data for other purposes.
Consent	You must always have the consent of a user before you disclose their data to other people.
Data lifetime	You must not keep data for longer than you need to. If a user deletes an account, you must delete the personal data associated with that account.
Secure storage	You must maintain data securely so that it cannot be tampered with or disclosed to unauthorized people.
Discovery and error correction	You must allow users to find out what personal data you store. You must provide a way for users to correct errors in their personal data.
Location	You must not store data in countries where weaker data protection laws apply unless there is an explicit agreement that the stronger data protection rules will be upheld.

Privacy


Understand GDPR Technical Requirements
01
02
Conduct Data Mapping and Classification
Implement Data Minimization Measures
03
04
Establish a User Consent Mechanism
Ensure Data Subject Rights Compliance
05
06
Manage Third-Party Services Effectively
Incorporate Privacy by Design and by Default
07
08
Enforce Data Security & Encryption Practices
Establish Data Breach Notification Protocols
09
10
Develop a Cookie Collection Policy
Conduct Data Protection Impact Assessments
11
12
Manage Cross-Border Data Transfer
Eliminate Security Questions to Enhance Privacy
13
14
Facilitate the Right to Portability
Enforce the Right to be Forgotten
15
16
Remove Data from Payment Gateways
Conduct Software Testing for GDPR Compliance
17
18
Perform Regular Audits and Ensure Updates

Privacy

1. EU Residents have the right to know what you are doing with their data
2. Time for data breach notification is 72 hours.
3. Right to be Forgotten - a user should be able to disappear from all of your data stores.
4. Control over the rights of the transmission of data.

Dark Patterns of Consent

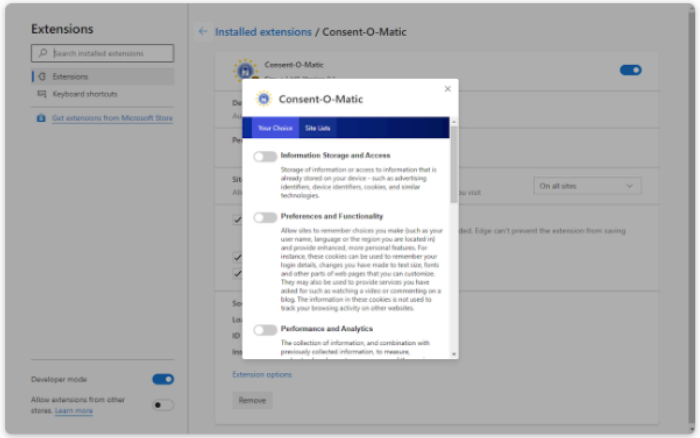
https://wideangle.co/blog/dark-patterns-examples-of-manipulative-consent-requests

Consent-O-Matic

Remove

Featured 4.0 ★ (142 ratings)

Extension | Privacy & Security | 100,000 users



Overview

Automatic handling of GDPR consent forms

Cookie pop-ups are designed to be confusing and make you 'agree' to be tracked. This add-on automatically answers consent pop-ups for you, so you can't be manipulated. Set your preferences once, and let the technology do the rest!

This add-on is built and maintained by workers at Aarhus University in Denmark. We are privacy researchers that got tired of seeing how companies violate the EU's General Data Protection Regulation (GDPR). Because the organisations that enforce the GDPR do not have enough resources, we built this add-on to help them out.


Kahoot!

Resources Used