

# USER AUTHENTICATION

MIKIAS ABERA

# AGENDA

*What is user authentication?*

*Security on the web*

*Types of authentication*

*Demo*



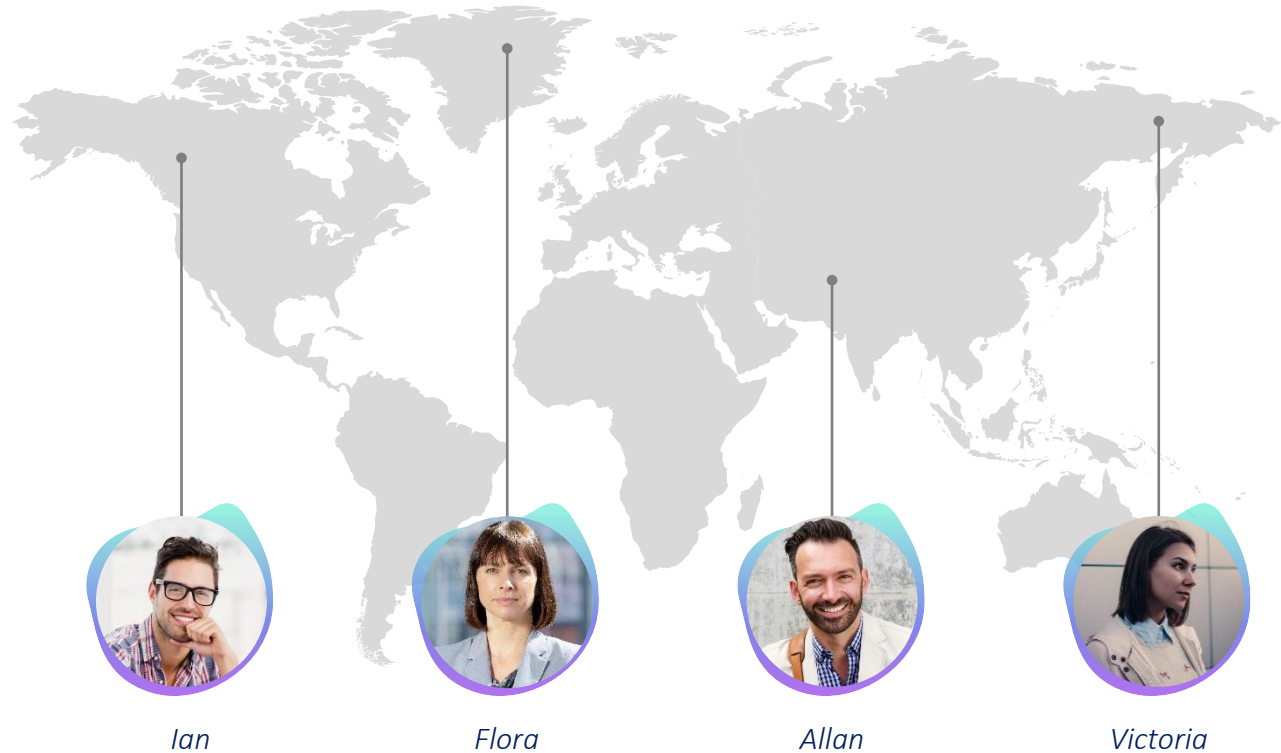
# What Is User Authentication?

*What is it?*

***A process that allows our application to identify the identity of someone who connects to our network.***

*Why do we want it?*

***We want to allow secure, reliable and private access to information to users anywhere in the network.***



# TINY APP, LESSONS LEARNED

*What mechanism was used to authenticate the user?*

*Plaintext cookie's using cookieParser*

*Encoded and signed cookies using cookieSession*

*What should we never put in a cookie?*

*Personal information, passwords, etc.*

*Because cookies can possibly be read and tampered with giving an attacker access to the data*

*What vulnerabilities were there?*

*Communication was over HTTP*

*Keys used to sign cookies were hard coded*

```
app.use(cookieSession({  
  name: 'session',  
  keys: ['not-secure-key-because-checked-into-git'], // !!!  
  maxAge: 1  
}))
```



# SECURITY *It's HARD!*

*Data breaches happen frequently!*

*Even large companies aren't safe.*

*Facebook stored **several hundred million** passwords in plaintext.*




<https://haveibeenpwned.com/>

*7 Billion pwned accounts and 364 pwned websites including LinkedIn, DataCamp and MyFitnessPal.*

*List of data breaches*

[https://en.wikipedia.org/wiki/List\\_of\\_data\\_breaches](https://en.wikipedia.org/wiki/List_of_data_breaches)

## *Hacker Job Opportunities*

 SERVICE	 BITCOIN <small>(Typical price range listed along with the highest listed price)</small>	 USD <small>(Typical price range listed along with the highest listed price)</small>
HACKING WEB SERVER (VPS OR HOSTING)	0.034 - 0.0449, 0.47	\$220 - \$500, \$3,000
SETTING UP KEYLOGGER	0.0263	\$170
DDOS (PRICES MAY VARY)	0.0534, 0.078 - 0.39	\$350, \$500 - \$2,500
HACKING PERSONAL COMPUTER	0.0364, 0.044 - 0.55	\$280, \$500 - \$3,500
HACKING CELL PHONES	0.047 - 0.093	\$300 - \$600
EMAIL HACKING	0.078 - 0.12	\$500 - \$800
SOCIAL MEDIA ACCOUNT HACKING	0.0352, 0.054 - 0.11	\$230, \$350 - \$700
CHANGE SCHOOL GRADES	0.19 - 0.58	\$1,200 - \$3,750
FUD RANSOMWARE + DECRYPTER	12 MO / 0.14	12 MO / \$900
	6 MO / 0.076	6 MO / \$490
	1 MO / 0.019	1 MO / \$120

Prices for services on a major darknet cybercrime forum, including for "fully undetectable" ransomware, found in October 2018, reflecting exchange rates in effect at that time (Source: WatchGuard)

*Dark Overlord job posting*

<https://thehustle.co/dark-overlord-hacker-cybercrime-software-engineer-hiring/>

# What can we do?



## ***How can we protect user data we store?***

*Use well supported encryption libraries*

*Use HTTPS*

*Don't store sensitive data*

## ***Why use third party solutions?***

*Offload responsibility*

*Gain access to user social data*

*Easy sign in process*

## ***Risks of using third party solutions?***

*Big companies get hacked too*

*Possibly dependent on their service*

*Not all users have social accounts*

# Secure Communication Over the Web

## *How do we communicate securely?*

HTTPS is an **application layer protocol** which includes several layers  
HTTP, SSL/TLS, TCP, IP, ETHERNET

**Secure Sockets Layer** and **Transport Layer Security** are cryptographic protocols.

## **Public Key Cryptography**

Public + Private Key Pair

Asymmetric cryptography provides **Privacy and Data Integrity**

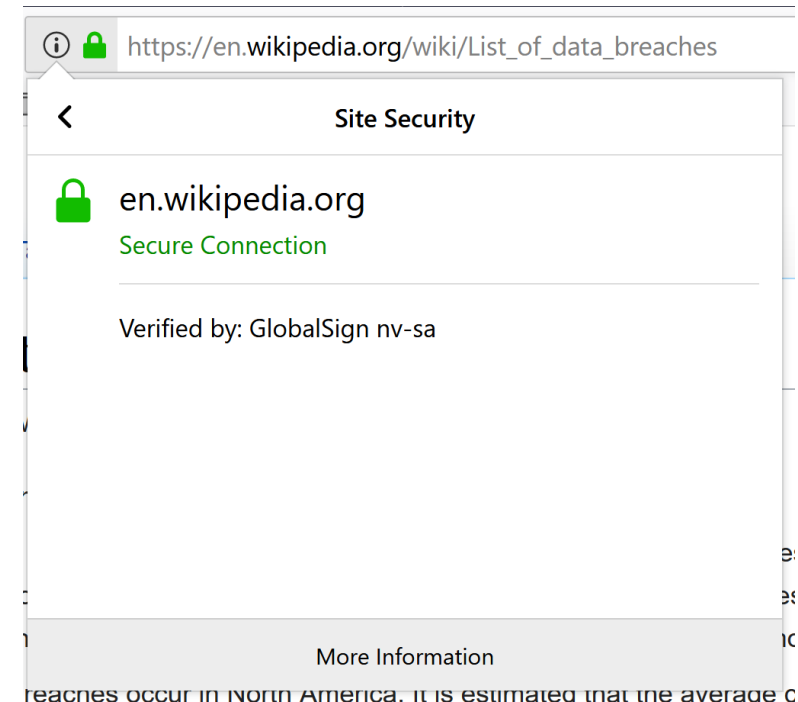
Ensures data integrity using signature (journalists, banks, etc.)

Example: SSH keys for Github

## *How do we share our public keys securely?*

We use a **Certificate Authority** that everyone trusts to hold and distribute our SSL certificates.

Letsencrypt (<https://letsencrypt.org>)



# TYPES OF AUTHENTICATION

## OAUTH

*Delegate authentication to 3<sup>rd</sup> party  
(Facebook, Google, Github, etc.)*



## EMAIL + PASSWORD

*Save email and encrypted  
password for later confirmation.*



## SINGLE SIGN ON (SSO)

*Create a single account  
and use to sign into  
multiple applications.*



## 2 FACTOR AUTHENTICATION

*Confirm authentication  
through mobile, email or  
other 'factor'.*



So many choices...



# OAuth

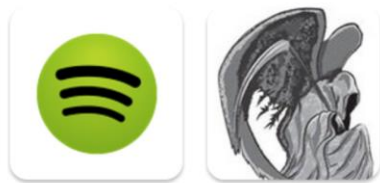
Protocol allowing a user to give one application access to data from another.

Supported by all major social platforms like:

Facebook, Google, Twitter, Github, etc.

## Example

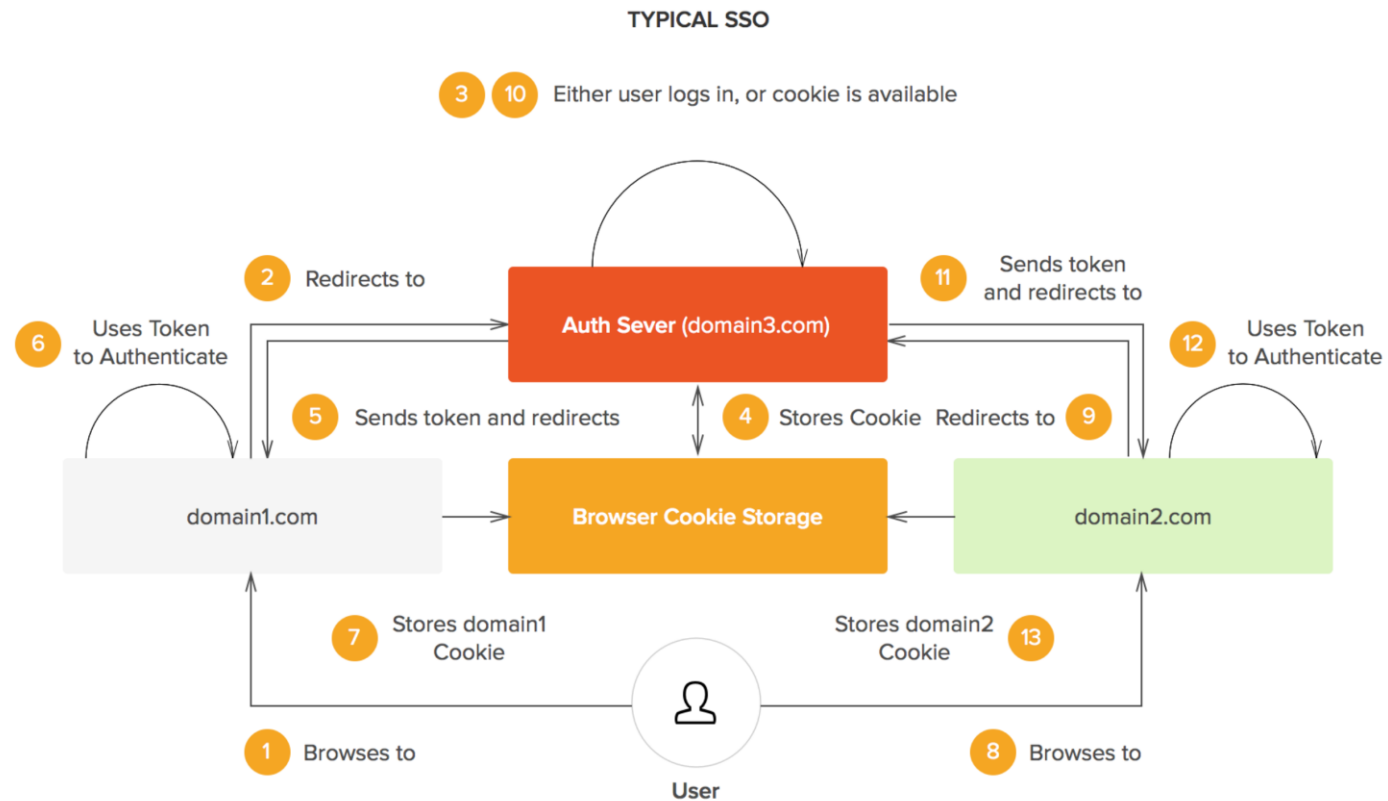
Login to Spotify with Facebook account



**Spotify** will receive the following info: your public profile. ⓘ

# SSO

Single Sign On allows a user to use a single set of credentials to login to multiple domains.



# DEMO

# Thank You

Now go forth and authenticate!

## *Links*

### ***Public Key Cryptography***

*[https://en.wikipedia.org/wiki/Public-key\\_cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography)*

*[https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman\\_key\\_exchange](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange)*

### ***Certificate Authorities***

*<https://letsencrypt.org/how-it-works/>*

### ***OAuth***

*<https://oauth.net/2/>*

### ***SSO***

*<https://auth0.com/blog/what-is-and-how-does-single-sign-on-work/>*