educative

Let's talk about…

SSL / TLS
and
HTTP / HTTPS !!!

Tech Stuff that'll come up today:

- Web servers
- HTTP / HTTPS
- Security
- SSL/ TLS
- SSL Certifications

What is SSL / TLS?

- **SSL** (*Secured Sockets Layer*) is a web protocol developed by Netscape in the 90s for enhancing web security.

- **TLS** (*Transport Layer Security*) was developed by the Internet Engineering Task Force (IETF) as an improvement on SSL.

NOTE: it is common for peeps to use "SSL" to refer interchangeably to both **SSL** and **TLS**.

The History

SSL

- SSL was originally developed by **Netscape** in 1995 with **SSL 2.0**
- **(SSL1.0** was never released to the public.)
- **SSL 2.0** was replaced by SSL 3.0 in 1996 after a number of vulnerabilities were found. *(Note: Versions 2.0 and 3.0 are sometimes written as **SSLv2** and **SSLv3**.)*

TLS

- TLS was introduced in 1999 as a new version of SSL and was based on SSL 3.0.
- As of 21 March 2018, **TLS 1.3** is an *Internet Draft* proposed to Internet Standard. (*It is based on the earlier TLS 1.2 specification.*)

What is an…

SSL Certificate?

SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details.

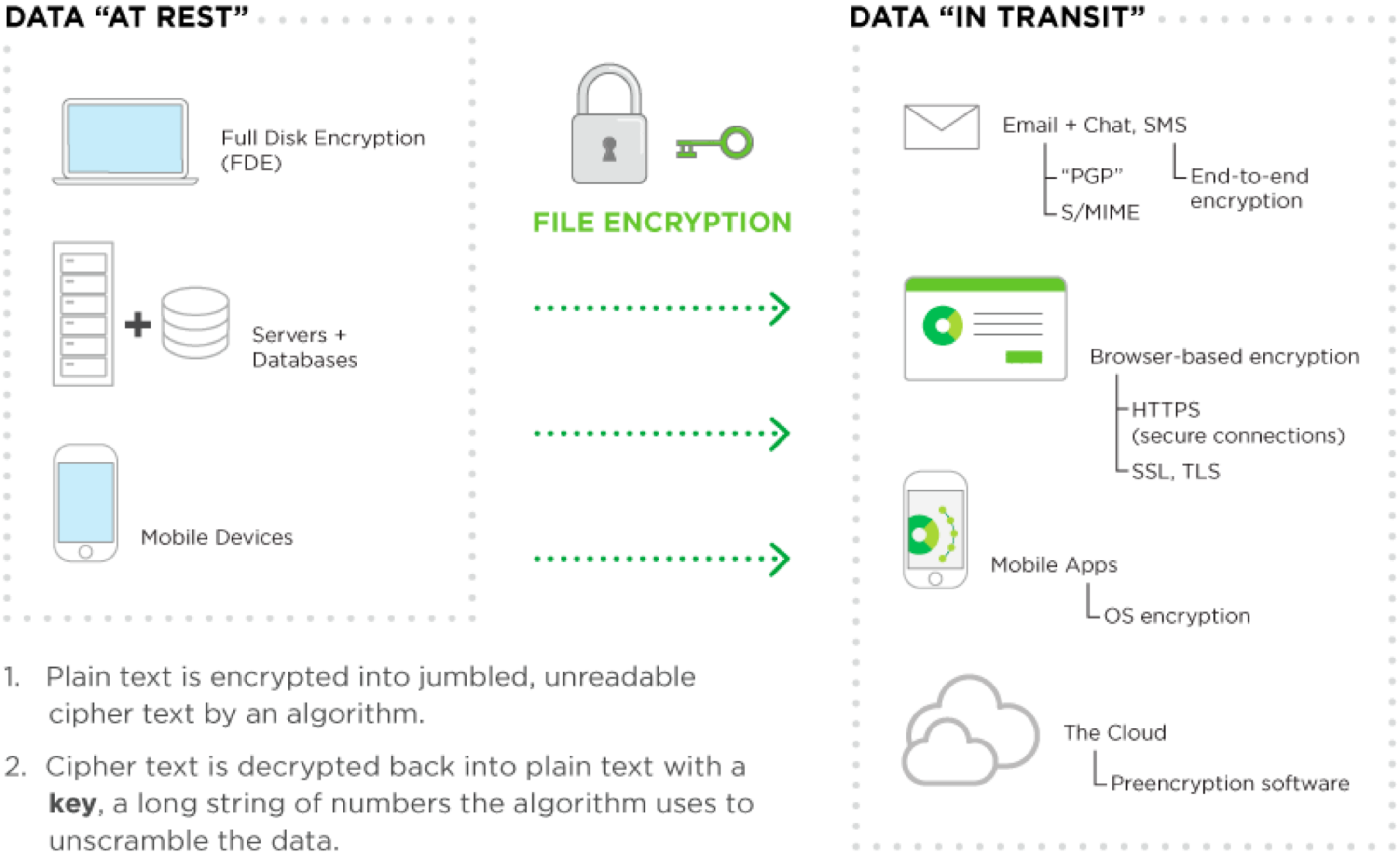
A cryptographic key is a string of bits used by an algorithm to transform plain text into cipher text or vice versa.

(i.e. ***encryption*** & ***decryption***)

When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.

Protecting Your Data With Encryption

There are two basic types of data that encryption is designed to protect: **at rest data** and **data in transit**. If a computer, hard drive, or database is hacked, encryption makes the data unreadable. If data that's in transit—between browsers, in email, or to the cloud—is intercepted, encryption keeps it safe.



DATA "AT REST"

Full Disk Encryption (FDE)

Servers + Databases

Mobile Devices

FILE ENCRYPTION

DATA "IN TRANSIT"

Email + Chat, SMS
- "PGP"
- S/MIME
- End-to-end encryption

Browser-based encryption
- HTTPS (secure connections)
- SSL, TLS

Mobile Apps
- OS encryption

The Cloud
- Preencryption software

1. Plain text is encrypted into jumbled, unreadable cipher text by an algorithm.
2. Cipher text is decrypted back into plain text with a **key**, a long string of numbers the algorithm uses to unscramble the data.

* Image credit goes to ***UpWork***: https://bit.ly/2jwFmIl

What does it look like?

- Here’s a very simple example. Say you want to encrypt this sentence:

  “Protect your data with encryption.”

- If you use a 39-bit encryption key, the encrypted sentence would look like this:

  “EnCt210a37f599cb5b5c0db6cd47a6da0dc9b728e2f8c10a37f599 cb5b5c0db6cd47asQK8W/ikwIb97tVolfr9/Jbq5NU42GJGFEU/N5j 9UEuWPCZUyVAsZQisvMxl9h9IwEmS.”

- Now you can send that encrypted message to someone, separately share the key…

And they’ll be able to **decrypt** it and **read** the original sentence! ☺

What does an… SSL Certificate even do ?

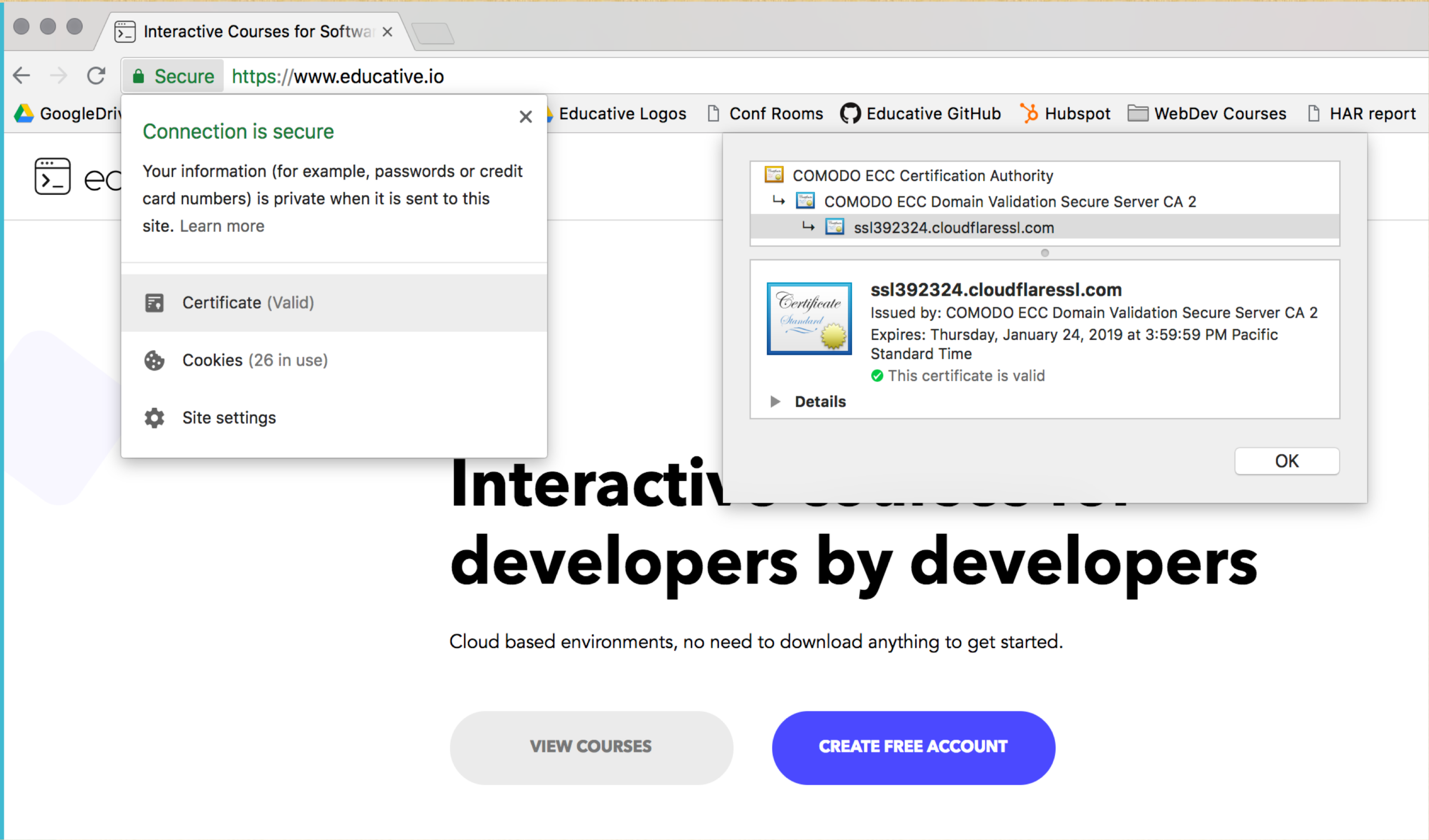
Overall, SSL is used to secure stuff like:

- ✓ **credit card transactions**
- ✓ **data transfer**
- ✓ **logins**
- ✓ But more recently, it's becoming the norm when **securing browsing of social media sites**.

SSL Certificates bind together:

- A **domain name, server name** or **hostname**.
- An **organizational identity** (*i.e. company name*) and **location**.

What does a website with an SSL Certificate installed look like?



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

ssl392324.cloudflaressl.com

Issued by: COMODO ECC Domain Validation Secure Server CA 2

Expires: Thursday, January 24, 2019 at 3:59:59 PM Pacific Standard Time

✓ This certificate is valid

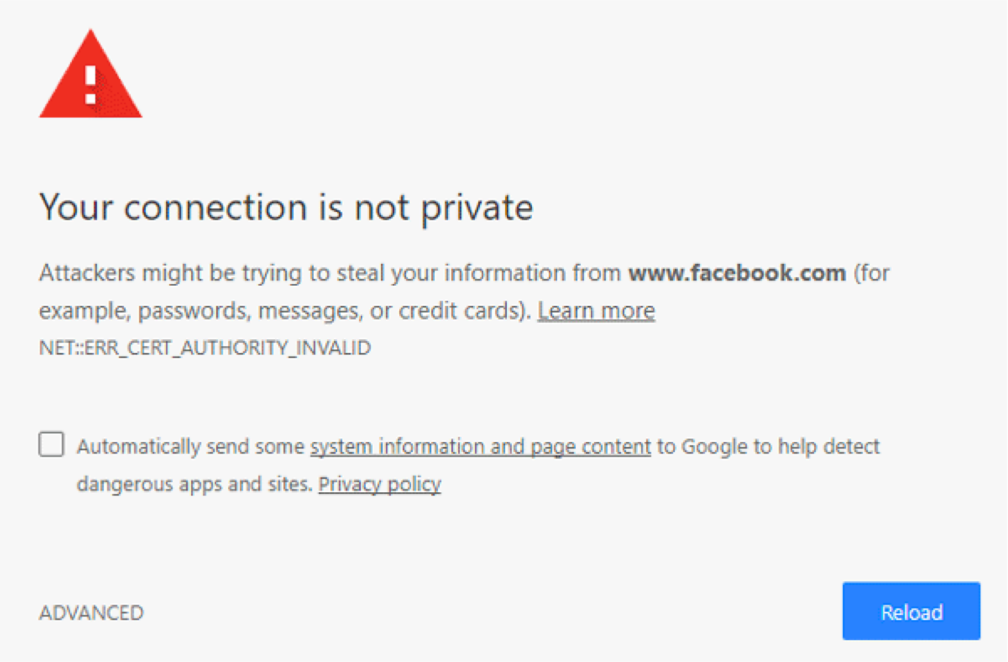
Interactive Courses for developers by developers

Cloud based environments, no need to download anything to get started.

What other types of **SSL certificates** are there?

Self-signed certificates:

- These aren't really used for authentication since they aren't issued by a *certificate authority*. ***(But** they **can** be used for encryption.)*
- These certificates **trigger the browser to raise a warning** for the user.
- Typically used by web dev teams as a cheap solution to setting up SSL-enabled web servers for testing/development.



Your connection is not private

Attackers might be trying to steal your information from **www.facebook.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

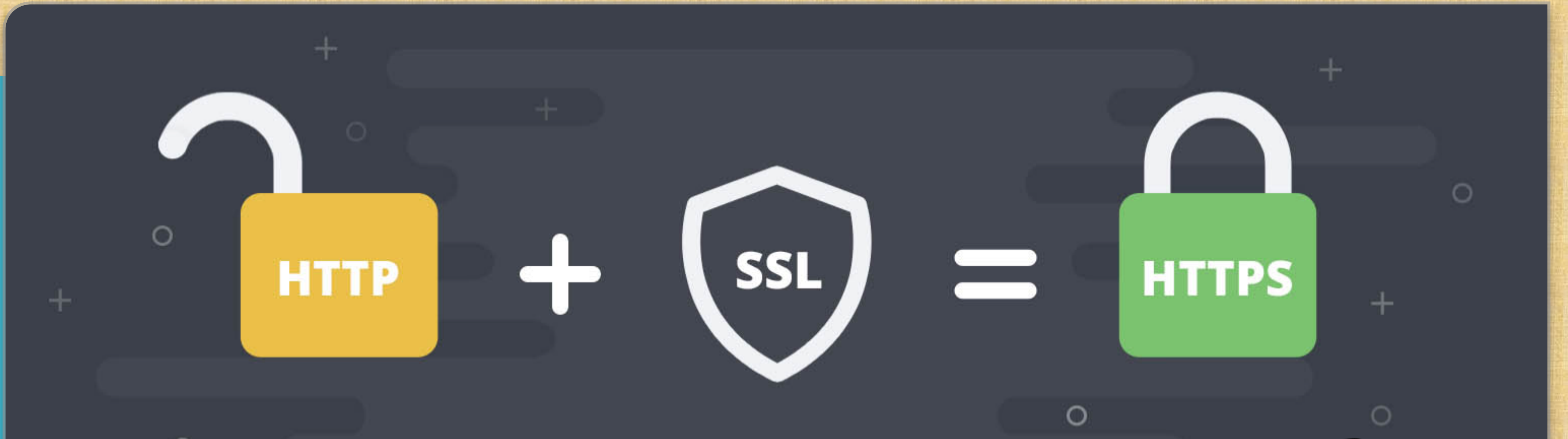
□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

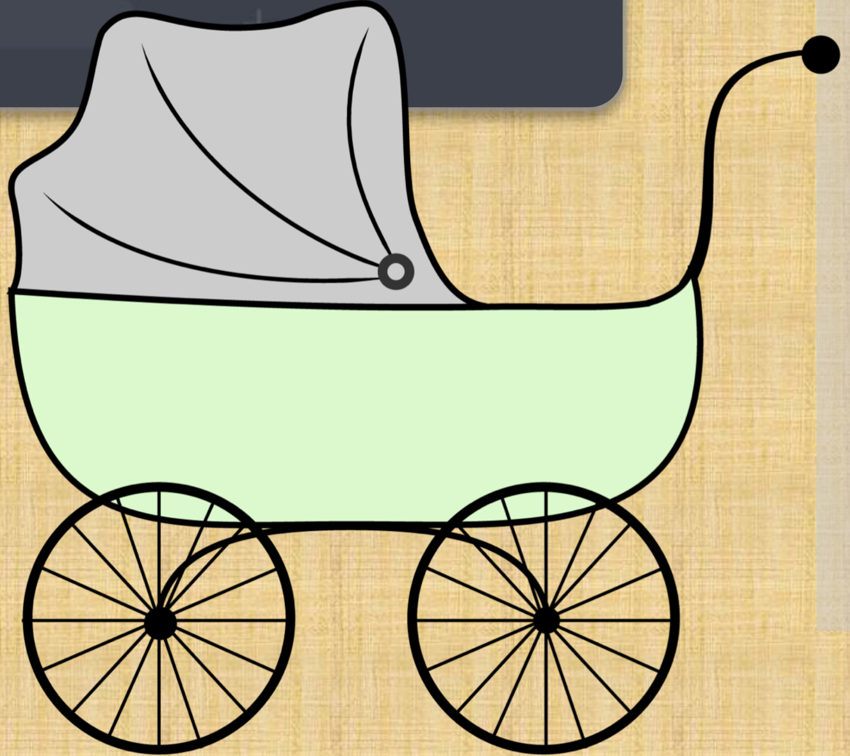
What is HTTP?

- HTTP stands for **H**yper**t**ext **T**ransfer **P**rotocol.
- HTTP is used to structure requests & responses over the internet.
- HTTP requires data to be transferred from one point to another over the network.

HTTP

https





The marriage of SSL & HTTP !

So… then what is **HTTPS** ?

1) HTTPS --*short for HTTP Secure*-- allows you to encrypt data that you **send** and **receive**.

2) HTTPS is important to use **when passing** *sensitive* **or** *personal* **information to** & **from websites**.

3) It is up to the businesses maintaining the servers to set it up.

4) In order to support HTTPS, the business must apply for an *SSL certificate.*

HTTPS

Congratulations !

Now you too can brag & nerd out with other techies about **SSL / TLS** and **HTTPS** stuff!