Do CPOs Need to Learn How to Code?

—

Paul Ohm (Georgetown), Joseph Lorenzo Hall (CDT)

Q: Do CPOs need to know how to code?

A: No.

Q: Do CPOs need to know how to code?

A: No. (but can’t hurt)

Introduction

Paul Ohm

Georgetown Law
Professor of Law

- Technical background
- Worked at DOJ/CCIPS (trial attorney) and FTC (policy advisor)
- Teaches “The Technology of Privacy” to law students
- Author of the only law review article that is also a working computer program: 54 Villanova Law Review 117

Joseph Lorenzo Hall

CDT
Chief Technologist

- Hard science background (astrophysics)
- Technical background (“hacking” voting machines)
- Raised by policy-focused lawyers (P. Samuelson, D. Mulligan), computer scientists (D. Wagner, E. Felten) and philosophers (H. Nissenbaum)

Goals for this session

Our goal: an interactive discussion around the technical insight C-level privacy and policy professionals must have to do their jobs well

We cannot possibly “make you technical” in the time we have

However, we can give you a flavor for places to do further research

And we can definitely give you insight into particular questions that bug you

Our Approach

Internet-centric

Specific technical concepts connected to real legal and policy conflicts

For each example:

- The benefits of “n++” knowledge
- Highlight misconceptions from “n” knowledge

Good decisions increasingly need technical input

Rep. Chaffetz discussing SOPA and Sandia National Labs letter

(open video below in Chrome)

https://josephhall.org/papers/ShmooCon-2015/pictures/bring-in-nerds.mp4

Let’s start with you!

What kinds of technical issues do you encounter on a regular basis that you’d like to get smarter about?

What do you secretly not understand as well as people think you do?

Outline

Basic layered framework of networks and computers

Examples:

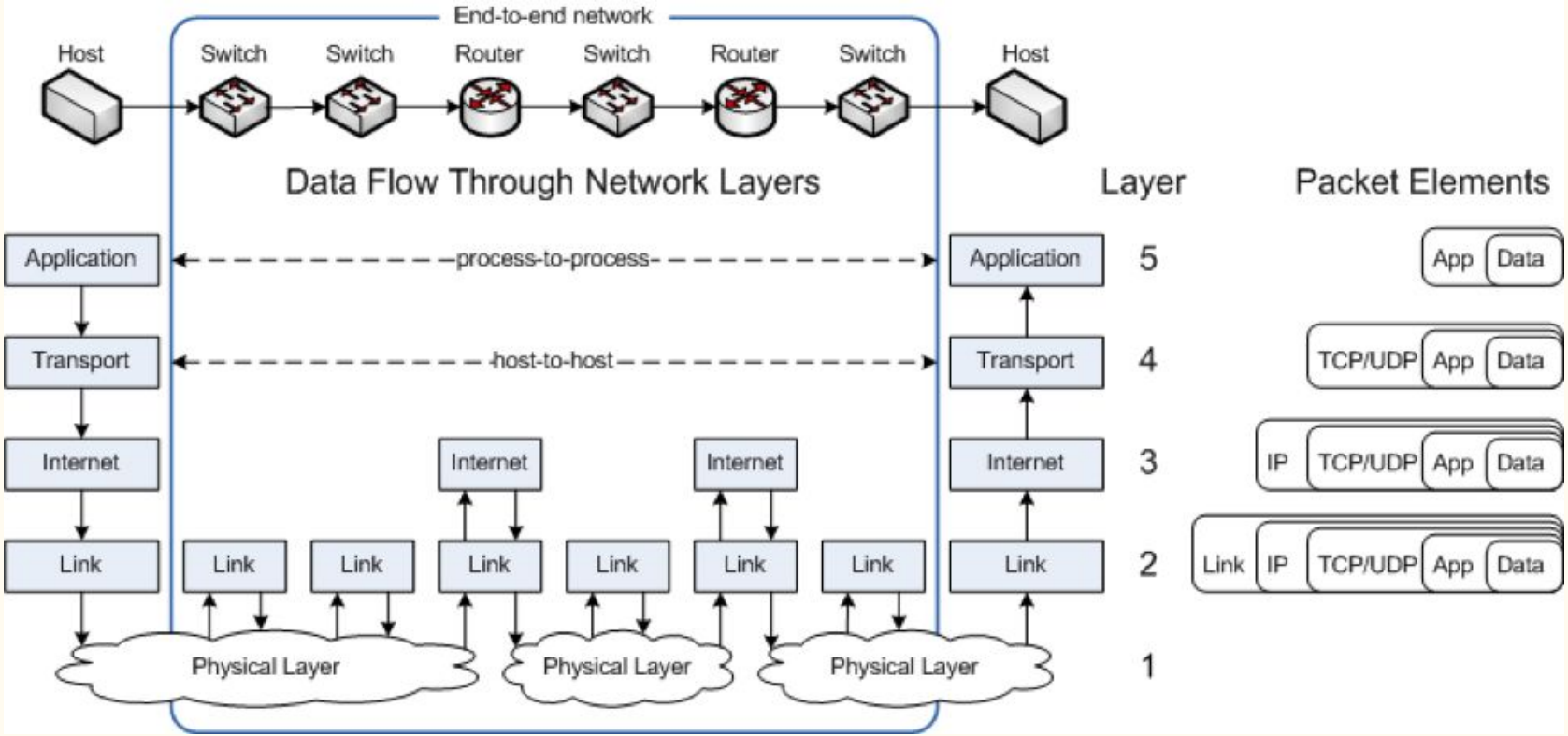
- -Internet Protocol addresses
- -Source vs. binary code
- -Software vulnerabilities
- -HTTP/HTTPS (web)
- -Crypto 101

“The Playbook”

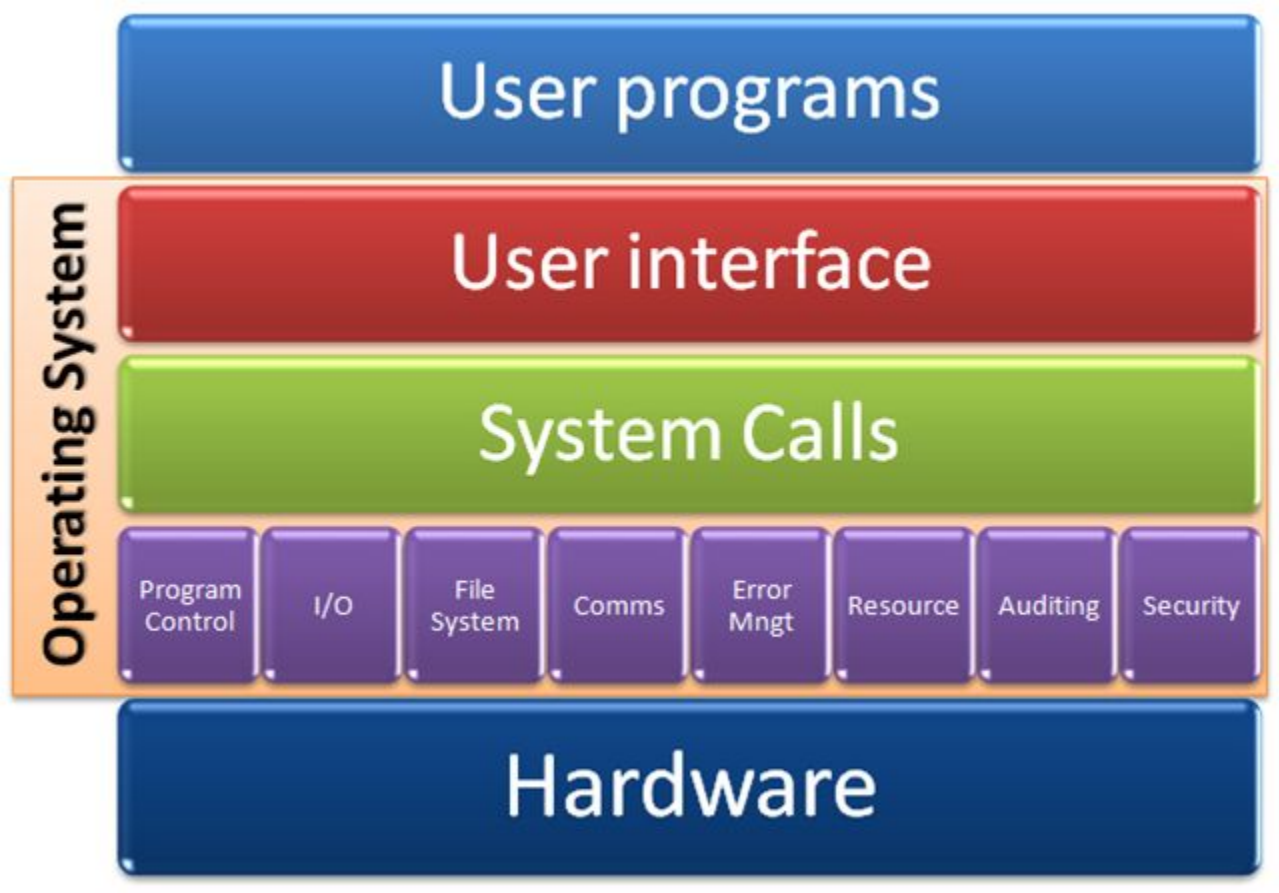
Acquiring Skills: Get your hands dirty!

A Framework

Network Model



Computer Model (or “software stack”)



Examples

Basic Internet Architecture – IP addresses

What they are: 141.161.191.223 or 104.20.11.17

How they are allocated

“Uniqueness”

Network Address Translation (NAT)

Log files as 21st century crime scene

```
69.41.16.195 - - [22/Oct/2015:16:35:36 -0700] "GET /drugs/cocaine/buy.cgi
HTTP/1.1" 200 4242 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5)
AppleWebKit/601.1.56 (KHTML, like Gecko) Version/9.0 Safari/601.1.56"
```

Basic Internet Architecture – DNS

Humans would rather remember www.cdt.org than 104.20.11.17 (IP Address)

The Domain Name System is a hierarchical, distributed resource for looking up IP addresses of domains

DNS can be an Internet chokepoint

- privacy implications

Relevant to SOPA/PIPA

- filtering of DNS traffic

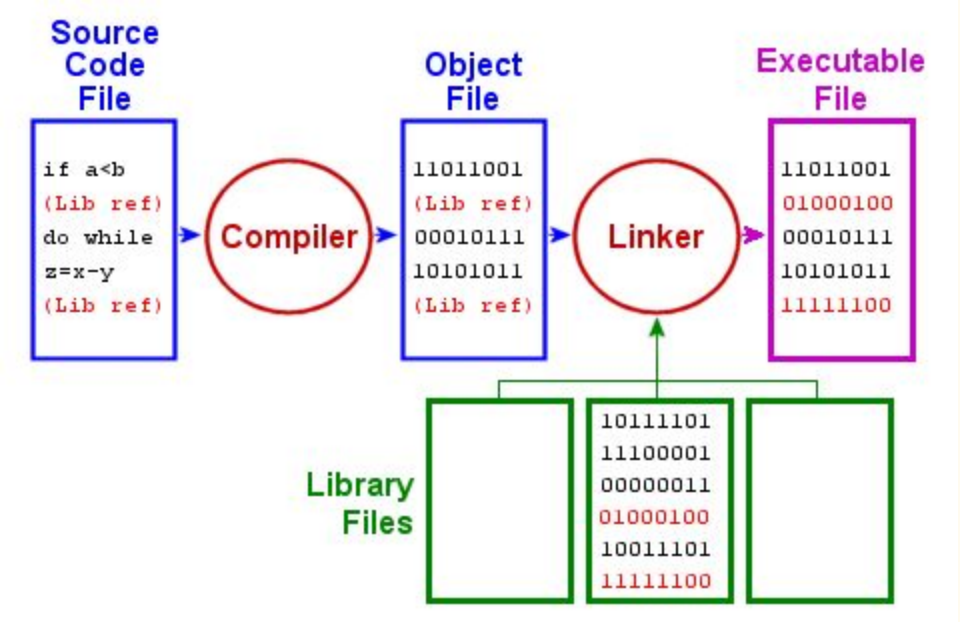
Source Code vs Executable (Binary) Code

source code is *compiled* into *object code* which is then *linked* to *libraries* to produce *executable (binary) code*

Most software is distributed in binary

Open source software distributes source, generously licensed

-Reverse engineering
-White vs black box testing
-Static analysis/fuzzing

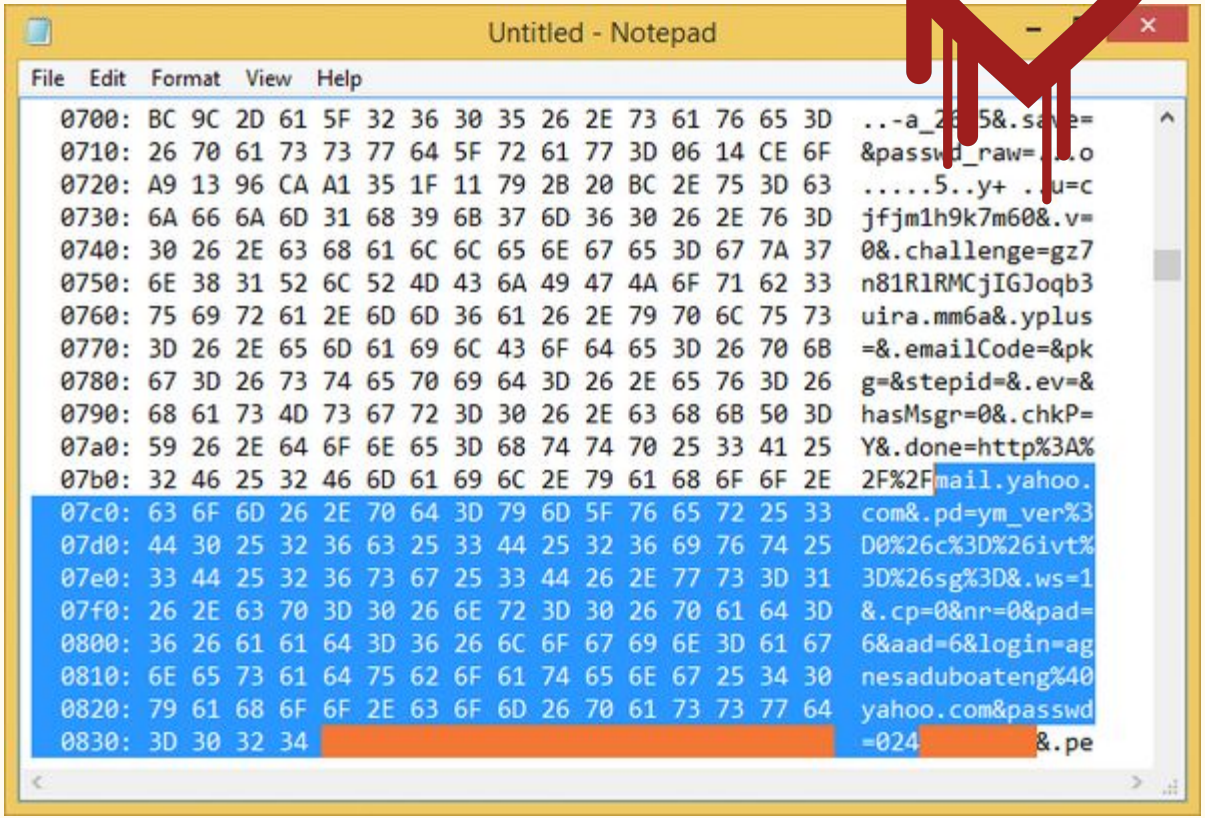


Software vulnerabilities and Safer code

Software has bugs!

Heartbleed was serious, due to a bug in OpenSSL

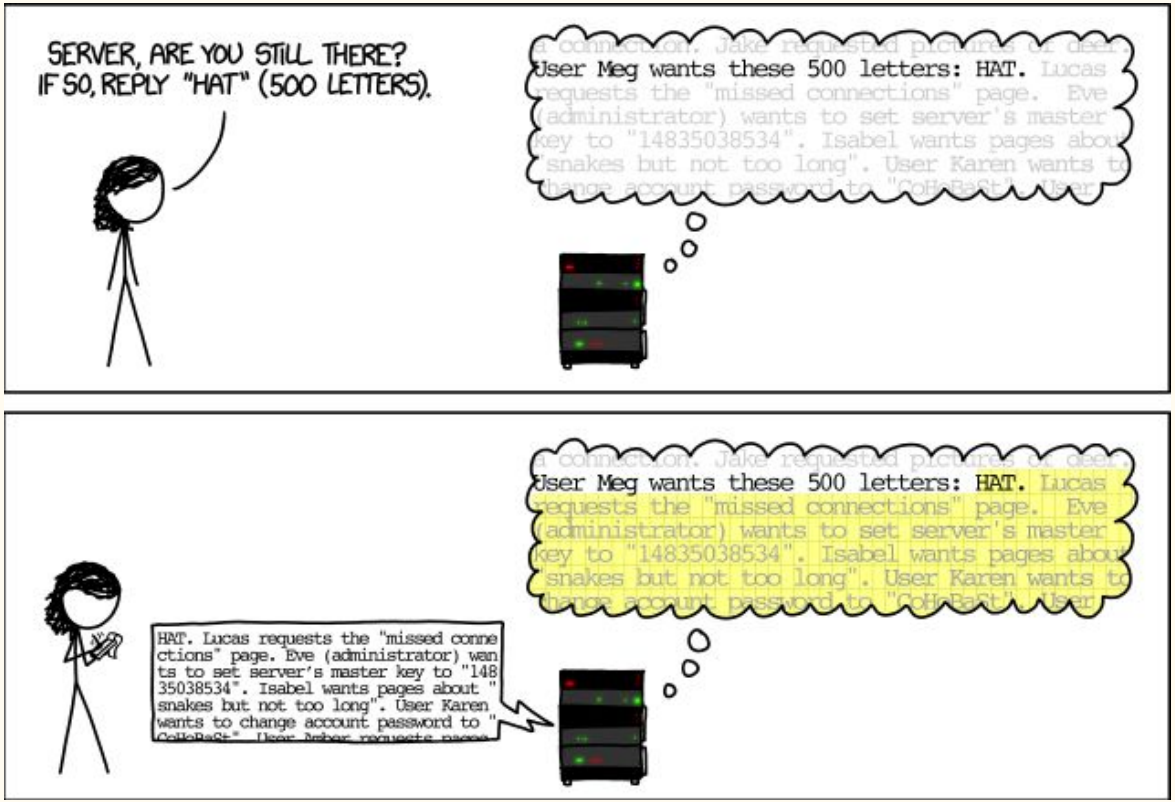
Allowed one to extract memory from 17% of trusted servers around the world!



Software vulnerabilities and Safer code

Data validation at the heart of heartbleed

Type safety and emerging coding standards help avoid these problems



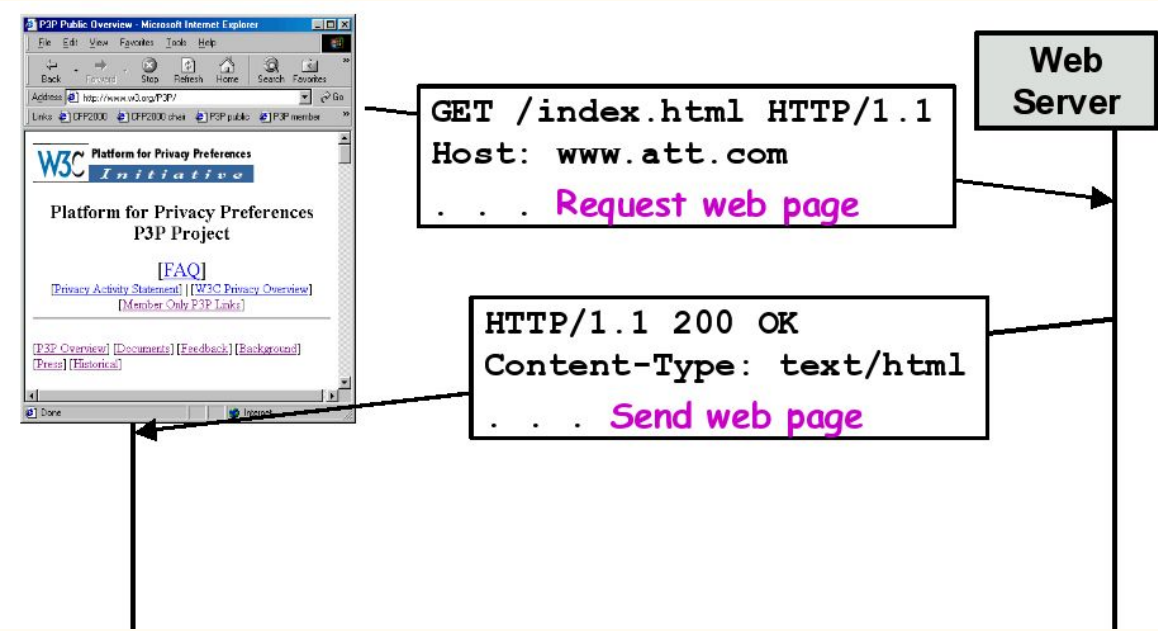
Protocols - HTTP/HTTPS

HTTP is the protocol of the web (hypertext)

HTTP URLs specify location on the web: http://www.cdt.org/

Structured set of message exchanges that result in the source code for a web page

Browsers then display



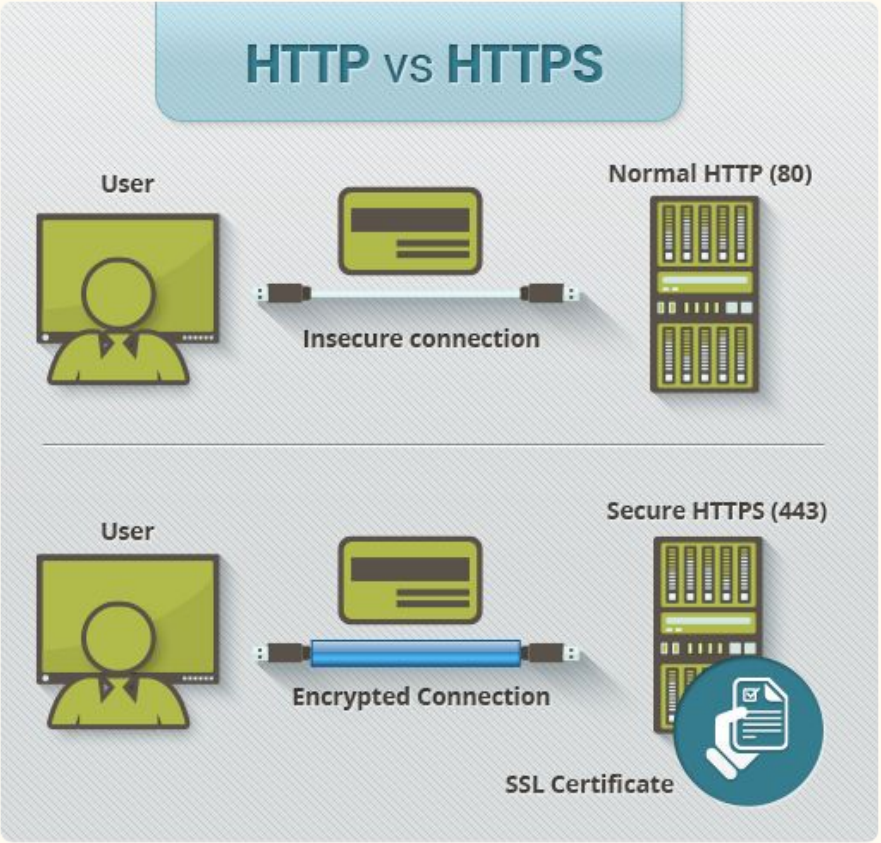
Protocols - HTTP/HTTPS

HTTPS is the *secure* version of HTTP

Authenticated and encrypted

Relies on SSL (sic) certificates

SSL is old, broken; TLS is the new hotness

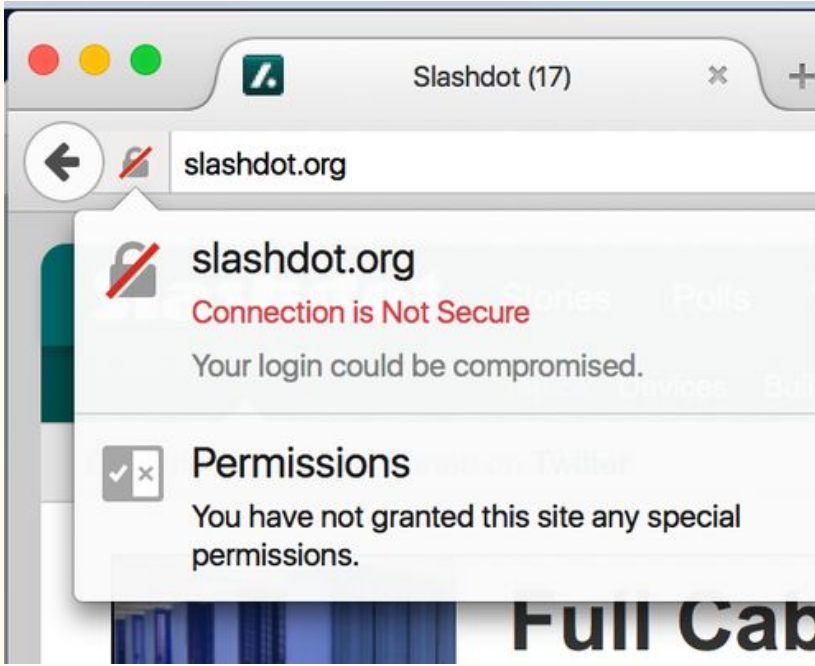


Protocols - HTTP/HTTPS

Increasing use of HTTPS since Snowden revelations

However, general recognition that *integrity* just as important as *confidentiality*

-Technical standards (IETF, W3C, IEEE)
-.gov HTTPS-Only by end of 2016
-Major content (news, video), advertising
-Browsers “deprecating” HTTP



Crypto 101: What's the point?

Confidentiality - only authorized parties can access information

Authentication - validation of a credential as identification of source

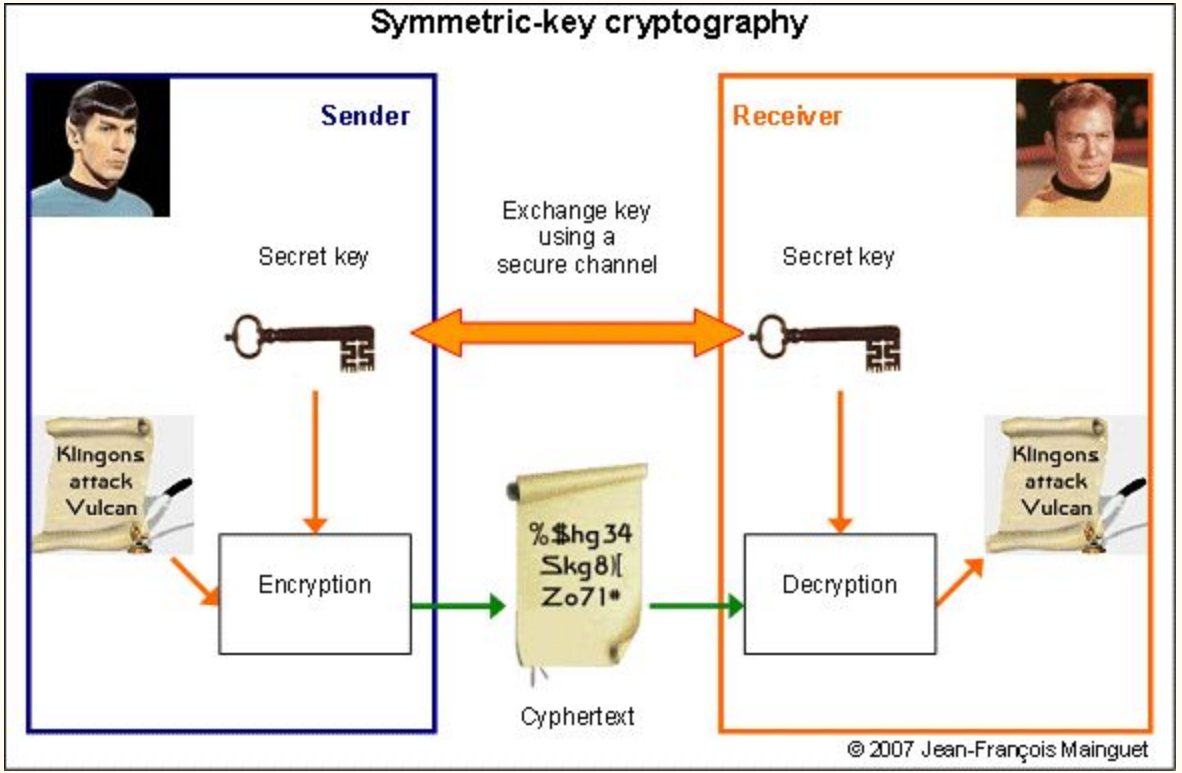
Integrity - information has not been modified (e.g., between sender/receiver)

Non-repudiation - cannot deny having encrypted information

Crypto 101: Symmetric cryptography

Works like a lock in the real world: Same key used to unlock and lock (decrypt and encrypt)

However, distributing the key then becomes the hard problem!

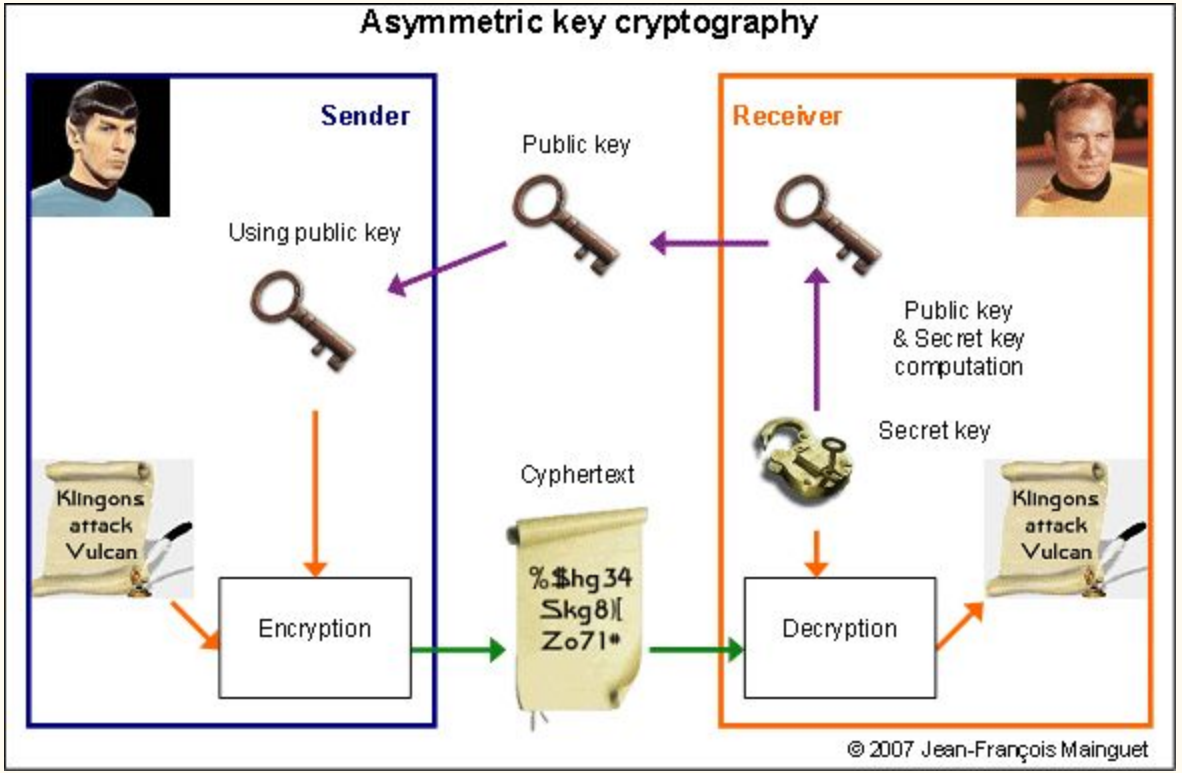


Crypto 101: Asymmetric cryptography

Works unlike locks in the real world: Different key for lock/unlock

Solves the key distribution problem: can share the locking key (the “public key”)

But keep the unlocking key (the “private key”) super-secret!



Crypto 101: Hashes and Signatures

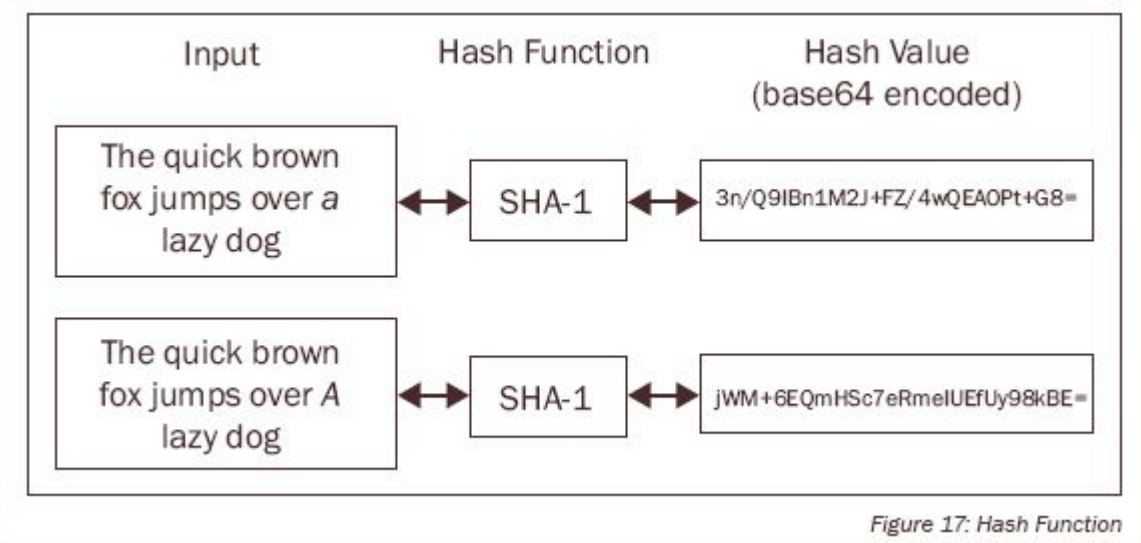
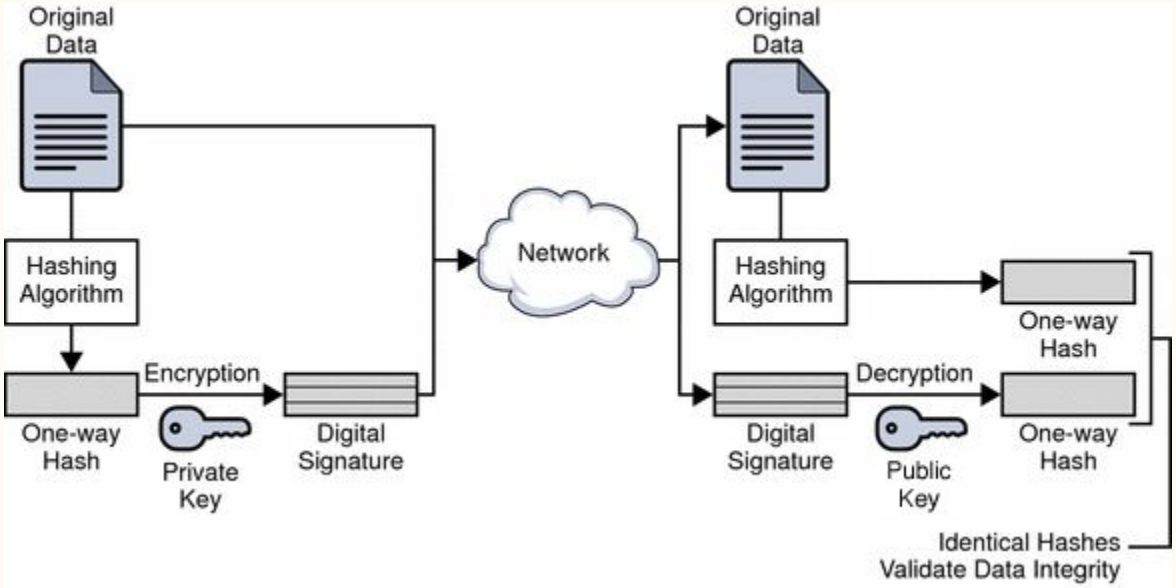


Figure 17: Hash Function

Crypto 101: Hashes and Signatures



Crypto 101: Certificate Authorities/PKI

PKI = Public Key Infrastructure

wraps *public key* in *cryptographic signature* to produce “certificate”

a certificate is simply the result of:

a trusted entity (a “certificate authority”)
vouching for/attesting to the fact that
a given named entity (“Joseph Hall”, “josephhall.org”)
possesses the secret key that corresponds to the private key.

“The Playbook”

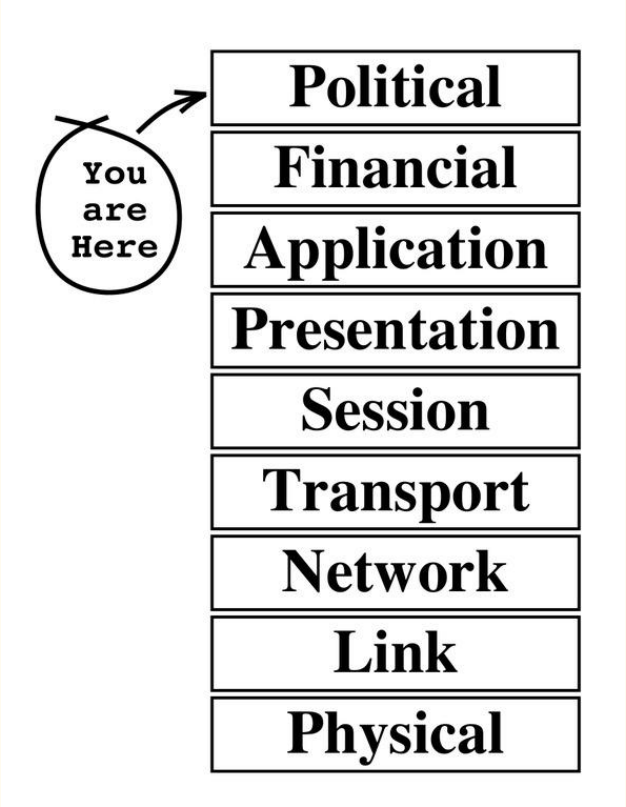
Analogies

“Her eyes were like two brown circles with two big black dots in the center.” (Russell Beland, Springfield)

“He was as tall as a six-foot-three-inch tree.” (Jack Bross, Chevy Chase)

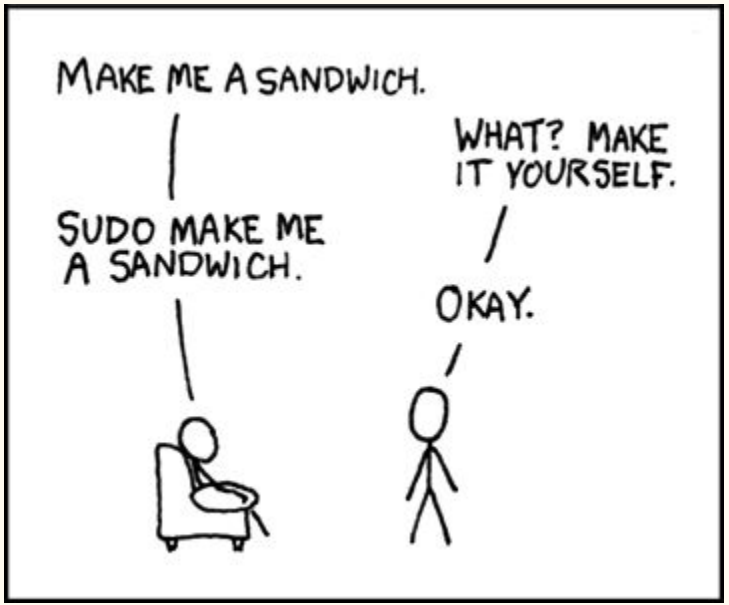
-- Honorable Mentions, Washington Post Style Invitational, “Simile Outrageous”, July 23, 1995

Layers of Abstraction



Credit:
Evi Nemeth

The Myth of the Superuser



More Pages from the Playbook

Felten's Third Law

Harry Surden's Theory of Structural Rights in Privacy

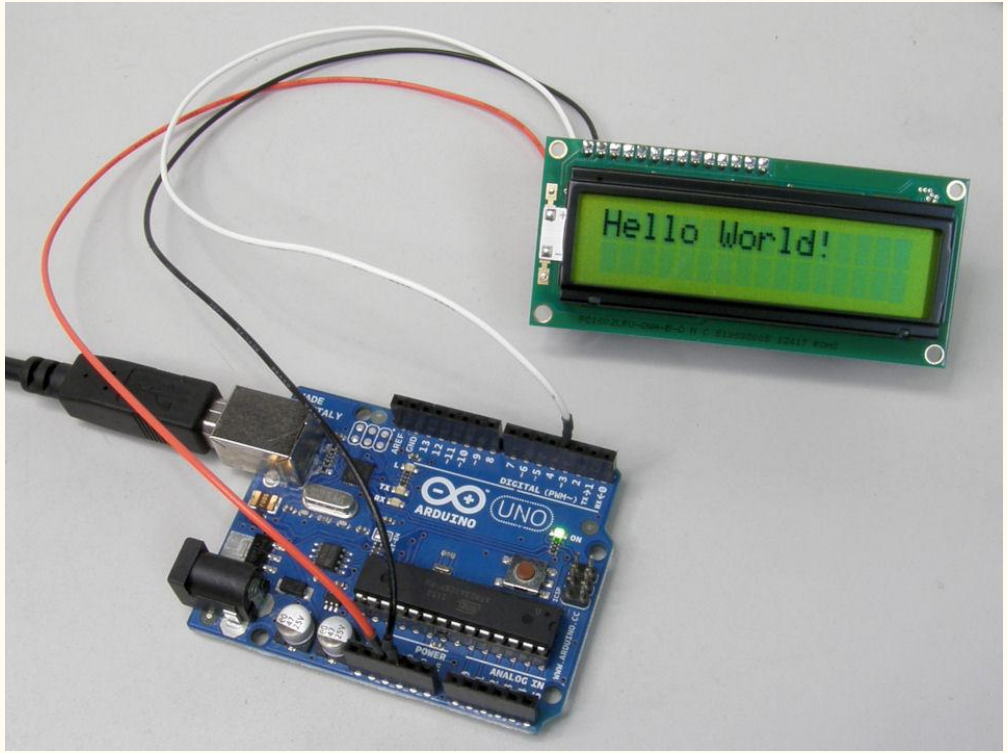
Code is Law (Lessig / Reidenberg), and why it matters

Tussle Spaces -- Dave Clark et al.

Others?

Acquiring Skills

Get Your Hands Dirty!



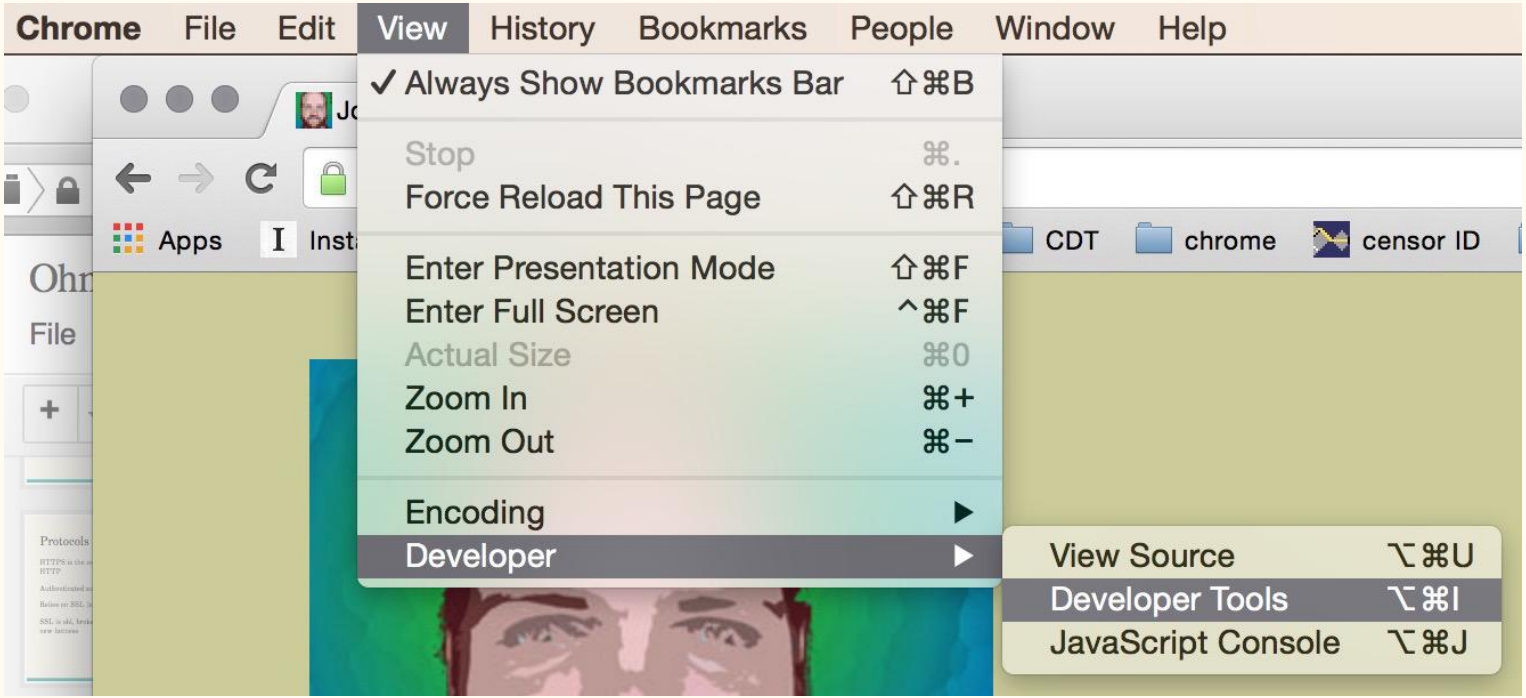
The Golden Age of Learning Technology

Chrome Developer Tools

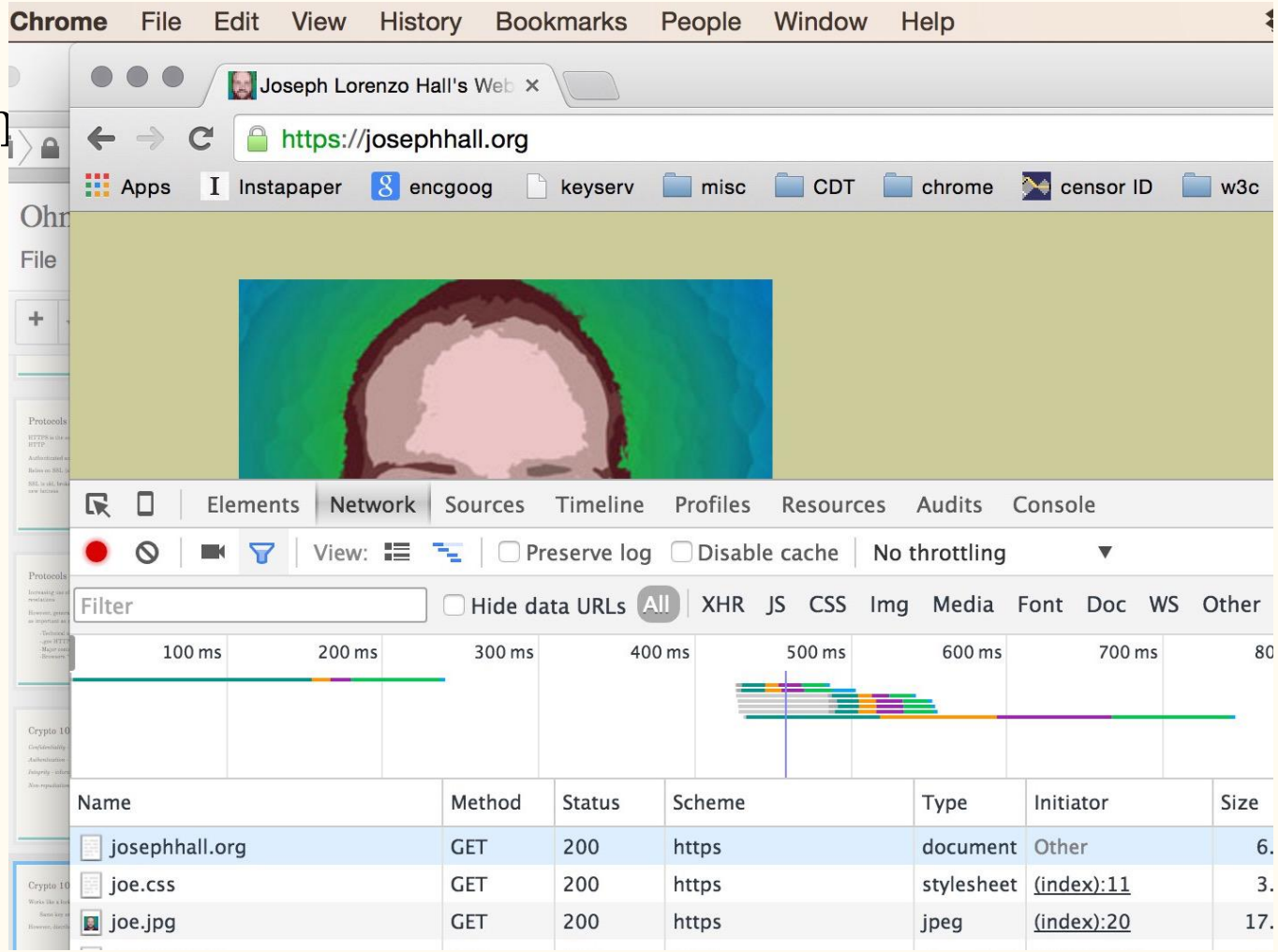
Amazon Web Services (or competitor service)

mitmproxy

Chrome Developer Tools



Chron


Chrome File Edit View History Bookmarks People Window Help
Joseph Lorenzo Hall's Web
https://josephhall.org
Apps Instapaper encgoog keyserv misc CDT chrome censor ID w3c
Elements Network Sources Timeline Profiles Resources Audits Console
View: Preserve log Disable cache No throttling
Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Other
100 ms 200 ms 300 ms 400 ms 500 ms 600 ms 700 ms
Name Method Status Scheme Type Initiator Size
josephhall.org GET 200 https document Other
joe.css GET 200 https stylesheet (index):11
joe.jpg GET 200 https jpeg (index):20

Thank you!