Lecture 19 - security - and signatures

News

1. The stimulus bill included a “digital currency”. https://www.forbes.com/sites/michaeldelcastillo/2020/03/25/trillion-dollar-stimulus-jumpstarts-project-to-issue-central-bank-currency-on-ethereum/#69f5d60c47bc

Personal Security - Why

Tell a story - AWS.

Why is this happening?

Systems that survive pay out to all the responsible parties in proportion to the level of responsibility.

“The Tragedy of the Commons”

Friction vs Access

Friction to get to the information you want is security to prevent unauthorized people from getting to the information that you don’t want them to get to.

People will choose convenience over security every time.

Data ownership. Equafax and what data you have as public.

Passwords

Top 10 List

```
123456
123456789
qwerty
12345678
111111
1234567890
1234567
password
123123
987654321
```

Represent 76% of passwords in use.

Top 10000 passwords are 92% of passwords in use.

Hash passwords: MD5, SHA1

Rainbow Tables

Salt and then Hash

use a hash that is appropriate: bcrypt, scrypt, or PBKDF2.

1. Generated Passwords (1password or other similar tools). `#!/bin/bash openssl rand –base64 20`
2. Never change passwords
3. Write it down.
4. Use a system that verifies that your password is not pwned.

Other security systems good/bad.

1. Auth0 - JWT
2. Password-less login systems
3. Biometrics
4. Biometrics that works
5. NFC
6. Wireless WiFi and security
7. IOT
8. Back doors into systems
9. Chipping dogs - why not people?
10. Software is never 100% fixed.

Security == Friction

“Making Password Cracking Harder: Slow Hash Functions” Proof of Work: PBKDF2.

Risk of pandemic is really an airline - high speed transpiration system.

Speed Limits: highways - approaches to airports. Drugs - require prescriptions.

Digital information moves limitlessly. The same design philosophy that accelerated the flow of correspondence, news, and commerce also accelerate the flow of phishing, ransomware, and

disinformation.

Free isn't free.

Sherman Antitrust Act: 1989 Supreme Court Decision - that evaluation of an illegitimate merger be based on price of goods produced.
We are now in a world where 0 price is common.

So if you give away your product (e.g. Facebook) then you purchase some other entity (Instagram) and give it away for free then the SAA will not apply to you.

Who Pays.

During the height of the recession, in 2009, we wasted 6.3 billion hours on the road.

Capitalism is suffering from its own success.

Real Solutions - public private keys and signatures

This is our homework - to sign a document and validate it on the server. I provided the server and part of the client (you get to make the library calls to do the "sign" part) and I provided a command line sign tool. (Hint - it has the sign code in it - look in the homework it will direct you to the correct file and functions)

For authentication you can use a zero-knowledge proof system called SRP6a - search for that "Secure Remote Password SRP6a" and there are implementations for most languages.

Interesting side note: the Wikipedia page on this has a Python program that sort of works to do SRP6a. It will work in sending stuff to a duplicate copy of the program and it has the correct algorithm in it. In one 4 line section of code it also has 5 type conversion errors that will cause about 1 in 16 messages to get the wrong results. YMMV on example code! (the code also appears in the standard for SRP6a!)

SRP6a is used in SSH for remote logins! so most of you have used it already. It has been around for a long time. The good side - the server has a validation number instead of your password - so - it can never leek your password. Also this is a "strong" authentication system based on cryptography - not just pass the password over the wire authentication.