

CSE 484 / CSE M 584: Final Words on Web Security & Authentication

Fall 2022

Franziska (Franzi) Roesner
franzi@cs

UW Instruction Team: David Kohlbrenner, Yoshi Kohno, Franziska Roesner. Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Announcements

- **Lab 2:** Ongoing
- **Today and this week's section:** Authentication
- **Guest lecture** on Wednesday
 - Emily McReynolds
 - Topic: Law & policy
 - No recording (please attend in person)

Cross-Origin Communication

- Sometimes you want to do it...
- Cross-origin Resource Sharing (CORS)
 - Access-Control-Allow-Origin: <list of domains>
 - Unfortunately, often:
Access-Control-Allow-Origin: *
- Cross-origin client side communication
 - HTML5 postMessage between frames
 - Unfortunately, many bugs in how frames check sender's origin

What about Browser Plugins?

- **Examples:** Flash, Silverlight, Java, PDF reader
- **Goal:** enable functionality that requires transcending the browser sandbox
- **Increases browser's attack surface**

Java and Flash both vulnerable—again—to new 0-day attacks

Java bug is actively exploited. Flash flaws will likely be targeted soon.

by Dan Goodin (US) - Jul 13, 2015 9:11am PDT

- **Good news:** plugin sandboxing improving, and need for plugins decreasing (due to HTML5 and extensions)

Goodbye Flash

Get ready to finally say goodbye to Flash — in 2020

Posted Jul 25, 2017 by [Frederic Lardinois \(@fredericl\)](#)



Next Story



“As of mid-October 2020, users started being prompted by Adobe to uninstall Flash Player on their machines since Flash-based content will be blocked from running in Adobe Flash Player after the EOL Date.”

<https://www.adobe.com/products/flashplayer/end-of-life.html>

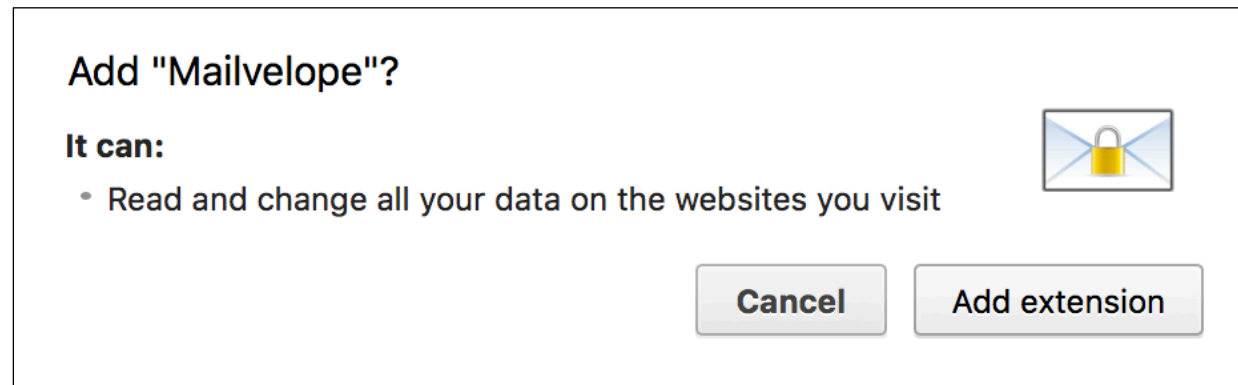
What about Browser Extensions?

- Most things you use today are probably extensions
- **Examples:** Adblock, Ghostery, Mailvelope
- **Goal:** Extend the functionality of the browser

- (Chrome:) Carefully designed security model to **protect from malicious websites**
 - **Privilege separation:** extensions consist of multiple components with well-defined communication
 - **Least privilege:** extensions request permissions

What about Browser Extensions?

- But be wary of malicious extensions: **not subject to the same-origin policy** – can inject code into any webpage!

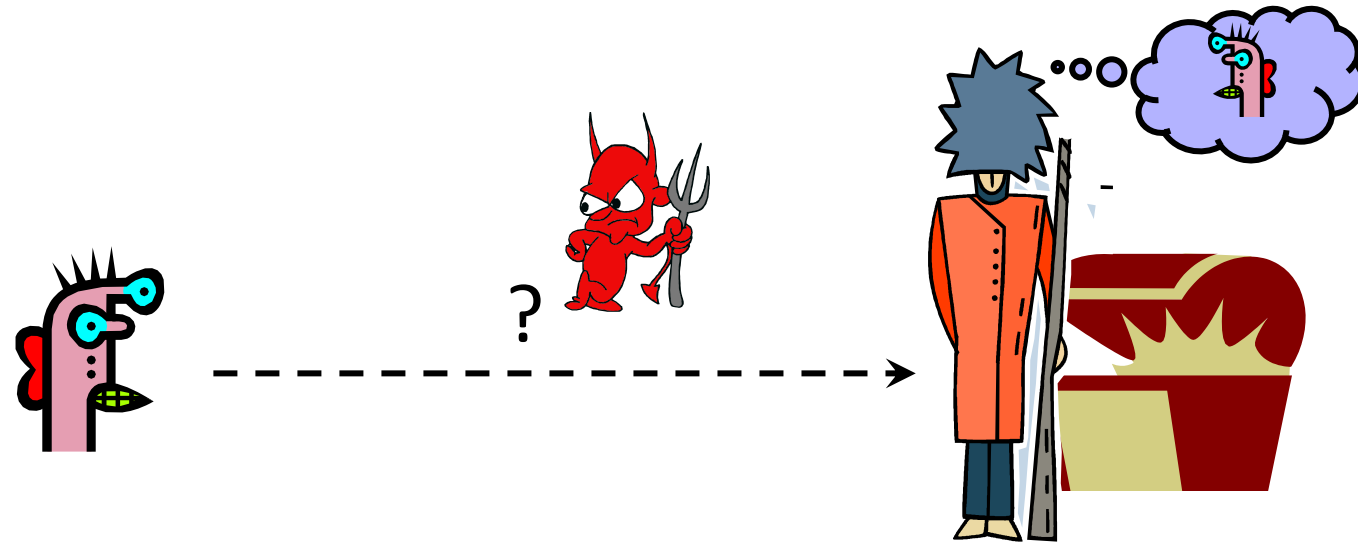


- Today: Extensions in flux – new “Manifest v3” specification from Google, trying to make things safer.

Web Security Summary

- Browser security model
 - Browser sandbox: isolate web from local machine
 - Same origin policy: isolate web content from different domains
 - Also: Isolation for plugins and extensions
- Web application security
 - How (not) to build a secure website

Basic Problem



Challenge: How do you prove to someone that you are who you claim to be?

Any system with access control must solve this problem.

Many Ways to Prove Who You Are

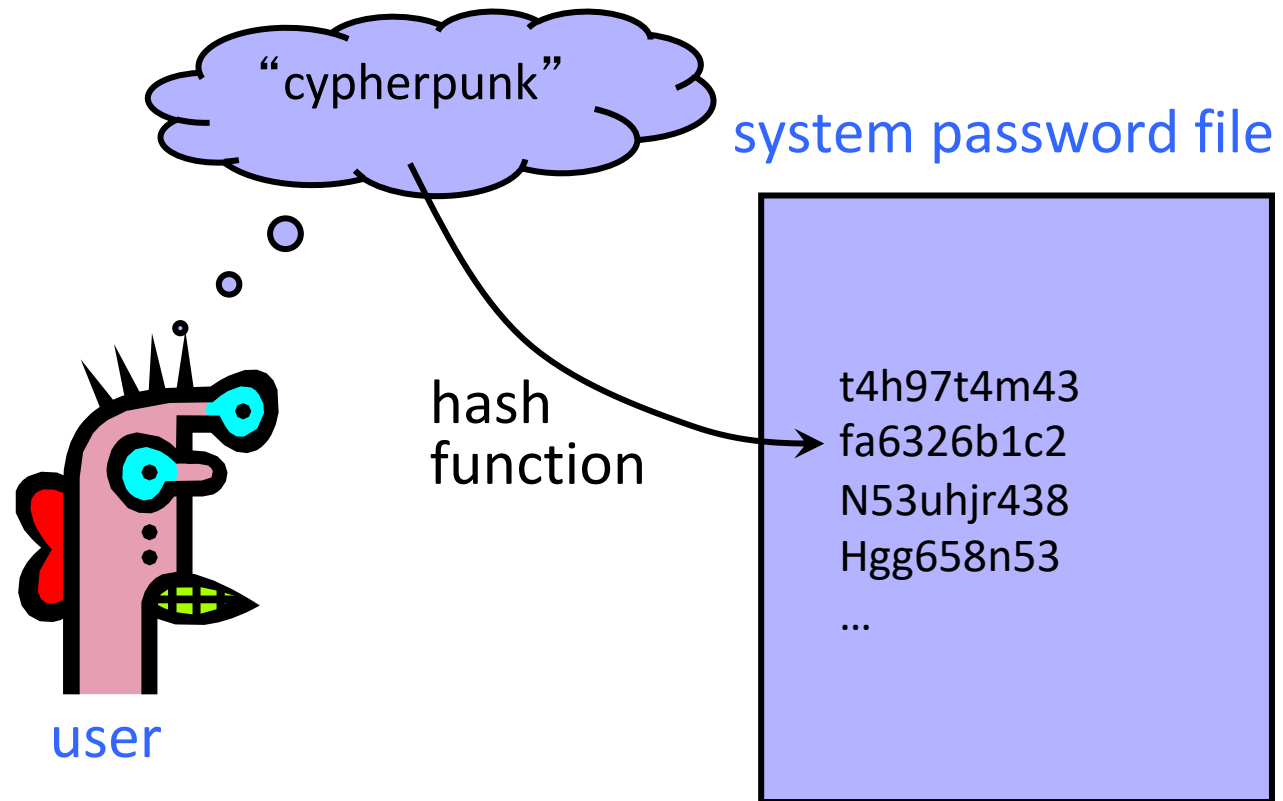
- What you know
 - Passwords
 - Answers to questions that only you know
- Where you are
 - IP address, geolocation
- What you are
 - Biometrics
- What you have
 - Secure tokens, mobile devices

Passwords and Computer Security

- In 2012, 76% of network intrusions exploited weak or stolen credentials (username/password)
 - Source: Verizon Data Breach Investigations Report
- In Mitnick's "Art of Intrusion" 8 out of 9 exploits involve password stealing and/or cracking
- First step after any successful intrusion: install sniffer or keylogger to steal more passwords
- Second step: run cracking tools on password files
 - Cracking needed because modern systems usually do not store passwords in the clear

Password Storage

- How should we store passwords on a server?
 - In cleartext?
 - Encrypted?
 - Hashed?



Password Hashing

- Instead of user password, store $H(\text{password})$
- When user enters password, compute its hash and compare with entry in password file
 - System does not store actual passwords!
 - System itself can't easily go from hash to password
 - Which would be possible if the passwords were encrypted
- Hash function H must have some properties
 - **One-way**: given $H(\text{password})$, hard to find password
 - No known algorithm better than trial and error
 - “Slow” to compute

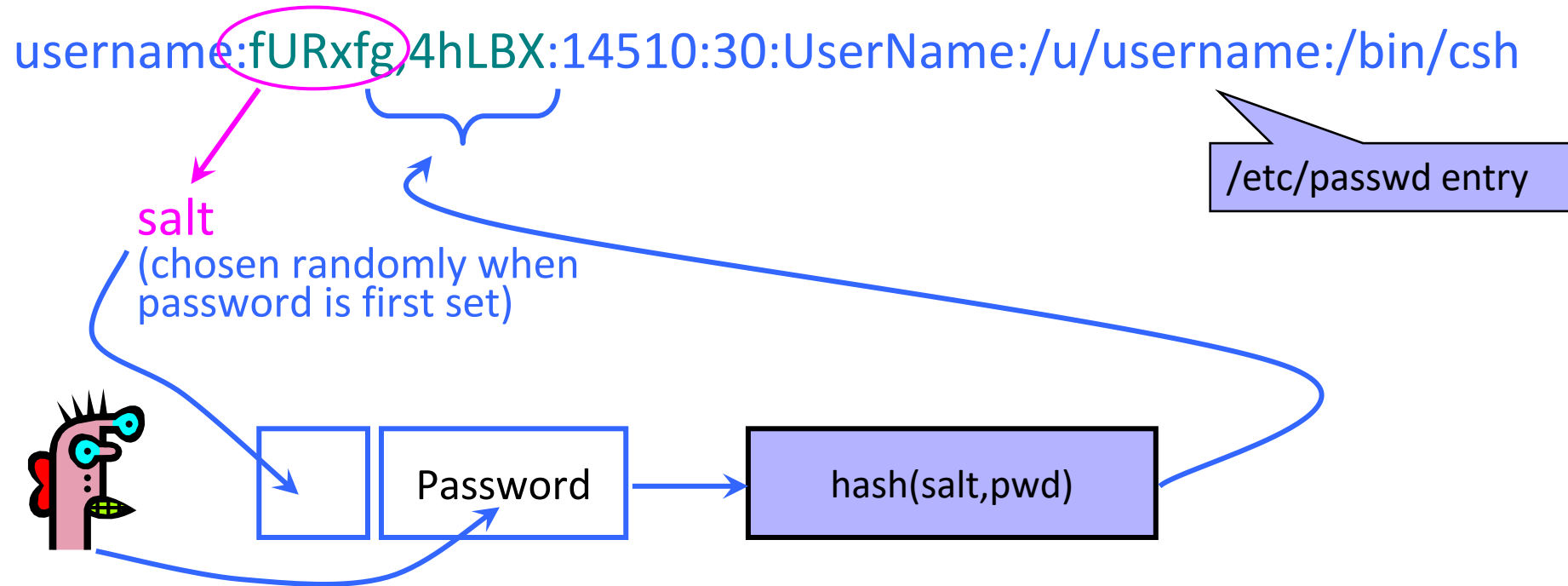
UNIX Password System

- Approach: Hash passwords
- Problem: passwords are not truly random
 - With 52 upper- and lower-case letters, 10 digits and 32 punctuation symbols, there are 94^8 == 6 quadrillion possible 8-character passwords ($\sim 2^{52}$)
 - **BUT:** Humans like to use dictionary words, human and pet names == 1 million common passwords

Dictionary Attack

- **Dictionary attack** is possible because many passwords come from a small dictionary
 - Attacker can **pre-compute** $H(\text{word})$ for every word in the dictionary. **This only needs to be done once!**
 - This is an offline attack
 - Once password file is obtained, cracking is instantaneous
 - Sophisticated password guessing tools are available
 - Take into account freq. of letters, password patterns, etc.

Salt



- Users with the same password have different entries in the password file
- Offline dictionary attack becomes much harder

Advantages of Salting

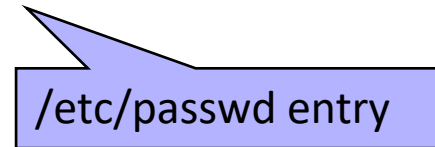
- Without salt, attacker can pre-compute hashes of all dictionary words once for all password entries
 - Same hash function on all UNIX machines
 - Identical passwords hash to identical values; one table of hash values can be used for all password files
- With salt, attacker must compute hashes of all dictionary words once for each password entry
 - With 12-bit random salt, same password can hash to 2^{12} different hash values
 - Attacker must try all dictionary words **for each salt value** in the password file
- Pepper: Secret salt (not stored in password file)

Shadow Password

username:x:14510:30:User Name:/u/username:/bin/csh



Hashed password is no longer stored in a world-readable file



Hashed passwords are stored in `/etc/shadow` file which is only readable by system administrator (root)

Other Password Security Risks

- Keystroke loggers
 - Hardware
 - Software (spyware)
- Shoulder surfing
- Same password at multiple sites
- Broken implementations
 - Recall TENEX timing attack
- Social engineering



AirDrive Forensic Keylogger

The **AirDrive Forensic Keylogger** is an innovative ultra-small USB hardware keylogger, only **0.4" (10 mm)** in length. It can be accessed with any Wi-Fi device such as a computer, laptop, tablet, or smartphone. It is the smallest hardware keylogger available on the market, making it a professional surveillance and security tool. The Pro version offers **time-stamping**, **E-mail reporting** and **data streaming**.

\$67⁹⁹ or €57⁹⁹

[More info](#)

Other Issues

- Usability
 - Hard-to-remember passwords?
 - Carry a physical object all the time?
- Denial of service
 - Attacker tries to authenticate as you, account locked after 3 failures

Default Passwords

- Examples from Mitnick's "Art of Intrusion"
 - U.S. District Courthouse server: "public" / "public"
 - NY Times employee database: pwd = last 4 SSN digits
- Mirai IoT botnet
 - Weak and default passwords on routers and other devices

Weak Passwords



- RockYou hack
 - “Social gaming” company
 - Database with 32 million user passwords from partner social networks
 - Passwords stored in the clear
 - December 2009: entire database hacked using an **SQL injection attack** and posted on the Internet
 - One of many such examples!

Weak Passwords

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Password Policies

- Old recommendation:
 - 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords...



Image from http://www.interactivetools.com/staff/dave/damons_office/

Password Policies

- Old recommendation:
 - 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords...
- **But ...** results in frustrated users and less security
 - Burdens of devising, learning, forgetting passwords
 - **Users construct passwords insecurely, write them down**
 - Can't use their favorite password construction techniques (small changes to old passwords, etc.)
 - Heavy password re-use across systems
 - **(Password managers can help)**

“New” (2017) NIST Guidelines 😊

- Remove requirement to periodically change passwords
- Screen for commonly used passwords
- Allow copy-paste into password fields
 - But concern: what apps have access to clipboard?
- Allow but don't require arbitrary special characters
- Etc.

<https://pages.nist.gov/800-63-3/sp800-63b.html>

Recovering Passwords: A Weak Link

Palin E-Mail Hacker Says It Was Easy

By [Kim Zetter](#)  September 18, 2008 | 10:05 am | Categories: [Elections](#), [Hacks and Cracks](#)

A p
obt
priv
sup
rev
too
Re|

after the password recovery was reenabled, it took seriously 45 mins on wikipedia and google to find the info, Birthday? 15 seconds on wikipedia, zip code? well she had always been from wasilla, and it only has 2 zip codes (thanks online postal service!)

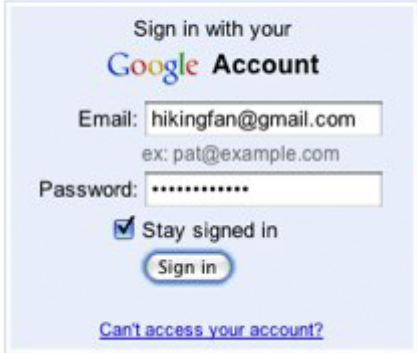
the second was somewhat harder, the question was "where did you meet your spouse?" did some research, and apparently she had eloped with mister palin after college, if youll look on some of the screenshits that I took and other fellow anon have so graciously put on photobucket you will see the google search for "palin eloped" or some such in one of the tabs.

I found out later though more research that they met at high school, so I did variations of that, high, high school, eventually hit on "Wasilla high" I promptly changed the password to popcorn and took a cold shower...

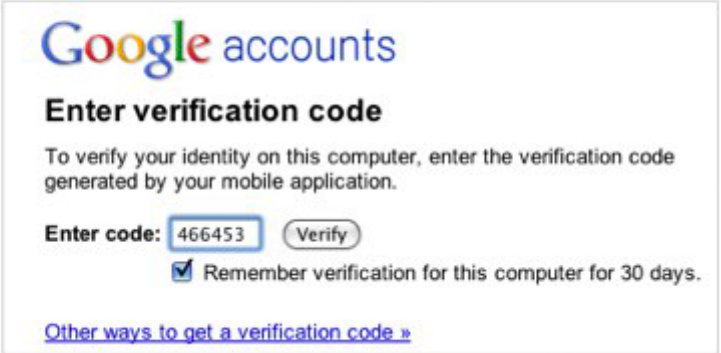
Improving(?) Passwords

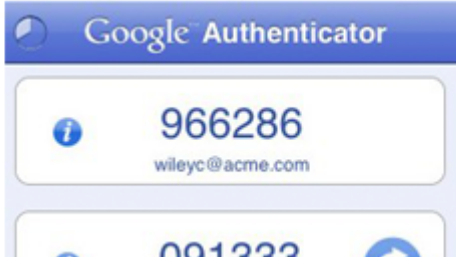
- Add biometrics
 - For example, keystroke dynamics or voiceprint
- Graphical passwords
 - Goal: easier to remember? no need to write down?
- Password managers
 - Examples: LastPass, KeePass, built into browsers
 - Can have security vulnerabilities...
- Two-factor authentication
 - Leverage phone (or other device) for authentication


Multi-Factor Authentication

1.  Sign in with your Google Account
Email: hikingfan@gmail.com
ex: pat@example.com
Password:
 Stay signed in

[Can't access your account?](#)

2.  Google accounts
Enter verification code
To verify your identity on this computer, enter the verification code generated by your mobile application.
Enter code: 466453
 Remember verification for this computer for 30 days.
[Other ways to get a verification code »](#)

 Google Authenticator
966286
wileyc@acme.com
001222

 Turn on Login Approvals
What is Login Approvals?
Login Approvals is a security feature that requires you to enter a code that we text to your phone when you log in from an unrecognized computer. You can enable this feature in a few simple steps.
If you ever lose access to your phone, you can always return to a previously-recognized computer to regain access to your account.
Note: You'll need to have your mobile phone with you to complete this process.

FIDO + Hardware Two Factors

