CSE 484 / CSE M 584
Computer Security: Authentication

TA: Jared Moore

jlcmoore@cs

Logistics

- Hw #3 due next Friday
- Final projects due 12/13

- Today:
  - Hw 3 questions.
  - Authentication grab bag.

HW3

- Questions?
- Demo?

Password Salting

- Servers shouldn't store passwords, but password hashes. (Why?)
- Threat: rainbow tables (pre-computed password hashes)
- Solution: salt
  - Each password is hashed/stored with a random value. Now a pre-computed table is useless.
  - Other benefits?

Measuring Password Strength

- How many possible passwords are there?
- How many passwords are likely to be chosen?
- How long will it take to guess?

- Bits of entropy: $\log_2$(# of guesses)

  Example: password of 10 bits chosen randomly

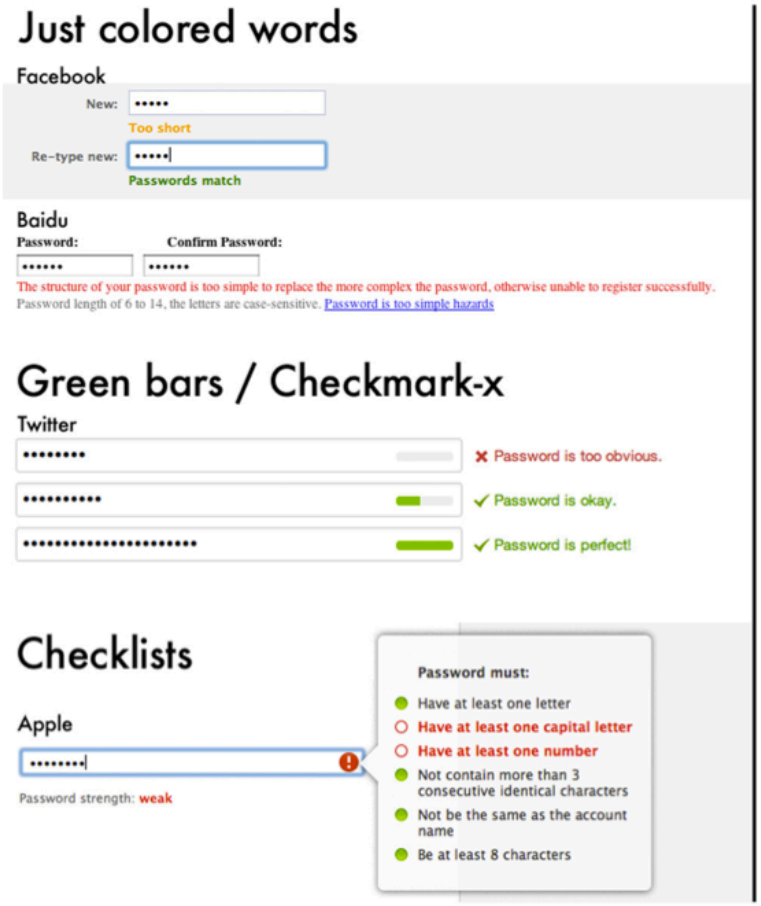
  Possible passwords = 2^10

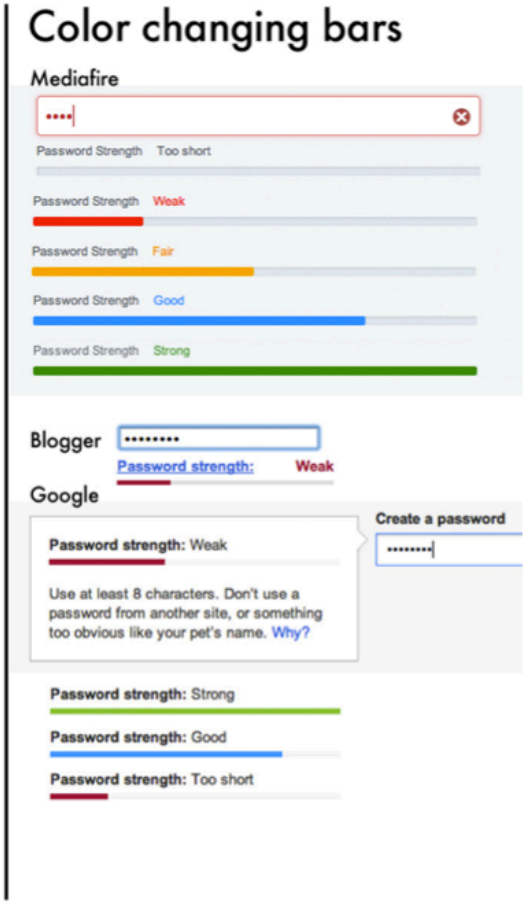
  Bits of entropy = $\log_2$(2^10) = 10

Additional bit of entropy doubles number of guesses needed.

IMPROVING PASSWORDS

Password Meters





[From "How does your password measure up? The Effect of Strength Meters on Password Creation", Ur et al., USENIX Security 2012]

Password Meters

- Meters lead to longer passwords.
- Are passwords harder to guess?
  - Visual feedback alone has no effect.
  - More stringent meters do lead to stronger passwords.
- Meters lead to people taking longer to create passwords, and change their mind during creation.
- Meters don't affect memorability.

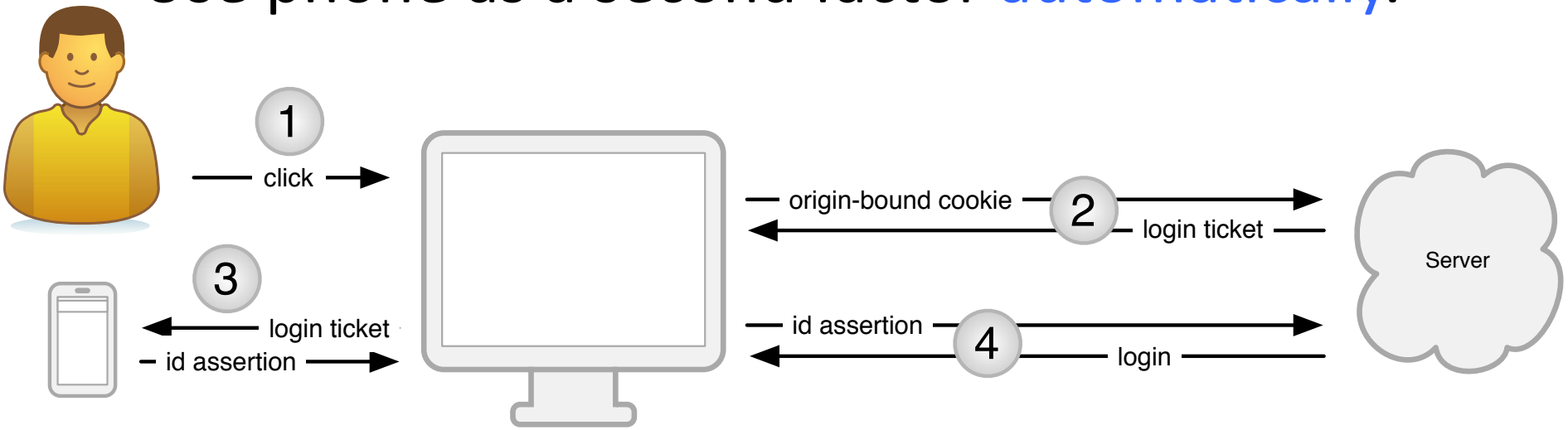
[From "How does your password measure up? The Effect of Strength Meters on Password Creation", Ur et al., USENIX Security 2012]

Password Managers

- Who uses a password manager?
- Allows the user to use one secure password to secure all other passwords
- Generate strong password for other sites
- Convenient for the user and help log in more securely
- Examples: LastPass, KeePass, built in browser password managers
- See this paper for drawback

Usable Two-Factor Authentication

- Use phone as a second factor automatically.



- What if phone is not present?
  - Server can treat login session differently (e.g., don't allow transactions above a threshold $ amount).

[From "Strengthening User Authentication through Opportunistic Cryptographic Identity Assertions", Czeskis et al., CCS 2012]

How are current authentication practices biased? Whom do they leave out?

Design Exercise

- How do we improve upon current authentication mechanisms?
- **In groups of four or more, spend the next ten minutes designing a new authentication mechanism that addresses constraints of passwords.**
- Then one of your group members will present your design to the class and address
  - Which population the design serves
  - Improvements on passwords
  - Constraints of the new design

ALTERNATE AUTHENTICATION

FIDO

- Fast Identity Online
- http://youtu.be/0tGk5-4wx-w
- Benefits?
- Tradeoffs?

[From https://www.yubico.com/2017/10/creating-unphishable-security-key/]

Thumprint: Socially-Inclusive Local Group Authentication Through Shared Secret Knocks

Sauvik Das Gierad Laput Chris Harrison Jason I. Hong
Carnegie Mellon University, Human-Computer Interaction Institute
5000 Forbes Ave., Pittsburgh, PA, 15213
sauvik@cmu.edu, {gierad.laput, chris.harrison, jasonh}@cs.cmu.edu

ABSTRACT
Small, local groups who share protected resources (e.g., families, work teams, student organizations) have unmet authentication needs. For these groups, existing authentication strategies either create unnecessary social divisions (e.g., biometrics), do not identify individuals (e.g., shared passwords), do not equitably distribute security responsibility (e.g., individual passwords), or make it difficult to share or revoke access (e.g., physical keys). To explore an alternative, we designed Thumprint: inclusive group authentication with a shared secret knock. All group members share one secret knock, but individual expressions of the secret are discernible. We evaluated the usability and security of our concept through two user studies with 30 participants. Our results suggest that (1) individuals who enter the same shared thumprint are distinguishable from one another, (2) that people can enter thumprints consistently over time, and (3) that thumprints are resilient to casual adversaries.

Author Keywords

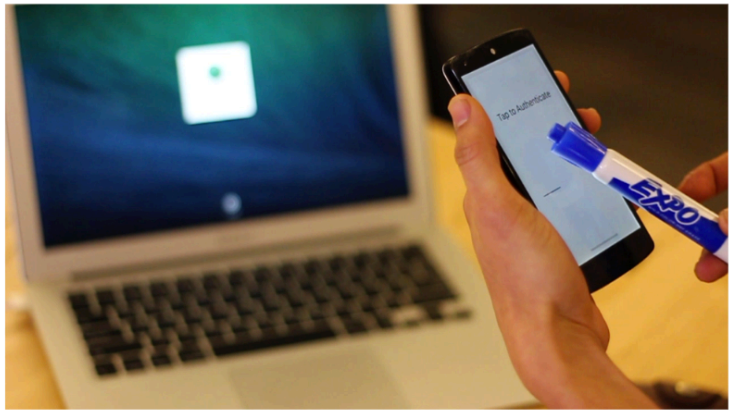


Figure 1. With Thumprint, groups of users learn a single, shared secret knock that they enter on a surface instrumented with (or containing) an accelerometer and microphone (here, a smartphone) in order to authenticate.

individual passwords for each family member is unwieldy and often subverted [23,26].

[From “Thumbprint: Socially-Inclusive Local Group Authentication Through Shared Secret Knocks”, Das et al., CHI2017]