



14 - Authentication in Practice

Lujo Bauer, Nicolas Christin,
and Abby Marsh

February 29, 2016

05-436 / 05-836 / 08-534 / 08-734
Usable Privacy and Security

Today's class

- Biometrics
- Two-factor authentication
- Backup authentication – secret questions

Biometrics

Biometrics — Hooray!

- Your fingerprint is your ID!
- Your fingerprint is pretty unique.
- Your finger is convenient to carry.

Biometrics — Hooray!

- Your fingerprint is your ID!
- Your fingerprint is pretty unique.
- Your finger is convenient to carry.

- Isn't this the solution to all our problems?

Biometrics — Hooray!

- Your fingerprint is your ID!
- Your fingerprint is pretty unique.
- Your finger is convenient to carry.

- Isn't this the solution to all our problems?

Well, maybe not so much.

Biometrics — ???

- Your fingerprint is your ID!
- Your fingerprint is pretty unique.
- Your finger is convenient to carry.

How can each of these benefits actually be a problem with biometrics?

Biometrics — Boo!

- Your fingerprint is your ID!
 - **Which means that your finger is a lot more valuable to other people than it used to be.**
- Your fingerprint is pretty unique.
- Your finger is convenient to carry.

Biometrics — Boo!

- Your fingerprint is your ID!
- Your fingerprint is pretty unique.
 - **You only have so many biometrics, so if Google and Amazon use the same biometric, they can authenticate as you to each other**
- Your finger is convenient to carry.

Biometrics — Boo!

- Your fingerprint is your ID!
- Your fingerprint is pretty unique.
- Your finger is convenient to carry.
 - **Unfortunately, biometric readers are a lot less convenient to deploy. They generally take specialized hardware.**

So where are biometrics used?

Unlocking your phone

- No need to deploy any more hardware.
- If the biometrics are kept local, it solves the cross-site authentication problem.



Two Factor Authentication

Phishing!

Two Factor Authentication

Phishing!

Two Factor Authentication

Shoulder Surfing!

Phishing!

Two Factor Authentication

Keyloggers!

Shoulder Surfing!

What Is Two Factor Authentication?

- Having two different factors for authentication.
- That way, if someone steals your password, your account can still be protected.

Example of Two Factor Authentication



&

Password

Example of Two Factor Authentication



&

Why don't we
do this anymore?

Password

Two Factor Authentication Today



Password

Two Factor Authentication Today



Authentication
requires both
password and a code
sent to a phone

Password

Two Factor Authentication Today



Do you use this?
Why or why not?

Password

Two Factor Authentication Today



How can this go wrong?

Password

It's No Secret

Measuring the security and reliability of authentication via 'secret' questions

Stuart Schechter

A. J. Bernheim Brush

Serge Egelman

Oakland 2009

Aol Mail.

YAHOO!®

Gmail
by Google

 Windows Live™

 Hotmail.

The efficient way to do email

Who uses this?

In This Paper

- How secure are secret questions against random guessing?
- Can acquaintances guess secret questions?
- Can users remember their own secret questions?

Findings

- Many bogus answers (e.g., 13% for hotmail)
- After 3-6 months, 20% of answers forgotten
- Answer statistically guessable if in top 5 guesses for that question
 - 13% total statistically guessable
- 17-28% guessed by acquaintance

Recommendations

- Lock out users who make incorrect but popular guesses
- Remove most easily guessed questions
- Disallow popular answers
- Occasionally ask secret questions after user has logged in successfully

Questions from the Time of the Paper

AOL Questions

- What is your pet's name?
- Where were you born?
- What is your favorite restaurant?
- What is the name of your school?
- Who is your favorite singer?
- What is your favorite town?

AOL Questions 2

- What is your favorite song?
- What is your favorite film?
- What is your favorite book?
- Where was your first job?
- Where did you grow up?

Google Questions

- What is your primary frequent flier number?
- What is your library card number?
- What was your first phone number?
- What was your first teacher's name?

Microsoft Questions

- Mother's birthplace
- Best childhood friend
- Favorite teacher
- Favorite historical person
- Grandfather's occupation

Yahoo! Questions

- Where did you meet your spouse?
- What was the name of your first school?
- Who was your childhood hero?
- What is your favorite pastime?
- What is your favorite sports team?

Yahoo! Questions 2

- What is your father's middle name?
- What was your high school mascot?
- What make was your first car or bike?
- What is your pet's name?

Can you do better?

- In your project groups, come up with 3 secret questions.
 - Can include alternate ways for doing backup authentication
- Write them on the board.
- We'll critique them as a class.