CSE 484: Computer Security and Privacy

Authentication

Spring 2024

David Kohlbrenner

dkohlbre@cs

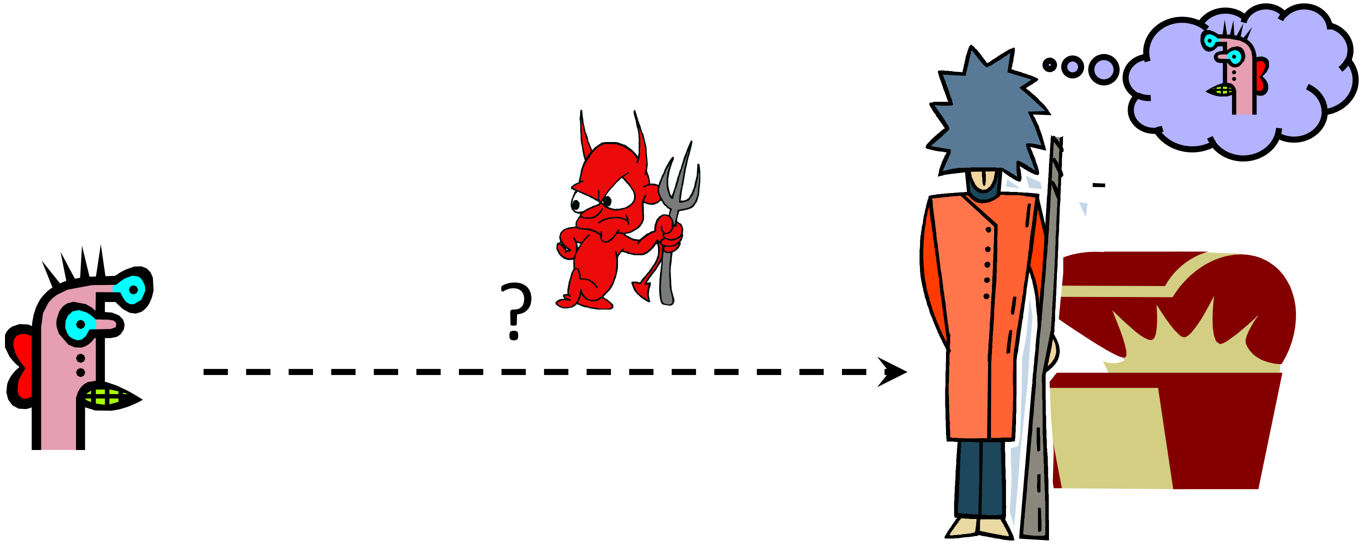
Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Logistics

- Lab 2 is due tomorrow
  - Remember we have a lot of resources/recordings on lab2 stuff!
  - Slow down and make sure each step of your attack works
    - Check the error page source/dom
    - Steal your own cookie
    - etc
- HW3 due next week
- Final Project (Lab3) will go out Monday
  - Monday’s class will be important for working on the lab

Authentication

Basic Problem



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

Any system with access control must solve this problem.

A slightly more fundamental question

- What are we trying to prove?

Many Ways to Prove Who You Are

- “Something you know”
  - Passwords
  - Answers to questions that only you know
- “Something you have”
  - Secure tokens, mobile devices
- “Something you are”
  - Biometrics

Passwords and Computer Security

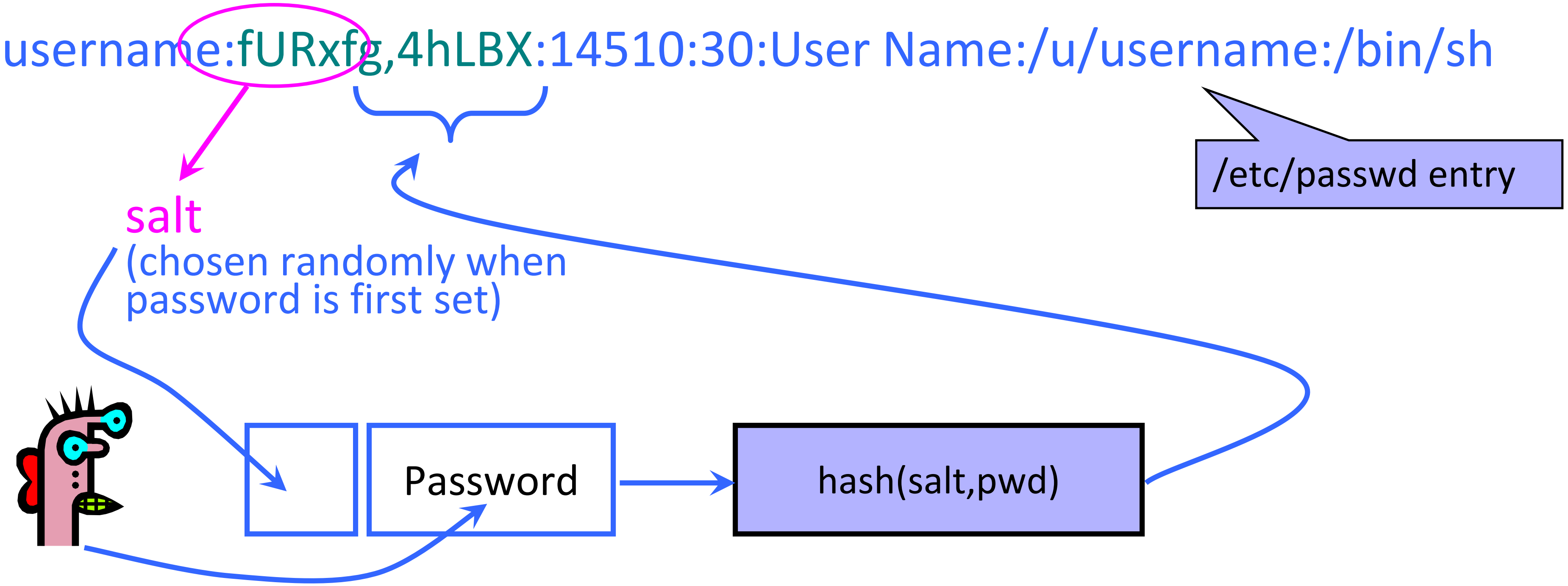
- In 2023, 24% of network intrusions exploited stolen credentials (username/password)
  - Source: 2024 Data Breach Investigations Report | Verizon
  - Was 80%+ in 2012!

- First step after any successful intrusion: steal more credentials (lateral movement)

Password Hashing

- Instead of user password, store H(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(password), hard to find password
    - No known algorithm better than trial and error
  - "Slow" to compute

Salt


username:fURxfg,4hLBX:14510:30:User Name:/u/username:/bin/sh
/etc/passwd entry
salt
(chosen randomly when password is first set)
Password
hash(salt,pwd)

- Users with the same password have <u>different</u> 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)

Other Password Security Risks

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

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 three failures

Default Passwords

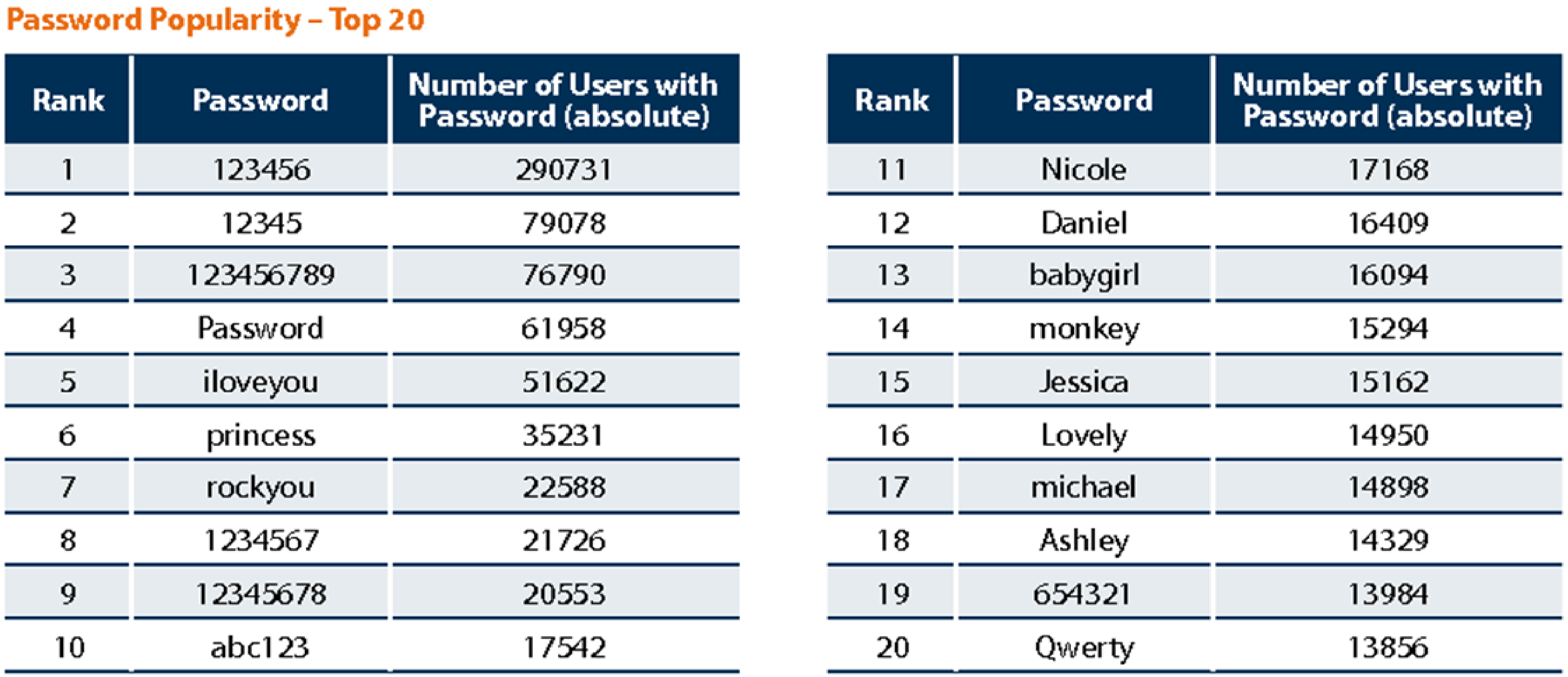
- Examples from Mitnick's "Art of Intrusion"
  - U.S. District Courthouse server: "public" / "public"
  - NY Times employee database: pwd = last 4 SSN digits
- Mirai IoT botnet
  - Weak and default passwords on routers and other devices

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

- RockYou hack
  - “
  - D
  - P
  - D
    p



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
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

[Inglesant and Sasse, “The True Cost of Unusable Password Policies”]

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…

[Inglesant and Sasse, “The True Cost of Unusable Password Policies”]

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 <u>less</u> 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

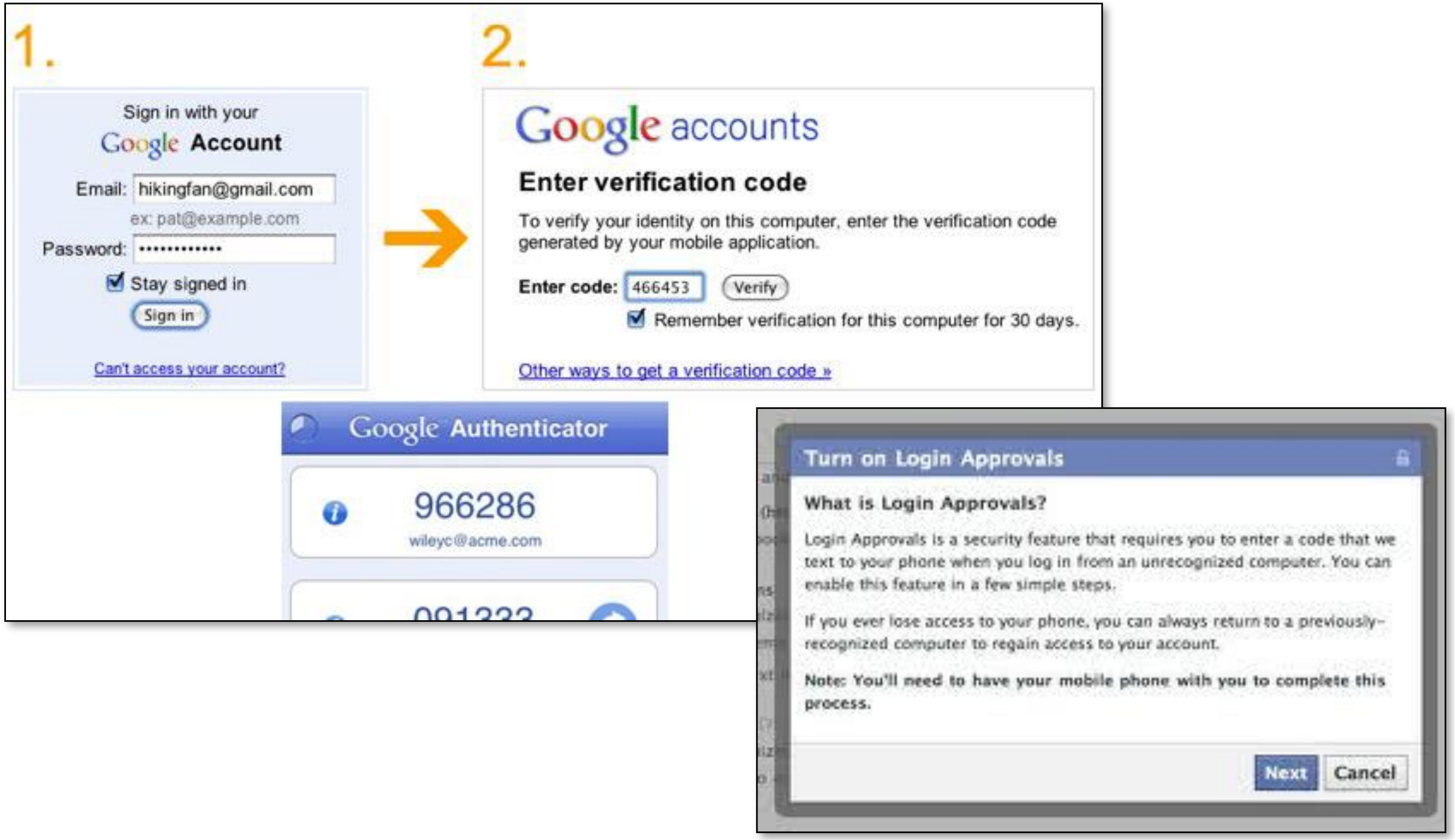
Improving(?) Passwords

- 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

Password managers

- Generation
  - Secure generation of random passwords
- Management
  - Allows for password-per-account
- Safety?
  - Single point of failure
  - Vulnerability?
  - Phishing?

Multi-Factor Authentication



1.

Sign in with your Google Account

Email: hikingfan@gmail.com

ex: pat@example.com

Password: •••••••••••••

☑ Stay signed in

Sign 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 Verify

☑ Remember verification for this computer for 30 days.

Other ways to get a verification code »

Google Authenticator

966286

wileyc@acme.com

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.

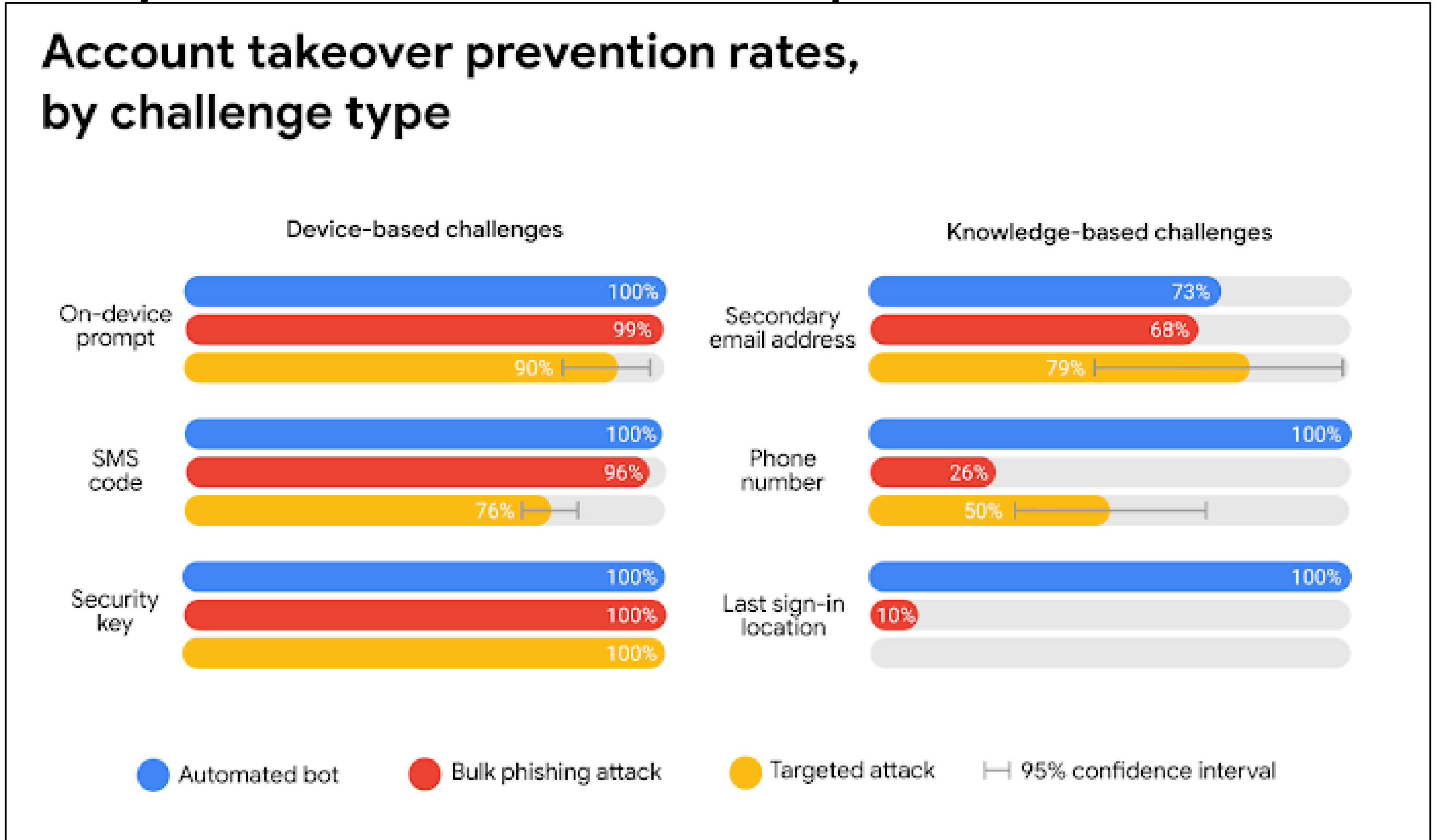
Gradescope:

Do you use 2-factor auth?
Do you use a password manager?
Why or why not?

How to compromise account protected with hardware second factor?

https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Secondary Factors Do Help!



Account takeover prevention rates, by challenge type

Both device- and knowledge-based challenges help thwart automated bots, while device-based challenges help thwart phishing and even targeted attacks.

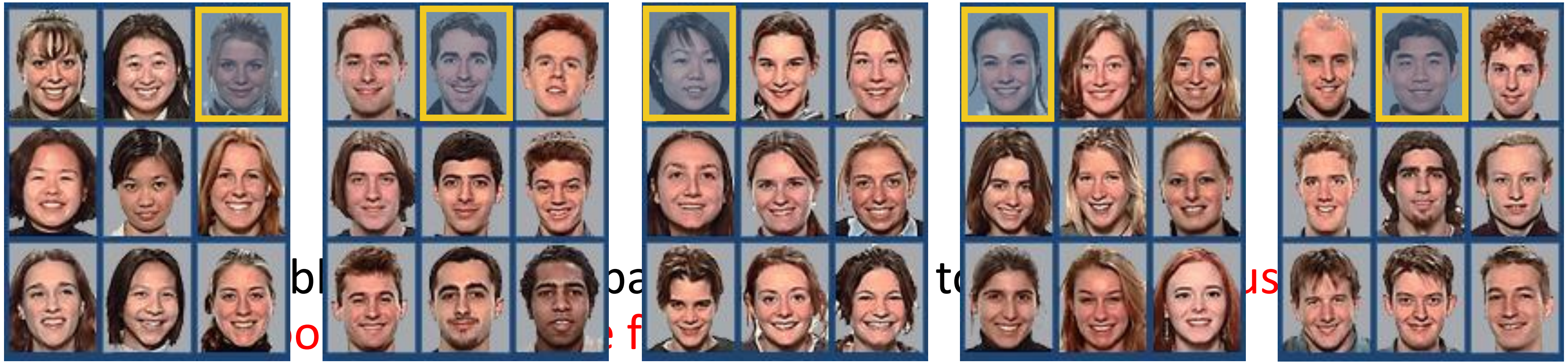
Why does 2FA (sometimes) work?

- Stops phishing, when it is hardware token
- Doesn’t when it is SMS ☹

Hardware 2FA tokens (U2F/FIDO)

Graphical Passwords

- Many variants… one example: Passfaces
  - Assumption: easy to recall faces

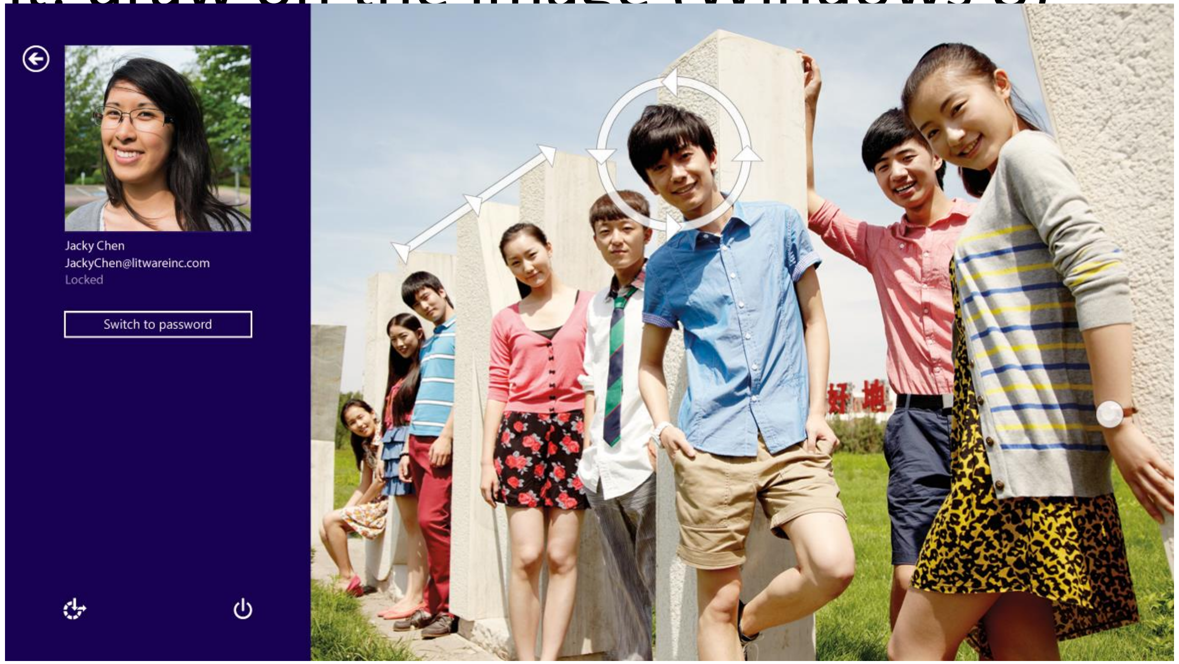


bl pa t us

o e f

Graphical Passwords

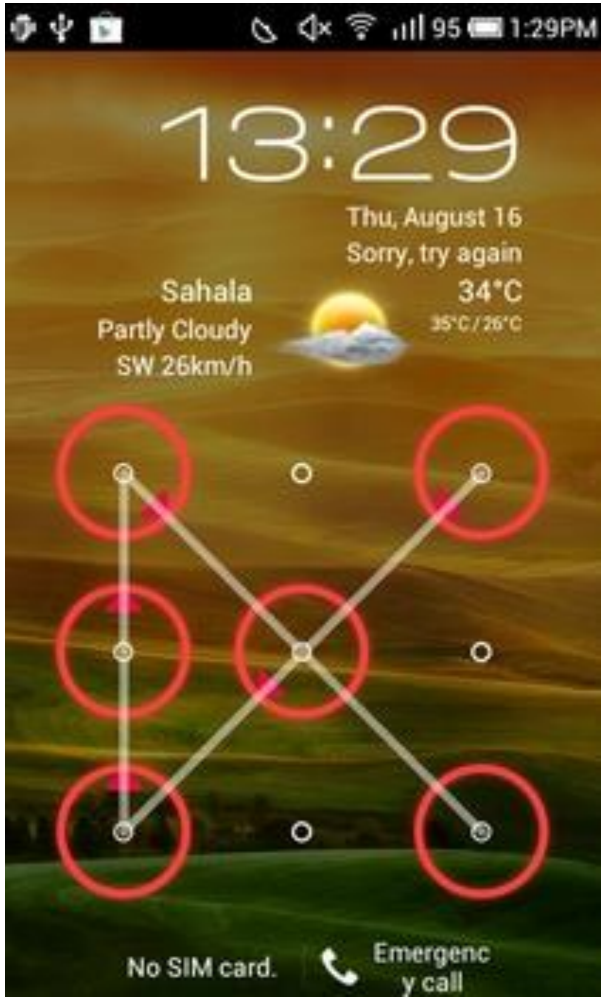
- Another variant: draw on the image (Windows 8)



Jacky Chen
JackyChen@litwareinc.com
Locked

- Problem: users choose predictable points/lines

Unlock Patterns



- Problems:
  - Predictable patterns (familiar pattern by now)
  - Smear patterns
  - Side channels: apps can use accelerometer and gyroscope to extract pattern!

What About Biometrics?

- Authentication: **What you are**
- Unique identifying characteristics to authenticate user or create credentials
  - Biological and physiological: Fingerprints, iris scan
  - Behaviors characteristics - how perform actions: Handwriting, typing, gait
- Advantages:
  - Nothing to remember
  - Passive
  - Can’t share (generally)
  - With perfect accuracy, could be fairly unique

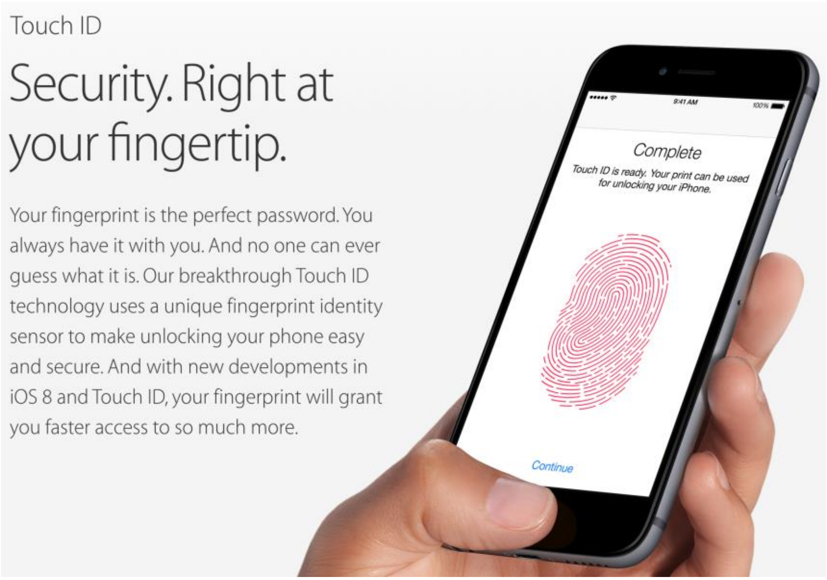
What are reasons to use/*not* use biometrics?

Issues with Biometrics

- Private, but not secret
  - Maybe encoded on the back of an ID card?
  - Maybe encoded on your glass, door handle, ...
  - Sharing between multiple systems?
- Revocation is difficult (impossible?)
  - Sorry, your iris has been compromised, please create a new one...
- Physically identifying
  - Soda machine to cross-reference fingerprint with DMV?
- Birthday paradox
  - With false accept rate of 1 in a million, probability of false match is above 50% with only 1609 samples

Attacking Biometrics

- An adversary might try to steal biometric info
  - Malicious fingerprint reader
    - Consider when biometric is used to derive a cryptographic key
  - Residual fingerprint on a glass



Touch ID

Security. Right at your fingertip.

Your fingerprint is the perfect password. You always have it with you. And no one can ever guess what it is. Our breakthrough Touch ID technology uses a unique fingerprint identity sensor to make unlocking your phone easy and secure. And with new developments in iOS 8 and Touch ID, your fingerprint will grant you faster access to so much more.

9:41 AM
100%
Complete
Touch ID is ready. Your print can be used for unlocking your iPhone.
Continue

Passkeys (2024ish)

- An actual, deployed, genuine *password replacement*
  - *Also a 2fa replacement!*
  - *And a username replacement!*

- Basic goals:
  - Store some sort of key on user end-devices
  - Use that key to login to Stuff
  - Don’t allow losing the key
  - Somehow make the key moving between devices Easy