# 14- Authentication beyond text passwords

Lorrie Cranor

March 6, 2017

*05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734*
*Usable Privacy and Security*

Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering & Public Policy

CyLab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

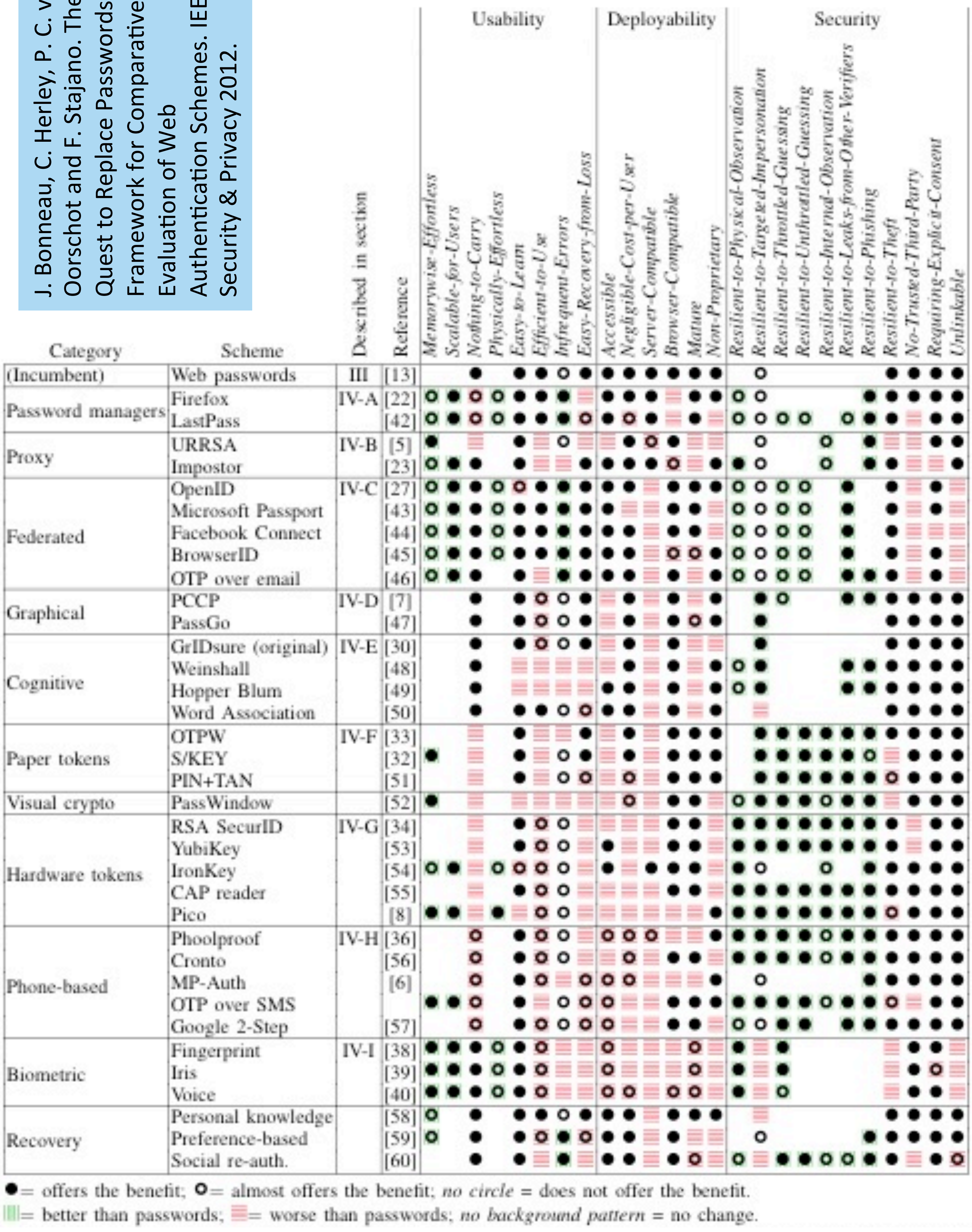
# Today's class

- What else is there?
- Graphical passwords
- Biometrics
- Two-factor authentication
- Backup authentication – secret questions

# What else is there besides text passwords?

- Graphical passwords
- Biometrics
- Hardware tokens
- Phone-based authentication
- Federated IDs
- Password managers
- Multi-factor authentication
- Password recovery
  - Via secret question
  - Via email link
  - Via social authentication

J. Bonneau, C. Herley, P. C. van Oorschot and F. Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. IEEE Security & Privacy 2012.



| Category | Scheme | Described in section | Reference | Usability | | | | | | | | Deployability | | | | | | Security | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Memorywise-Effortless* | *Scalable-for-Users* | *Nothing-to-Carry* | *Physically-Effortless* | *Easy-to-Learn* | *Efficient-to-Use* | *Infrequent-Errors* | *Easy-Recovery-from-Loss* | *Accessible* | *Negligible-Cost-per-User* | *Server-Compatible* | *Browser-Compatible* | *Mature* | *Non-Proprietary* | *Resilient-to-Physical-Observation* | *Resilient-to-Targeted-Impersonation* | *Resilient-to-Throttled-Guessing* | *Resilient-to-Unthrottled-Guessing* | *Resilient-to-Internal-Observation* | *Resilient-to-Leaks-from-Other-Verifiers* | *Resilient-to-Phishing* | *Resilient-to-Theft* | *No-Trusted-Third-Party* | *Requiring-Explicit-Consent* | *Unlinkable* |
| (Incumbent) | Web passwords | III | [13] | | | ● | | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● | | ○ | | | | | | ● | ● | ● | ● |
| Password managers | Firefox | IV-A | [22] | 🟩○ | 🟩● | 🟥○ | 🟩○ | ● | ● | 🟩● | 🟥 | ● | ● | ● | 🟥 | ● | ● | 🟩○ | ○ | | | | | 🟩● | ● | ● | ● | ● |
| | LastPass | | [42] | 🟩○ | 🟩● | 🟥○ | 🟩○ | ● | ● | 🟩● | 🟥○ | ● | 🟥○ | ● | 🟥 | ● | 🟥 | 🟩○ | ○ | 🟩○ | 🟩○ | | 🟩○ | 🟩● | ● | 🟥 | ● | ● |
| Proxy | URRSA | IV-B | [5] | 🟩● | | 🟥 | | ● | 🟥 | ○ | 🟥 | 🟥 | ● | 🟥○ | ● | 🟥 | 🟥 | | ○ | | | 🟩○ | | 🟩● | 🟥 | 🟥 | ● | ● |
| | Impostor | | [23] | 🟩○ | 🟩● | ● | | ● | 🟥 | 🟥 | ● | ● | ● | ● | 🟥○ | 🟥 | ● | 🟩● | ○ | | | 🟩○ | | 🟩● | ● | 🟥 | 🟥 | ● |
| Federated | OpenID | IV-C | [27] | 🟩○ | 🟩● | ● | 🟩○ | 🟥○ | ● | 🟩● | ● | ● | ● | 🟥 | ● | ● | ● | 🟩○ | ○ | 🟩○ | 🟩○ | | 🟩● | | ● | 🟥 | ● | 🟥 |
| | Microsoft Passport | | [43] | 🟩○ | 🟩● | ● | 🟩○ | ● | ● | 🟩● | ● | ● | 🟥 | 🟥 | ● | ● | 🟥 | 🟩○ | ○ | 🟩○ | 🟩○ | | 🟩● | | ● | 🟥 | ● | 🟥 |
| | Facebook Connect | | [44] | 🟩○ | 🟩● | ● | 🟩○ | ● | ● | 🟩● | ● | ● | ● | 🟥 | ● | ● | 🟥 | 🟩○ | ○ | 🟩○ | 🟩○ | | 🟩● | | ● | 🟥 | 🟥 | 🟥 |
| | BrowserID | | [45] | 🟩○ | 🟩● | ● | 🟩○ | ● | ● | 🟩● | ● | ● | ● | 🟥 | 🟥○ | 🟥○ | ● | 🟩○ | ○ | 🟩○ | 🟩○ | | 🟩● | | ● | 🟥 | ● | 🟥 |
| | OTP over email | | [46] | 🟩○ | 🟩● | ● | | ● | 🟥 | 🟩● | ● | ● | ● | 🟥 | ● | 🟥 | ● | 🟩○ | ○ | 🟩○ | 🟩○ | | 🟩● | 🟩● | ● | 🟥 | ● | 🟥 |
| Graphical | PCCP | IV-D | [7] | | | ● | | ● | 🟥○ | ○ | ● | 🟥 | ● | 🟥 | ● | 🟥 | ● | | 🟩● | 🟩○ | | | 🟩● | 🟩● | ● | ● | ● | ● |
| | PassGo | | [47] | | | ● | | ● | 🟥○ | ○ | ● | 🟥 | ● | 🟥 | ● | 🟥○ | ● | | 🟩● | | | | | | ● | ● | ● | ● |
| Cognitive | GrIDsure (original) | IV-E | [30] | | | ● | | ● | 🟥○ | ○ | ● | 🟥 | ● | 🟥 | ● | 🟥 | 🟥 | | 🟩● | | | | | | ● | ● | ● | ● |
| | Weinshall | | [48] | | | ● | | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | ● | 🟥 | ● | 🟥 | ● | 🟩○ | 🟩● | | | | 🟩● | 🟩● | ● | ● | ● | ● |
| | Hopper Blum | | [49] | | | ● | | 🟥 | 🟥 | 🟥 | 🟥 | ● | ● | 🟥 | ● | 🟥 | ● | 🟩○ | 🟩● | | | | 🟩● | 🟩● | ● | ● | ● | ● |
| | Word Association | | [50] | | | ● | | ● | ● | ○ | 🟥○ | ● | ● | 🟥 | ● | 🟥 | ● | | 🟥 | | | | | | ● | ● | ● | ● |
| Paper tokens | OTPW | IV-F | [33] | | | 🟥 | | ● | 🟥 | 🟥 | ● | 🟥 | ● | 🟥 | ● | ● | ● | | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | ● | ● | ● | ● |
| | S/KEY | | [32] | 🟩● | | 🟥 | | ● | 🟥 | ○ | ● | 🟥 | ● | 🟥 | ● | ● | ● | | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩○ | 🟥 | ● | ● | ● |
| | PIN+TAN | | [51] | | | 🟥 | | ● | 🟥 | ○ | 🟥○ | 🟥 | 🟥○ | 🟥 | ● | ● | ● | | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟥○ | ● | ● | ● |
| Visual crypto | PassWindow | | [52] | 🟩● | | 🟥 | | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥○ | 🟥 | ● | ● | 🟥 | 🟩○ | 🟩● | 🟩● | 🟩● | 🟩○ | 🟩● | 🟩● | 🟥 | ● | ● | ● |
| Hardware tokens | RSA SecurID | IV-G | [34] | | | 🟥 | | ● | 🟥○ | ○ | 🟥 | 🟥 | 🟥 | 🟥 | ● | ● | 🟥 | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | ● | 🟥 | ● | ● |
| | YubiKey | | [53] | | | 🟥 | | ● | 🟥○ | ○ | 🟥 | ● | 🟥 | 🟥 | ● | ● | 🟥 | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | ● | 🟥 | ● | ● |
| | IronKey | | [54] | 🟩○ | 🟩● | 🟥 | 🟩○ | 🟥○ | 🟥○ | ○ | 🟥 | ● | 🟥 | ● | ● | ● | 🟥 | 🟩● | ○ | | | 🟩○ | | 🟩● | ● | ● | ● | ● |
| | CAP reader | | [55] | | | 🟥 | | ● | 🟥○ | ○ | 🟥 | 🟥 | 🟥 | 🟥 | ● | ● | 🟥 | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | ● | ● | ● | ● |
| | Pico | | [8] | 🟩● | 🟩● | 🟥 | 🟩● | 🟥 | 🟥○ | ○ | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | ● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩● | 🟥○ | ● | ● | ● |
| Phone-based | Phoolproof | IV-H | [36] | | | 🟥○ | | ● | 🟥○ | ○ | 🟥 | 🟥○ | 🟥○ | 🟥○ | 🟥 | 🟥 | ● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩○ | 🟩● | 🟩● | ● | ● | ● | ● |
| | Cronto | | [56] | | | 🟥○ | | ● | 🟥○ | ○ | 🟥 | 🟥 | 🟥○ | 🟥 | ● | ● | 🟥 | 🟩● | 🟩● | 🟩● | 🟩● | 🟩○ | 🟩● | 🟩● | ● | ● | ● | ● |
| | MP-Auth | | [6] | | | 🟥○ | | ● | 🟥○ | 🟥 | 🟥○ | 🟥○ | 🟥○ | 🟥 | 🟥 | 🟥 | ● | | ○ | | | | | 🟩● | ● | ● | ● | ● |
| | OTP over SMS | | | 🟩● | 🟩● | 🟥○ | | ● | 🟥 | ○ | 🟥○ | 🟥○ | 🟥 | 🟥 | ● | ● | ● | 🟩● | 🟩● | 🟩● | 🟩● | 🟩○ | 🟩● | 🟩● | 🟥○ | 🟥 | ● | ● |
| | Google 2-Step | | [57] | | | 🟥○ | | ● | 🟥○ | ○ | 🟥○ | 🟥○ | 🟥 | 🟥 | ● | ● | 🟥 | 🟩○ | ○ | 🟩● | 🟩● | | 🟩● | 🟩● | ● | ● | ● | ● |
| Biometric | Fingerprint | IV-I | [38] | 🟩● | 🟩● | ● | 🟩○ | ● | 🟥○ | 🟥 | 🟥 | 🟥○ | 🟥 | 🟥 | 🟥 | 🟥○ | 🟥 | 🟩● | 🟥 | 🟩● | | | | | 🟥 | ● | ● | 🟥 |
| | Iris | | [39] | 🟩● | 🟩● | ● | 🟩○ | ● | 🟥○ | 🟥 | 🟥 | 🟥○ | 🟥 | 🟥 | 🟥 | 🟥○ | 🟥 | 🟩● | 🟥 | 🟩● | | | | | 🟥 | ● | 🟥○ | 🟥 |
| | Voice | | [40] | 🟩● | 🟩● | ● | 🟩○ | ● | 🟥○ | 🟥 | 🟥 | 🟥○ | 🟥○ | 🟥 | 🟥○ | 🟥○ | 🟥 | 🟩● | 🟥 | 🟩○ | | | | | 🟥 | ● | ● | 🟥 |
| Recovery | Personal knowledge | | [58] | 🟩○ | | ● | | ● | ● | ○ | ● | ● | ● | 🟥 | ● | ● | ● | | 🟥 | | | | | | ● | ● | ● | ● |
| | Preference-based | | [59] | 🟩○ | | ● | | ● | 🟥○ | 🟩● | 🟥○ | ● | ● | 🟥 | ● | 🟥 | 🟥 | | ○ | | | | | 🟩● | ● | ● | ● | ● |
| | Social re-auth. | | [60] | | | ● | | ● | 🟥 | 🟩● | 🟥 | ● | ● | 🟥 | ● | 🟥○ | 🟥 | 🟩○ | 🟥 | 🟩● | 🟩● | 🟩○ | 🟩○ | 🟩● | ● | 🟥 | ● | 🟥○ |

●= offers the benefit; ○= almost offers the benefit; *no circle* = does not offer the benefit.
🟩= better than passwords; 🟥= worse than passwords; *no background pattern* = no change.

# Graphical passwords

# Types of graphical password systems

- Recall
  - – Drawing a picture, tracing a pattern, tapping specific points
- Recognition
  - – Recognizing images
- Cued-recall
  - – Drawing or taping on top of an image cue

# Advantages and disadvantages

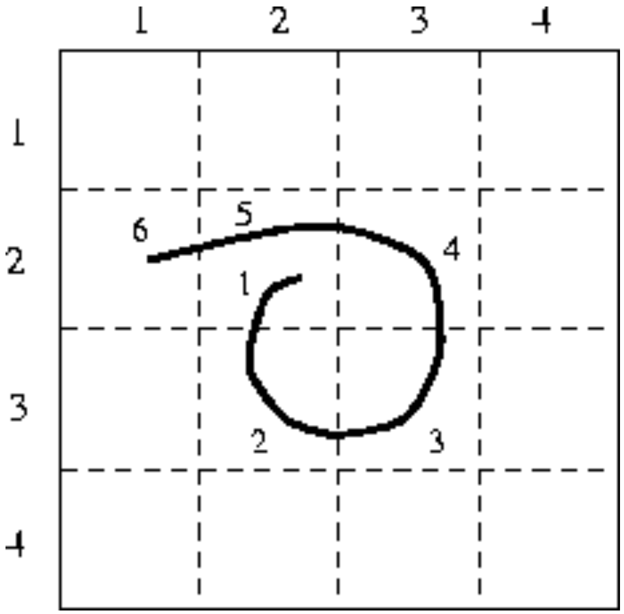
## Advantages

- Images and visual patterns may be easier to remember than characters
  - But password inference not well studied
- Pointing/clicking/tapping/drawing may be easier/faster than typing
- Seems more appealing/fun than text passwords
- May be harder to store or share password
- Less susceptible to phishing attacks

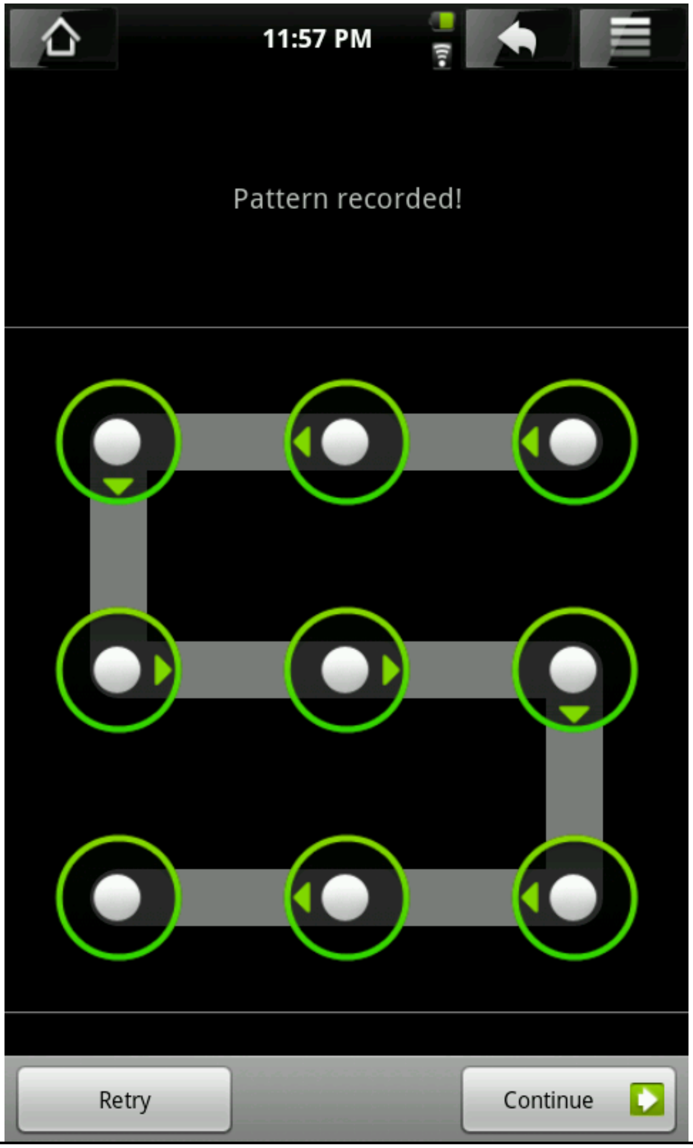
## Disadvantages

- Doesn't work for vision impaired
- Requires a screen (sometimes of high resolution and color)
- Some types particularly vulnerable to shoulder surfing
- Some types have very small password space
- User chosen systems vulnerable to predictable user behavior
- Some types hard to store (for people who want help remembering)

# Draw a Secret (Jermyn et al 1999)

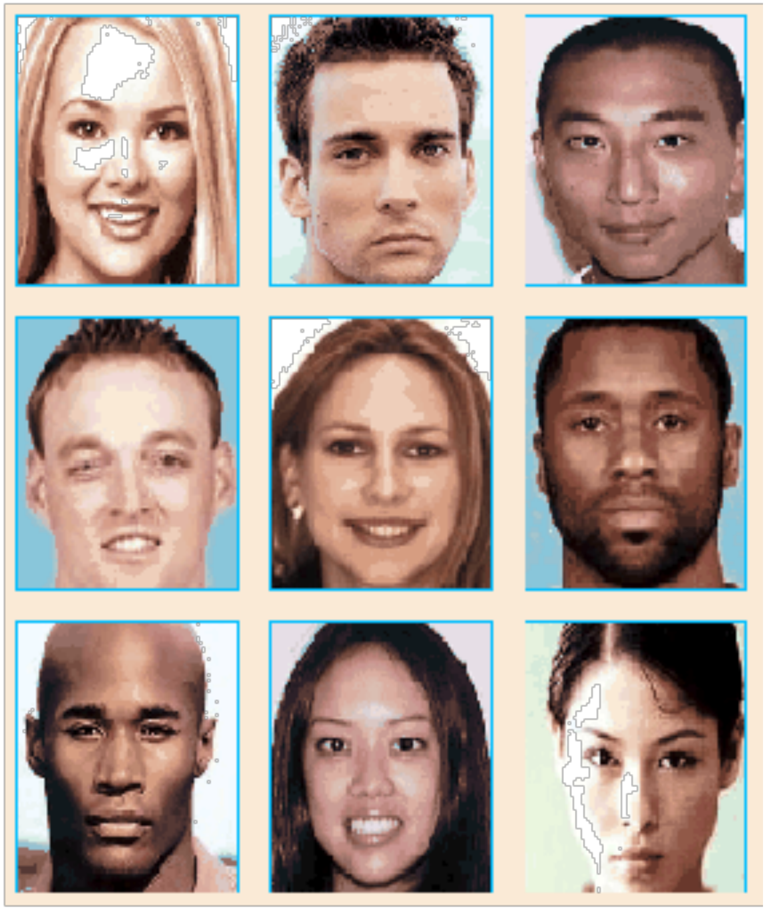


# Android unlock patterns

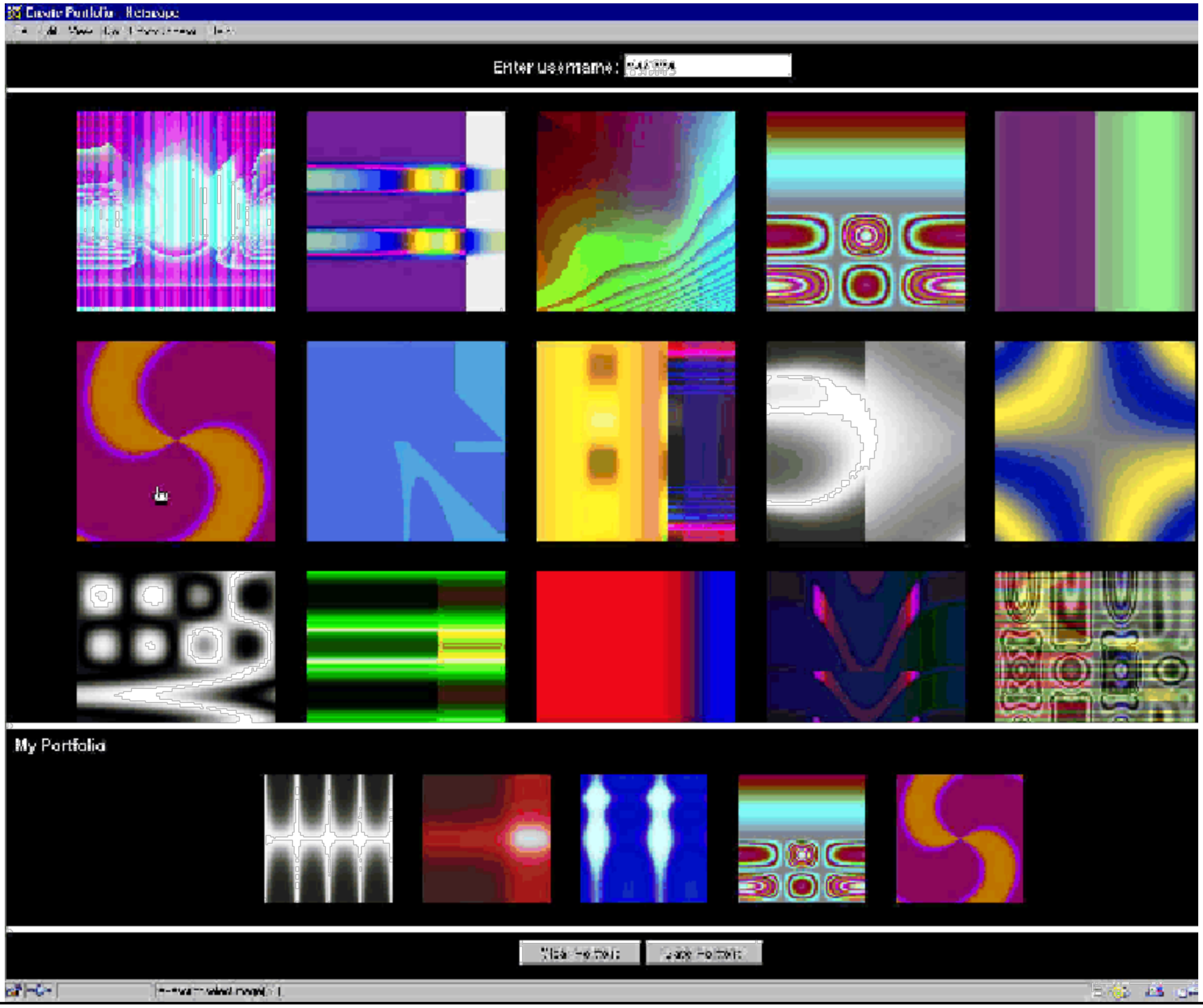


Pattern recorded!

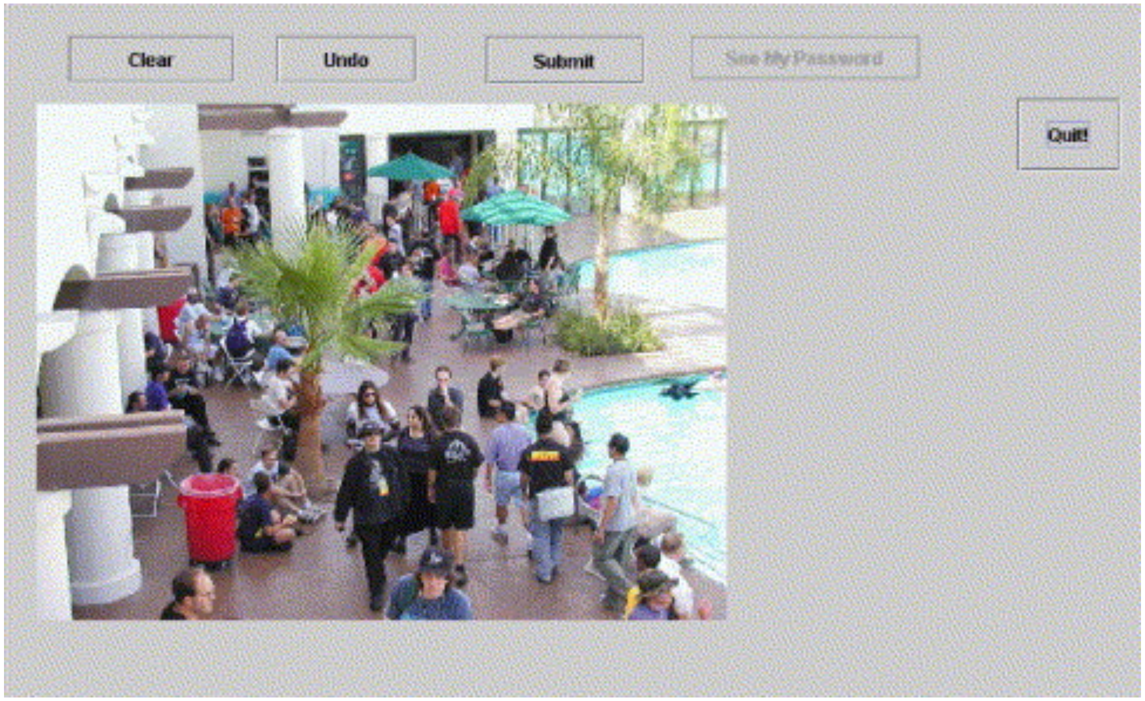
# Passfaces



# Déjà vu (Dhamija and Perrig 2000)



# PassPoints (Wiedenbeck et al 2005)



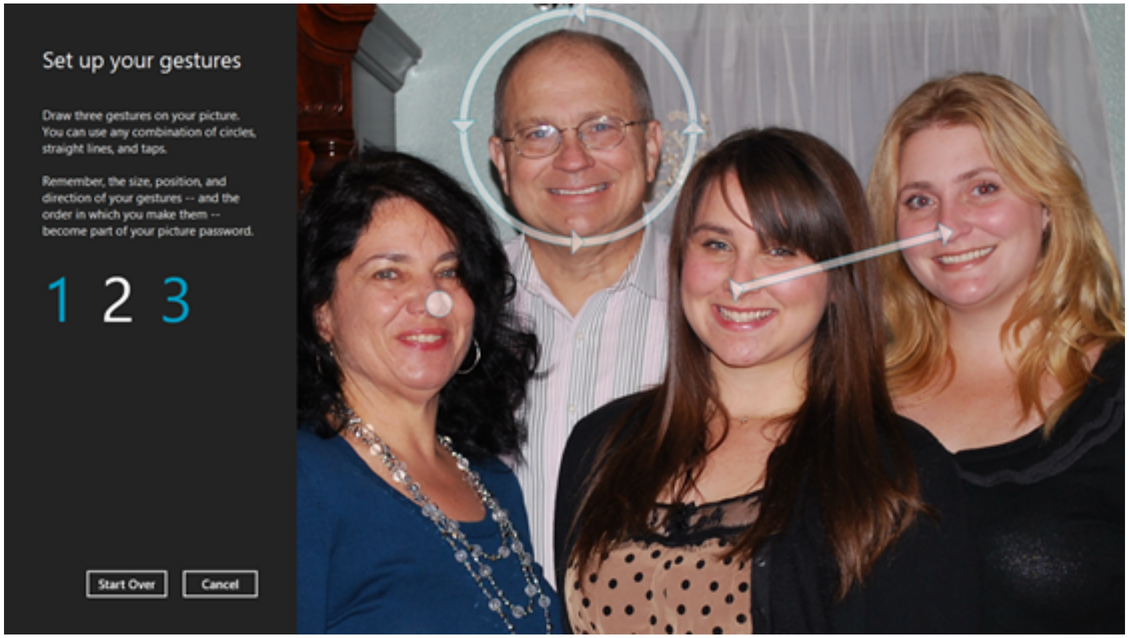
Susan Wiedenbeck,  Jim Waters,  Jean-Camille Birget,  Alex Brodskiy,  Nasir Memon

**PassPoints: Design and longitudinal evaluation of a graphical password system**

International Journal of Human-Computer Studies, Volume 63, Issues 1–2, 2005, 102–127

http://dx.doi.org/10.1016/j.ijhcs.2005.04.010

# Windows 8 picture password

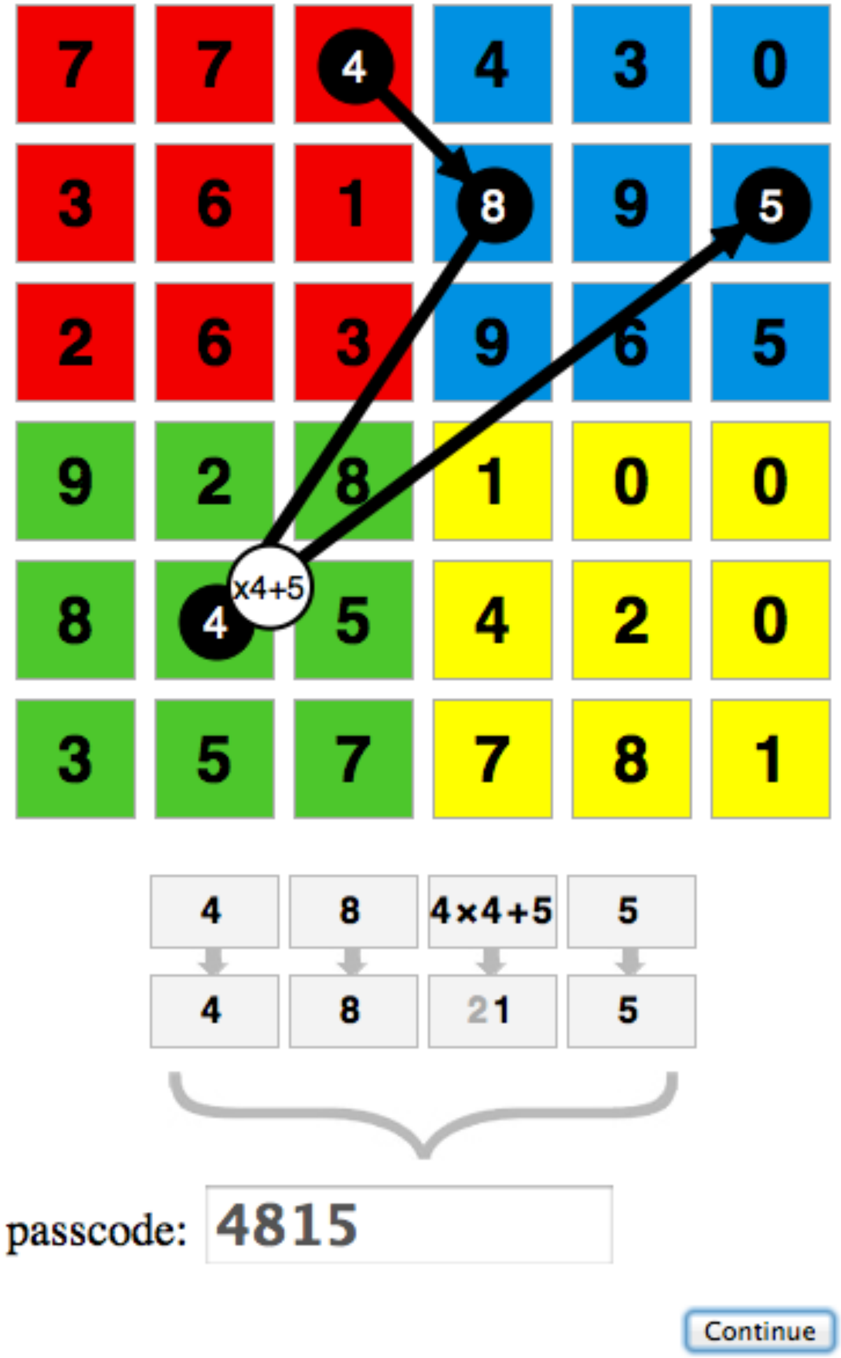


Set up your gestures

Draw three gestures on your picture. You can use any combination of circles, straight lines, and taps.

Remember, the size, position, and direction of your gestures -- and the order in which you make them -- become part of your picture password.

# PassGrids



| | | | | | |
|---|---|---|---|---|---|
| 7 | 7 | 4 | 4 | 3 | 0 |
| 3 | 6 | 1 | 8 | 9 | 5 |
| 2 | 6 | 3 | 9 | 6 | 5 |
| 9 | 2 | 8 | 1 | 0 | 0 |
| 8 | 4 | 5 | 4 | 2 | 0 |
| 3 | 5 | 7 | 7 | 8 | 1 |

| | | | |
|---|---|---|---|
| 4 | 8 | 4×4+5 | 5 |
| 4 | 8 | 21 | 5 |

passcode: 4815

P.G. Kelley, S. Komanduri, M.L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin and L.F. Cranor. The impact of length and mathematical operators on the usability and security of system-assigned one-time PINs. USEC 2013.

# Biometrics

# Examples of biometrics used for authentication

- Fingerprint
- Face
- Hand geometry
- Voice
- Handwriting
- Iris
- Retina
- Heart rhythm
- Keystroke dynamics
- Gait

# Advantages

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

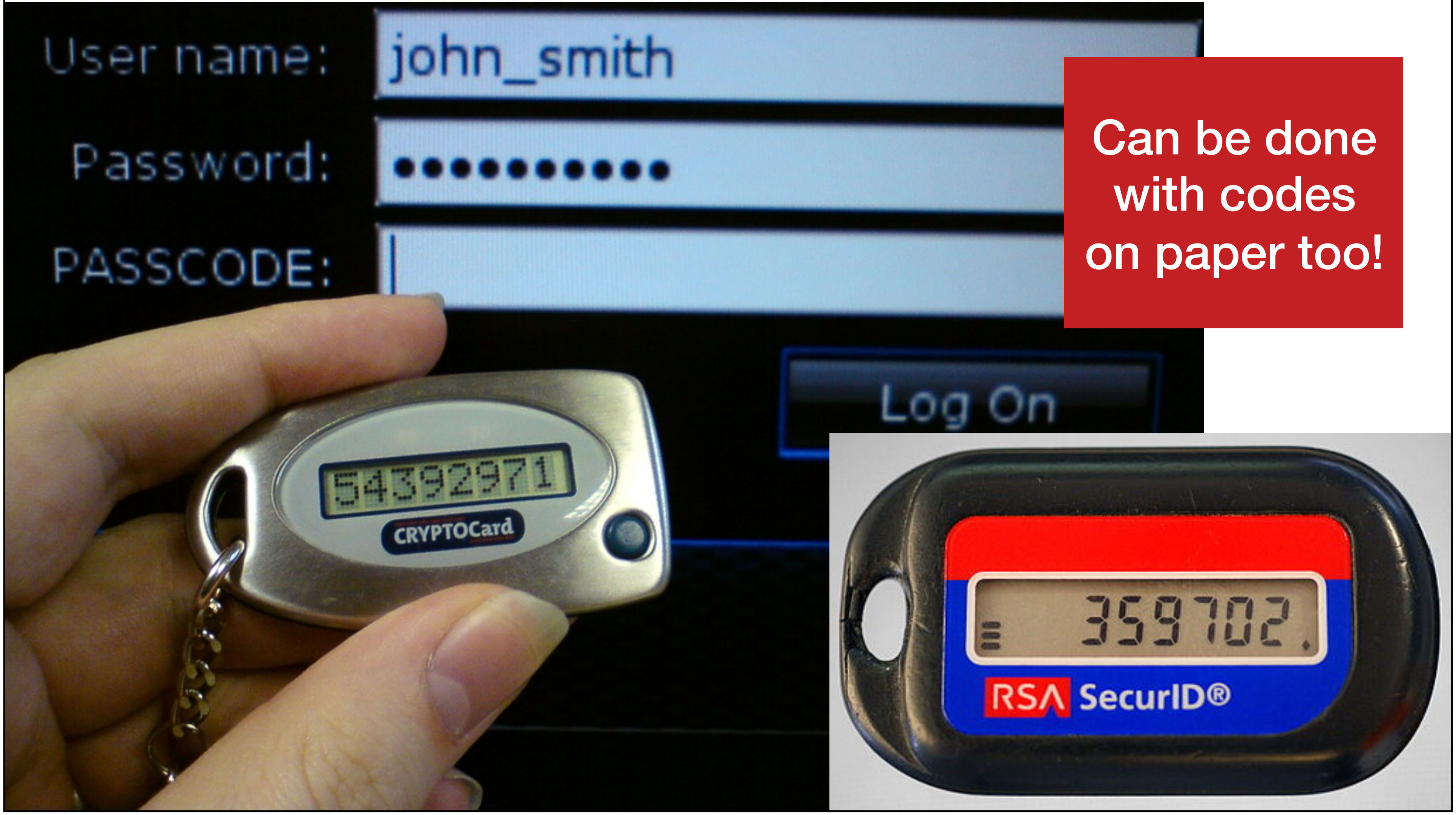
*Why are biometrics not the ultimate authentication solution?*

# Biometrics: issues and limitations

- High accuracy requires expensive and large special equipment (today)
- Some biometrics difficult to capture under some conditions (low light, dry skin, injury, etc.)
- Some biometrics change over time
- May increase value of a person’s body parts to an attacker
- May be difficult to cancel or reset
- May leak personal information
- Privacy concerns

# Two-factor authentication

# One-time password tokens



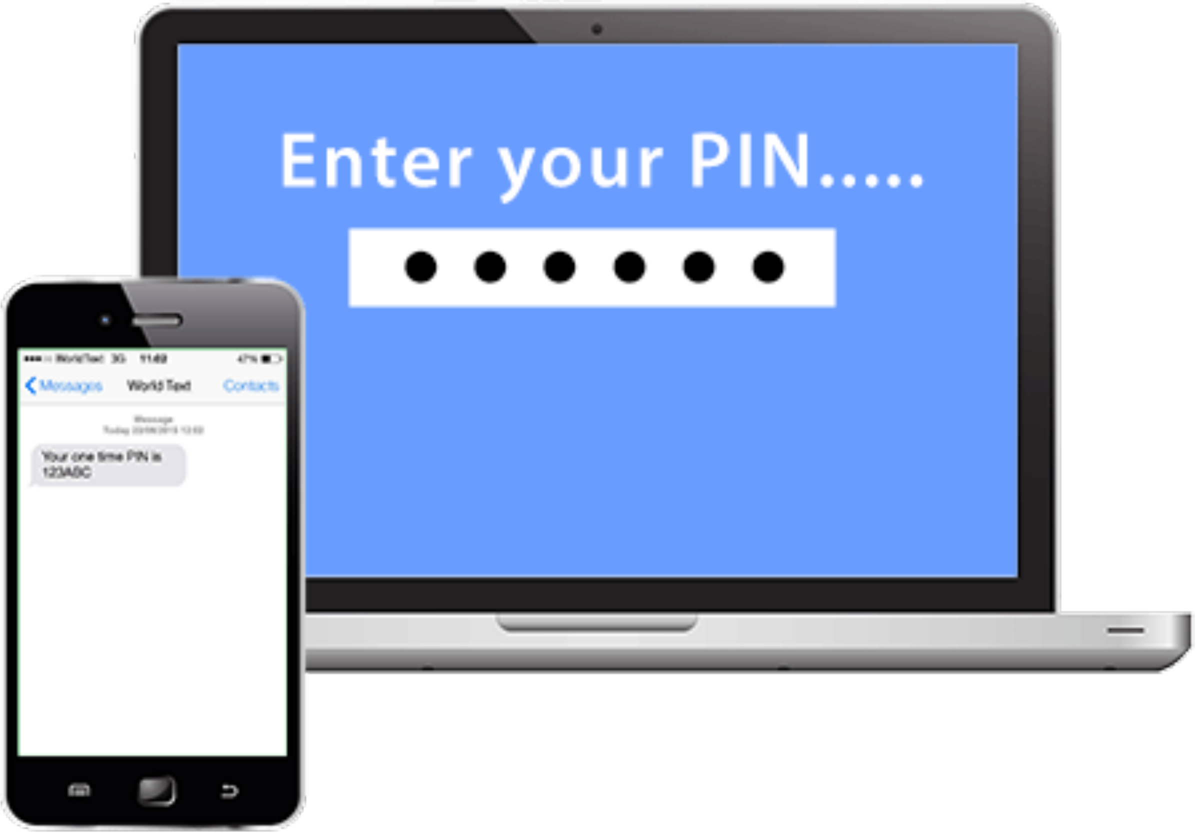
User name: john_smith

Password: •••••••••••

PASSCODE:

Can be done with codes on paper too!

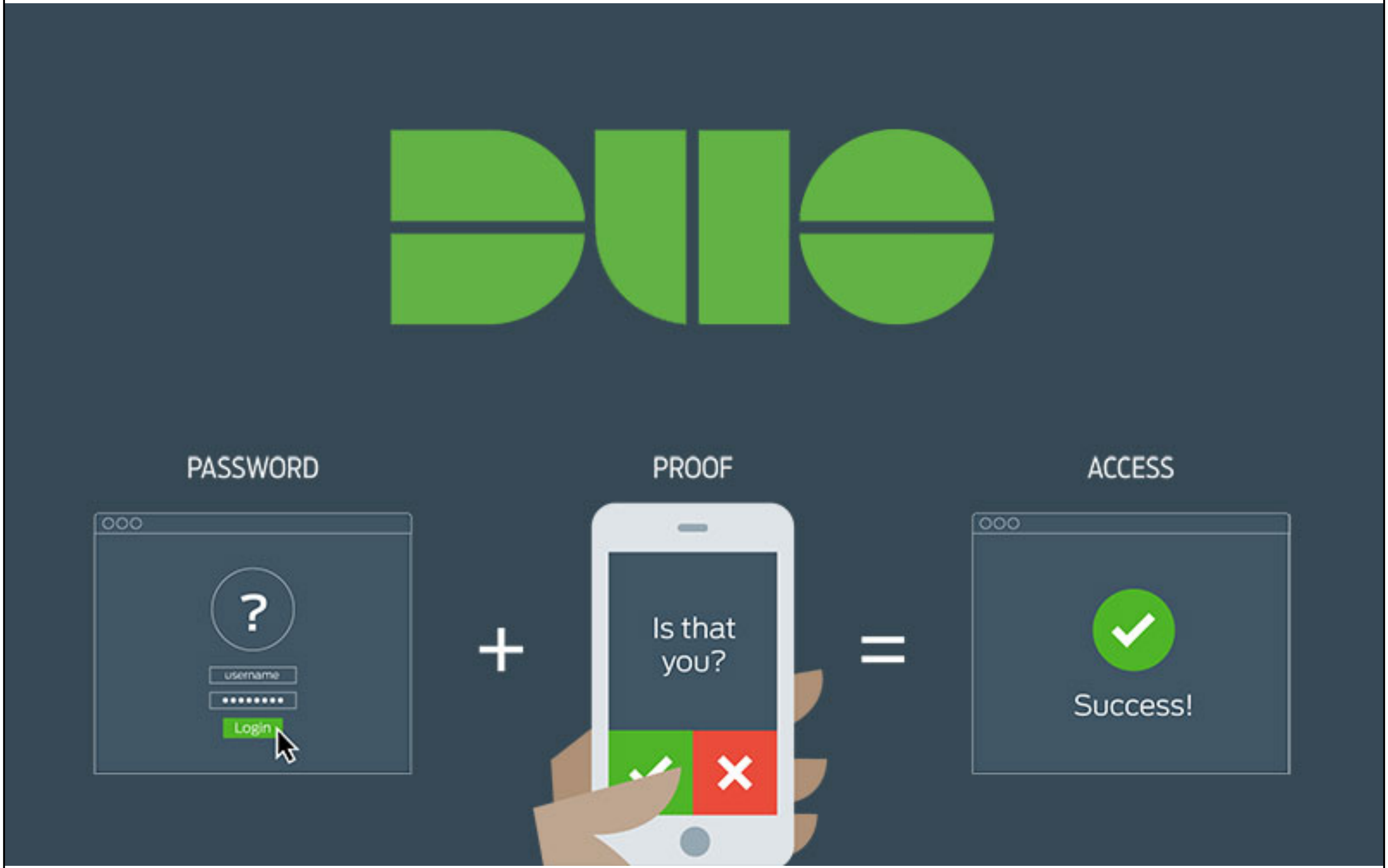
# SMS PIN



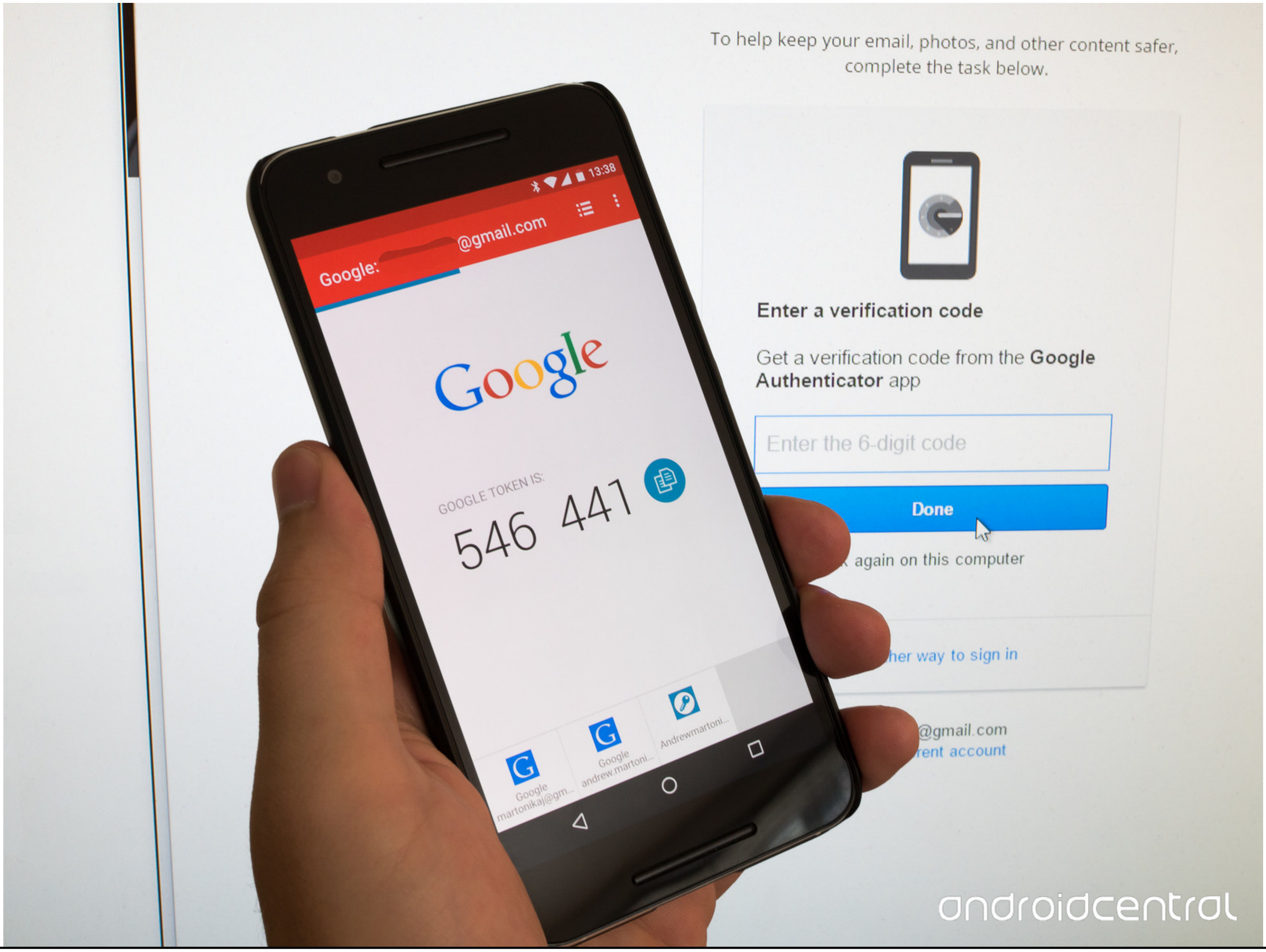
Enter your PIN.....

●●●●●●

Your one time PIN is 123ABC


PASSWORD
?
username
Login
+
PROOF
Is that you?
=
ACCESS
Success!

# Google authenticator app



To help keep your email, photos, and other content safer, complete the task below.

**Enter a verification code**

Get a verification code from the **Google Authenticator** app

Enter the 6-digit code

Done

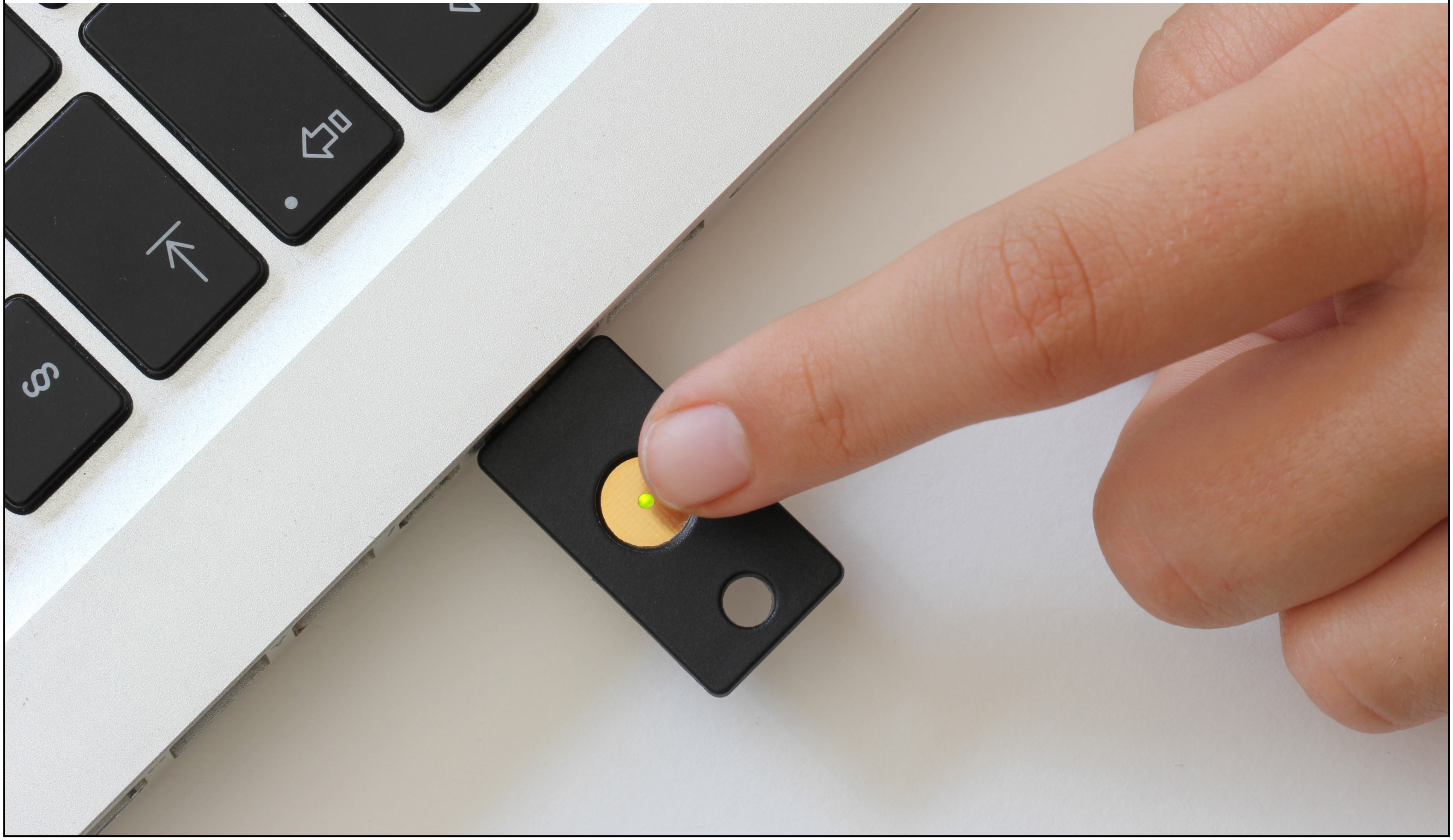
again on this computer

her way to sign in

@gmail.com

rent account

# YubiKey



# 2fa advantages and disadvantages

## Advantages

- Adds extra layer of security on top of passwords
  - Stealing a password is not enough
- Usually does not rely on human memory

## Disadvantages

- Slows down login process
  - Some are slower than others
- Hardware tokens cost money, inconvenient to carry, might be lost
- Some vulnerable to certain types of attacks
  - Man-in-the-middle
  - Phone hijacking
  - Social engineering

# Backup authentication

# Why use secret questions?

- Inexpensive, may be able to avoid helpdesk call
- Webmail providers can’t use email for reset unless the user has another email account
- Seems like it should be easy (it’s not)
- Seems like it should be secure (it’s not)
  - Studies in 1990 and 1996 demonstrated this

# Secret questions

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

Stuart Schechter, A. J. Bernheim Brush, and Serge Egelman. It's No Secret: Measuring the Security and Reliability of Authentication via 'Secret' Questions. IEEE Security and Privacy 2009.

# Study method

- 130 participants, recruited in pairs
- Lab study
  - Move to room separate from partner
  - Answer demographic questions
  - Authenticate to Hotmail using personal question
  - Answer personal questions for top four webmail services
  - Describe relationship with partner
  - Guess partner’s answers to personal questions
  - Attempt to recall answers to own personal questions
  - Second chance to guess partner’s questions using online research
- 3-6 months later: Attempt to recall answer to own personal questions in online survey

# Secret questions of major webmail providers from March 2008

- Note, most of these have since changed

# AOL Questions

Aol Mail.

- 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?
- 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

The efficient way to do email

- 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?
- 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?

# 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 from other participants (excluding partner)
  - 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

# Latest NIST draft recommendations

- Don’t use secret questions

# Can you do better?

- Working in groups, come up with 3 secret questions and/or an alternative approach to backup authentication
- Write them on the board
- We'll critique them as a class