User Authentication - 2

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

28/01/2025

THE UNIVERSITY of EDINBURGH

How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation

Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass,
Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas,
Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University
{*bur, pgage, sarangak, jlee, mmaass, mmazurek, tpassaro,*
rshay, tvidas, lbauer, nicolasc, lorrie}*@cmu.edu*

Abstract

To help users create stronger text-based passwords, many web sites have deployed password meters that provide visual feedback on password strength. Although these meters are in wide use, their effects on the security and usability of passwords have not been well studied.

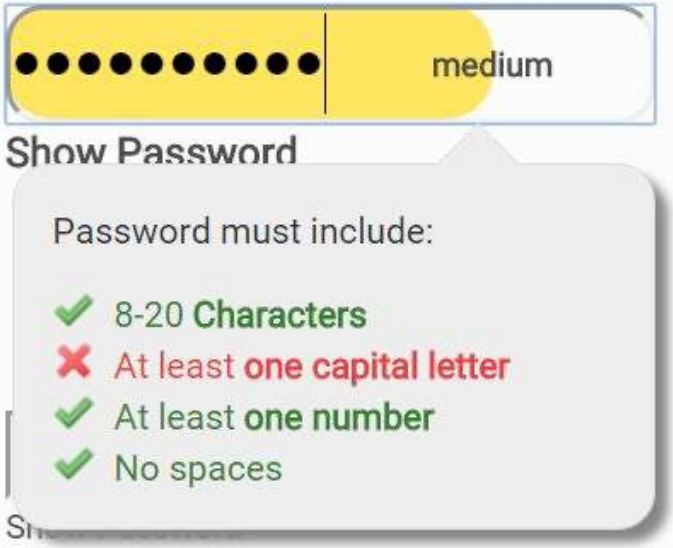
We present a 2,931-subject study of password creation in the presence of 14 password meters. We found that meters with a variety of visual appearances led users to create longer passwords. However, significant increases in resistance to a password-cracking algorithm were only achieved using meters that scored passwords stringently.

or write them down [28]. Password-composition policies, sets of requirements that every password on a system must meet, can also make passwords more difficult to guess [6, 38]. However, strict policies can lead to user frustration [29], and users may fulfill requirements in ways that are simple and predictable [6].

Another measure for encouraging users to create stronger passwords is the use of password meters. A password meter is a visual representation of password strength, often presented as a colored bar on screen. Password meters employ suggestions to assist users in creating stronger passwords. Many popular websites, from Google to Twitter, employ password meters.

The effect of strength meters on password creation

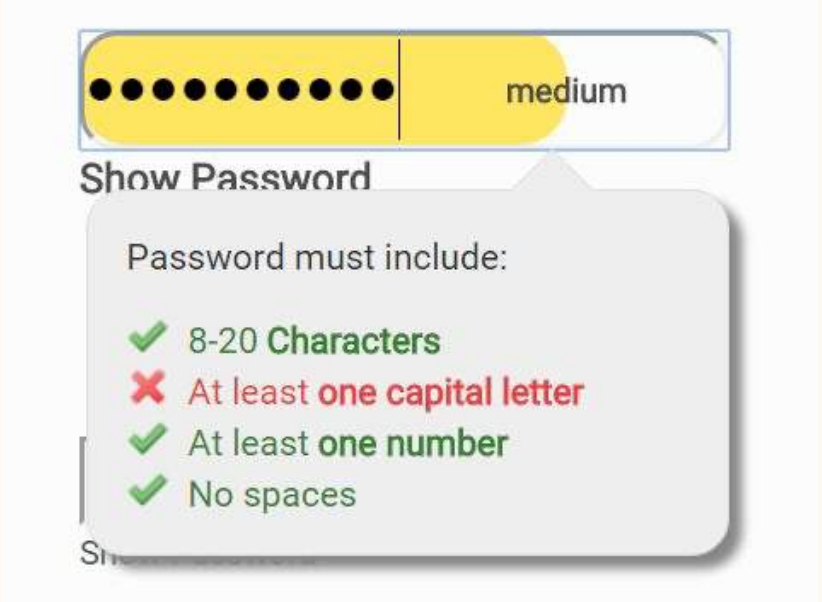
- Phase 1: What kinds of meters are being used by websites right now?
- Phase 2: What are “good” measures of password quality?
- Phase 3: How do different meter designs impact the passwords created? If so, which meters perform best?



Ur, Blase, et al. "How does your password measure up? The effect of strength meters on password creation." *Presented as part of the 21st USENIX Security Symposium*. 2012.

Phase 1: What kinds of meters are being used by websites right now?

- Reviewed login pages of Alexa top 100 most popular websites
- 96 allowed a login
- 70 gave some type of password feedback
- Common types of meters
  - Bar-like (50%)
  - Checkmark or X system (41.3\%)
  - Text indicating problems (21.2\%)



Ur, Blase, et al. "How does your password measure up? the effect of strength meters on password creation." *Presented as part of the 21st USENIX Security Symposium*. 2012.

Phase 1: Understand the security technology

- Good idea to start any security project by first **understanding the technology** you are working with.
  - Security concepts can often be non-obvious in how they work or interact with other technology.
- Determine the current **state-of-the-art**.
  - How do other people solve this problem now?
  - Why are they doing it that way and has anyone decided what solution is “best”?
- Formulate **a question about the technology** based on what you find.

Just colored words

Facebook

New: •••••

Too short

Re-type new: •••••

Passwords match

Baidu

Password: **Confirm Password:**

••••••

The structure of your password is too simple to replace the more complex the password, otherwise unable to register successfully.
Password length of 6 to 14, the letters are case-sensitive. Password is too simple hazards

Green bars / Checkmark-x

Twitter

••••••••

✖ Password is too obvious.

••••••••••

✓ Password is okay.

••••••••••••••••••••••

✓ Password is perfect!

Checklists

Apple

••••••••

Password strength: weak

Password must:

- Have at least one letter
- **Have at least one capital letter**
- **Have at least one number**
- Not contain more than 3 consecutive identical characters
- Not be the same as the account name
- Be at least 8 characters

Segmented bars

Weibo

* Create a ••••••••

弱 中 強

弱 中 強

弱 中 強

Mail.ru

Уровень сложности: слабый

Уровень сложности: сильный

Paypal

Fair

- ✓ Include at least 8 characters
- ✓ Don't use your name or email address
- ▪ Use a mix of uppercase and lowercase letters, numbers, and symbols
- ✓ Make your password hard to guess - even for a close friend

Strong
Fair
Weak

Yahoo.jp and Yahoo

baseball1 パスワードの安全性 低 Strong

Aaaaaa1! パスワードの安全性 中 Very strong

Gradient bars

Wordpress.com

Bad

Live.com

Weak

Medium

Strong

Color changing bars

Mediafire

••••

Password Strength Too short

Password Strength Weak

Password Strength Fair

Password Strength Good

Password Strength Strong

Blogger

••••••••

Password strength: Weak

Google

Create a password

••••••••

Password strength: Weak

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?

Password strength: Strong

Password strength: Good

Password strength: Too short

Phase 2: What are “good” measures of password quality?

- Look at scientific literature to understand what other people have already learned.
- Two well known ways to measure password strength:
  - **Basic16** - password must have at least 16 characters.
  - **Comprehensive8** – password must have at least eight characters, including an uppercase letter, a lowercase letter, a digit, and a symbol. It must also not already be in a wordlist of common passwords.

- password
- P@ssw0rd
- iloveyou123
- monkey
- thisisasuperlongpasswordthatisawesome
- VV@yBetter123

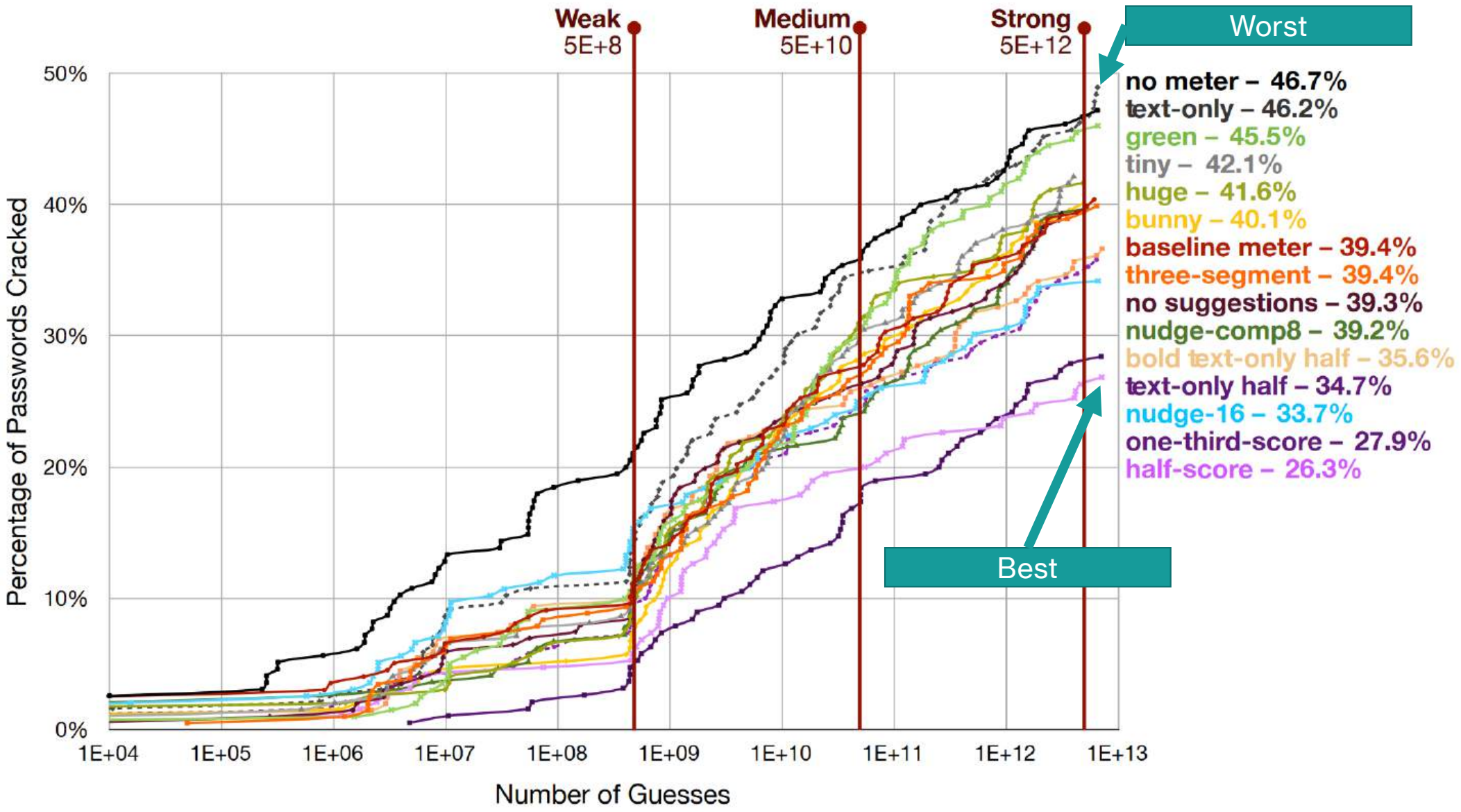
Phase 3: How do different meter designs impact the passwords created?

- Online survey study using Amazon Mechanical Turk
- 15 different conditions (next slide)
- 2931 participants
- 2 phase study:
  - Setup a password
  - 2 days later, log in using the original password

Ur, Blase, et al. "How does your password measure up? the effect of strength meters on password creation." *Presented as part of the 21st USENIX Security Symposium*. 2012.

Conditions

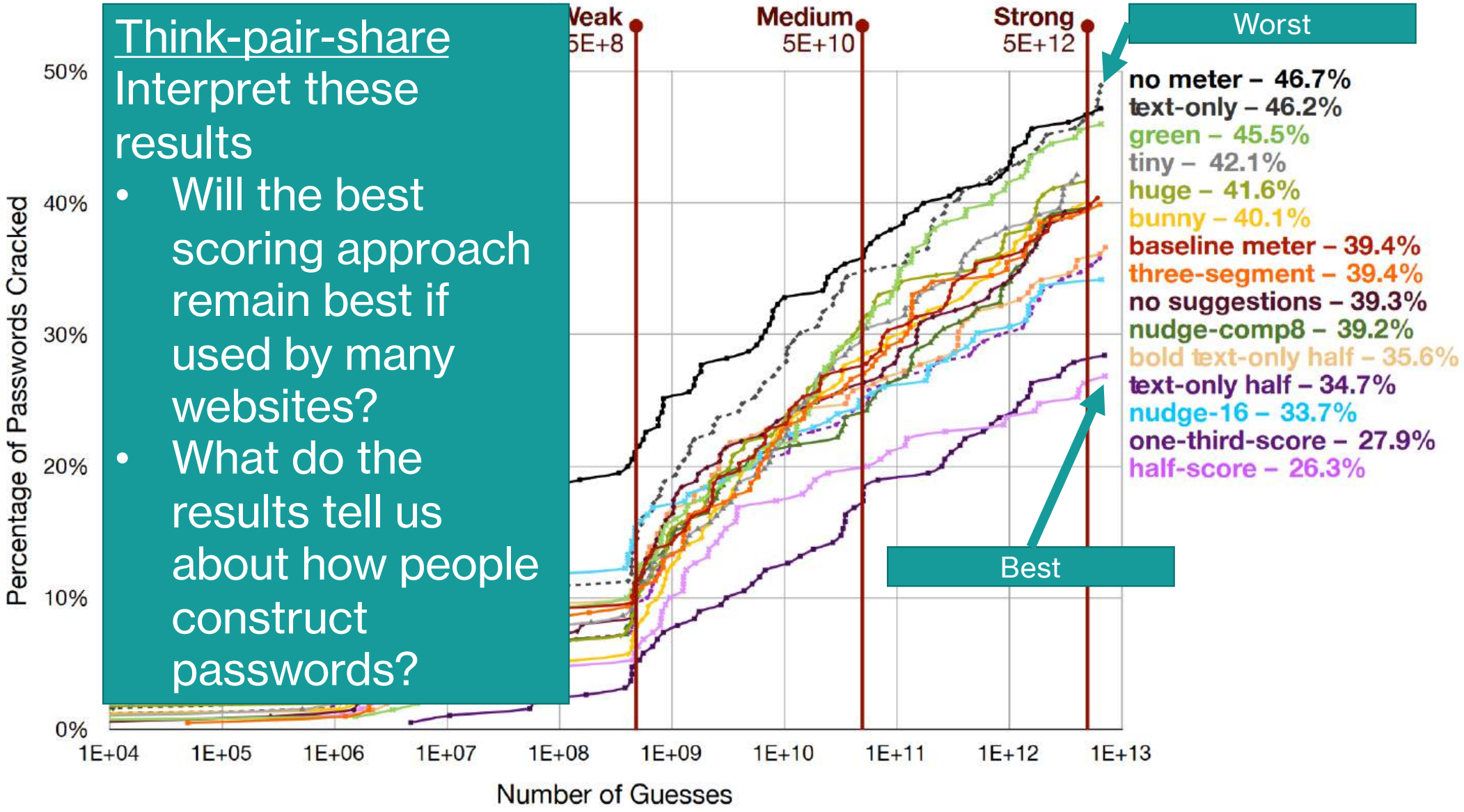
- **Control**
  - No meter
  - Baseline meter based on real ones – colored bar with text hints
- **Appearance variations**
  - Three-segment
  - Green – bar is always green
  - Tiny – bar is very small
  - Huge – bar is very large
  - No suggestions – bar, but no helpful feedback
  - Text-only – feedback, but no bar
- **Scoring**
  - Half-score – bar shown half as full as would be in baseline
  - One-third-score
  - Nudge-16 – score uses the Basic16 metric
  - Nudge-comp8 – score uses Comprehensive8 metric
- **Multiple variations**
  - Text-only & half-score
  - Bold text-only & half score
  - Bunny – running bunny instead of a meter


Weak
5E+8
Medium
5E+10
Strong
5E+12
Worst
Best
no meter – 46.7%
text-only – 46.2%
green – 45.5%
tiny – 42.1%
huge – 41.6%
bunny – 40.1%
baseline meter – 39.4%
three-segment – 39.4%
no suggestions – 39.3%
nudge-comp8 – 39.2%
bold text-only half – 35.6%
text-only half – 34.7%
nudge-16 – 33.7%
one-third-score – 27.9%
half-score – 26.3%
Percentage of Passwords Cracked
50%
40%
30%
20%
10%
0%
1E+04
1E+05
1E+06
1E+07
1E+08
1E+09
1E+10
1E+11
1E+12
1E+13
Number of Guesses

Think-pair-share

Interpret these results

- Will the best scoring approach remain best if used by many websites?
- What do the results tell us about how people construct passwords?



Overview

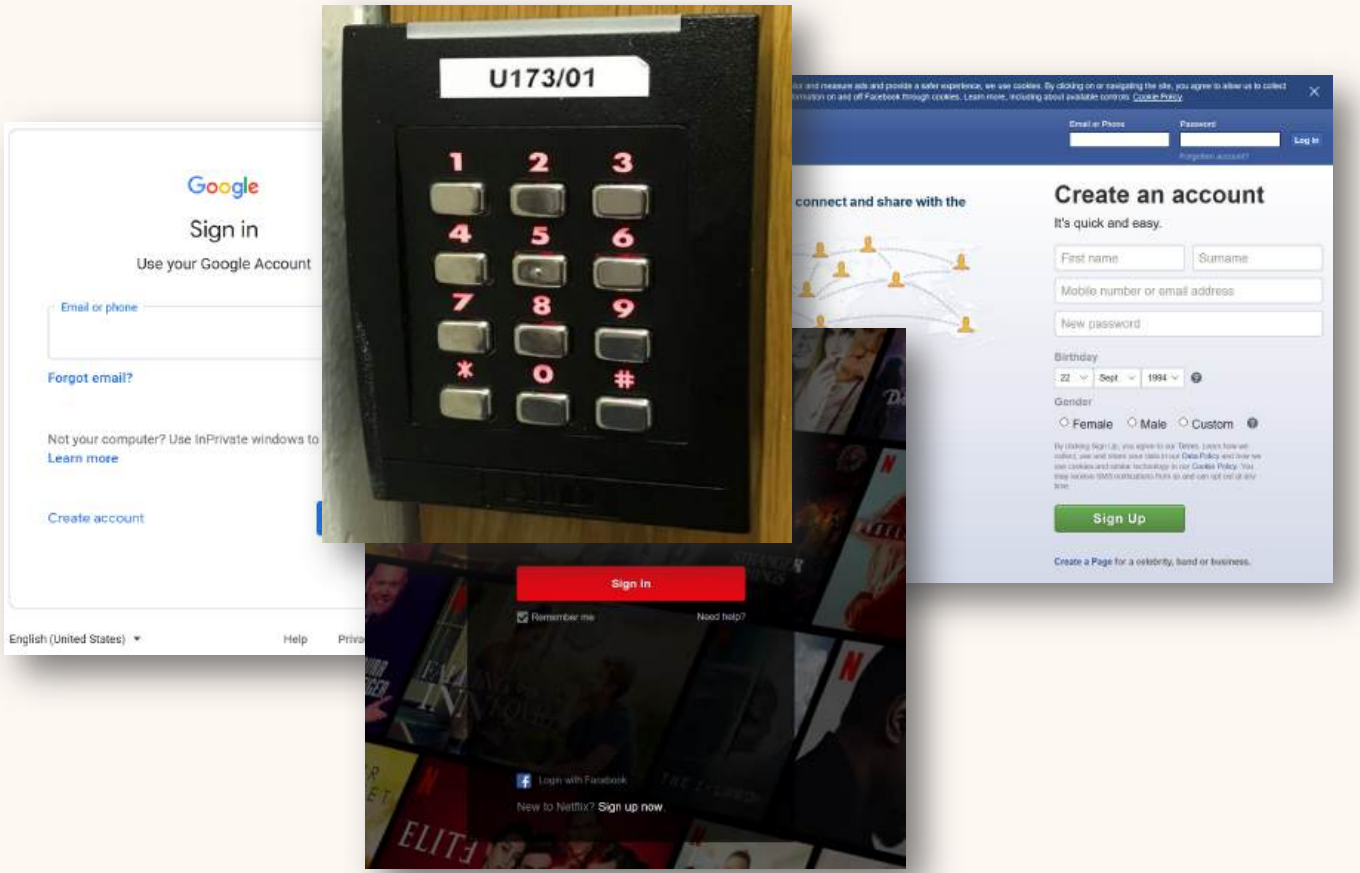
- Reminder, warm-up, and recap
- Biometrics
- Take-home

Reminder

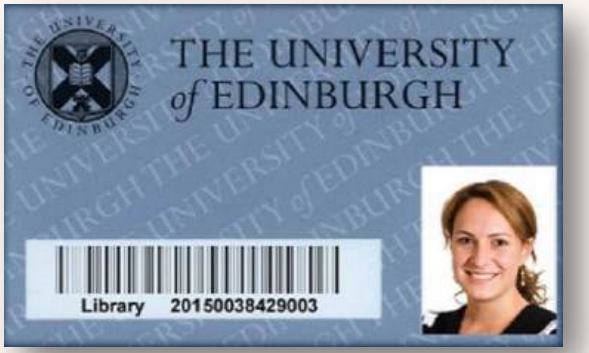
- Tutorial starting next Monday 10am! (finally :))
- Blog related questions and discussion

Anyone know what is this?

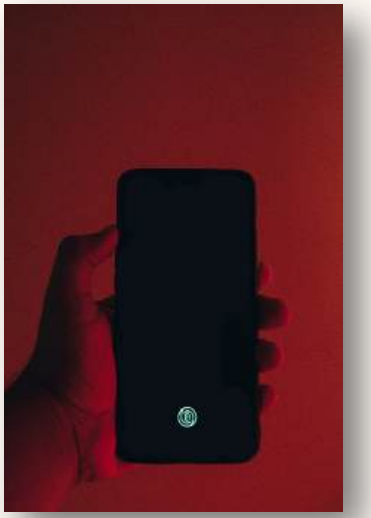
Authentication



What you know



What you have



Who you are

Usable Authentication is:

- User friendly
- Reasonable to implement
- Protects against attacks

Bonneau, Joseph, et al. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012.

One time password over SMS

Good Poor Bad

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

Reasonable to implement

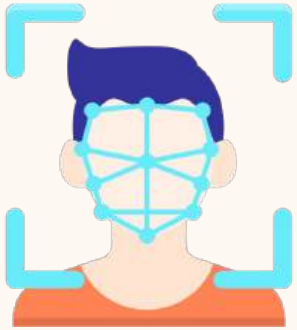
- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

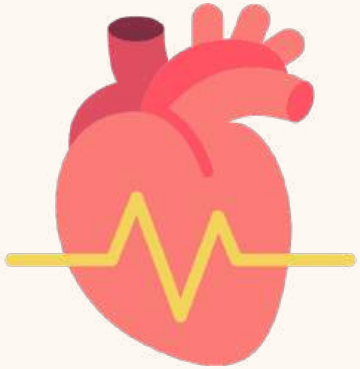
- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Physiological

DNA



Faceprint



Heartbeat

palmprint

Behavioural

Gait

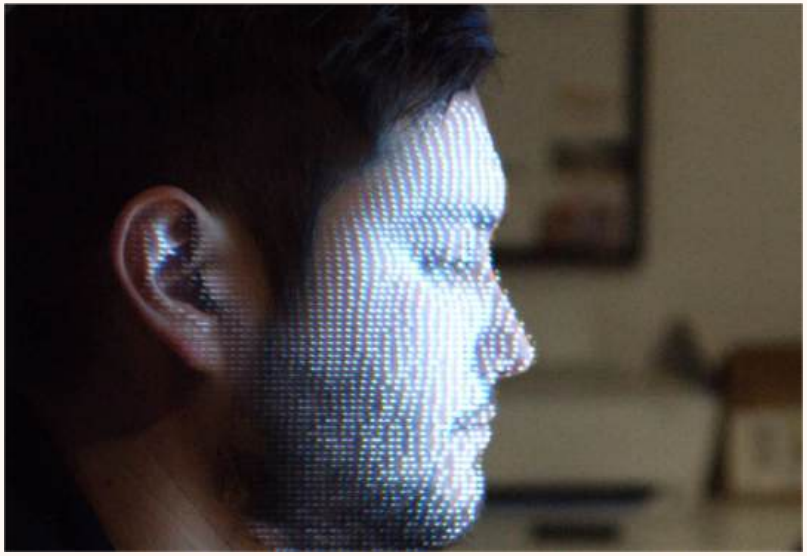
Keystroke

Voiceprint

Signature

Fingerprint: History

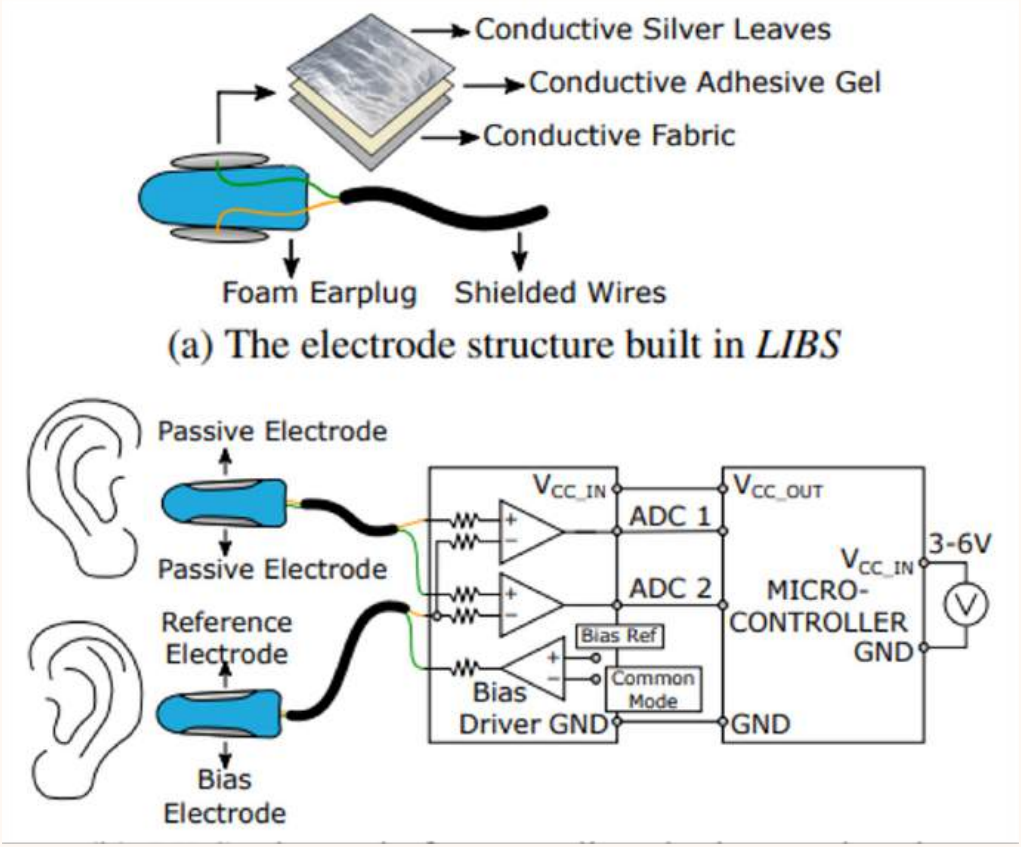
- **Prehistoric** potters identify their works with an impressed fingerprint
- **200 BC:** Chinese sign legal documents using fingerprints
- **1400 AD:** Persia used fingerprint for identification
- **1685:** Marcello Malpighi (University of Bologna), formalized fingerprint, introduced ridges, minutiae points
- **1858:** The British started using fingerprint in India (Hoogly district, Bengal) to sign contracts
- **1880s**: Scientists (including Charles Darwin)began observing fingerprints for identification
- **1903:** NYC State Prison started using fingerprinting inmates
- **1905:** US army started using fingerprints for personal identification
- **1924:** FBI Identification Division to collect and consolidate fingerprints
- **2012:** Automated Fingerprint Identification System (AFIS)

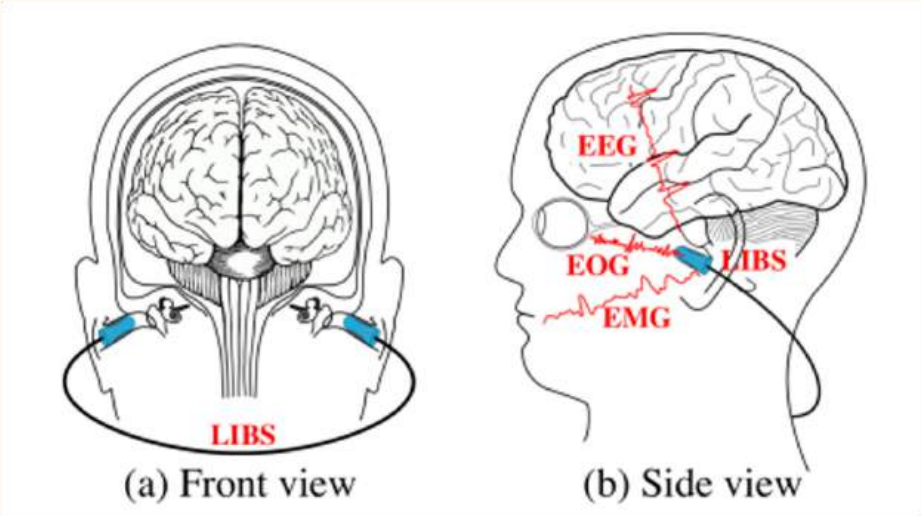


Face ID: more than an image

“The TrueDepth camera captures accurate face data by projecting and analyzing thousands of invisible dots to create **a depth map** of your face and also captures **an infrared image** of your face.” – Apple

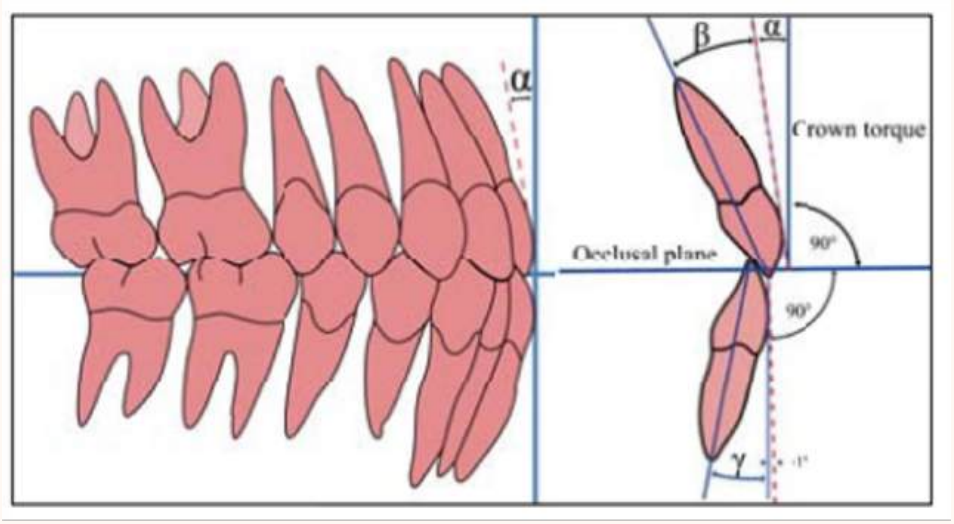
Emerging Biometrics: Earable





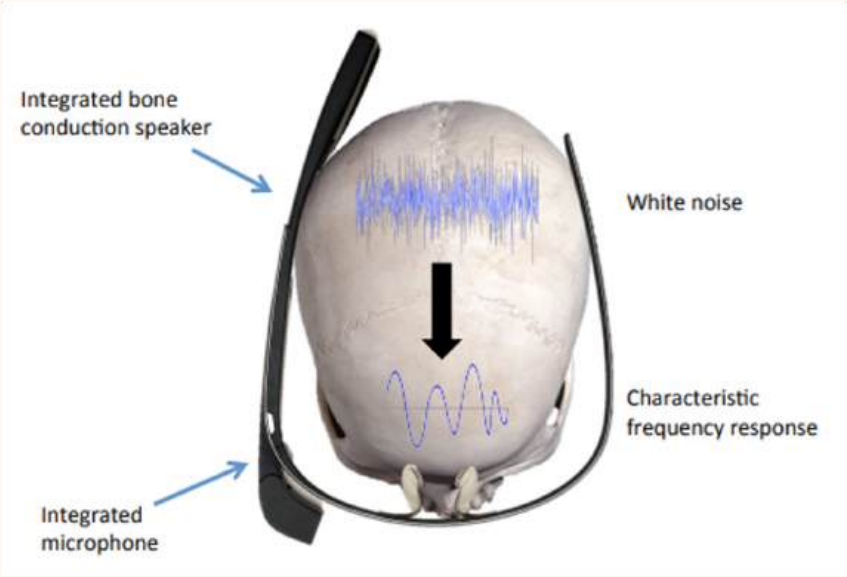
Nguyen, Anh, Raghda Alqurashi, Zohreh Raghebi, Farnoush Banaei-Kashani, Ann C. Halbower, and Tam Vu. "A lightweight and inexpensive in-ear sensing system for automatic whole-night sleep stage monitoring." In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, pp. 230-244. 2016.

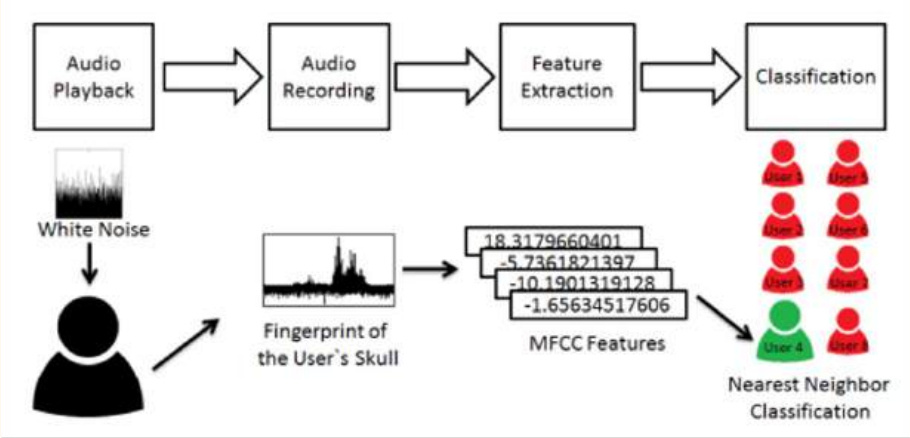
Emerging Biometrics: Teeth Interface



Zou, Y., Zhao, M., Zhou, Z., Lin, J., Li, M. and Wu, K., 2018. BiLock: User authentication via dental occlusion biometrics. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(3), pp.1-20.

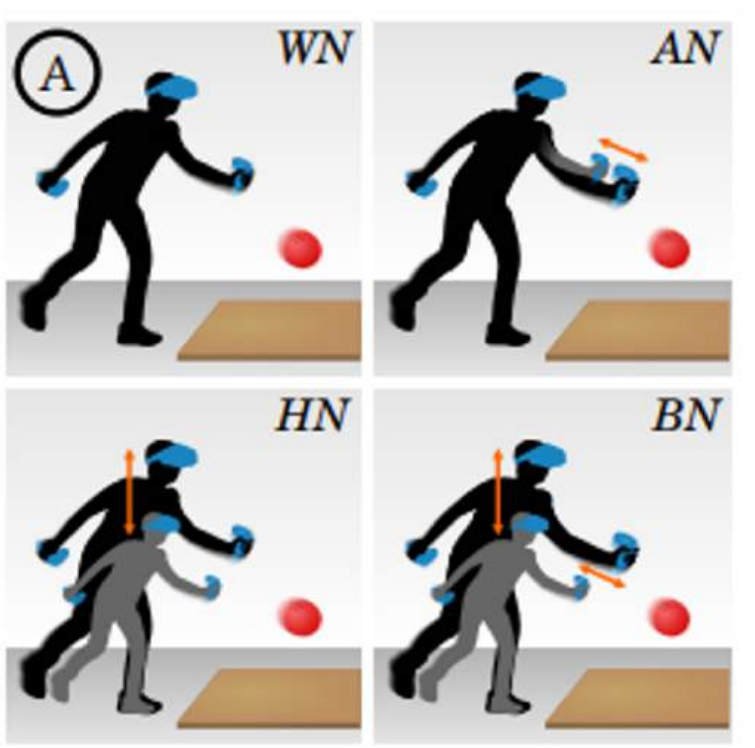
Emerging Biometrics: Bone Conduction

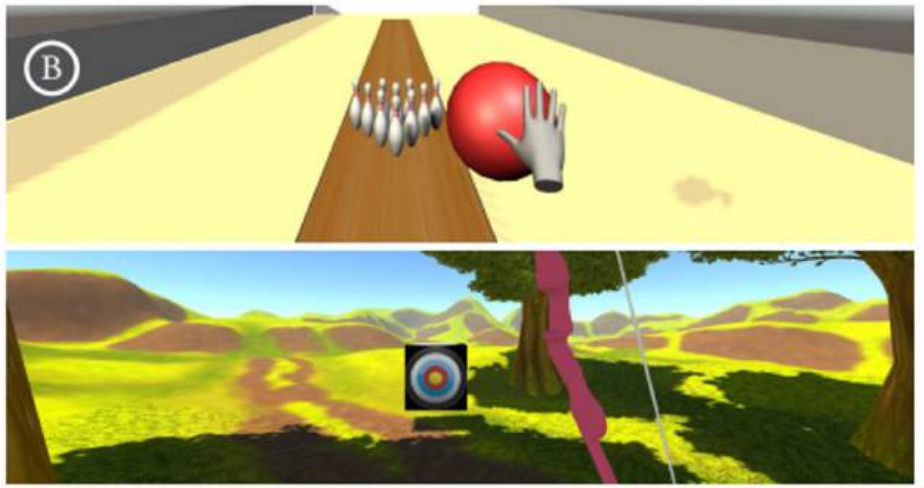




Schneegass, Stefan, Youssef Oualil, and Andreas Bulling. "SkullConduct: Biometric user identification on eyewear computers using bone conduction through the skull." In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 1379-1384. 2016.

Emerging Biometrics: VR Motion





Liebers, Jonathan, Mark Abdelaziz, Lukas Mecke, Alia Saad, Jonas Auda, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. "Understanding user identification in virtual reality through behavioral biometrics and the effect of body normalization." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1-11. 2021.

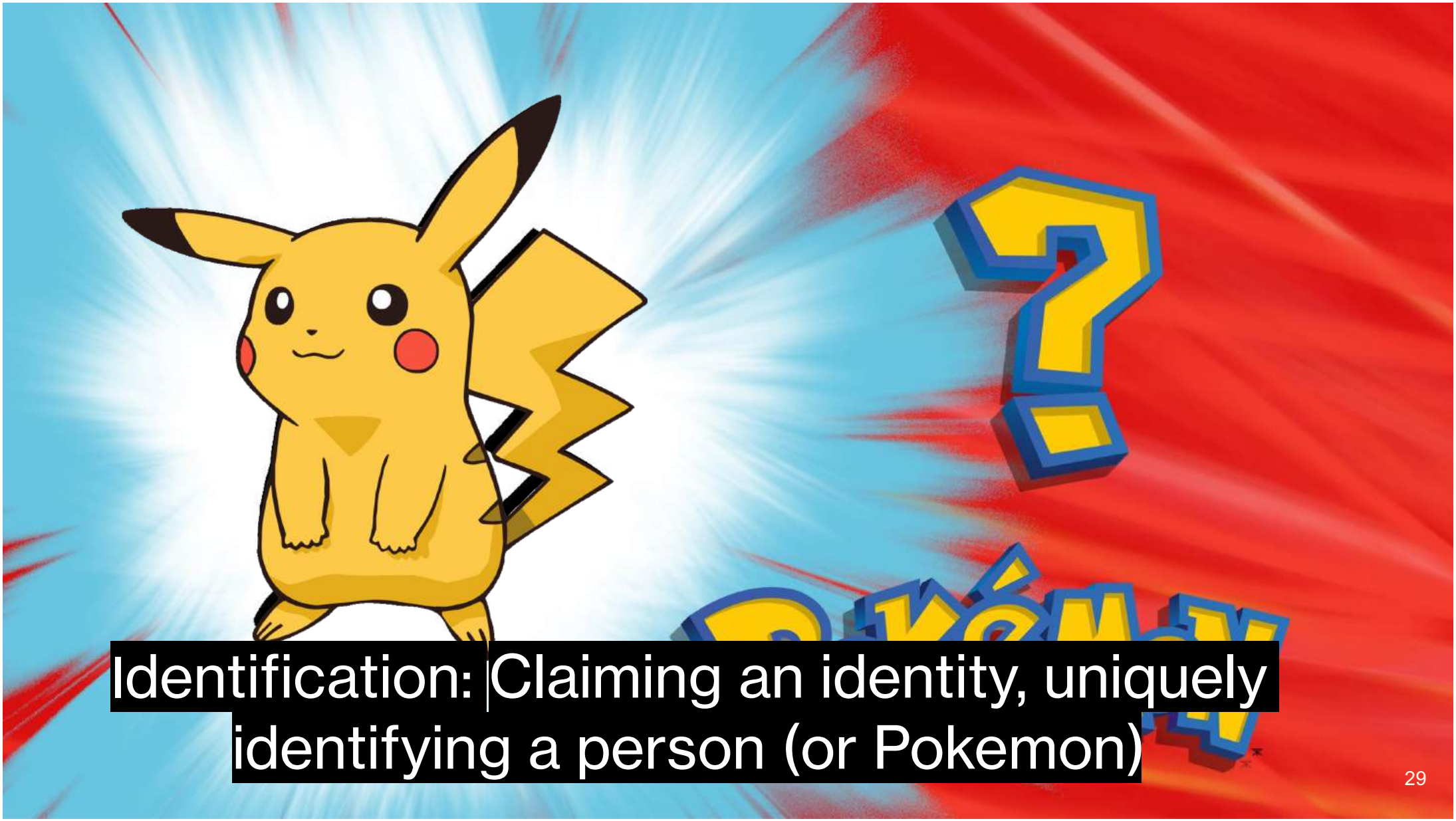
Fingerprint vs. Face ID? Which one do you prefer?

Attributes of a “good” biometric feature

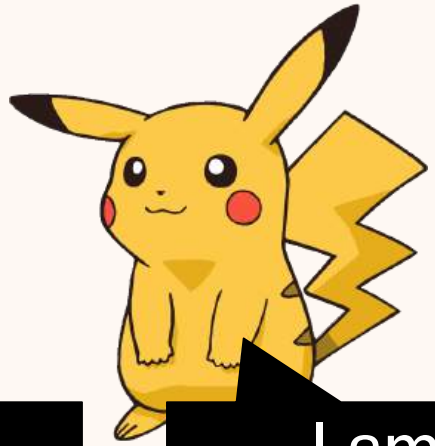
1. **Universality:** Does everyone have it?
2. **Distinctiveness:** Is it different for everyone?
3. **Permanence:** Does the feature change over time/age?
    - bad: face, good: fingerprint
4. **Collectability:** How easy it is to collect/measure the feature?
    - Very hard: DNA, relatively easy: fingerprint
5. **Performance:** How difficult to match?
6. **Acceptability**
7. **Circumvention:** How easy to spoof?
    - Voice recognition

https://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf

Identification vs. Authentication? What is the difference?


Identification: Claiming an identity, uniquely identifying a person (or Pokemon)

I am Pikachu



I am Pikachu

I am Pikachu

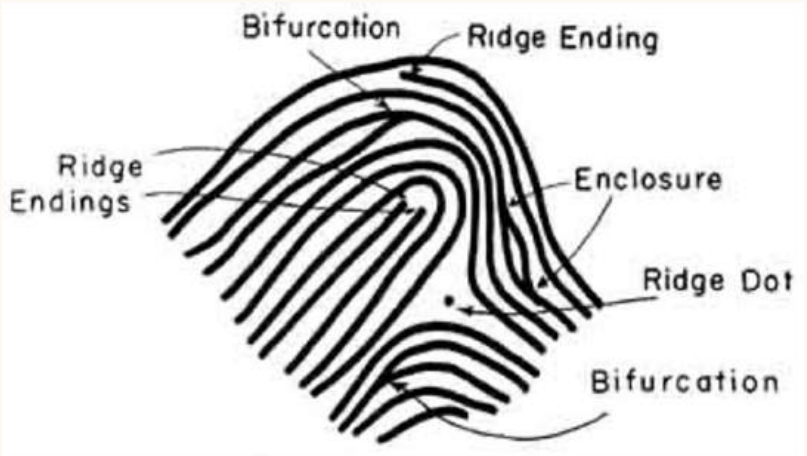
Authentication: proving the identity

Fingerprint: How does it work?

Image acquisition

Optical, Capacitive, Ultrasound sensors

Image processing

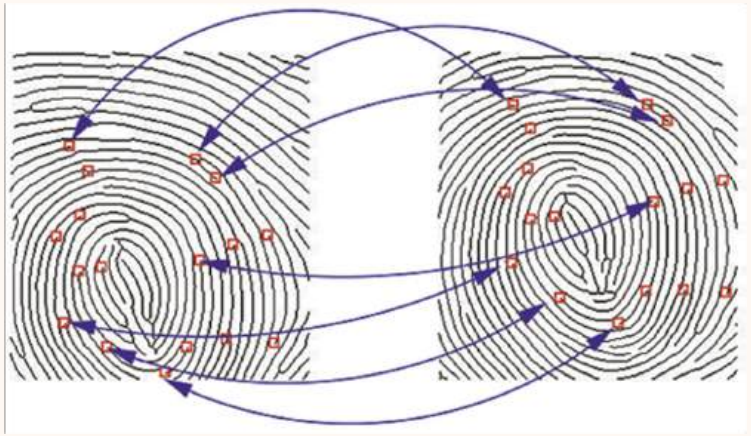


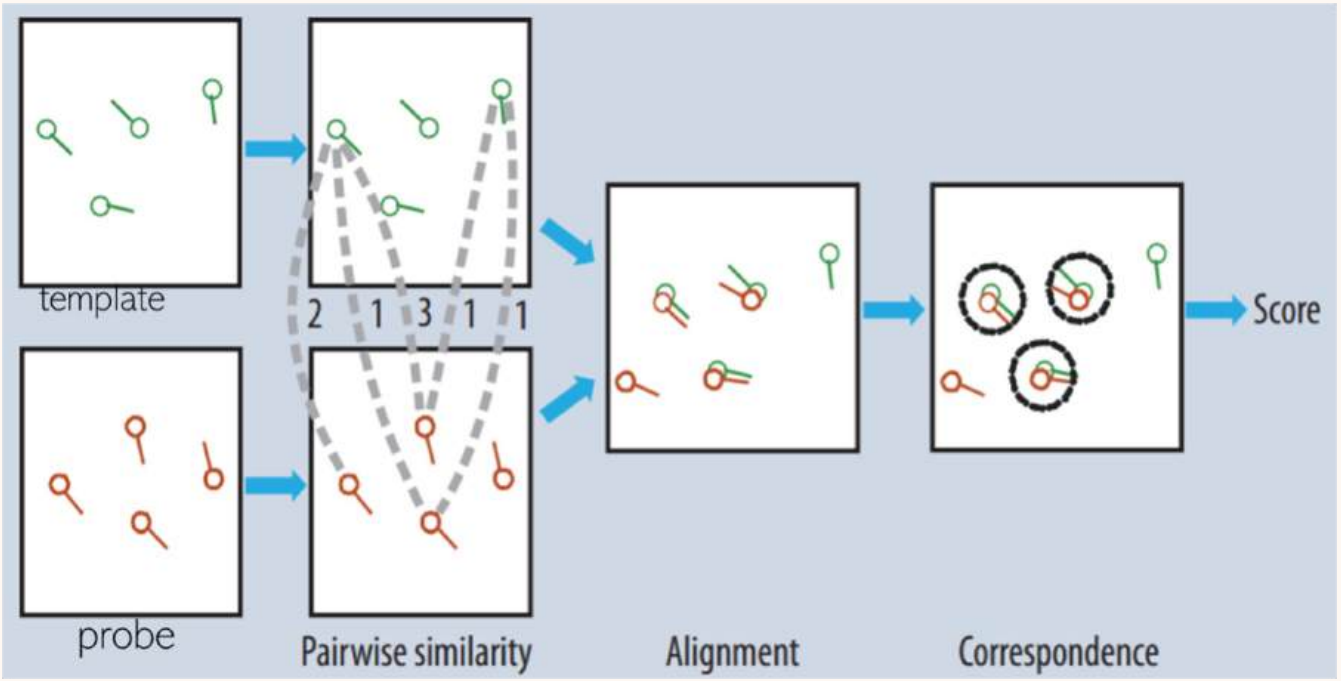
Minutiae extraction

Store f in the database with username

$$f = \{(x_1, y_1, \theta_1), (x_2, y_2, \theta_2), \ldots (x_n, y_n, \theta_n)\}$$

Fingerprint Matching





Matching Accuracy

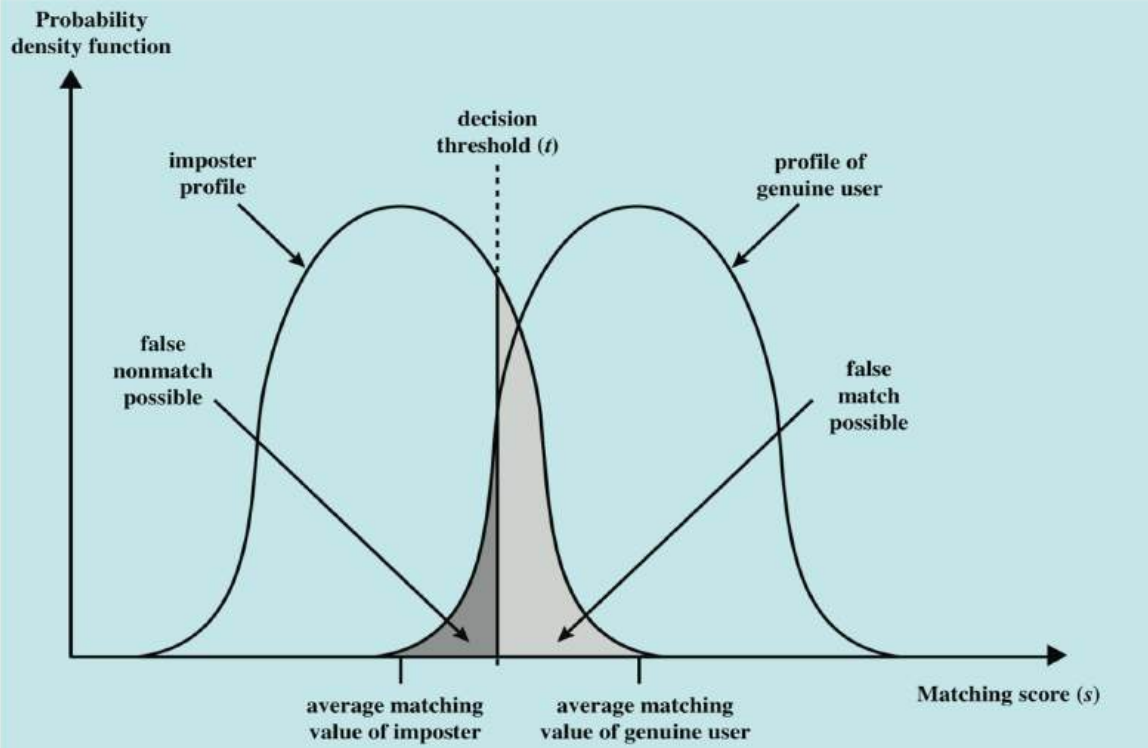


Figure 3.7 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared.

Matching Accuracy

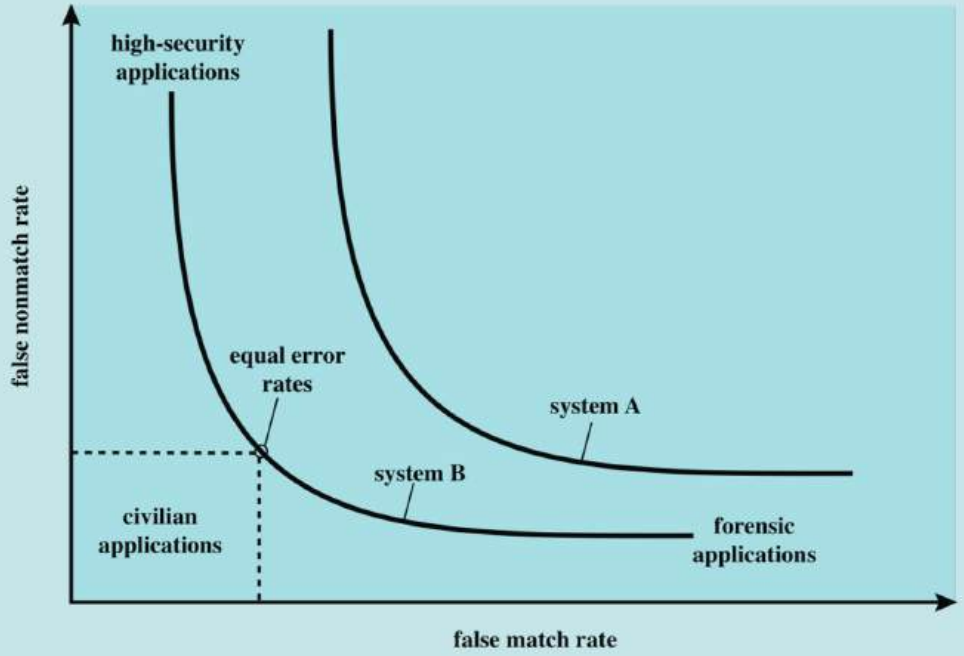


Figure 3.8 Idealized Biometric Measurement Operating Characteristic Curves. Different biometric application types make different trade-offs between the false match rate and the false nonmatch rate. Note that system A is consistently inferior to system B in accuracy performance. [JAIN00]

Challenge with Biometrics

- **Low accuracy**
  - High False Non-Matching Rate (FNMR) (a.k.a false rejection rate (FRR)
  - iPhone fingerprint matching has 1 in 50,000 false matching rate (FMR)
- **Noise** from biometric readers
- High error rate for **some users**
- Speed and scale matching process is **slow**
- **Cannot be hashed**, since every reading is different
  - Hash output will be completely different, and therefore cannot match
  - Cryptographic hash functions reveal nothing beyond strict equality

Correct – belongs to the **same users** – biometric readings are rejected

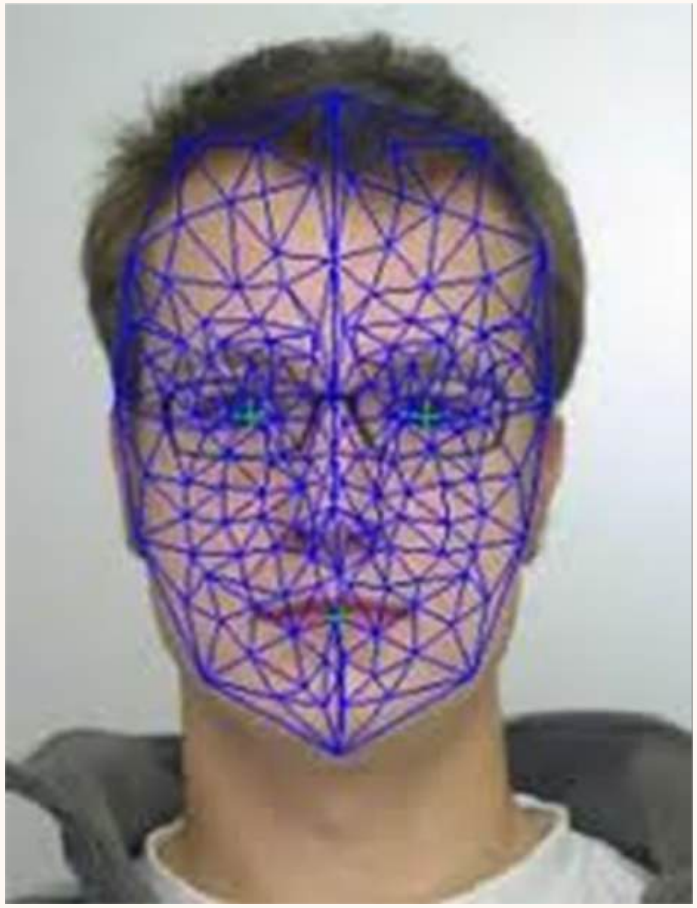
Incorrect – belongs to **different users** – fingerprints are accepted

Vascular Pattern

- LED infrared light
- May change overtime

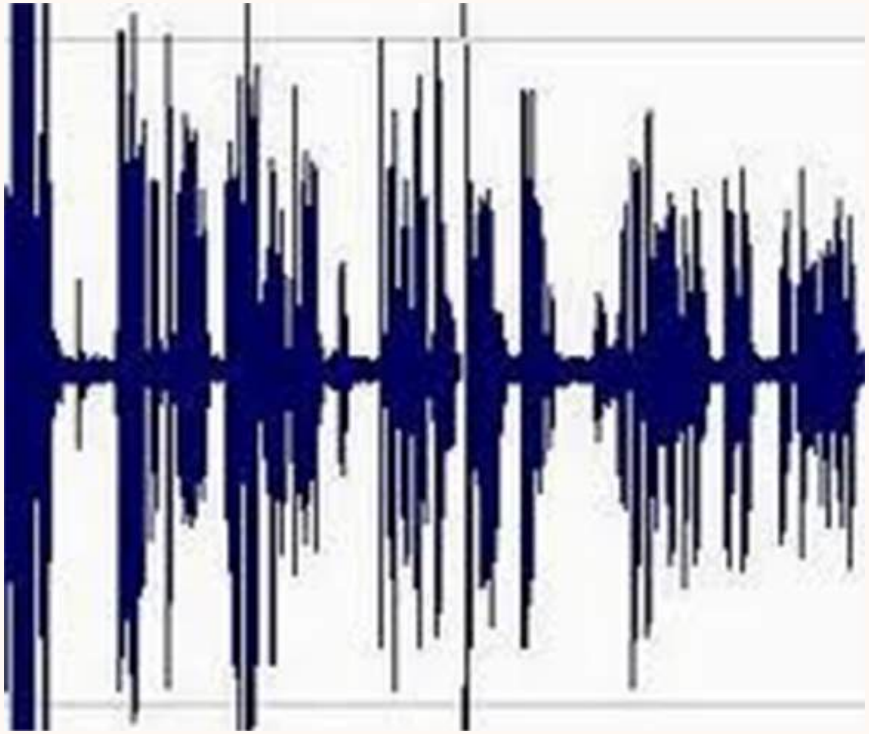
Face Recognition

- Location and position of facial features
- Dependent on background and lighting conditions



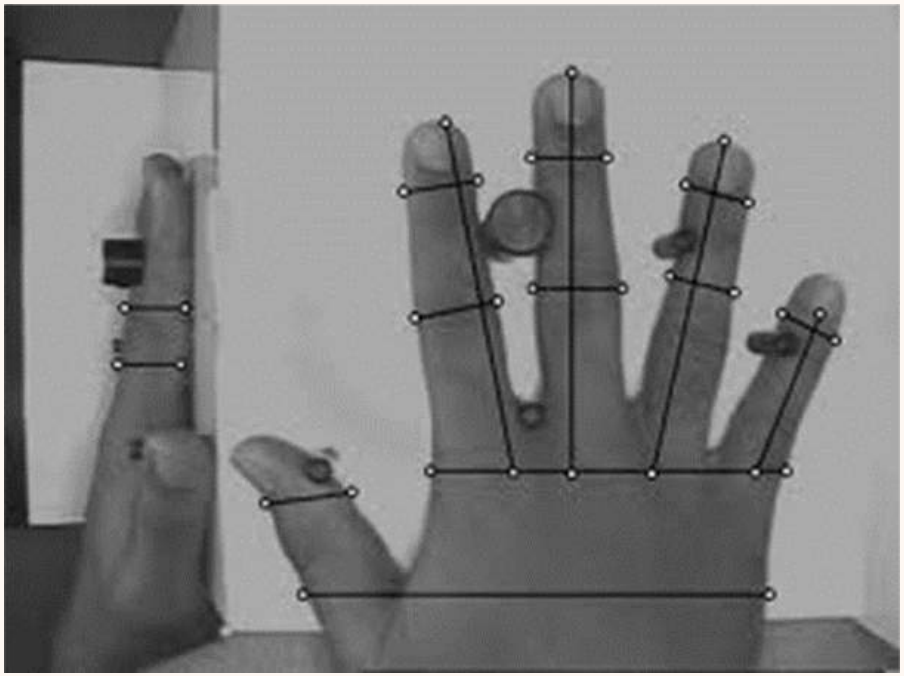
Voice Biometrics

- Factors: pitch, intensity, quality and duration
- Problems: include background noise



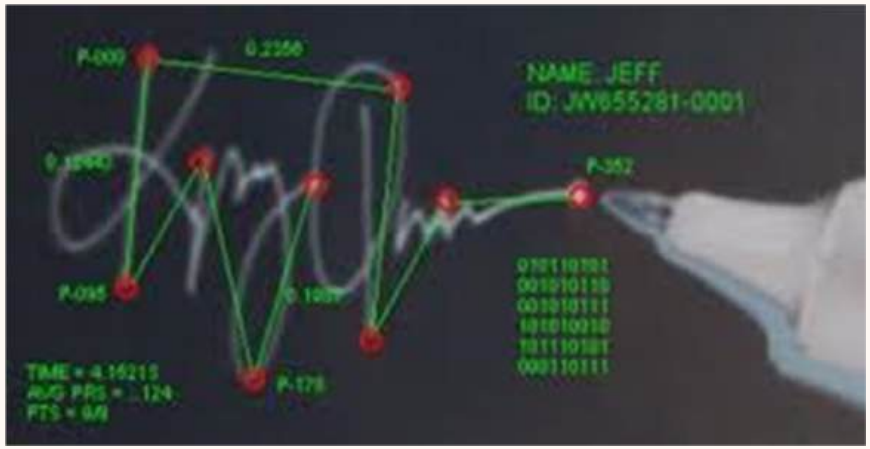
Hand Geometry

- Scan both sides of hand
- Not as accurate as other methods



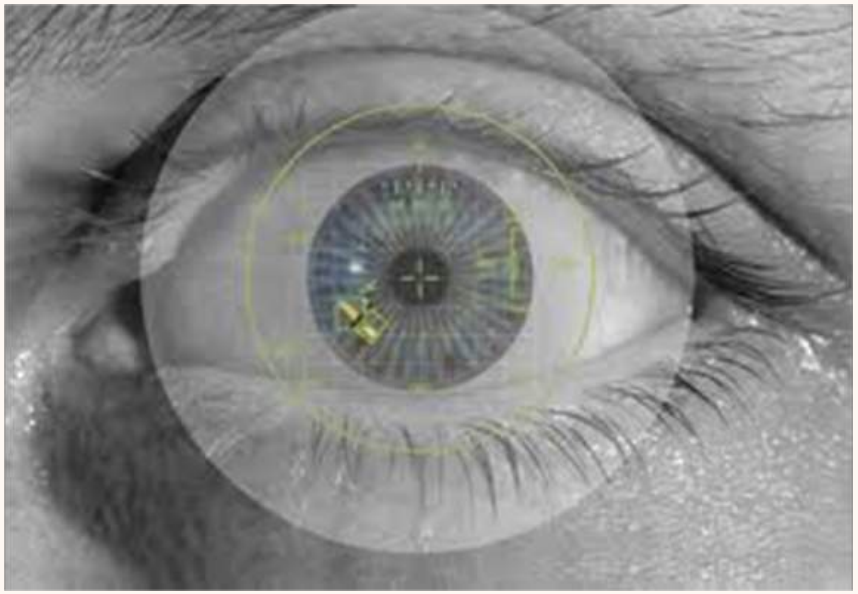
Dynamic Signature

- Factors: velocity, acceleration and speed
- Problems: forgers could reproduce



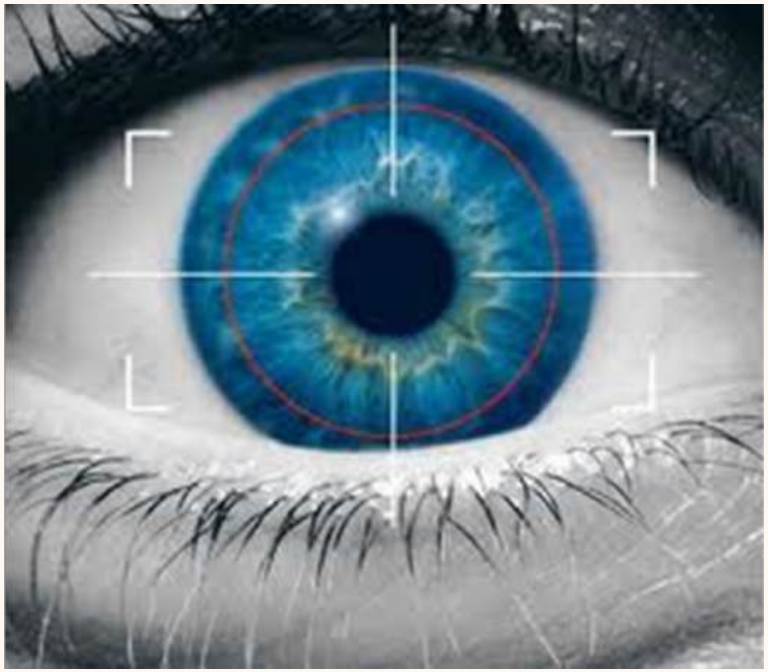
Iris Recognition

- Iris photography using visible or near infrared light
- Subject to environmental conditions



Retina Recognition

- One of the most secure means of biometrics
- Unique to each person
- Unique to each eye
- Problems: intrusive (flashing light into eyes)



Biometrics Application: Commercial

- Computer login
- Electronic Payment
- ATMs
- Record Protection

Biometrics Application: Government

- Passport control
- Border control
- Access Control

Biometrics Application: Forensic

- Missing persons
- Corpse identification
- Criminal investigations

What could go wrong?

User

Terminal

Network

Server

Model

Your biometrics are not safe!

- Shoulder-surfing
- Network sniffing
- Storage compromise
- Model poisoning
- … (many other surfaces!)


RIGINAL
DERPFAKE


BBC
NEWS

Challenge-Response Biometrics Authentication

VELODY: Nonlinear Vibration Challenge-Response for Resilient User Authentication

Jingjie Li
University of Wisconsin–Madison
jingjie.li@wisc.edu

Kassem Fawaz
University of Wisconsin–Madison
kfawaz@wisc.edu

Younghyun Kim
University of Wisconsin–Madison
younghyun.kim@wisc.edu

ABSTRACT

Biometrics have been widely adopted for enhancing user authentication, benefiting usability by exploiting pervasive and collectible unique characteristics from physiological or behavioral traits of human. However, successful attacks on "static" biometrics such as fingerprints have been reported where an adversary acquires users' biometrics stealthily and compromises non-resilient biometrics.

To mitigate the vulnerabilities of static biometrics, we leverage the unique and nonlinear hand-surface vibration response and design a system called VELODY to defend against various attacks including replay and synthesis. The VELODY system relies on two major properties in hand-surface vibration responses: uniqueness, contributed by physiological characteristics of human hands, and nonlinearity, whose complexity prevents attackers from predicting the response to an unseen challenge. VELODY employs a challenge-response protocol. By changing the vibration challenge, the system elicits input-dependent nonlinear "symptoms" and unique spectrotemporal features in the vibration response, stopping both replay and synthesis attacks. Also, a large number of disposable challenge-

'19), November 11–15, 2019, London, United Kingdom. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3319535.3354242

1 INTRODUCTION

The mass proliferation of "smart" devices has created unprecedented security and privacy concerns to their users. One of the significant security concerns comes from unauthorized entities accessing and controlling user devices. Stronger access control goes a long way towards alleviating security and privacy threats to users and their devices. User authentication, where a user has to prove their identity to a system, is one core mechanism to achieve adequate access control.

Biometric user authentication, which relies on the unique physiological or behavioral traits of the user to verify their identity, has been touted as the solution that meets both security and usability goals. Thanks to its low cognitive burden, it is more attractive to the users who wish to authenticate themselves to their devices without having to memorize a password or use an additional security device.

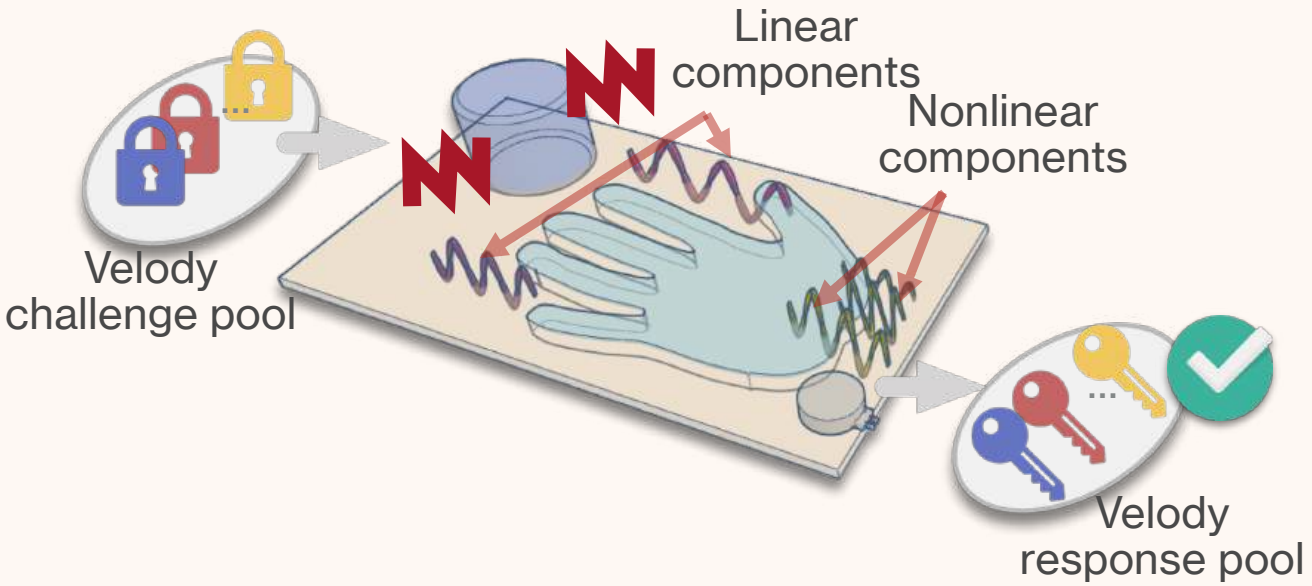
PITFALLS OF REUSING STATIC BIOMETRIC

- **Static:** reusing same information
- **Non-resilient:** cannot be recovered

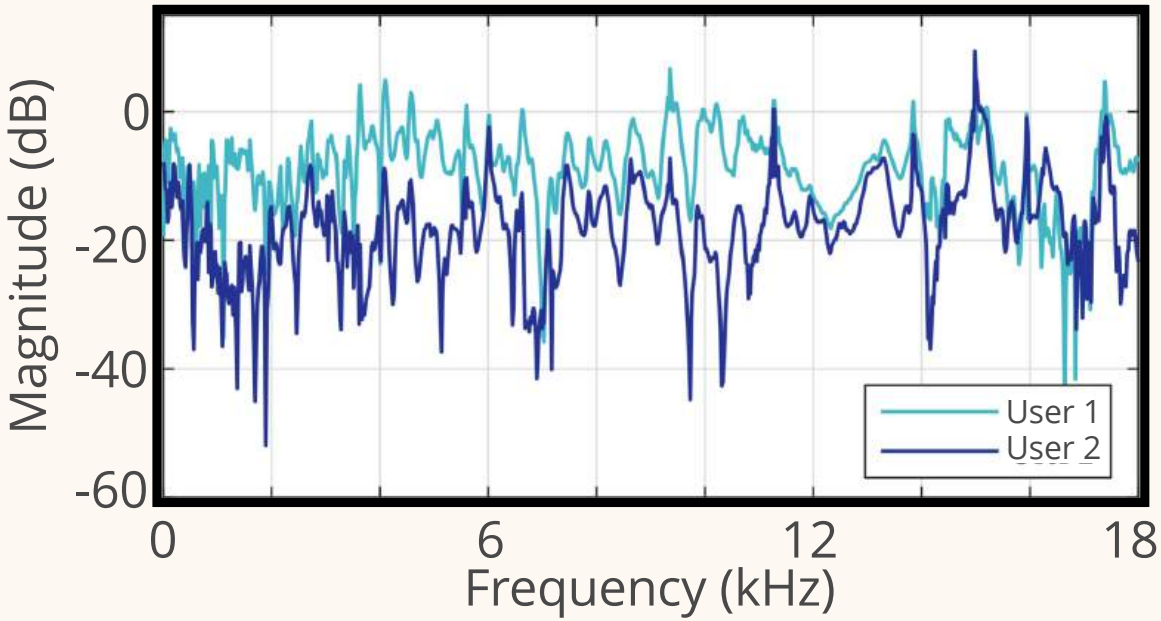
CHALLENGE-RESPONSE BIOMETRIC

- **Modality:** respond dynamically to different stimuli (challenges)
- **Security:** harvest sufficient secret keys
- **Usability:** enroll and authenticate with low effort

VELODY: OVERVIEW



Unique Hand-Surface Vibration



Hand-surface vibration responses of frequency chirp

- Vibration as an **interaction** modality
- Vibration for user **identification** (VibID, 2016) and **authentication** (VibWrite, 2017)
- **Uniqueness** from different hand geometries and compositions

Yang, L., Wang, W. and Zhang, Q., 2016, April. Vibid: User identification through bio-vibrometry. In Proceedings of the 15th International Conference on Information Processing in Sensor Networks (p. 11). IEEE Press.

Liu, J., Wang, C., Chen, Y. and Saxena, N., 2017, October. VibWrite: Towards finger-input authentication on ubiquitous surfaces via physical vibration. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 73-87). ACM.

Background: Nonlinear Vibration Response

Input:

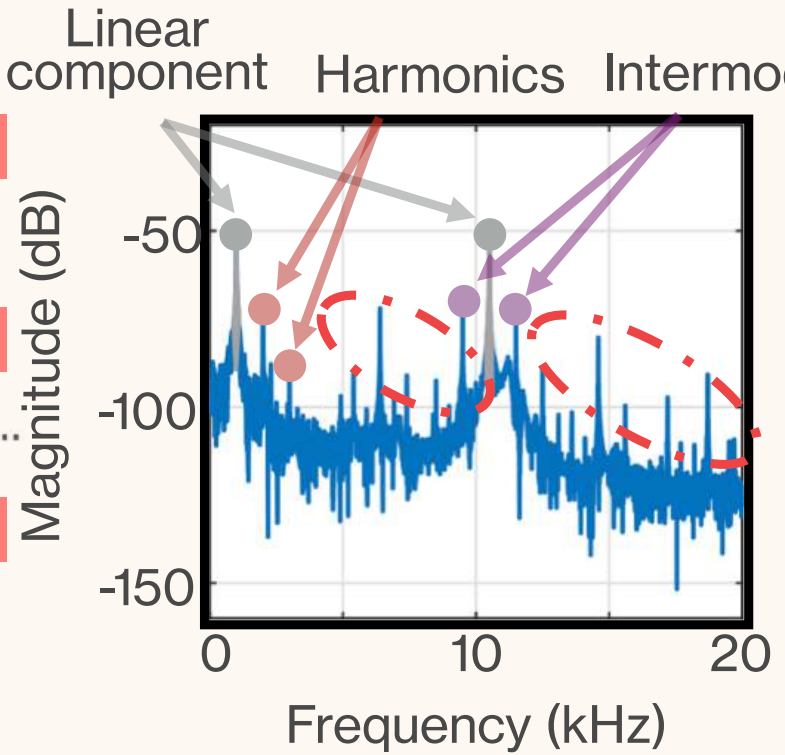
f_1, f_2

Harmonics:

$2f_1, 2f_2, 3f_1, 3f_2, \ldots$

Intermodulation:

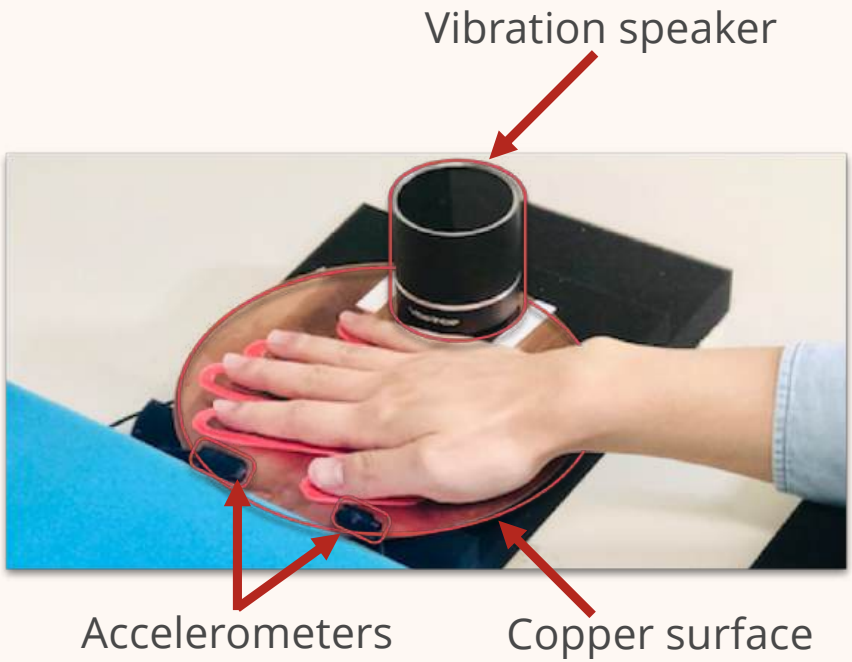
$f_1 + f_2, f_1 - f_2, \ldots$



- **Frequency generation** in nonlinear vibration channel
- **Non-analytic** response dependent on the stimulus-induced state of the channel

→ **Hard to model** hand-surface vibration channel

Experimental Setup

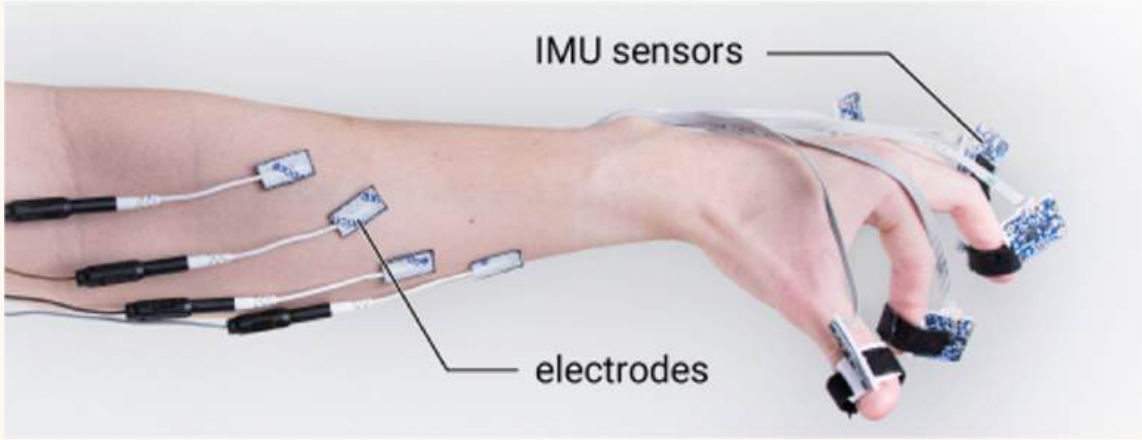


- 15 subjects during 1.5 months (approved by IRB of UW-Madison)
- Session length: 20–30 minutes
- 100 challenges per user
- Enrollment per session: <15 minutes
- Authentication duration: <1 second

Experimental Setup

- 15 subjects during 1.5 months (approved by IRB of UW-Madison)
- Session length: 20–30 minutes
- 100 challenges per user
- Enrollment per session: <15 minutes
- Authentication duration: <1 second

Other Challenge Response Biometrics



Sluganovic, Ivo, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. "Using reflexive **eye movements** for fast challenge-response authentication." In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1056-1067. 2016.

Lin, Feng, Kun Woo Cho, Chen Song, Wenyao Xu, and Zhanpeng Jin. "Brain password: A secure and truly cancelable **brain biometrics** for smart headwear." In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*, pp. 296-309. 2018.

Chen, Y., Yang, Z., Abbou, R., Lopes, P., Zhao, B.Y. and Zheng, H., 2021, May. User authentication via **electrical muscle stimulation**. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-15).

What is the usability issue here?

Experts' vs Non-experts' view on biometrics

"Pretty Close to a Must-Have:" Balancing Usability Desire and Security Concern in Biometric Adoption

Flynn Wolf
UMBC
flynn.wolf@umbc.edu

Ravi Kuber
UMBC
rkuber@umbc.edu

Adam J. Aviv
United States Naval Academy
aviv@usna.edu

ABSTRACT

We report on a qualitative inquiry among security-expert and non-expert mobile device users about the adoption of biometric authentication using semi-structured interviews (n=38, 19/19 expert/non-expert). Security experts more readily adopted biometrics than non-experts but also harbored greater distrust towards its use for sensitive transactions, feared biometric signature compromise, and in some cases distrusted newer facial recognition methods. Both groups harbored misconceptions, such as misunderstanding of the functional role of biometrics in authentication, and were about equally likely to have stopped using biometrics due to usability. Implications include the need for tailored training for security-informed advocates, better design for device sharing and co-registration, and consideration for usability needs in work environments. Refinement of these features

1 INTRODUCTION

Biometric authentication has the potential to increase the usability of mobile devices. Frequent screen unlocking and application authorization is accomplished with a quick glance or touch rather than recalling and entering long/complex passcodes [19]. Despite the benefits, adoption can be uneven due to usability issues [9, 29] and user misunderstanding or security concern [14].

From a security-conscious perspective, allowing a new technology to record and store a permanent signature of one's self and use it to control access to sensitive data transactions might cause deep concern. Research has documented biometric adoption [2, 25], experts' sophisticated mental models of network security that are distinct from those of everyday users [1, 4, 5, 26, 30, 33], and the influence that usability [12, 15, 16] and similar models of security have

Experts' views

- More influenced by work and BYOD requirements than non-experts
- More likely to have used BAM immediately when available than non-experts
- Change authentication approach more frequently than non-experts
- Device choices more influenced by security concern compared to non-expert

Non-experts' views

- Less concerned than experts about compromise of their biometric signatures
- Less afraid than experts of using biometric unlocking on mobile payment/banking apps
- Less likely than experts to have initially thought consumer biometrics were a good idea

Both's views

- Frequently mistake biometric unlocking as the primary rather than secondary method
- Equally likely to have stopped using biometric unlocking because of usability problems
- Security concern motivated by fear of physical loss/theft
- Similar proportions initially thought consumer biometrics were a bad idea

Questions?

Take-home

- (**Blog**) MIT Technology Review - The hack that could make face recognition think someone else is you
- (**Blog**) Lassak, L., Hildebrandt, A., Golla, M. and Ur, B., 2021. " It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About {FIDO2} Biometric {WebAuthn}. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 91-108).