CS 858 - User Authentication

Recent Trends

Fall 2022

1

Types of User Authentication

- Something you know
- Something you have
- Something you are
- Something about your context

- Traditional "something you know" raises security and usability concerns so it is being replaced/enhanced with some of the other methods

2

2

Overview

- **Websites**
  - **Two-factor Authentication (2FA)**
  - Risk-Based Authentication
  - FIDO2
- Devices
  - Biometric authentication
  - Smart Lock and similar
  - Behavioural authentication

3

3

Two-factor Authentication

- Introduce a second authentication factor that is of a different type than the first one
- Examples:
  - Fob displaying a one-time secret, USB/NFC-connected fob, app-based push confirmation, one-time secret sent in SMS message
- Issues:
  - Usability
    - Often slow to use, time consuming to set up, broken/lost physical second factors
  - Security
    - Knowledge-based second factors can be phished, 2FA fatigue, SMS messages can be rerouted in a social engineering attack

4

4

Overview

- **Websites**
  - Two-factor Authentication (2FA)
  - **Risk-Based Authentication**
  - FIDO2
- Devices
  - Biometric authentication
  - Smart Lock and similar
  - Behavioural authentication

5

5

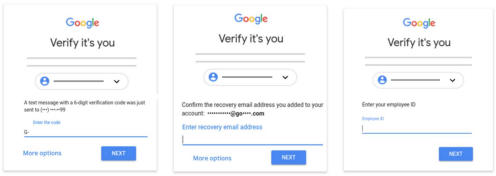
Risk-Based Authentication

- Used widely in addition to password-based authentication
  - Google, Microsoft, Facebook, Amazon, banks, credit card companies,…
- Is the user's current environment different from the user's usual environment, leading to an increase in risk?
- Depending on the risk level: grant access, ask for additional information, or block access (should be rare)
- Additional information can range from solving a CAPTCHA to proof of access to a registered device
- Considered environment factors: Black box, well-kept secret
- Possible or observed examples: IP address, geolocation, time, browser, device

6

6

Login challenges



https://cloud.google.com/blog/products/identity-security/best-practices-for-a-more-secure-login-in-google-cloud

7

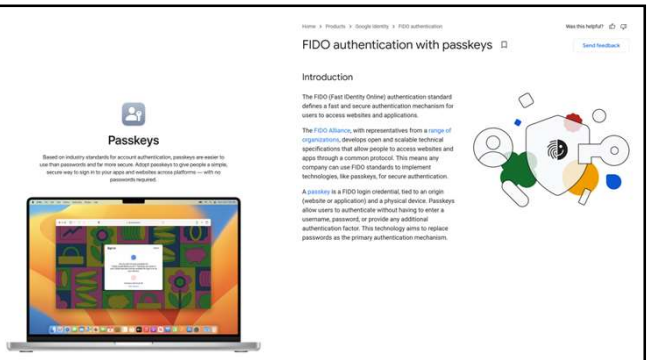
7

Overview

- **Websites**
  - Two-factor Authentication (2FA)
  - Risk-Based Authentication
  - **FIDO2**
- Devices
  - Biometric authentication
  - Smart Lock and similar
  - Behavioural authentication

8

8



9

9

FIDO2 (Fast IDentity Online Alliance)

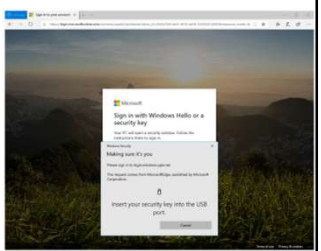
- Replace passwords with a challenge-response protocol
  - Addresses replay attacks and password leaks
- Enrolment: For each website, user creates a public/private key pair and gives public key to the website
- Authentication:
  - Website sends challenge to user
  - User cryptographically signs challenge (and identity of website) with their private key and returns signature to website
  - Website checks authenticity of signature with user's public key
- Inclusion of website identity in signature addresses phishing attacks
- Problem: Users are not good at remembering private keys and doing cryptography in their heads
  - Use trusted hardware

10

10

FIDO2 Terminology

- Relying Party: Website, server
- Client: Browser
- Authenticator: Stores private key using hardware-backed security
  - Roaming Authenticator: external, connects to Client platform with USB, Bluetooth, or NFC
    - Security Key (separate token), Android/iPhone
  - Platform Authenticator: embedded in Client platform
    - TPM (Windows), Secure Element (Android), Secure Enclave (iOS)



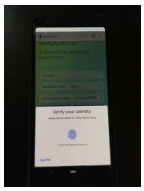
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key

11

11

FIDO2 User Presence/Verification

- User needs to authorize use of private key by Authenticator with User Presence or User Verification, as determined by Relying Party
  - User Presence
    - Show someone is in control of the Authenticator
    - E.g., by pushing a button on a Security Key
  - User Verification
    - Show owner is in control of the Authenticator
    - Requires Security Key with a fingerprint reader
    - Or fingerprint/face/PIN-based authentication for Platform Authenticator



https://www.yubico.com/products/yubikey-bio-series/

12

12

Passkeys

- Key pair is bound to an Authenticator, backup of private key is not possible
- Loss of single Authenticator requires adding a new Authenticator
  - Easy in a company environment, difficult for private users
- Passkeys are extractable private keys that can roam across user's devices using syncing mechanism provided by a platform
  - Roaming across vendor platforms will likely be supported by third-party password managers
- Passkeys are being pushed by Google and Apple as the ultimate password replacement

13

13

Typical Login Experience with Passkeys

- Easy if device is already known to website
  - I.e., website has your public and key, and device is in the set of devices across which your private key is synced
  - Simply authenticate to the device with your fingerprint or face
- What if you log in from an unknown device?
  - Website displays a QR code
  - Scan QR code with your phone
    - Phone becomes authenticator for the new device
  - Authenticate to your phone with your fingerprint or face
  - Optionally: have website remember device for future logins

14

14

FIDO2 Discussion

- FIDO2 is being integrated in all popular OSs and browsers
- Make sure to set up multiple Authenticators for a Relying Party to deal with theft/loss/destruction of an Authenticator
- Authenticator can also be used as a second device in U2F-based 2FA
- Ensure that recovery method is not weaker than FIDO2 method
- User studies have shown that users are (wrongly) concerned about fingerprint/face being submitted to Relying Party
- Optional attestation allows Relying Party to specify trusted authenticators
- See https://webauthn.io/ for setting up a demo account

15

15

Overview

- Websites
  - Two-factor Authentication (2FA)
  - Risk-Based Authentication
  - FIDO2
- **Devices**
  - **Biometric authentication**
  - Smart Lock and similar
  - Behavioural authentication

16

16

Biometric Authentication

- Face and fingerprint authentication is now widely used for device authentication both on computers and smartphones
- Voice authentication is starting to be used by voice assistants, call centers, and e-banking apps
- Iris authentication and similar for specialized, high-security environments
- Usually authentication occurs upon login (or upon a sensitive transaction), not continuously (yet)

17

17

Overview

- Websites
  - Two-factor Authentication (2FA)
  - Risk-Based Authentication
  - FIDO2
- **Devices**
  - Biometric authentication
  - **Smart Lock and similar**
  - Behavioural authentication

18

18

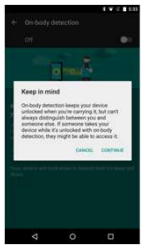
Android's Smart Lock

- "On-body detection" – keeps device unlocked while it is in motion
- "Trusted places" – keeps device unlocked at or close to a pre-configured location
- "Trusted devices" – keeps device unlocked while connected over Bluetooth to a pre-configured device

- Originally Smart Lock also provided automatic device unlocking but now it is strictly a mechanism that prevents device locking
  - Likely because the conditions above are relatively easy to fool

19

19



https://www.androidcentral.com/body-detection-explained

20

20

iOS' Unlock with Apple Watch

- Automatic iPhone unlocking if
  - Face ID recognizes a face mask,
  - there's a secure connection to the owner's Apple Watch,
  - Apple Watch is passcode protected and currently unlocked
  - Apple Watch is nearby and on user's wrist

21

21

Windows Hello's Trusted Signals

- Trusted signals can serve as a secondary authentication factor
- Supported trusted signals:
  - Nearby Bluetooth device
  - Current network configuration
  - Current WiFi network

22

22

Overview

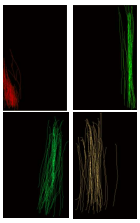
- Websites
  - Two-factor Authentication (2FA)
  - Risk-Based Authentication
  - FIDO2
- **Devices**
  - Biometric authentication
  - Smart Lock and similar
  - **Behavioural authentication**

23

23

Behavioural Authentication (BA)

- Different users use their smartphone in different ways
- BA continuously authenticates smartphone users by transparently monitoring their behaviour
- Explicit authentication (passcode, pattern) if observed behaviour is different from usual behaviour

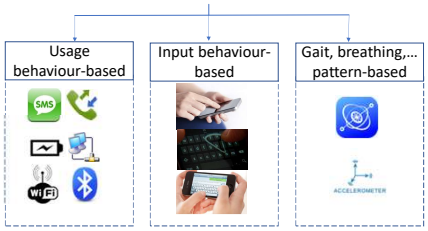


Swiping behaviour of four users [Frank et al., 2013]

24

24

Proposed BA Schemes



25

25

Behavioural Authentication (BA)

- Many BA schemes have been proposed
- Underlying research usually shows that a proposed scheme has good accuracy
  - Legitimate user is recognized as such, illegitimate users are rejected
- But what do users think about behavioural authentication?
- Can users' behaviour be mimicked?

26

26

Usability and Security Perceptions of BA

- False rejects – Legitimate user is classified as an intruder
  - Current task is interrupted and user is explicitly authenticated to establish identity

  } Usability issue due to interrupt-authenticate
- False accepts – Intruder is classified as a legitimate user
- Detection delay – Classification score is not readily available

} Security concern

27

27

Lab Experiment – Non-BA Session

Optional and based on users' real-life security preferences

28

28

Lab Experiment – BA Session

Interrupted to authenticate with a 20% false reject rate

29

29

Field Study

- Simulated false rejects during daily smartphone use

30

30

Usability: Task Performance

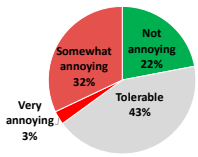
- Authentication overhead
  - Interrupted tasks in BA took 8-20 seconds longer
- Overall task completion time for BA session
  - 7% decrease for people who currently use explicit authentication
  - 9% increase for people who currently use no authentication
- Task error rate
  - No statistically significant differences across
    - interrupted and uninterrupted tasks
    - BA and non-BA session

31

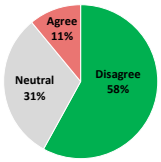
31

Usability: Annoyance due to Interruptions

How annoying were the interruptions for authentication?



Agree with: 'BA is annoying'?



32

32

Overall Usability of BA

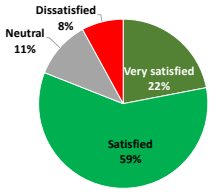
- No statistically significant difference between overall system usability scores of BA and explicit authentication
- For individual questions when compared to explicit authentication:
  - Would like to use BA frequently
  - BA easier to use
  - BA more inconsistent
  - Need to learn more

33

33

Perceptions of BA Security

How satisfied with the level of protection provided?



34

34

Perceptions of BA Security

- False accepts a concern for 8/37
  "No one can use it without entering the PIN but here someone 'can' use it"
- Detection delay a concern for 10/37
  "… you can see the screen right away before it can lock you out and that will make it a little unsettling for me"
- Feasibility of mimicry attacks a concern for 4/37
  "… that is my impression of it is that if someone watches you for a longer time then he might be able to bypass it"

35

35

Willingness to Adopt BA

Willingness to adopt and top reasons for particular responses

Yes, as a primary (33%)	Convenient, saves time, better than none
Yes, as a secondary (30%)	Test it more, additional security against insiders
Maybe (30%)	Test/learn more about it
No (7%)	Unacceptable detection delay, EA suits better, nothing to protect

36

36

Other Concerns

- BA as a background service raised concerns

"So looking at.. I see there is no lock. Sometimes I felt... the lock exists or not? When PIN is used, I know [it] every time. Now there is no way to discriminate if someone has hacked my phone and removed the lock. PIN is a secure feeling that the phone is safe"

- Interrupts serve a purpose beyond authentication

"Yeah the interruptions are annoying and I guess then I have to say to myself, practically it is not good but as soon as I see it, I know that it is protecting me"

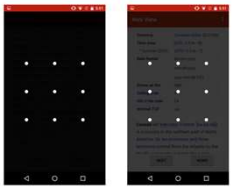
Should security be unobtrusive?

37

37

Re-authentication Strategies

- BA (maybe erroneously) decides that current user is an intruder and needs to be re-authenticated
- Should user be locked out immediately?
- Should user be allowed to finish current task?
- How should dialog box for entering passcode/pattern look like?



38

38

Mimicry Attacks on Behavioural Authentication

- Many BA schemes have been shown to have good accuracy
- Accuracy evaluation usually shows that natural behaviours of different users are different enough
- What if adversary observes victim and tries to mimic their behaviour?

39

39

Getting to know you: a more personal approach to user ID on smartphones

CTV NEWS

Those in the tech community of a more neurotic disposition have already suggested that thieves may be tempted to amputate a person's finger in order to steal their phone if fingerprint scanners catch on, but in order to dupe SilentSense the criminal in question would have to be a method actor of a caliber greater than Brando, Hoffman or triple Oscar winner, Daniel Day Lewis, and when someone is that great a mimic, there are much easier and better ways of making money than by taking other people's property.

40

40

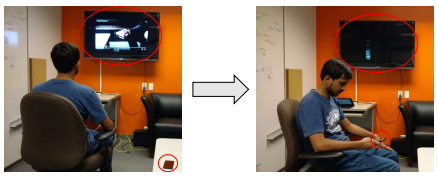
Mimicry Attacks on Touch Input BA

- Simulated shoulder-surfing attacks
- Recorded video of victims swiping on screen
- Attackers watched recordings, maybe multiple times, and tried to mimic victim's swiping pattern

41

41

Shoulder-Surfing Attacks on Touch Input BA



Success rate of 86% after less than two minutes observation time

42

42

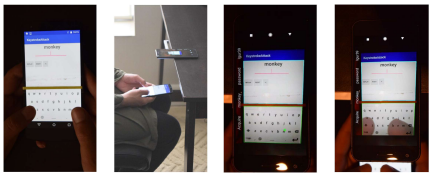
Mimicry Attacks on Keystroke BA

- Attackers used a training app to train themselves to type like their victim
- In addition, attackers used an Augmented Reality app for real-time guidance during attack

43

43

Augmented-Reality Attacks on Keystroke BA



Victim's device | Device placement | Attacker's View I | Attacker's View II

97% of successful training sessions result in successful attacks

44

44

Aside: Smartphone Shoulder Surfing

[Source: 3M]

45

45

How effective are shoulder-surfing defences?

- Widely used: Tilt device screen away
- Suggested by researchers: Apply more pressure to some digits

46

46

Findings

- Tilting provides limited protection
  - Only angles greater than 70° led to guessing
- Applying pressure to some digits provides no protection
  - Due to timing side channel
- Shoulder surfing attacks from distance are effective

47

47

Overview

- Websites
  - Two-factor Authentication (2FA)
  - Risk-Based Authentication
  - FIDO2
- Devices
  - Biometric Authentication
  - Smart Lock and similar
  - Behavioural authentication
- Note that in practice the boundaries are not as strict
  - Biometrics can be used by authenticator in FIDO2 while authenticating to a website
  - Some security startups provide behavioural authentication for websites and apps

48

48