RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: IDY-T10

PASSWORDS AND FINGERPRINTS AND FACES—OH MY! COMPARING OLD AND NEW AUTHENTICATION

Jackson Shaw

Sr. Director
One Identity, LLC

@RSA on Tuesday, February 24, 2004

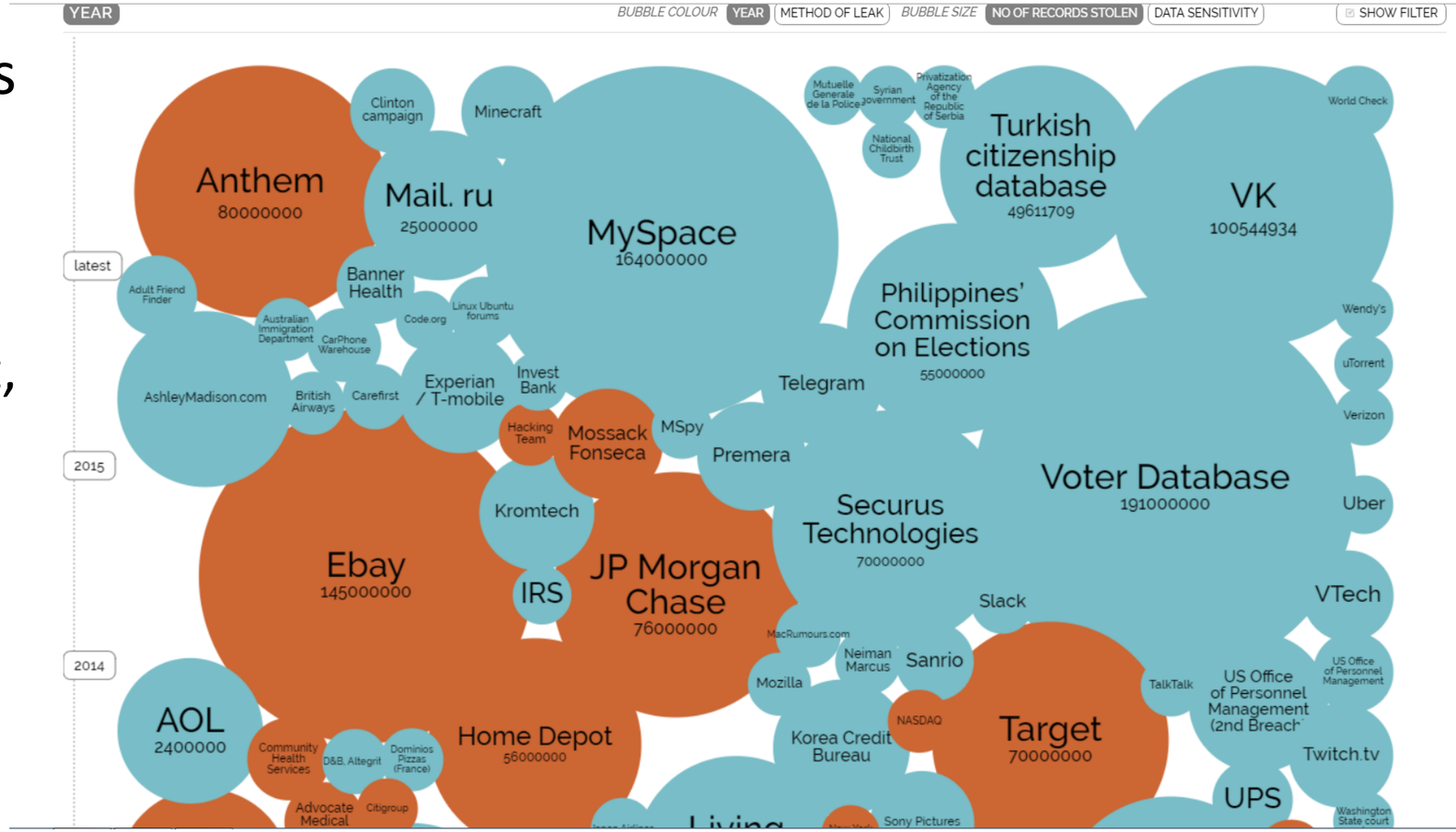
"There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure."

In the meantime…

- The average person has 27 discrete online logins
- 20-50% of all helpdesk calls are for password resets and cost ~$25 each
- There's a whole cottage (>$7B) industry around:
  - Self-service password reset
  - Stronger authentication
  - Government ID systems
- **COSTS** continues to rise.

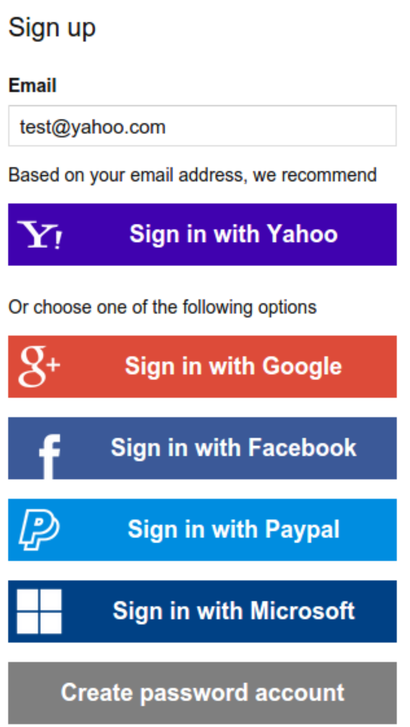
In the meantime…

- 63% of all breaches involve weak, default or stolen pswds
- Hackers have become more sophisticated
- COTS, OSS, military, government, banking, healthcare, insurance, mom and pop, and even our election systems are being targeted and are not safe
- **RISK** continues to rise



In the meantime…

- Industry & technology have rallied to “help”:
  - Password “wallets”
  - OTP & SMS Tokens
  - Federation & single sign-on
  - QR codes
  - Everyone – and their dog – are creating software tokens



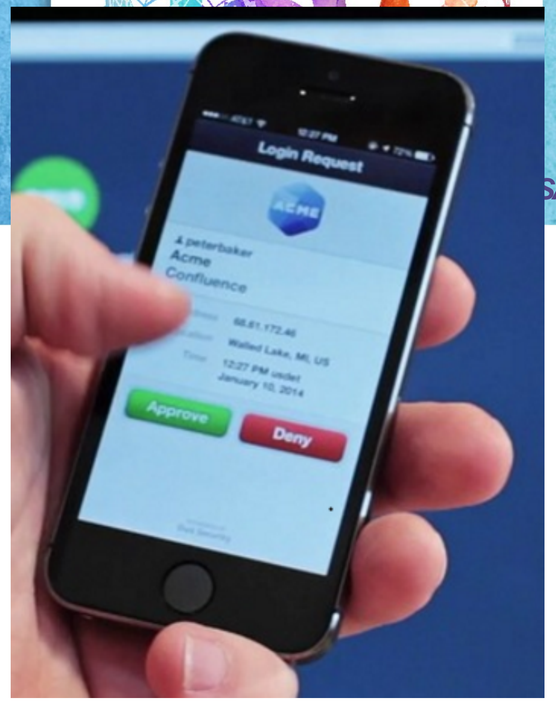
- **USABILITY** is not getting better!

In the meantime…

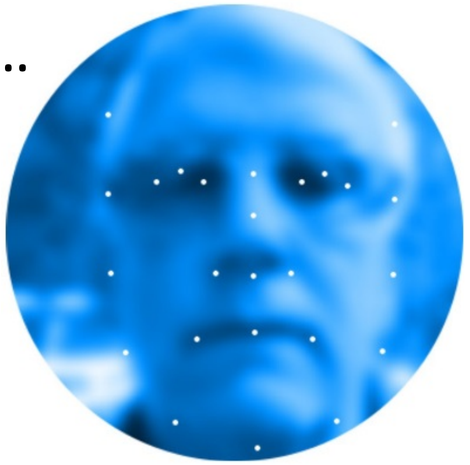
- The Dark Web is the place to find compromised credentials
- You can easily check a password or an e-mail address to see if it has been compromised
- Web sites and password reset products are starting to check these databases to prevent compromised passwords from being used
- How long before the set of compromised e-mails and credentials significantly overlaps what hasn't already been compromised?

https://haveibeenpwned.com/

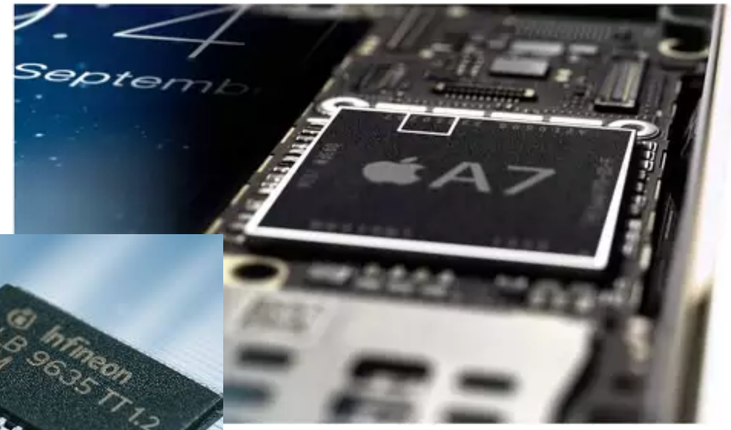
Today



- I believe we are getting close to a tipping point, or at least a series of tipping points around h/w…
  - Biometrics are becoming more acceptable
    - Apple iPhone (and Samsung, shortly)
    - Windows Hello

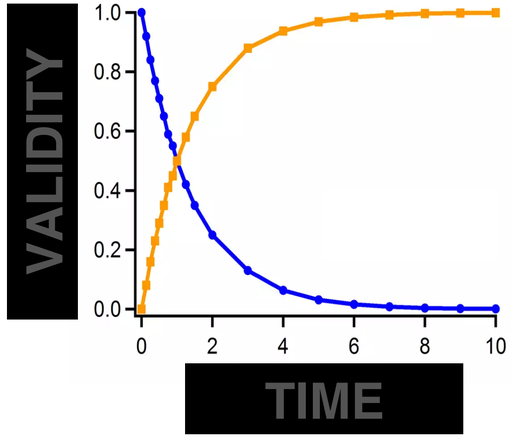


- Securing account information is becoming easier…
    - Apple's "Secure Enclave"
    - FIDO
    - TPM chips & cloud-based h/w security modules



Today

- …and around s/w:
  - Concerns about cloud security continue to decrease
  - Cloud-based solutions enable “patch and done” security
  - Rise of solutions like:
    - Azure Identity Protection and user behavioral analysis & risk-based authentication continue to evolve
    - Risk-based access: temporal, location, conditional
  - Passwords are starting to have a “half-life”
    - The days of the use of passwords, as a sole authenticator, are limited
    - There’s a huge UX issue with shorter half-lifes – who wants to change passwords more frequently? Or make them more complex?



Password SWOT

Strengths
- Well understood
- Legacy

Weaknesses
- Infinite ways passwords have been implemented
- Policy differences between systems
- Sticky note syndrome
- Threat vectors related to storage

Opportunities
- FIDO 2.0
- Integration of SMS/OTP and Push-to-Approve (P2A) and Push-to-Confirm (P2C)
- Integration with dark-web compromised accounts and credentials (and enforcement)

Threats
- Biometrics (good ☺)
- The long tail of any replacement
- Usability (always trumps security)
- The Dark Web

Fingerprints as an authenticator

- Have been used as an authenticator for many years in certain use cases
  - Time keeping
  - Physical access
  - Borders
  - G2C use cases
- Many laptops ship with scanners…

  …that aren't enabled; and,

  …servers don't so there's additional capital acquisition costs

Fingerprint biometric SWOT

Strengths
- Nothing to remember
- Shipping in iPhone & other phone manufacturers
  Off-target secret storage = one less threat vector
- Mathematical representation of biometric
- 1:50,000 probability of a false positive

Weaknesses
- May require positive enrollment
- Sensor acquisition & cleanliness
- Gummy bear legacy
- Business/personal “mixed use”
- Requires application integration

Opportunities
- Wrapping applications around the biometric unlock
- FIDO 2.0
- Integration of SMS/OTP or out-of-band tokens
- Use of push-to-Approve (P2A) &
  Push-to-Confirm (P2C)
- Biometrics combined with analytics

Threats
- Privacy misunderstanding
- The government aka “them”
- Usability (always trumps security)

Facial biometrics as an authenticator

- The iPhone X is a catalyst – “Attentive face”
  - TrueDepth camera projects 30K dots
  - Depth map and 2D infrared image
  - Randomized 2D images and maps
  - API for Face ID; passcode & keychain

Facial biometric SWOT

Strengths
- Nothing to remember + non-repudiable
- Shipping in iPhone X; other phone manufacturers
- The iPhone X “learns”
  Off-target secret storage = one less threat vector
- 1:1,000,000 probability of a false positive

Weaknesses
- “Specialist” cameras remain a barrier to adoption
- May require positive enrollment
- Business/personal “mixed use”
- Limited enterprise usage
- Requires application integration

Opportunities
- FIDO 2.0
- Integration of SMS/OTP and Push-to-Approve (P2A) and Push-to-Confirm (P2C)
- Biometrics & analytics

Threats
- Privacy misunderstanding
- The government aka “them”
- Usability (always trumps security)
- 3D printers?

Comparison of Methods

Passcode (4-digit)

- 1:10,000 (1:1 if shared)
- Increased # of digits or complexity yields UX similar to passwords
- Bypass hacks
- Additional security measures should be used (# of failed entries, etc.)

Fingerprint

- 1:50,000
- Sensors are sensitive to sweat, rain, cuts & Band-Aids
- Calibration can be difficult
- Positive enrollment might be required
- Passcode as fallback
- App integration required

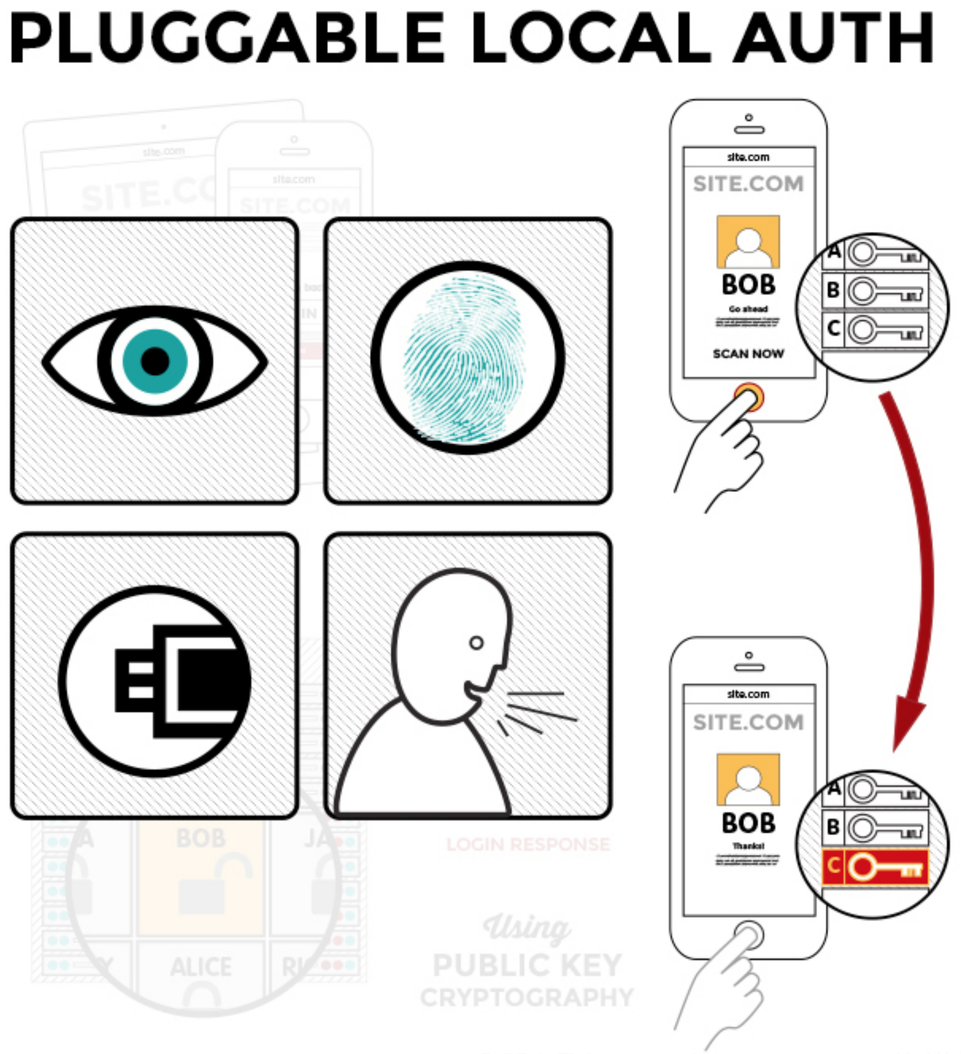
Facial

- 1:1,000,000
- Won't work if eyes closed
- Must adapt to changing facial characteristics or accessories
- Positive enrollment might be required, but less so
- Passcode as fallback
- App integration required

Fast Forward – FIDO

Fast IDentity Online

- Based on well accepted standards
  - Public Key Cryptography
  - Secret keys or biometrics not stored on FIDO server
- Supports password-less and hardware-based tokens
- Resistant to phishing, man-in-the-middle attacks
- Supported by key industry players
  - Aetna, American Express, Bank of America, Dell, Google, ING Bank, Intel, MasterCard, Microsoft, PayPal, USAA, VISA, Wells Fargo



Fast Forward - Blockchain

- Blockchain technology offers a solution to many digital identity issues, where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner
- Some *potential* use cases:
  - Ledger of compromised credentials or devices
  - Single sign-off across federated IDPs
  - Tying an authenticated device to an identity
  - Social media profiles to identities
  - Broadcasting suspicious behavior or compromised credentials
  - Improve trust

BLOCKCHAIN

Final remarks

- Gartner: By the end of 2022, 70% of enterprises will *combine biometric methods with analytics* and either mobile push modes or embedded public-key credentials across multiple use cases, up from almost nil today
- Biometrics are risky to store – you don't want to store them (i.e., on-prem – like the Office of Personnel Management did with 5.6M people)
- Biometric authentication is a paradigm shift but we cannot afford to forget security
- Progressive "thermal-to-face" biometrics recognition
- The password has outlived its usefulness but there will be an associated "long-tail" just like we had (have!) with mainframes

Final remarks

- A whole series of authentication tipping points are at hand
- Software and hardware seem to be similarly aligned – for a change
- I believe these catalysts are going to increase the # of interoperable solutions available to us, reduce costs and increase customer usability
  - FIDO
  - Microsoft Hello
  - Cloud
  - Risk-based authentication for consumers and the enterprise
  - Blockchain
- Don’t underestimate the Apple or Microsoft effect – in both directions
- Delighting your customer: Usability, usability, usability

LATE BREAKING NEWS!!! (Apr 10)

- **FIDO Alliance and W3C Achieve Major Standards Milestone in Global Effort Towards Simpler, Stronger Authentication on the Web**
- **With support from Google Chrome, Microsoft Edge and Mozilla Firefox, FIDO2 Project opens new era of ubiquitous, phishing-resistant, strong authentication to protect web users worldwide**
- WebAuthn defines a standard web API that can be incorporated into browsers and related web platform infrastructure which gives users new methods to securely authenticate on the web, in the browser and across sites and devices.
- It enables an external authenticator, such as a security key or a mobile phone, to communicate strong authentication credentials locally over USB, Bluetooth or NFC to the user's internet access device (PC or mobile phone). The FIDO2 specifications collectively enable users to authenticate easily to online services with desktop or mobile devices with phishing-resistant security.

http://fidoalliance.org/fido-alliance-and-w3c-achieve-major-standards-milestone-in-global-effort-towards-simpler-stronger-authentication-on-the-web

Apply What You Have Learned Today

- When you get home…READ
  - FIDO 2.0 https://fidoalliance.org/
  - Blockchain as it affects identity and authentication. http://buff.ly/2bKR274
  - Apple Face ID Security Guide - https://images.apple.com/business/docs/FaceID_Security_Guide.pdf
- In the next quarter…PROPOSE
  - What critical applications in your enterprise would benefit from P2A/P2C or biometrics?
  - Have a discussion with your team, management or security folks about implementing a use case for trial (e.g., password reset)
  - Ask your vendor(s) what their biometric plans are – are they integrating w/FaceID?
- IMPLEMENT

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: **IDY-T10**

THANK YOU!! QUESTIONS?

Jackson.Shaw@OneIdentity.com **@JacksonShaw**