Authentication Beyond Passwords

Jim Fenton
@jimfenton

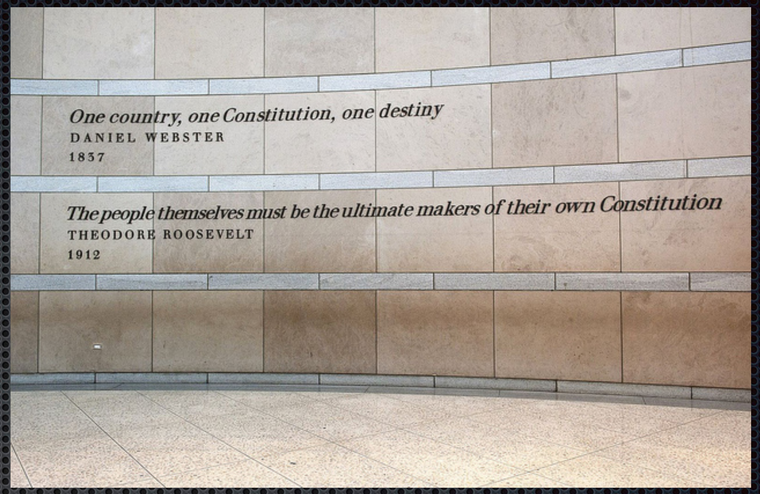
Just a little about me…

- Consultant (2013-present)
  - Authentication standards: NIST SP 800-63-3
  - IETF: REQUIRETLS email security proposal
- CSO at OneID (2011-2013)
  - Authentication startup
- Distinguished Engineer at Cisco (-2011)
  - Various things including DKIM email signatures

Disclaimer

- I’m a consultant for the US National Institute of Standards and Technology
  - Worked on the SP 800-63-3 update
  - Currently working on errata, guidance for US agencies
- Everything here is my own (hopefully informed) opinion
  - I don’t speak for NIST!
- Please contact NIST if you need an official answer

Guiding principles



- Emphasize user experience
  - People cheat when things are not user-friendly
- Have realistic security expectations
  - Many things need 2-factor authentication
- Burden the verifier rather than user wherever possible
- Don’t ask the user to do things that don’t significantly improve security

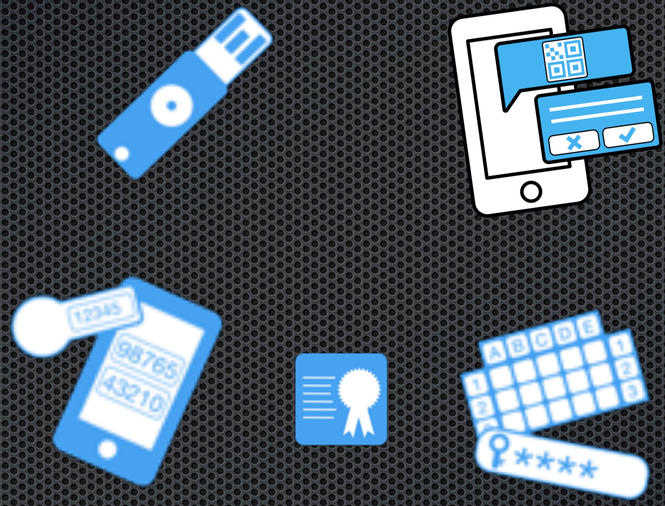
Who are the users?

- Everybody:
  - Non-English speakers
  - Homeless people
  - Disabled veterans
  - Hospital patients
  - Physicians
  - Elderly
  - Students
- Usability needs to consider all of these

Photo by Rob Curran on Unsplash

Authentication factors

Something you know
(password)

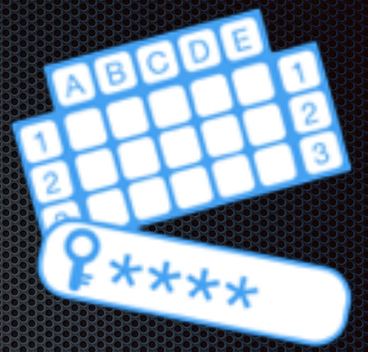


Something you have

Something you are
(biometric)

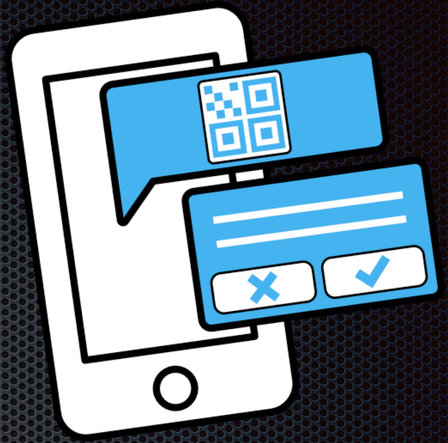
Two-factor means two *different* factors

Look-up secrets



- Take many forms, often wallet cards or sheets of “recovery secrets”
- What you have is the piece of paper, card, etc.
- Advantage: inexpensive, easy to use for very occasional authentications
- Disadvantage: Limited number of authentications possible

Out-of-band authenticators



- Out-of-band communication to confirm possession and control of “something you have”
- Can work in different ways:
  - Authentication secret sent through separate channel to user, entered on primary channel
  - Authentication secret sent on primary channel, sent by user on secondary
  - User compares secrets on primary and secondary channels, confirms on secondary
- Requirements
  - Uniquely addressable, separate from primary authentication channel
  - Use good crypto (secondary channel isn’t necessarily TLS)
  - Authenticate the OOB device securely

SMS as OOB authenticator

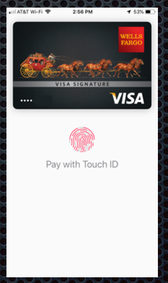
- Plaintext SMS is very popular for OOB authentication, but isn't very good
  - Better than single-factor, but worse than most second factors
  - Easy for attackers to get a target's phone number reassigned to a device they control
  - Need to accommodate users who change their phone numbers or phones
  - Also: SS7 attacks, forwarding, smartphone malware
- Make sure the SMS doesn't go to a VoIP number — wouldn't establish possession of something
- Encrypted SMS (using secret stored in SIM) is OK
- Applies to PSTN voice as well

OTP devices and apps

- Two types: time-based and usage-based
- At least 6 decimal digits of output (~20 bits entropy)
- Use throttling to foil guessing attacks
- Disadvantage: Verifier has to store the user's RNG seed, this could be compromised (RSA Security breach, 2011)

Cryptographic devices and software

- Take many forms:
  - Smart cards
  - USB devices
  - NFC or other wireless connected devices
  - Client certificate (software)
- Always directly connected to endpoint



Cryptographic authenticators

- Implement a challenge-response protocol with the verifier
- Contain a secret, typically an asymmetric private key
- May implement strong man-in-the-middle resistance, discussed later

Biometrics

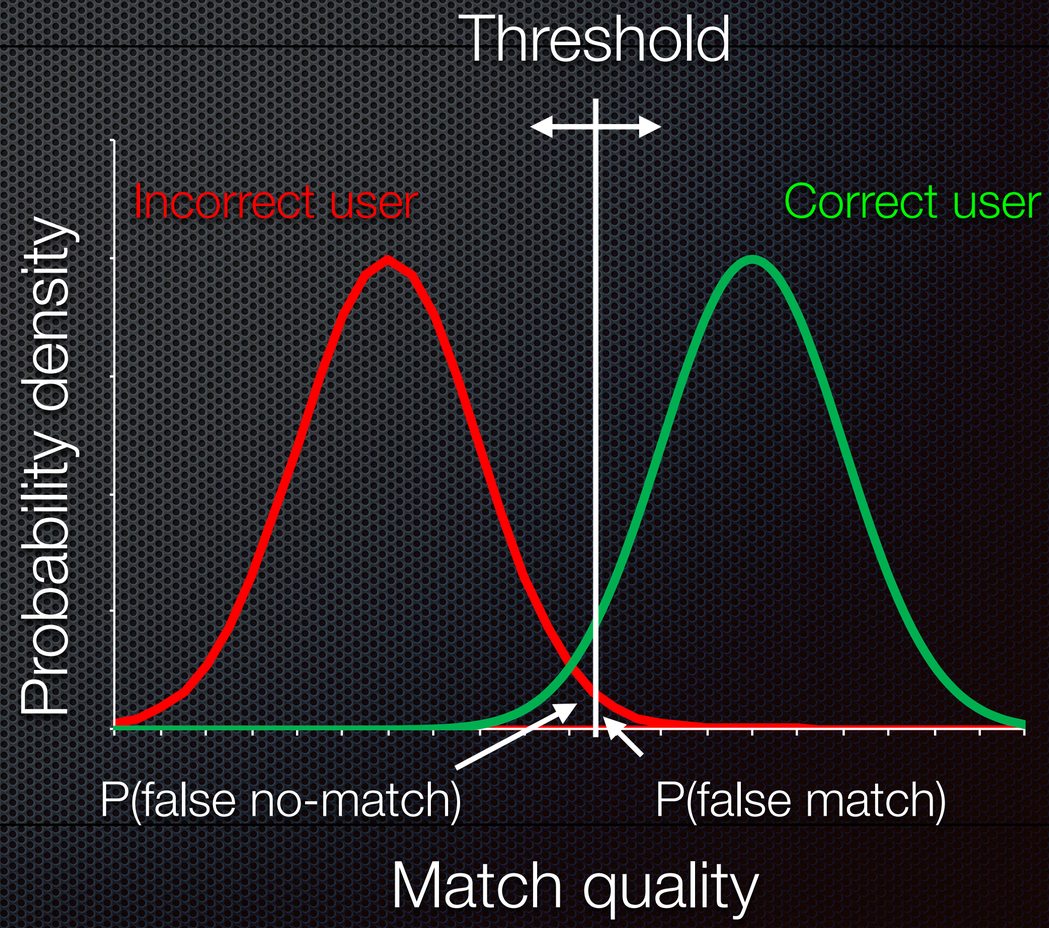
- Not nearly as good as they're often portrayed
  - Zero-effort attacks: typically 1 in 1000 to 1 in 10,000 false accept rate
  - False reject rate too, especially under adverse conditions
- They don't work under all conditions
  - Fingerprint with dirty or wet hands
- You leave biometrics everywhere
- Hard to revoke

Biometric modalities

- Physical
  - Fingerprint
  - Iris pattern, retina
  - Face geometry
  - Voice
- Behavioral
  - Typing cadence
  - Walking gait
- For authentication, performance is the primary consideration

Biometrics and measurement noise

- There is always measurement noise (dust, etc.)
- Threshold represents tradeoff between false match and false no-match
- Want low false match rate, but don't want frustrated users
- Effort by impostor can move red graph to right, increasing P(FM)



Using biometrics effectively

- Bind biometrics tightly to a specific authenticated device
  - Therefore always part of a multifactor authenticator
  - Mitigates revocation problem (revoke the associated device)
- Impose a hard limit (10) consecutive failed attempts
  - Looser limit is OK if Presentation Attack Detection (PAD) used
- Have a backup activation factor, e.g., memorized secret
  - This addresses attempt lockout, poor conditions

Common Considerations

Throttling

- Primary defense mechanism for online attacks
- Example: Limit failed authentication attempts to 100 in 30-day period per account
- Consider using CAPTCHAs, delays, or IP whitelists when approaching the limit
- Consider use of risk-based or adaptive techniques for throttling
- Don’t over-throttle: can result in denial of service for legitimate user

Verifier impersonation resistance

- AKA “Phishing Resistance”, “Strong MITM Resistance”
- Goal: make it impossible for a man-in-the-middle to authenticate their own session
- Do not depend on the user to detect fraud
- Establishes a binding between the authentication and the TLS session it uses
- All VIR authenticators are cryptographic, but
  not all cryptographic authenticators are VIR
- Examples: client-authenticated TLS, FIDO

Attestation

- If a user supplies their own authenticator, how do you know how strong it is?
- Attestation certificates describe the authenticator
- Avoid identifying a specific authenticator, if possible (privacy issue)
- Particularly important when user can access/manipulate information other than their own

Verifier compromise resistance

- Extent to which a compromise of the verifier gives the attacker the ability to authenticate
- Generally determined by the authenticator type
  - Public keys (most cryptographic authenticators) are considered VCR
  - Symmetric keys (OTP verification) not VCR
  - Passwords may or may not be, depending on how stored

Replay resistance

- Extent to which authentication is immune to recording/replay attacks
- Resistant:
  - Challenge/response protocols (with nonces), e.g. crypto authenticators
  - OTP devices, look-up secrets
- Passwords are not replay resistant

Authentication intent

- Goal: block access to directly-connected authenticators by malware
- Approaches:
  - Hardware button (e.g., FIDO)
  - Re-entry of PIN
  - Reconnection of authenticator for each authentication

Two-factor authenticator or two authenticators?

Two-factor authenticator	Two authenticators
Fewer authenticators to manage	Easier to determine strength of BYO authenticators
Less centralized storage of activation secret	Easier to throttle activation secret guesses (at verifier)

Questions?

References

- Apple, Inc. “Face ID Security”, November, 2017. https://www.apple.com/business/site/docs/FaceID_Security_Guide.pdf.
- Grassi, Paul A, James L Fenton, Elaine M Newton, Ray A Perlner, Andrew R Regenscheid, William E Burr, Justin P Richer, et al. 2017. “Digital Identity Guidelines: Authentication and Lifecycle Management.” NIST SP 800-63b. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b.