Age-Based Access: Potential Impacts

Steven M. Bellovin
https://www.cs.columbia.edu/~smb

CS@CU

Biometric Verification

- How old am I? (Just look at me; no fair doing research…)
- Answers from the workshop:

64	1
65	1
70	1
73	1
80	1

Biometric Verification

- How old am I? (Just look at me; no fair doing research!)
  - None of the guesses were right…
- Likely worse for some ages, races, genders

It doesn't work well enough for legal purposes

We need credential-based verification for many purposes

Credential-Based Verification

- Who has the necessary credentials?
- In countries with digitally enabled national ID cards, e.g., Estonia, it's *relatively* easy
- In others, e.g., the US, many people do not have a single, strong ID—or they have more than one (passport (possibly more than one), driver's license, etc.)
  - Getting such IDs can be expensive and logistically difficult, especially for the poor, the elderly (and perhaps the young), the unhoused, those in rural areas, etc.
  - Do such people even have the necessary "breeder documents"?
- Note well: this can affect zero-knowledge protocols, too: how do you authenticate your age to the identity provider?

Cryptographic vs. Credential-Based

- Credentials: easy to move around, easy to steal
  - Vulnerable to sign-up by permitted party on young person's device
- Credential verification at site enrollment time: easy to resell, especially if only one client wants each site
  - Clearly doesn't work for Facebook et al…
- Cryptographic: protects entire session
  - Relatively hard to steal private key from secure storage (TPM chips, T2 chips, Secure Enclave, etc.)
  - Relatively hard to move keys between devices, especially in multi-vendor environments
  - Still vulnerable to bogus signups, but would have to happen on users' devices

Cryptographic authentication is better if key movement is solved

CS @CU

In-House or Third-Party?

- In-house
  - Favors big, entrenched companies
  - Tends to penalize startups
- Third-Party
  - One-stop shopping for attackers
  - Privacy issues—the third party has the documentation and knows what sites you're visiting
  - Who pays? How? Again, favors large companies.

Legal Issues

- How is this enforced across borders?
  - Must ISPs block access to offshore sites that don’t enforce local age limits?
    - (What about sites that share IP addresses?)
- How are third party certification sites regulated across borders?
- What is the liability of such sites for assessing credential authenticity?

Conclusions

- The protocol-level stuff is relatively straightforward, though there are multiple options
- The procedural and economic issues are challenging
- There are also jurisdictional issues

Questions?

Millennium Bridge, London, 9 January 2024

CS@CU