


Sun City Computer Club

Cyber Security Seminar Series

Identity
Credentials
Passwords
Passphrases
Authenticator
Security Keys
AND More

- [Audio Recording of this session](#)
- Use the link above to access MP4 audio recording

identity

 ī-děŋ'tī-tē

noun

1. The condition of being a certain person or thing.
2. The set of characteristics by which a person or thing is definitively recognizable or known.
3. The awareness that an individual or group has of being a distinct, persisting entity.

Identity

- Differentiate you from any/everyone else

IDentity

- Misnomer
- Identity cloning
- <https://www.usa.gov/identity-theft>

Identity Theft

- Definition(s):

Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources.

Credentials

- Cryptography
- Hash

A **cryptographic hash function (CHF)** is a **hash algorithm** (a **map** of an arbitrary binary string to a binary string with fixed size of n bits) that has special properties desirable for a **cryptographic** application:^[1]

- Any length input
- Fixed length output
- One way
- Collision resistant
- Entire Library of Congress - remove 1 letter hash change

Segue

- **Account name**

Unique to function

Our generation reduces future generations options

Reuse?

Encoded *NOT encrypted*

Account name collisions

Clear text – Internet

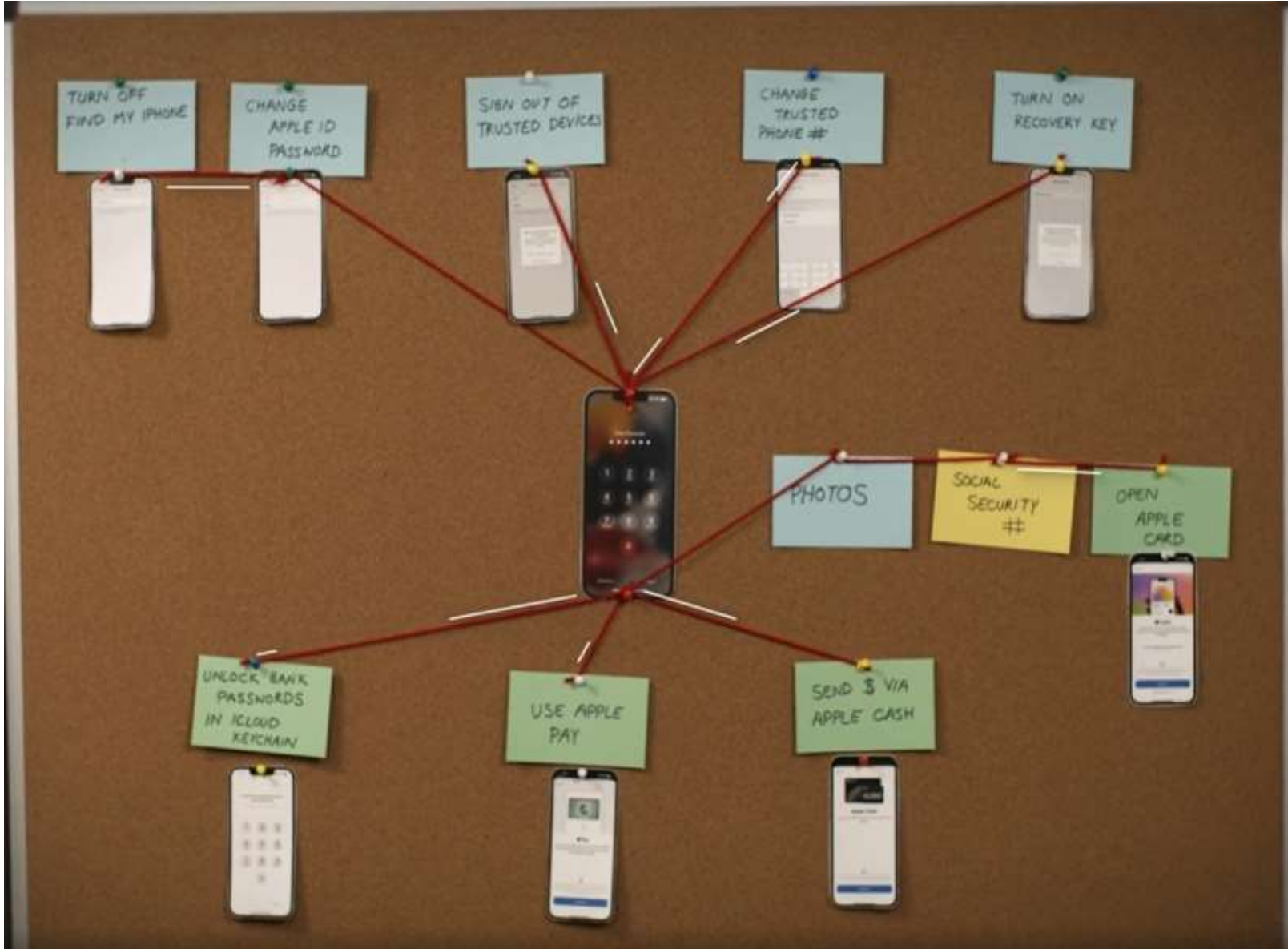
8 billion people many billions of entities

If you can see all of them, all of them ...

Credentials - Digital

- Prove I am me
- With the whole world watching
- In the presence of many determined adversaries
- *Credential stuffing*
- Strong
- Protected
- Guarded who and why are they asking?
- Unique

“That’s me, not anyone else”



- Passcode
- Steal phone passcode obtained prior to theft
- AppleID & iCloud Digital lives Financial lives
- Change AppleID, turn off Find My, access keychain, open photos to find SSN or DL, lock account of associated devices, change recovery key
- Now Apple protections prevent YOU from YOUR digital lives/data
- Apple cash
- SMS unlock code from bank to the stolen phone
- New Titanium Apple Pay card
- “Here, add your contact info to my phone”
- Or, record passcode entry

Smart Device

- STRONGER PASSCODES
- Max number of digits mixed with alphanumeric
- Treat passcode like ATM passcode
- Use increased protections (factors)
- Delete photos/scans with sensitive personal information
- Move to protected storage

General Protections

- Clear text passwords
- Encryption
- Password hash
- Brute force
- Dictionary attack
- Salt
- Rainbow tables
- We have been using passwords for a long time - Treehouses, forts, military guards

Password

- Now we use hundreds of passwords
- Password managers

Browsers

Applications

Local vault

Cloud vault

Insider threat

Vulnerabilities - theirs, others

Passwords

- Keyloggers
- Memory scraping
- Shoulder surfing
- Phishing
- Social Engineering
- Once on Internet, forever on Internet
- Secret -> second entity -> Not Secret
- Unique & Secret Difficult human endeavor
- Forget
- Account password reset
- Password managers – Master password

Passwords

- Backups of customer's password vaults
- Said vaults encrypted by customer's Master Passphrase
- Passphrase -> crypto *key* fixed length
- Rainbow tables -> Multiple iterations
- What is in the customer vaults?
- XML file - decode yield?
- ECB & CBC
- Yeahbut No brute force??

LastPass

- Password managers
 - Generate & store - complex and unique
- At least 4 levels
 - Don't care – I'll never return to this site
 - Some care – but
 - Great care
 - Me and only me
- Length beats strength
- Engrained in memory
- Store **HINT** not passphrase

Passphrases

- Factors

- Something you know - password

- Something you have - smart phone, token, security key,

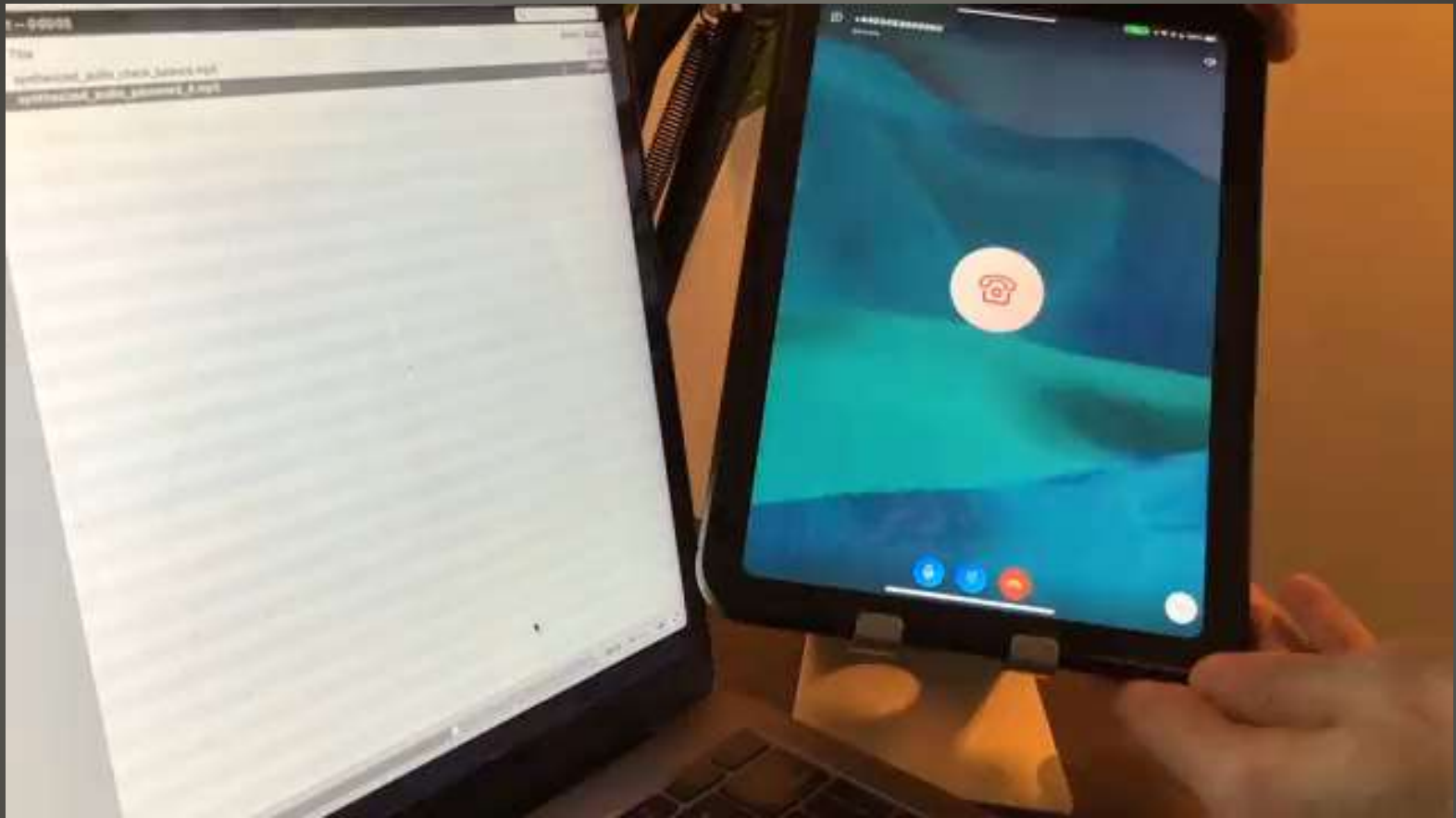
- Something you are - biometrics

- Retinal scan, fingerprint, facial recognition, voice

- Something you can do

- Typing cadence

Multi Factor Authentication



Voice Recognition

Multi Factor Authentication After

- Passwords & passphrases require entering
- Passkeys designed to NOT require entry
- New methods to avoid that entry
- Will require a lot of setup
- You, the provider, the developer, the Internet
- Biometrics, PIN, pattern, ...
- Second factor
- Digital credential
 - User account WEB site and/or application
- You register – new account
- Login with existing method

Passkeys

- Create a passkey request
- UNLOCK *the* device
- Passkey stored on that device
- Each & every passkey is unique to both parties
- Each passkey requires an associated device
- Each platform may synch passkeys
- Once used another passkey is stored on the just used platform
- Biometrics never leave the device
- Passkey managers end-to-end encryption

Passkeys

- Based on public/private key cryptography
- Protection against un-genuine sites/apps

- Requires network
- Not cross platform - yet
- Biometric drawbacks
- How to transfer **AFTER**

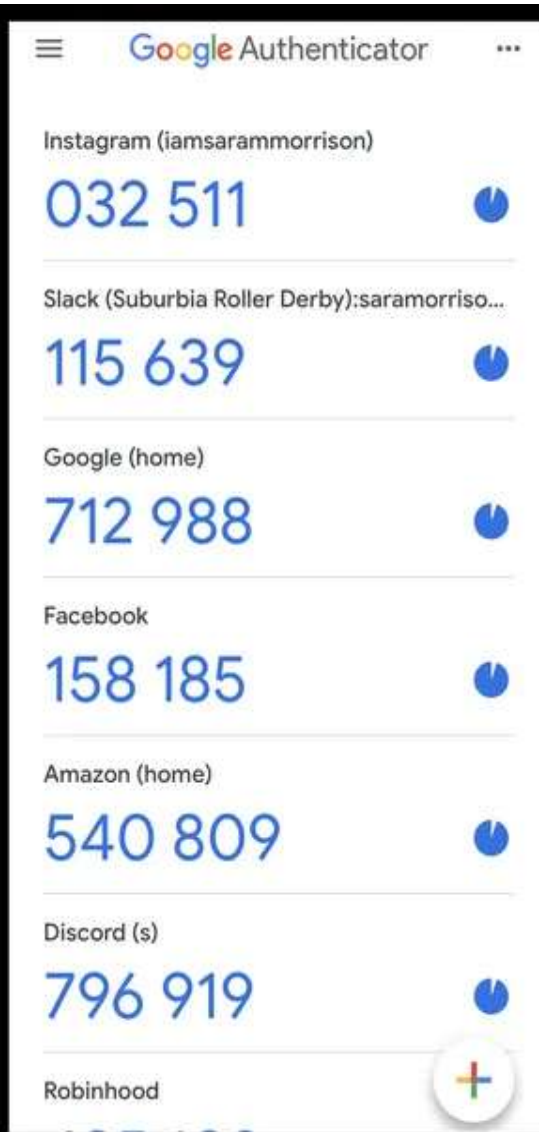
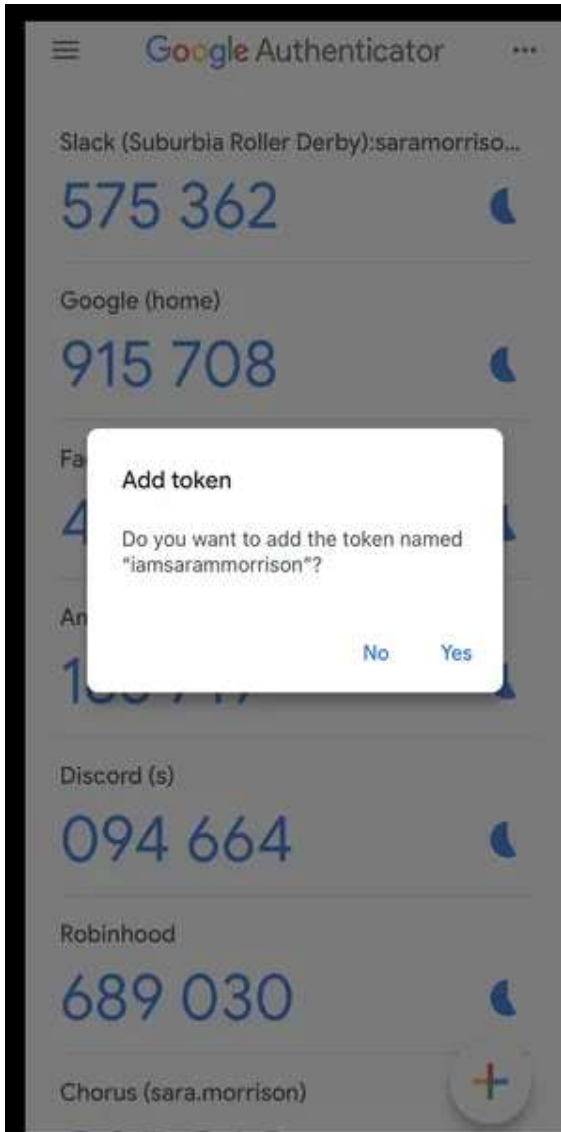
Passkeys

- Most are discoverable if rote
- Better if you provide question and answer
- Better for **After**
- Lie
- Have an Internet life

Security Questions – Two step

- Google
- Microsoft
- 2FAS, Duo Mobile, Twilio Authy
- SIMjacking SMS
- Yet Another App QR codes tokens
- *QR code scanning caution
- Token delivered to authenticator app
- Token changes often

Authenticator Apps



- And then
- Backup codes
- Print this
- Secure this

- To use enter code or approve push notification
- NOT SMS Remove SMS if possible
- New device? Move authenticator app

- Those backup codes – **After** demise

Authenticator Apps

- FIDO standard
- Fast IDentity Online
- Something you have factor
- Can plug in NFC <radio>
- Easier to pass to **After**
- No ability to “lock” the hardware key
- Biometric enabled FIDO keys



Hardware Security Keys

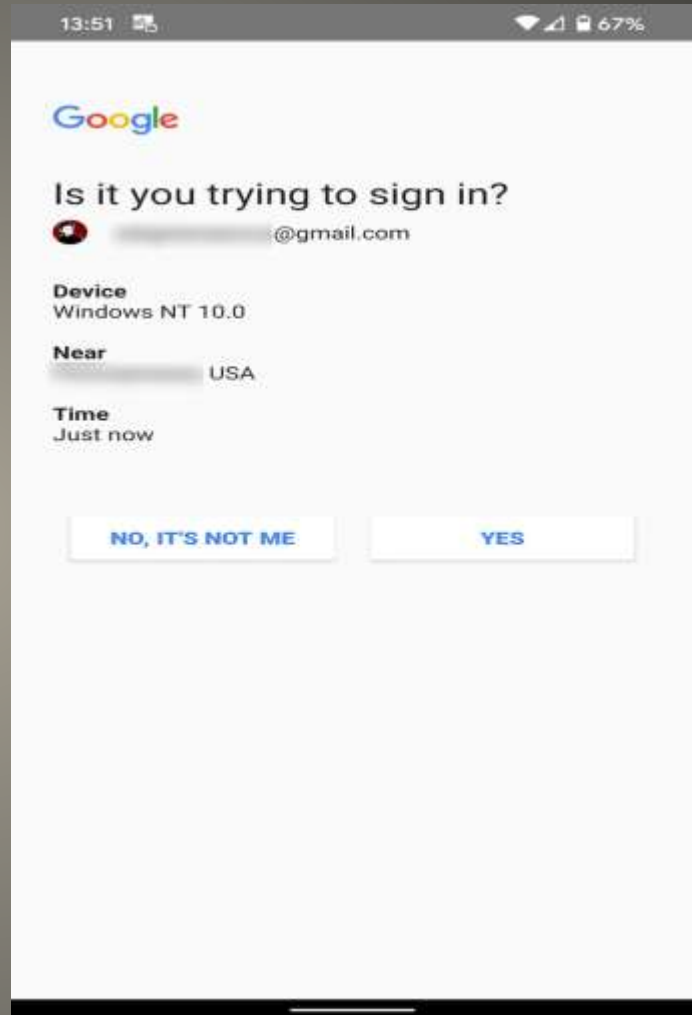
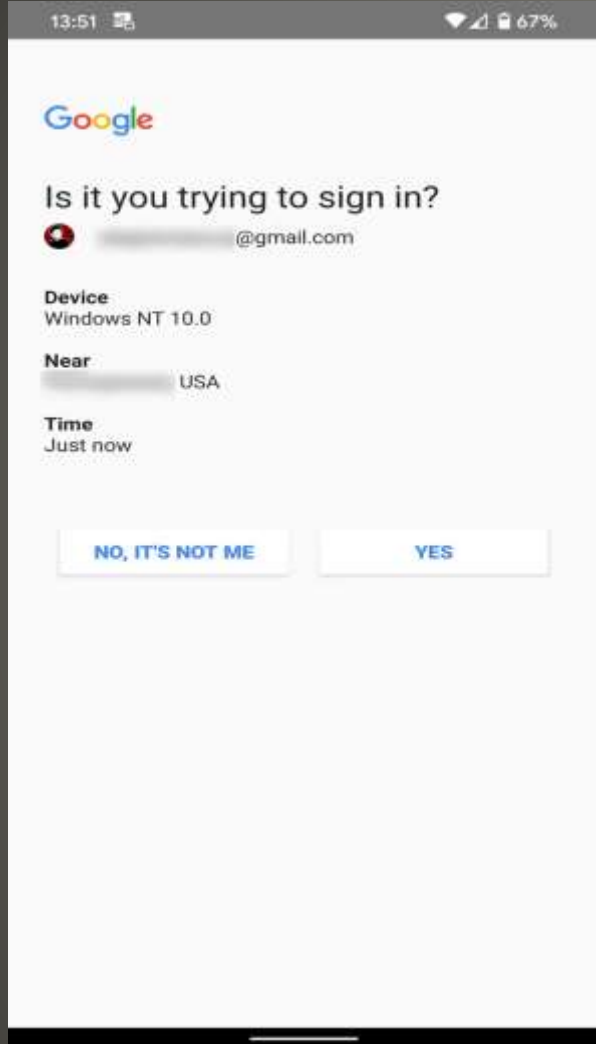
- RSA hack 2011
- Hardware & Software
- On Demand token
- Infrastructure to supply “seed”
- Serial number on device
- PIN
- Duress PIN
- Some attacks



RSA SecureID Token

- Can be swipe, chip, NFC
- Multi purpose in enterprises
- Cloning, theft, borrowing

Smart Cards



Push Notifications

- Check the information

Push Notifications

- Short Message Service
- SIMjacking
- Very few pad message to NOT appear in notification
- Register multiple phone numbers
- You must provide your phone number

SMS

- Fingerprint, voice recognition, facial recognition, and others
- Difficult to hack
- Change is for life
- Difficult for **After**
- More tied to the device

Biometrics

- Public / Private cryptography
- Hash
- Certificate Authority
- Primary use Site asserting its IDentity

Digital Certificate

PIN or Pattern

- Multi < 2 < 1 factor
- Good balance Authenticators
Backup codes
Tracking
- More Security keys
Cost inconvenient
- SMS convenient
- <https://www.cisa.gov/MFA>