Second Factor Authentication (2FA)
Second Factor Authentication (2FA)

- SMS verification
- Time-based One Time Password (TOTP)
- Universal 2\textsuperscript{nd} Factor (U2F)
SMS Messaging

- Service provider texts client a code to enter after username/password stage

- Advantage
  - Simple! Convenient for all users!

- Disadvantage
  - SIM swapping – attacker convinces phone company they are you and purchased a new phone
  - Your phone number goes to their phone now
  - Discouraged in 2017 NIST guidelines
    - [https://pages.nist.gov/800-63-3/](https://pages.nist.gov/800-63-3/)
Time-based One Time Password (TOTP)

How it works
Enabling two-factor

Secret key is randomly generated

QR code is generated from secret key and other info

User scans QR code using Google Authenticator

It starts generating time based codes or tokens

423267
me@brool.com

126184
nuno@test-box1

433406
root@mail01.linuxdrops.com
Time-based One Time Password (TOTP)

https://blog.trezor.io/why-you-should-never-use-google-authenticator-again-e166d09d4324
(Written by vendor of hardware keys...)
Time-based One Time Password (TOTP)

**Strengths**
- Better than only one factor (password)
- Resistant to replay attacks if password is stolen or guessed
- Resistant to attackers stealing your phone number
- Simple / implementable in software apps

**Weaknesses**
- User and service provider share the same secret
- Secret must be accessible in plaintext to combine with time and compute hash
- Service provider hacked?
  - Secret lost
  - Second factor for all users lost
FIDO Alliance

- FIDO Alliance
- Fast IDentity Online (FIDO)
- Industry consortium

- Interoperability for strong authentication devices
FIDO Alliance

Passwordless Experience
FIDO UAF (Universal Authentication Framework)

Second Factor Experience
FIDO U2F (Universal Second Factor)
LOCAL DEVICE AUTHENTICATION
1. Insert Dongle
2. Press Button

ENABLES MANY AUTHENTICATION OPTIONS | EACH SERVICE PROVIDER HAS ITS OWN UNIQUE SECURITY KEYS
Universal 2\textsuperscript{nd} Factor (U2F)

- Open standard for USB or NFC security devices
- Developed by Google and Yubico
- Multiple vendors of hardware devices

Use cases
- Computer login (Windows, OS X, Linux)
- Second factor login for online services supporting U2F protocol
  - Websites: Google, Dropbox, GitHub, Bitbucket, Facebook, Salesforce
  - Browsers: Chrome, Firefox, Opera
Universal 2\textsuperscript{nd} Factor (U2F)

https://blog.trezor.io/why-you-should-never-use-google-authenticator-again-e166d09d4324  
\textit{(Written by vendor of hardware keys...)}
Universal 2\textsuperscript{nd} Factor (U2F)

User - Browser - Server

- User
- Browser
- Server
- Username and Password
- Challenge
- Generate Challenge
- Verify Login
- Response
- Verify Response
- Alice Presses Button

Alice Presses Button

User

Browser

Server
Universal 2\textsuperscript{nd} Factor (U2F)

- No shared secret – Private key is locked in hardware
- Automated – no typing of one-time codes
- Hardware stores private key which can sign challenge message (random number) from service provider, which validates signing with matching public key
U2F Example: YubiKey

yubico

YubiKey Product Family

YubiKey 4  YubiKey 4 Nano  YubiKey NEO  FIDO U2F Security Key
What if I lose my U2F key?
- You’ve lost your second factor 😞
- Account recovery up to your service provider

Recommendations
- Register two U2F devices with each service provider so you have a backup
- Save backup codes (if any) from provider in secure location
YubiKey 4

- Multiple standards supported
  - Touch to trigger FIDO U2F
  - HMAC-SHA1
  - Smart card (PIV)
  - Yubico OTP
  - Code Signing
  - OpenPGP
  - Challenge-Response
  - OATH (TOTP and HOTP)
  - Secure static password
Google Advanced Protection Program
Targeted Attacks on Public Figures

Revealed: Top Hillary aide John Podesta's opened himself to massive Russian hacking effort by using Gmail instead of secure official server


Nov 3 2017

Targeted attack on public figure
- SIM switch via T-Mobile
- Reset Google password
- Two-factor SMS code goes to attacker
- Change Google password
- Reset Coinbase password – email goes to Gmail
- Profit!

Hacking Coinbase: The Great Bitcoin Bank Robbery


Aug 22 2017
Security v Convenience

Google Advanced Protection Program
- Launched October 2017
- Free *(after buying hardware)*
- Favors security over convenience

2nd factor
- No SMS
- No TOTP / Google Authenticator app
- **Must have** two FIDO/U2F hardware keys

Software
- No non-Google software
- Only Chrome and first-party apps
- No third-party site that authenticates via Google account

Password resets
- No backup codes
- No reset via email / SMS
- Only manual account review - “cooling off” period will take a few days
Google Advanced Protection Program

Target audience

- Campaign staffers preparing for an upcoming election
- Journalists who need to protect the confidentiality of their sources
- People in abusive relationships seeking safety
- Human rights defenders, environment campaigners and civil society activists working on any number of sensitive issues
- High net-worth individuals
- VIPs
- Perhaps politicians and company management using a Google account in a personal capacity