Google Declares War on the Password

Kyle Kodani

Why Passwords Don't Work (HACKING)

- Passwords are old, and haven't aged well

- Many, many accounts with similar passwords

- Hacker needs no physical presence

- What is a "strong" password?
  - Only protects against brute force attack
  - Vulnerable to keyloggers
  - Vulnerable to social engineering/phishing

- The age of Google

Current Countermeasures:
Two-Factor Authentication

YubiKey
By Yubico

- 25$ for one

- Small, fits inside a wallet

- Plugs into a USB port
    - Working on wireless connection

- Compatible with popular operating systems and browsers
    - No need for extra software, change is made server side
    - Working on compatibility with mobile devices
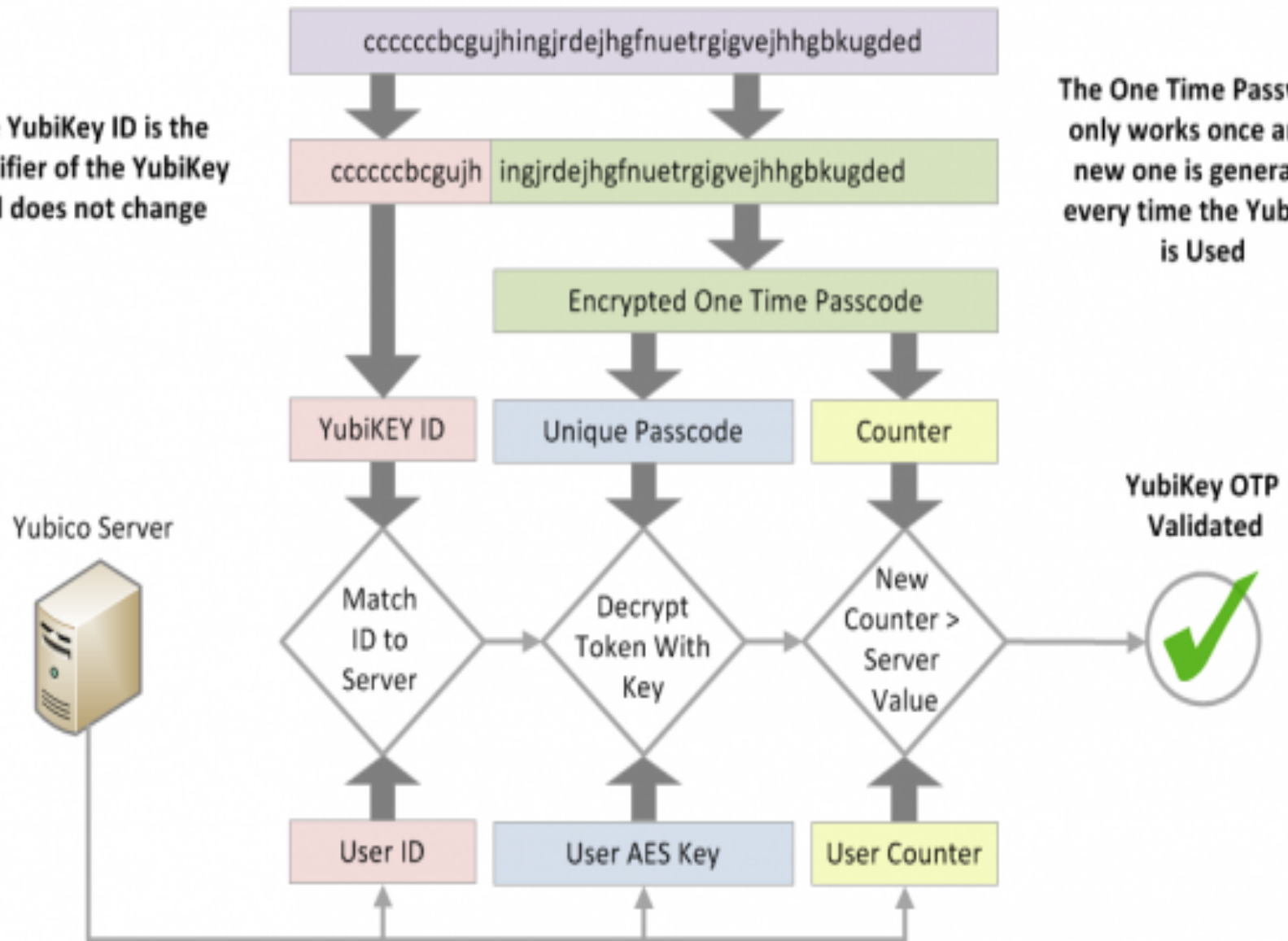
- Durable, no moving part or battery

Biggest problem is losing the key

How it Works

cccccccbcgujhingjrdejhgfnuetrgigvejhhgbkugded

cccccccbcgujh	ingjrdejhgfnuetrgigvejhhgbkugded

Encrypted One Time Passcode

The YubiKey ID is the Identifier of the YubiKey and does not change

The One Time Password only works once and a new one is generated every time the YubiKey is Used

YubiKEY ID	Unique Passcode	Counter

YubiKey OTP Validated

Yubico Server

Match ID to Server	Decrypt Token With Key	New Counter > Server Value

User ID	User AES Key	User Counter

YubiKey in Action

- http://www.youtube.com/watch?v=yyABX0zAYTQ&list=UUX5_RgRVo8KVQ6yQy2lAatQ

Biometrics:
The Way of the Future?
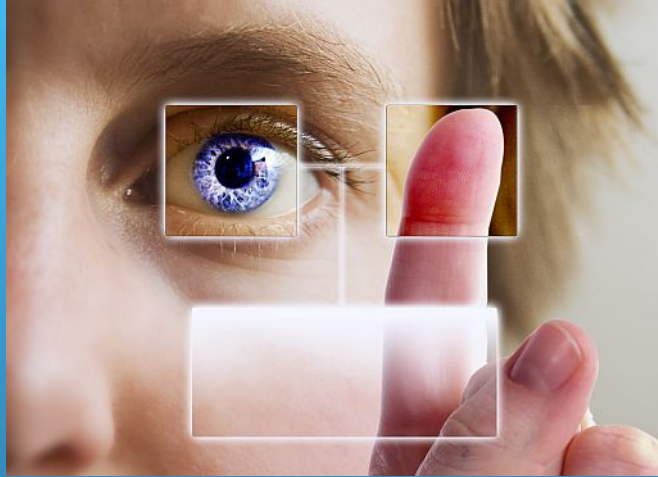
- Retinal scan, face scan, fingerprint, signature, voice, genetics, combination

- Unique, secure

- Requires extra hardware, software, data space

Articles

- http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/all/

- http://www.wired.com/wiredenterprise/2013/01/google-password/all/

- http://en.wikipedia.org/wiki/Password

- http://www.yubico.com/products/yubikey-hardware/yubikey/technical-description/

- http://en.wikipedia.org/wiki/Biometrics