Segurança de Sistemas e dados (MSI 2020/2021)

Aula 3

Rolando Martins

DCC – FCUP

Slides Adaptados do Prof. Manuel Eduardo Correia

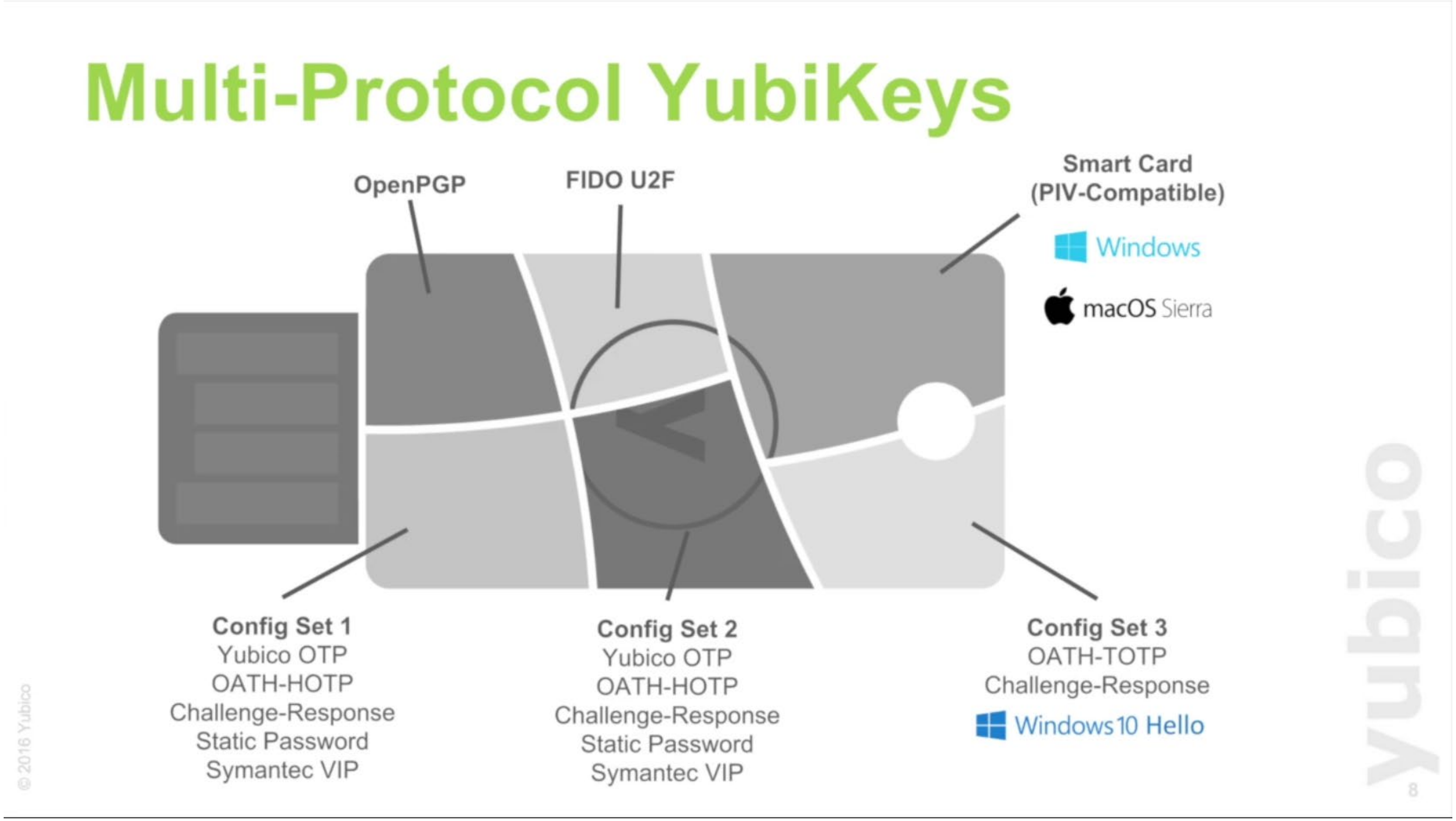
More Flexible Factor Two Authentication tokens

- Yubikeys:
  - Low cost one time password (OTP) generator token (40 chars).
  - Connects to USB port.
  - Acts like a keyboard, no driver required.
  - Press button with your finger to generate a new OTP.
  - Very easy to integrate with legacy login/password authentication schemes.
  - Token validation service on the cloud.
  - Widely deployed by well know Internet companies (Paypal, Google, LastPass,…)
  - Direct support currently being integrated into Google chrome for a more seamless authentication with HTML5 sites.

More Flexible Factor Two Authentication tokens

- Yubikeys:
  - Current Version has two slots. Each can store 128bits.
  - These can be used in several modes:
    - Yubikey OTP
    - OAUTH-HOTP (RFC 4226)
    - Static 128 bit password
    - Challenge Response
  - Newer models are NFC enabled.
    - Yubikey NEO
  - Yubikey software is mostly open Source.
  - For the server side Yubico also supply a low cost HSM to securely protect shared secrets.

Newer Generation YubiKeys



Multi-Protocol YubiKeys

OpenPGP

FIDO U2F

Smart Card
(PIV-Compatible)
Windows
macOS Sierra

Config Set 1
Yubico OTP
OATH-HOTP
Challenge-Response
Static Password
Symantec VIP

Config Set 2
Yubico OTP
OATH-HOTP
Challenge-Response
Static Password
Symantec VIP

Config Set 3
OATH-TOTP
Challenge-Response
Windows 10 Hello

yubico

Other Branded MultiApp USB Tokens

https://www.ftsafe.com/products/FIDO/NFC

FEITIAN
WE BUILD SECURITY

- USB and NFC communications
- FIDO U2F, OATH HOTP
- GIDs (Generic Identity Device Specification) and Windows Hello
- Java smartcard

- Supported in Android, Windows, Linux and MacOs

Ubiquitous Authentication tokens ?

- Classical Authentication tokens are very expensive do deploy on a large scale.
- Are difficult to use by the targeted regular users.
- There is however another popular device that can be used as a factor 2 authentication token and:
  - Nowadays it is as common as House Keys:

The Mobile Phone

Using your Mobile Phone as na Authentication token

- Everyone has a mobile phone.
- Every phone has SMS capabilities.
  - The cell phone authentication infrastructure is reasonably secure.
- We can use a SMS message as a side channel to share a temporary secret that only the possessor of a mobile phone can see.
  - The Online banking industry was one of the first to use SMS messaging as a means to authenticate critical operations.
  - Nowadays it is almost impossible use online banking services without a registered phone.

Using your mobile smart Phone/Apps as an Authentication token

- SMS messaging has a cost.
- It can be substantially expensive if you are abroad.
- It could not work if messaging takes too much time (60 seconds delay).
- It is cumbersome to use.
- It is not safe as it used to be:
  - **Sting Ray Devices:** When operating in active mode, the Stingray device mimics a wireless carrier cell tower in order to force all nearby mobile phones and other cellular data devices to connect to it. (https://en.wikipedia.org/wiki/Stingray_phone_tracker)
  - **Signaling Systems n° 7 (SS7) Vulnerabilities:** dates back to the 1970s - “*89% of subscribers’ SMS can be intercepted; 58% of subscribers can be tracked, and half of all phone calls can be wiretapped*” (https://secure-voice.com/ss7_attacks)
- Nowadays the mobile phone can do much more then just “texting”.
- We can do so much more !

Using your Phone as a secure Authentication token

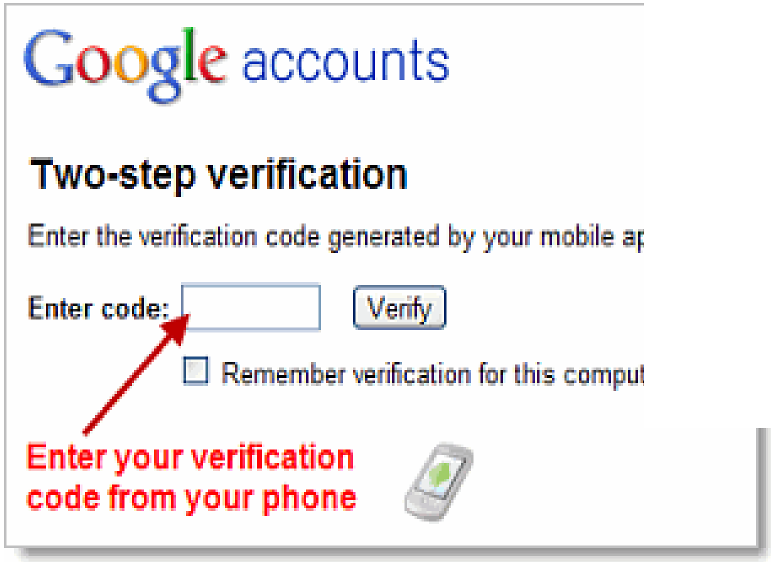
- Smart phones run APPs
- Recent Android phones come with their own Secure Element (SE) Built-in .
  - Google Nexus – Google Wallet; Myfare emulation.
- Near Field Communication (NFC) and card emulation capacity is becoming common place in the more recent Android Devices
  - It is now possible to emulate smart cards at the application level.
  - Combine this with the (SE) and we open a whole new set of potential applications .
    - Physically access (Myfare Locks); Innovative mobile payment systems; Transportation cards; Loyalty cards; etc…
  - All cards in our wallets could all be securely integrated into our NFC enabled smartphone equipped with a SE element.

Using your smart Phone/Apps as an Authentication token

- Google had a serious problem with authentication.
  - Solely based on login/password
  - Highly vulnerable to MITM attacks for credentials harvesting as attested by the chinese incident of 2009/2010 – Operation Aurora (https://en.wikipedia.org/wiki/Operation_Aurora)
- You can secure your google account with an **APP acting as a factor2 authenticator (Google Authenticator)** implementation of one-time passcode generators for several mobile platforms.
  - Support the HMAC-Based One-time Password (HOTP) algorithm specified in RFC 4226
  - Time-based One-time Password (TOTP) algorithm
  - https://github.com/google/google-authenticator

Using your smart Phone/Apps as an Authentication token

- With the Google Authenticator you can declare a certain browser at a certain computer to be trustable.
- All the others will require the proof of possession of your mobile device for the login to succeed.



Google accounts

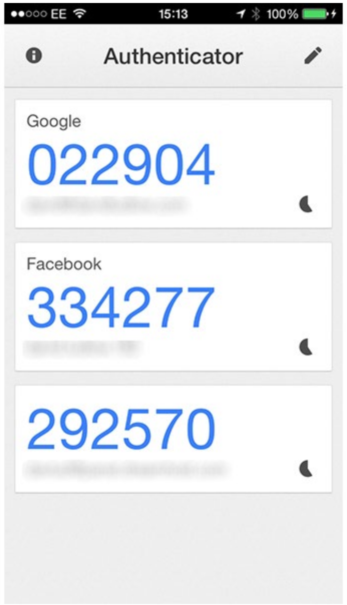
Two-step verification

Enter the verification code generated by your mobile ap

Enter code:

□ Remember verification for this comput

Enter your verification code from your phone



●●○○○ EE 15:13 100%

Authenticator

Google
022904

Facebook
334277

292570

Using your smart Phone/Apps as an Authentication token

- The security of of this scheme is based on wall clock time synchronization and an **initial shared secret** between Google and your phone.
- There is a **secure and practical way to share this secret** and at the same time configure the Google authenticator App.
  - Mobile Tagging
    - **QR codes.**

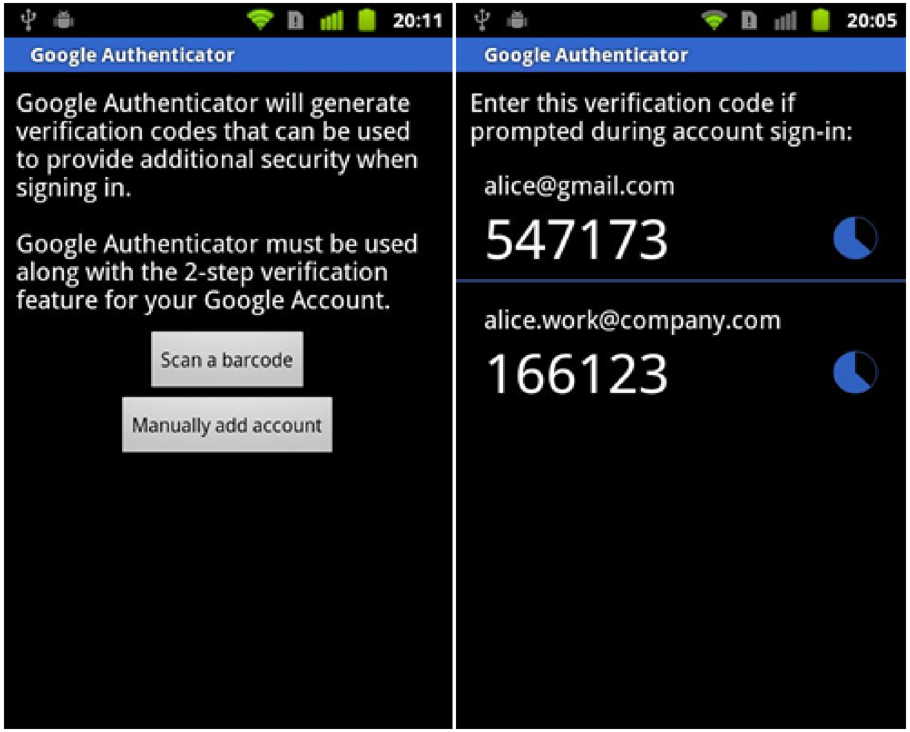
Mobile Tagging constitutes a very convenient mechanism to convey information into a mobile device

- Completely standardized as ISO/IEC 18004:2006
- Plenty of space for secret sharing and configuration purposes.
  - Numeric only Max. 7,089 characters
  - Alphanumeric Max. 4,296 characters
  - Binary (8 bits) Max. 2,953 bytes
- *A QR code is displayed on the screen and is then conveyed to the mobile phone through the mobile phone camera.*

Anda bisa mencoba QR Code di atas ini, bila berhasil maka QR Code ini akan teridentifikasi sebagai alamat website kami (www.otakku.com).

Mobile Tagging is a convenient mechanism to share secrets with a mobile device

- Google Authenticator and QR codes. A very versatile match.



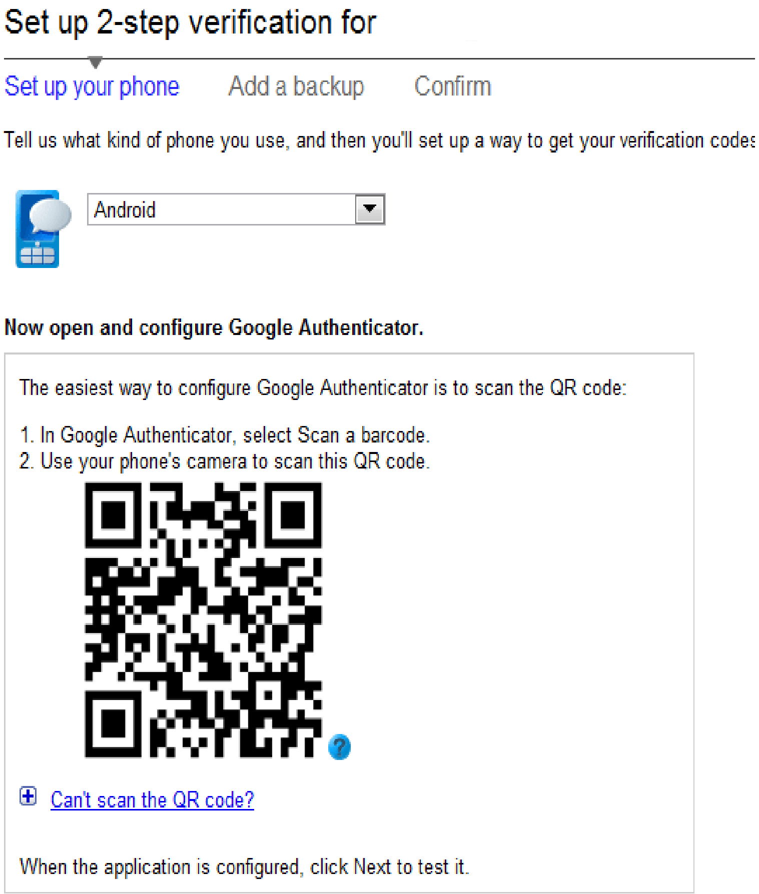
Google Authenticator will generate verification codes that can be used to provide additional security when signing in.

Google Authenticator must be used along with the 2-step verification feature for your Google Account.

Enter this verification code if prompted during account sign-in:

alice@gmail.com
547173

alice.work@company.com
166123



Set up 2-step verification for

Tell us what kind of phone you use, and then you'll set up a way to get your verification codes

Android

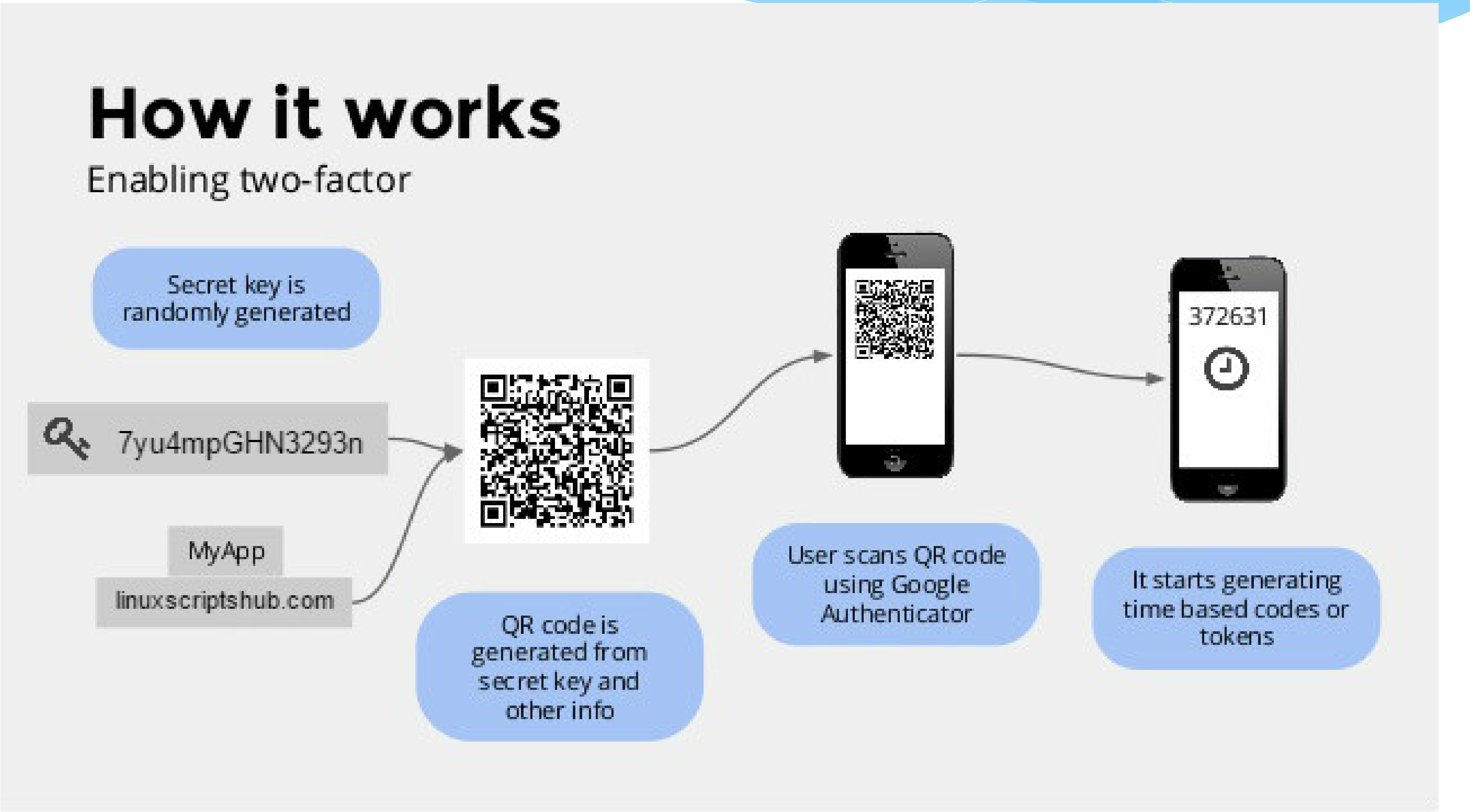
Now open and configure Google Authenticator.

The easiest way to configure Google Authenticator is to scan the QR code:

1. In Google Authenticator, select Scan a barcode.
2. Use your phone's camera to scan this QR code.

When the application is configured, click Next to test it.

Google Authenticator in a Nutshell



How it works

Enabling two-factor

Secret key is randomly generated

QR code is generated from secret key and other info

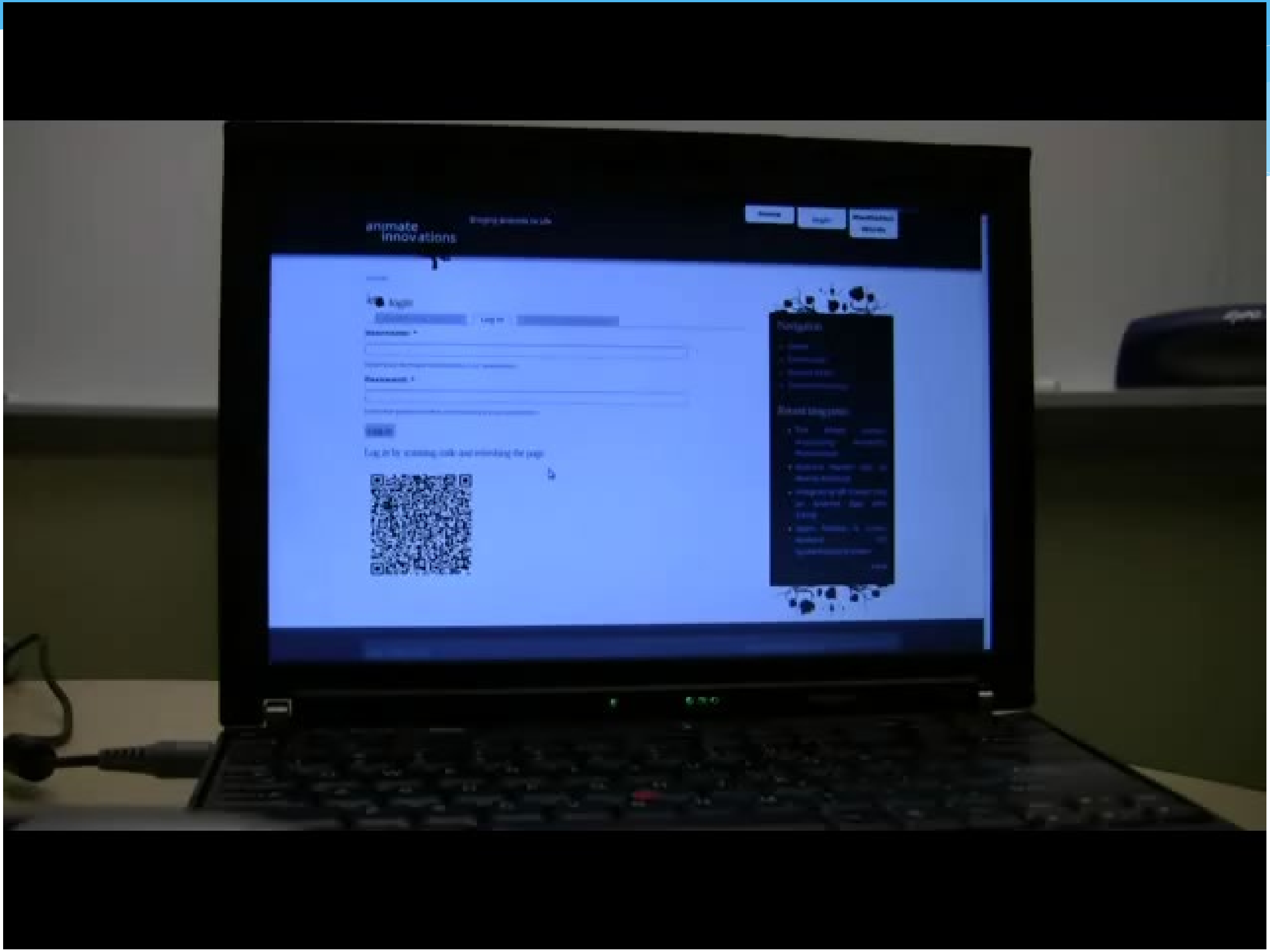
User scans QR code using Google Authenticator

It starts generating time based codes or tokens

Google Authenticator OTP

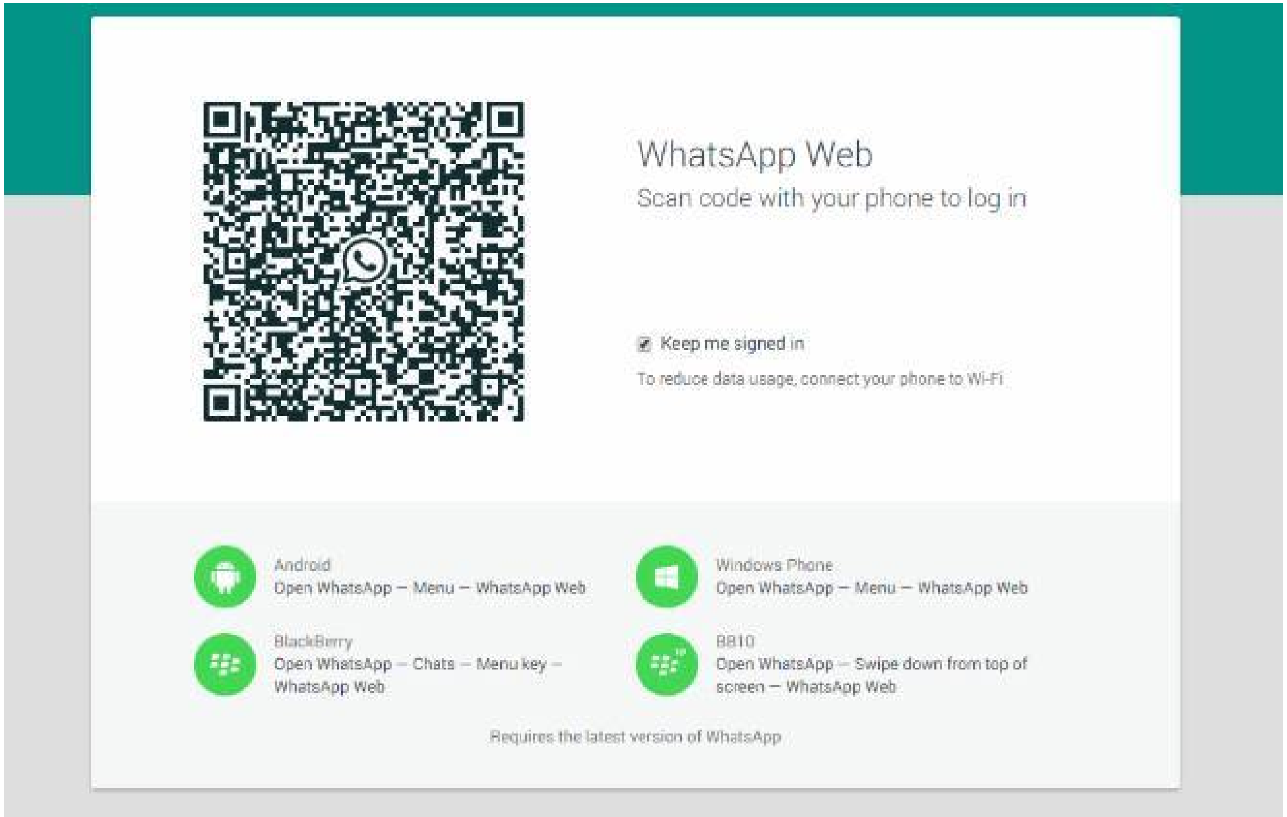
- The google Authenticator, once configured, does not need communication channels to provide the correct answer to the server challenge.
  - *Only correct wall time clock needed.*
- It solves the previously identified problems with SMS based schemes.
- Currently deployed at many high profile sites: *Gmail, Google Apps, DropBox, LastPass, Facebook, etc…*
- *The YubiTOTP Android Widget is able to generate an **OATH Timebased One Time Passcodes (TOTP)** from a secret stored in a YubiKey NEO (NFC enabled).*
- *What else can we do with this to improve security ?*
  - Mobile smart phones have Internet connectivity.

QR-Login/Authentication using an Internet Connected Mobile Phone



WhatsApp uses this idea to associate your smartphone to its web backend

https://web.whatsapp.com/



WhatsApp Web

Scan code with your phone to log in

☑ Keep me signed in

To reduce data usage, connect your phone to Wi-Fi

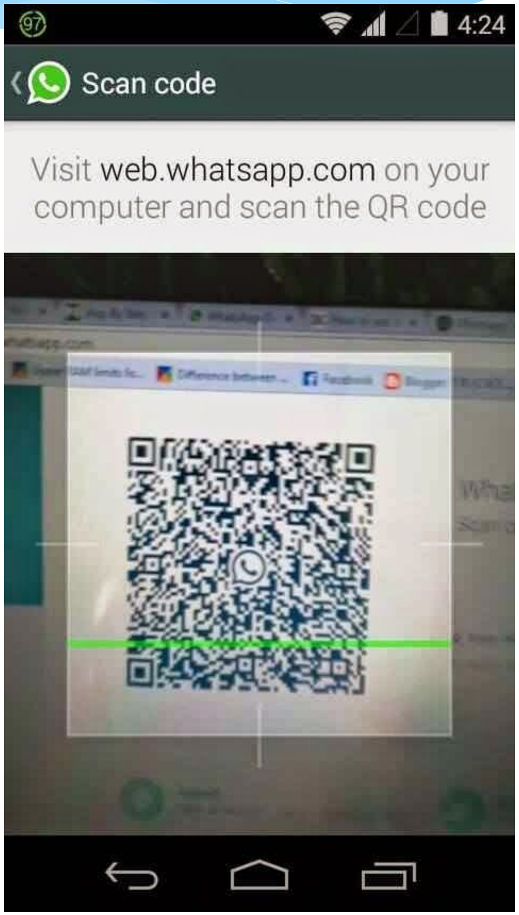
Android
Open WhatsApp – Menu – WhatsApp Web

Windows Phone
Open WhatsApp – Menu – WhatsApp Web

BlackBerry
Open WhatsApp – Chats – Menu key – WhatsApp Web

BB10
Open WhatsApp – Swipe down from top of screen – WhatsApp Web

Requires the latest version of WhatsApp



Scan code

Visit web.whatsapp.com on your computer and scan the QR code

QR-Login main advantages

- With QR-codes the login process is quicker and more convenient than typing a username and password.
- Since the shared secret (the password) does not have to be memorized, or even typed in by a human, it can be long and complex.
- A virus-installed keylogger or shoulder-surfer cannot capture the password.
- The user can securely use an untrusted computer (such as one in an Internet cafe or hotel) without revealing their password.
- A phishing web site cannot capture the user password by tricking them into typing it in. The phone sends the shared secret, and will only send it to the web site in its database.
- By using different logins the user's account on one web site cannot be associated with the user's account on another web site.

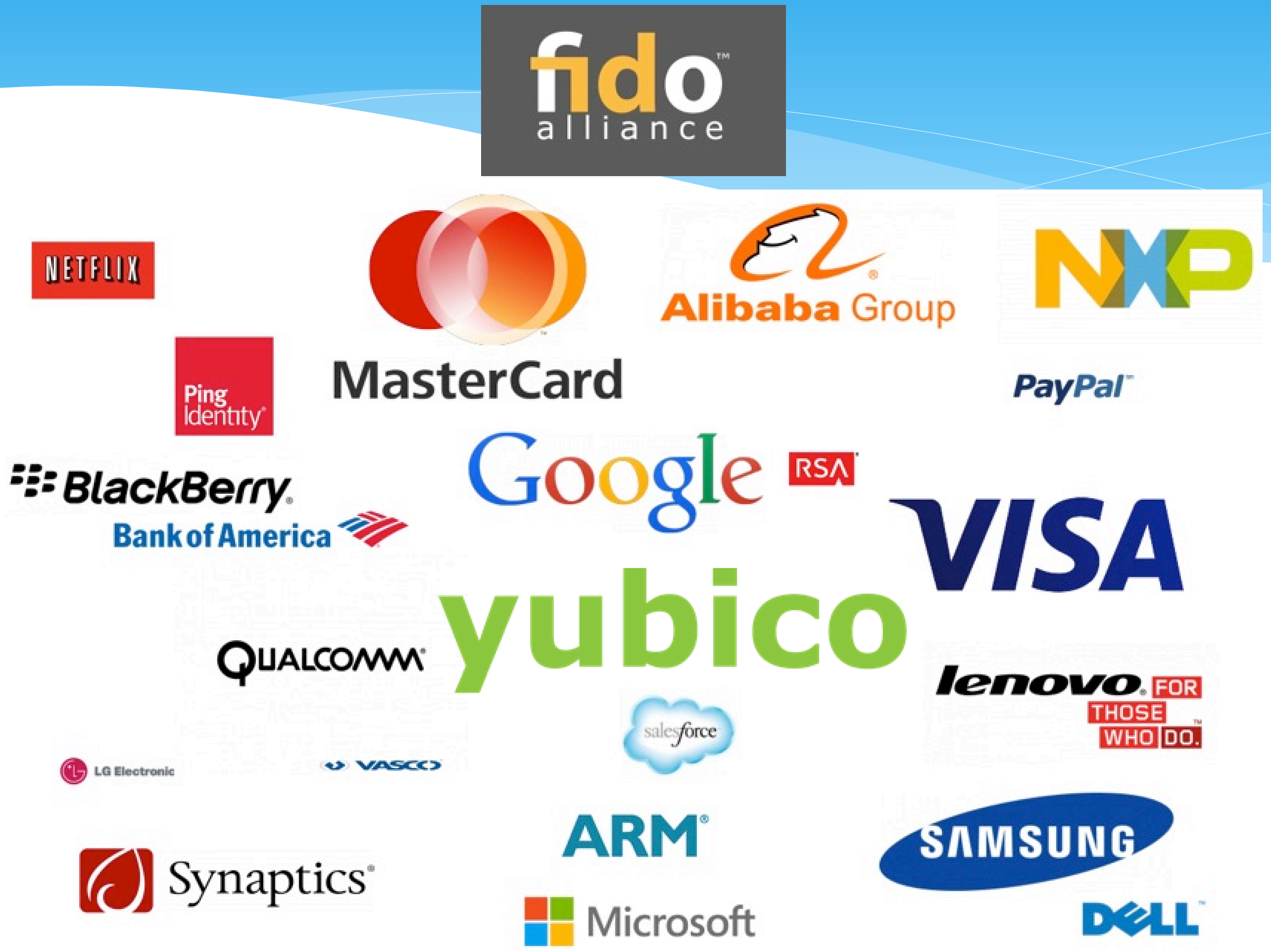
QR-Login main advantages

- The password can be randomly generated.
  - If the user chooses to use a randomly generated username, the user's account on one web site cannot be associated with the user's account on another web site, again as happened in the Gawker password database spill.
- Users have more privacy options since it is easier to generate and recall random logins and passwords.
- The user will not lose access to a web site because they cannot remember a password.
- Since the authentication code is sent encrypted, and the web site authenticates itself to the user via HTTPS, the random secret can't be intercepted to authenticate another user's session.
- Finally, the login process is quicker and easier than typing a username and password.

fido™ alliance

simpler
stronger
authentication

The FIDO Alliance was formed in the summer of 2012



To Change Authentication Online by:

(a) Developing unencumbered Specifications that define interoperable mechanisms that supplant reliance on passwords

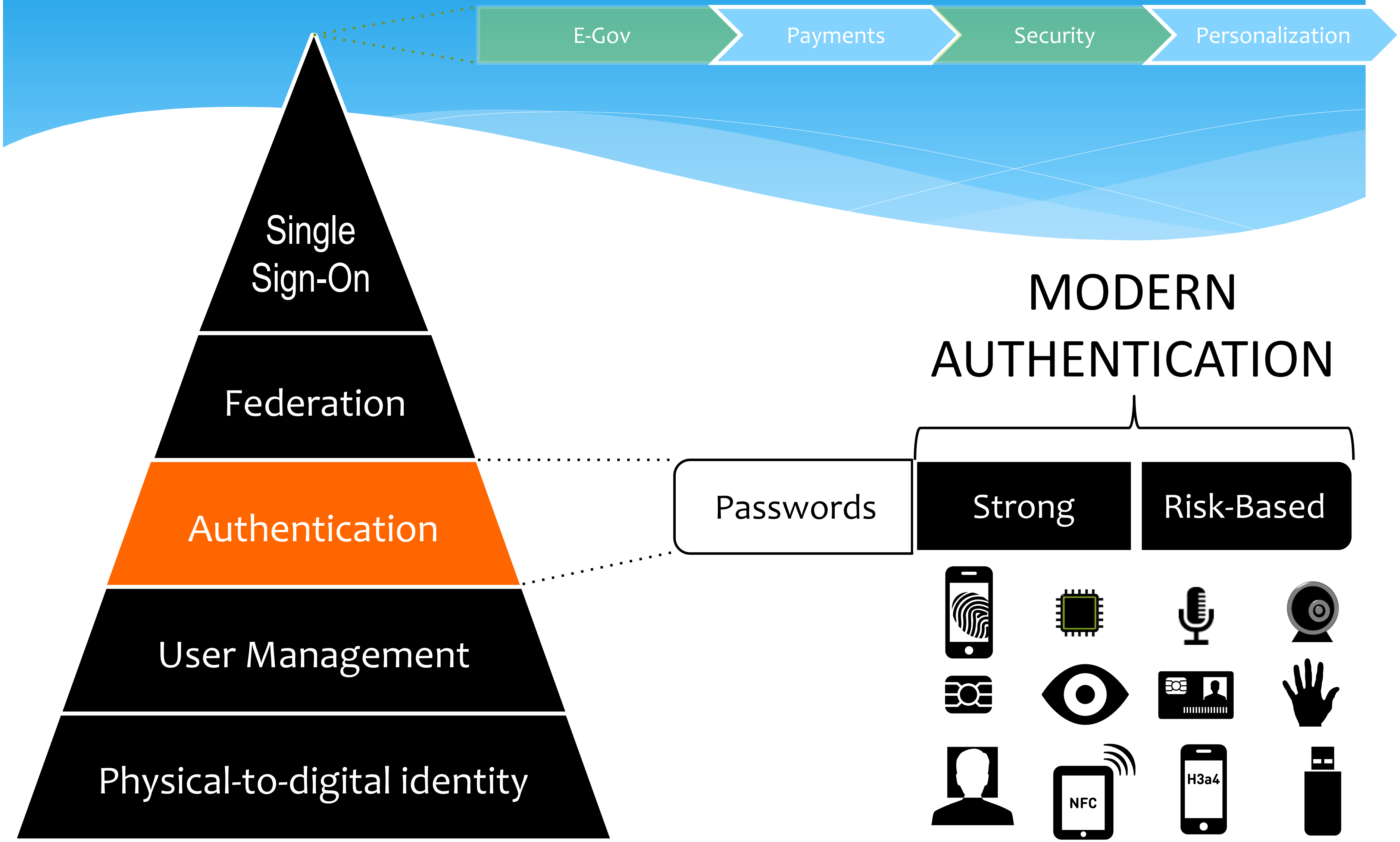
(b) Operating programs to help ensure industry adoption

(c) Submitting mature Specifications for formal standardization

FIDO Alliance’s Role…

- “Paper” Specifications
- Interoperability and Conformance testing
- Trademark licensing against criteria
- Thought leadership, nurture ecosystem
- The Alliance does not ship products!
- Implementations left to commercial vendors

Identity & Authentication Building Blocks



E-Gov

Payments

Security

Personalization

Single Sign-On

Federation

Authentication

User Management

Physical-to-digital identity

MODERN AUTHENTICATION

Passwords

Strong

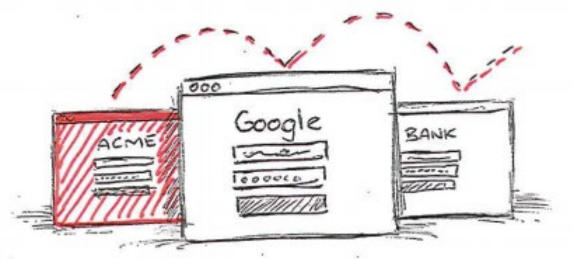
Risk-Based

Why Authentication is Cybersecurity Priority #1

Poor authentication mechanisms are a commonly exploited vector of attack by adversaries; the 2013 Data Breach Investigations Report (conducted by Verizon in concert with the U.S. Department of Homeland Security) noted that 76% of 2012 network intrusions exploited weak or stolen credentials.

-- NIST Roadmap for Improving Critical Infrastructure Cybersecurity,12-Feb-2014

Today’s Passwords



REUSED

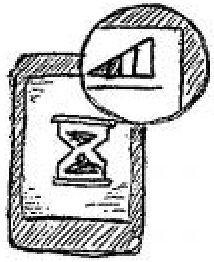
AMCE
joe@gmail.com
SIGN IN

PHISHED

KEYLOGGED

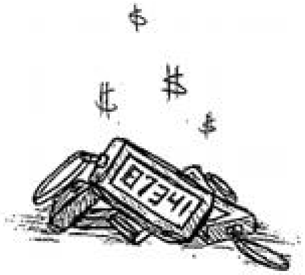
Today's Password Alternatives

One Time Codes with SMS or Device



SMS USABILITY

Coverage | Delay | Cost | Unsecure

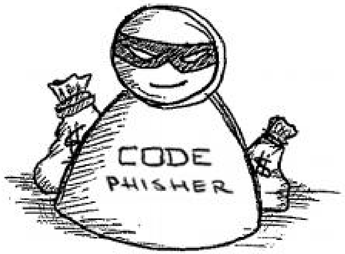


DEVICE USABILITY

One per site | $$ | Fragile

USER EXPERIENCE

User find it hard



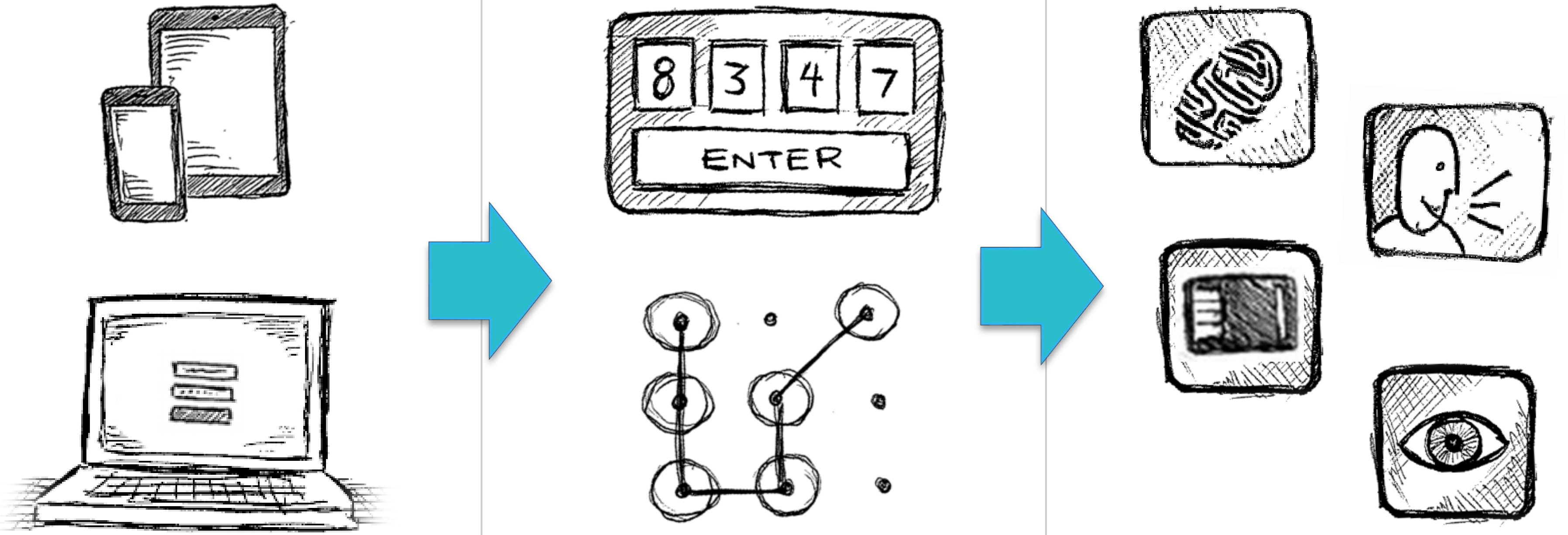
STILL PHISHABLE

Known attacks today

Major Industry Trend

Simpler, Stronger Local Device Auth

PERSONAL DEVICES	LOCAL LOCKING	NEW WAVE: CONVENIENT SECURITY
Carry Personal Data	Pins & Patterns today	Simpler, Stronger local authentication



Putting It all Together

The problem:
Simpler, Stronger online
The trend:
Simpler, Stronger local device auth

Why not:
Use local device auth for online Auth?

This is the core idea behind FIDO standards!