Practical Security for start-ups

by Pablo Endres - www.PabloEndres.com - Startplatz

Köln 27.11.2013

Agenda

- About me
- Why are we here?
- Nightmare scenarios from real life
- Device security
- Passwords and why the are not enough
- Internet security
- Questions

About me

Pablo Endres

IT Security consultant / researcher

Email: epablo@pabloendres.com
Twitter: @epablosensei
Blog: http://pabloendres.com

- Design and implementation of secure cloud environments
- Penetration and security testing (design, planning and execution)
- Development of security programs and concepts
- Project management
- Certified: CISSP, OPSA, OPST
- Active researcher @ ISECOM and contributor to Hacker High School
- Hands on experience in the telecommunications industry: wireless carriers, ITSPs, ISP and hosting providers
- I have a thing for start ups

endres
IT Security

WHY ARE WE HERE?

Why are we here?

- Just wanted to see what this is all about …
- To stop being low hanging fruit
- Curious about IT Security
- Want practical tips that can be implemented
- Are really worried about the security aspects of you start up and client data

endres
IT Security

Security breaches, those will **never** happen to me?

NIGHTMARE SCENARIOS

endres
IT Security

Quick statistic

Who uses …

- Hotpots (hotel, airport, cafe ..)
- Public transportation (train, bus …)
- A laptop
- Smartphone
- CMS
- Social Media: Facebook, Twitter, other

endres
IT Security

Security breaches, those will **never** happen to me?

SCENARIO :: USING A HOTSPOT?

Scenario :: Using a hotspot?

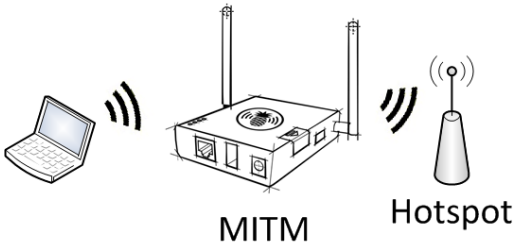
As usual, around 10 – 11am …

- You walk into you regular cafe and order your usual caffeine mix
- Sit down and after a while open your laptop to:
  - update your blog, upload a file to the site
  - check ~~facebook~~ emails
  - have a look at your dashboard / CRM

endres
IT Security

What you didn't know is … :: Using a hotspot

- An attacker had a rogue hotspot running (MITM hot-spot) or just his laptop



- He **captured your credentials**
  - a bot just **defaced your website**
  - Created a user with **access to your emails**
  - sent a ton of **spam emails from your account**

endres
IT Security

Hotspot :: Is this for real?

This a really common scenario

- Most hosting providers still offer **clear-text protocols** for email and is the **default**
- If not explicitly configured admin access to applications is **not encrypted** i.e.
  - CMS – Wordpress, joomla, Typo3
  - CRM – SugarCRM
- Traffic in hotspots / Wi-Fi is available to anyone logged into it

How does this work :: Using a hotspot

- Wireless LAN is a public medium
  - Anyone logged into it, can read all the traffic (sniffing)
  - Maybe even inject traffic

Live Demo :: Using a hotspot

Practical Security :: Using a hotspot

- Check the network name
- Turn off sharing
  - Windows:
    - Setup the network as public when asked by the firewall
    - Turn off file and printer sharing
    - Disable discovery mode
  - Mac:
    - Enable stealth mode

- Use secure protocols
  - Look for SSL encryption: HTTPS, IMAPS, POPS, SSH, SFTP
  - SSL / TLS / Encryption check mark
  - Make sure access to your dashboards , admin interfaces are encrypted (HTTPS)

- Turn off wireless (when not using it)
  - Use the Hw switch if available
- Use a firewall
- **Use a VPN**
  - All your traffic will be encrypted *
  - You can setup up with your office or home router
  - There a many good VPN providers out there
- **Use Tor**
  - All traffic will be encrypted*
  - Can use multiple exit nodes

Source: http://www.pinterest.com/pin/241998179949327635/

endres IT Security

#PracticalSecurity

Security breaches, those will **never** happen to me?

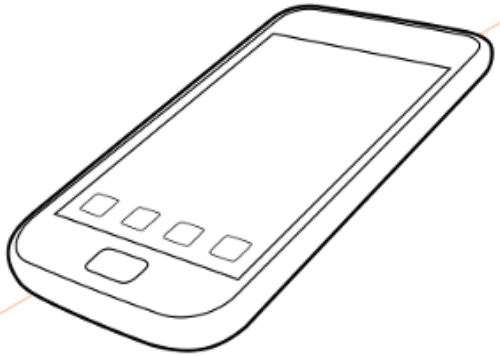
SCENARIO :: LOST SMARTPHONE

endres
IT Security

Scenario :: Lost Smartphone

Just ate a great Dönner-Kebbab, maybe had a couple of beers

- The place is kind of loud, because its after-party hours
- The phone just happens to fall out of your pocket on the floor
- After an hour or two you notice the phone is gone



endres
IT Security

What you didn't know is … :: Lost Smartphone

- Someone found your Smartphone
  - Did some calls
  - Saw the pictures and videos on your phone
  - Took a look at your Facebook and posted some embarrassing photos
  - Read your email
  - Gave it back when you called for it (if your are really lucky)

Think about…

- **All the things that are associated to your email accounts**
  - **All the information stored in your smartphone**

endres
IT Security

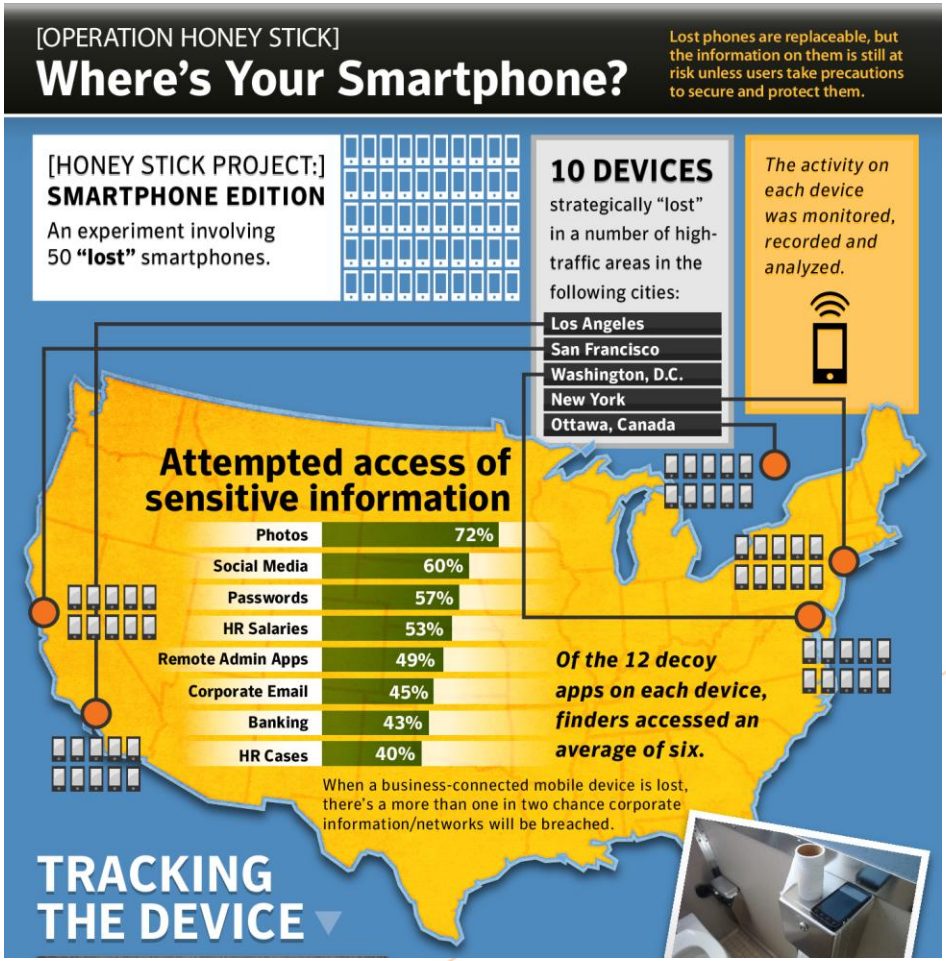
What you didn't know is … :: Lost Smartphone

- What he could of done (if interested - targeted) is:
  - Find out lots about your personal life
  - Impersonate you – *steal digital identity*
    - Get access to your accounts (lots of them) and manipulate data
    - Most of the password reset features run via email
    - Make changes to your Infrastructure
    - Deface your website
    - Access your company information: CRM, ERP (billing), etc
    - Create a user to obtain backdoor access to your systems
  - Perform back transactions (Bank APP + MobileTAN)

_____ It will be hard to get back to normal state!

endres
IT Security

Symantec Honey Stick Project

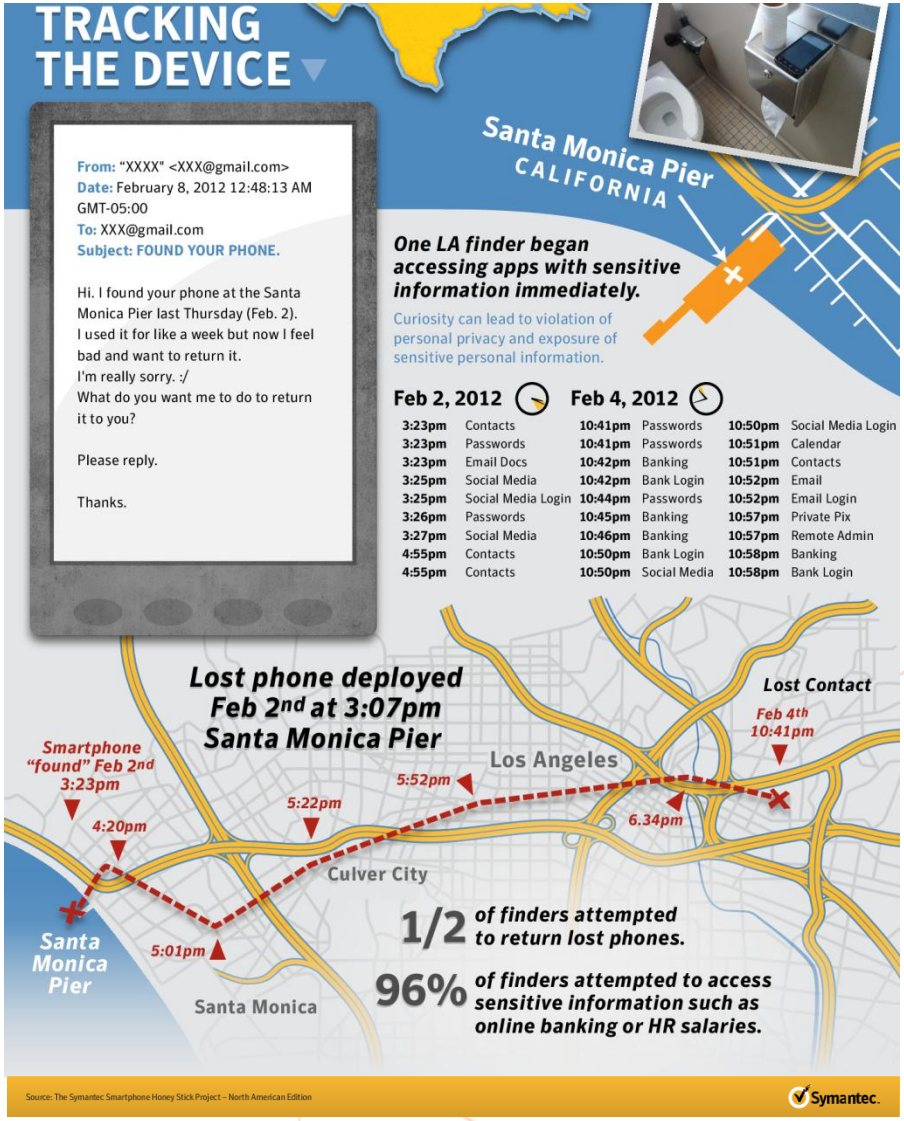


Source: http://www.symantec.com/content/en/us/about/presskits/b-honey_stick_wheres_your_smartphone.en-us.pdf

endres
IT Security

Symantec Honey Stick Project

- People are curious
- If tempted will probably fall



endres IT Security

Practical Security :: Lost Smartphone

End users

- Use screen lock feature
  - Strong password
  - Draw to unlock
- Remote lock and wipe capabilities
  - Keep data safe
  - Increase possible retrieval
- Encrypt the device (if possible)
- Be aware / mindful of your device
- Focus on protecting information!!

Companies

- Setup a strong security policy
- Implement with a Mobile Device Management (MDM) Solution
  - Have an inventory
  - Have a guideline on what to do
  - Create a process -> what to do when device is lost
- Focus on protecting information
- Awareness (talk about the risks – like we are doing now)
- Integrate mobile devices in the overall security

Source: The Symantec Honey Stick Project

endres IT Security

#PracticalSecurity

Security breaches, those will **never** happen to me?

SCENARIO :: LOST LAPTOP

endres
IT Security

Scenario :: Lost laptop

Source: http://www.flickr.com/photos/22541812@N03/4382974102/ 390017

On your normal commute to work …

- Get caught in a conversation with the person next to you
- Run out of the train because this is your stop
- Left your folder in the overhead compartment
- The folder has your brand new laptop

- You notice the missing laptop when you sit at your desk …

endres
IT Security

Scenario :: Lost laptop

What worries you the most?

a) Replacing the laptop: cost + time + effort to configure
b) Someone can read all the data on it
c) The customer data (ID, phone numbers, payment records, etc) that got lost
d) Your vacation photos

- If “**a**” is your only worry, congratulations

endres
IT Security

Statistics :: Lost laptop

- Only 5% of lost laptops are ever recovered
- 43 % lost off-site, 33% in travel, 12% workplace
- Controls in place
  - 30% Encrypted
  - 29% Backups
  - 10% other anti-theft measures
- Cost of the lost laptop
  - Device cost is the smallest part (5%)
  - Data breach (80%)

Source: Ponemon Institute - The billion dollar lost laptop problem – 10/2010

endres
IT Security

Practical Security :: Lost laptop

- Encrypt the hard drive
  - Windows: Bitlocker, Truecrypt …
  - Mac: FileVault2 (Lion+, FDD) …
  - Linux: LUKS, Truecrypt (when dual booting)

Practical Security :: Lost laptop

Perform regular (daily, weekly, monthly) automated backups

- Windows: backup & restore, MozyHome, Syncback
- Mac: timemachine, other comercial Sw
- Linux: Déjà Dup, Back in Time, Duplicity

* Store your backups online (encrypted) or on an external HDD (at least 2x bigger then your drive)

What was I supposed to do to secure my device?

DEVICE SECURITY

Device Security :: Notebooks

Recommended controls

	Encrypt HDD	Backups	Firewall	AV
Windows	X Truecrypt, bitlocker, others	X others	X Windows Firewall other	X Free Comercial Whitelist ++
Mac	X FileVault2 others	X Timemachine others	X Integrated (activate)	- Not required yet
Linux	X LUKS Truecypt	X Déjà Dup Back in Time, Duplicity	X Integrated (activate if off)	- Not required yet

Device Security :: Smartphones / Tablets

Recommended controls

	Device Access	Application stores	Backups	Encrypt device
Android	Pattern PIN Passcode	Setup PIN (not by default)	Online Automatic Offline recommended	Built in since 3.0+
Iphone	PIN Passcode	Apple ID	Online Automatic Offline recommended	Since IOS 4
BB	PIN Passcode	BBID	Online req. setup Offline recommended	yes

Why passwords are not enough to secure everything

PASSWORDS

Passwords

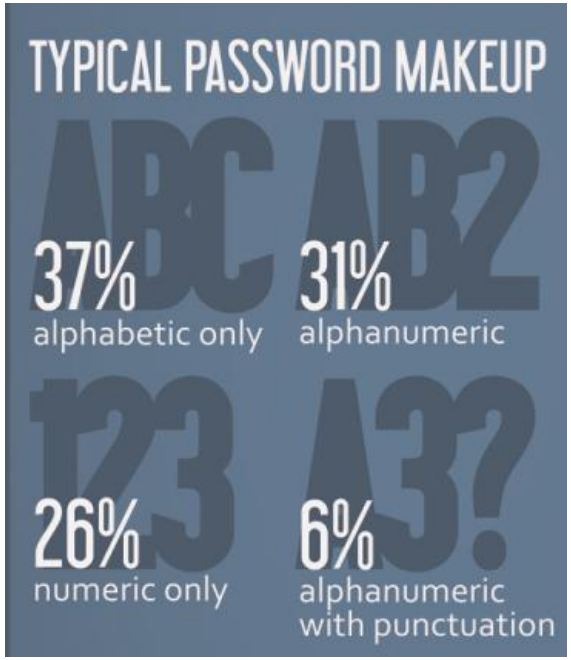
- Passwords are not secure
  - I’ve said it and won’t take it back!
- Reset questions are even worse
  - Based on personal information – easy to find

Passwords :: habits

Source: http://www.pinterest.com/pin/241998179948702156/

endres
IT Security

Passwords :: habits



Source: http://www.pinterest.com/pin/241998179949325446/

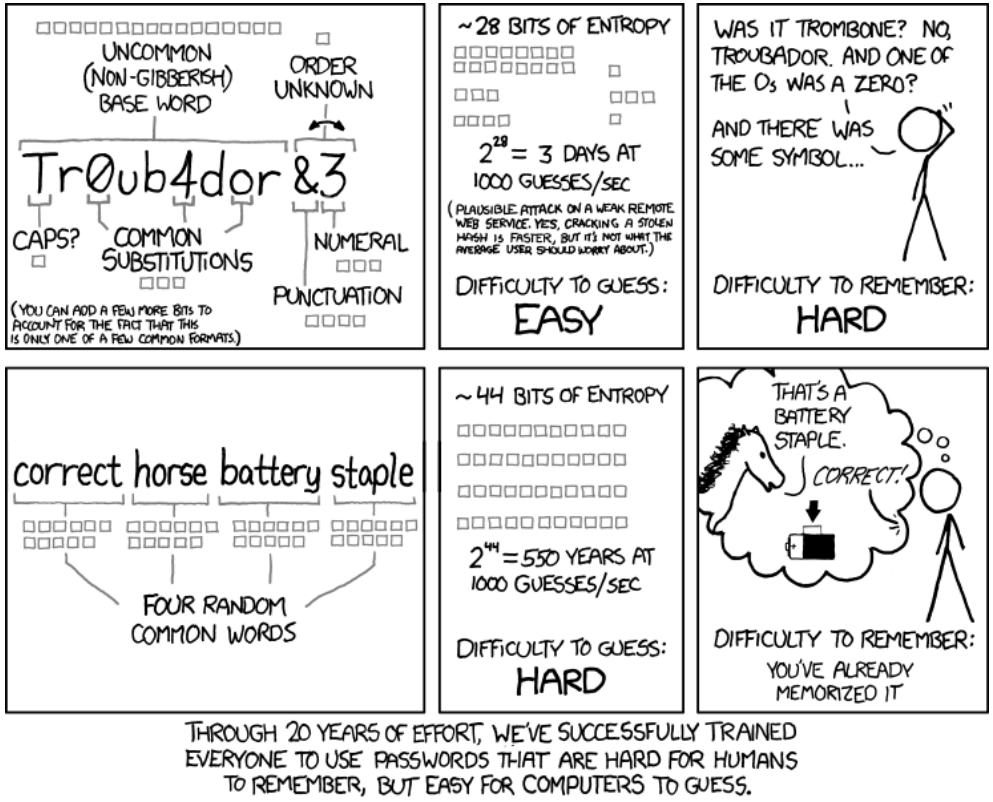
endres
IT Security

Passwords :: Dont's

- **Reuse passwords**
  - One account to rule them all
- **Use a dictionary word**
  - String several together into a pass phrase
  - The less sense they make together the better
- **Use standard number substitutions**
  - P455w0rd is N0t a g00d password
  - Cracking tools now have those built in
- **Use a short password**
  - Your best defense is still the longest possible password.

endres
IT Security

Passwords :: XKCD



Source: http://xkcd.com/936/

endres
IT Security

Passwords :: Do

- **Enable multi-factor authentication** - when offered.
  - You have a Token like device or sends an SMS
  - Yes, that can be cracked, but it raises the bar
- **Use a passphrase instead of a password**
  - Combine unrelated words with symbols or numbers: elephant4tonight@breakfast
  - Make it long! – 20-30 characters
- **Give bogus answers to security questions**
  - Think of them as a secondary password
  - Just keep your answers memorable or store them in a secure place
- **Use a password manager like KeePass**
  - Protect it with a strong passphrase
  - Some even have good random password generators in them

Passwords :: Multi-factor authentication

Identification can be based on different things:

- Something you **are - Biometric**
- Something you **have – Token, Card, Cert**
- Something you **know – Password, PIN**

- Multi-factor authentication uses 2 o more of these factors to be certain of your identity

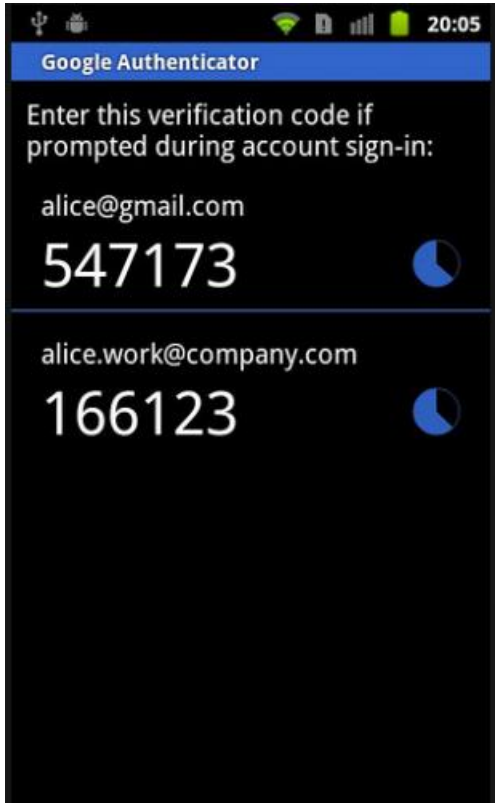
- That is why you can use short PINs with Credit Cards
  - New cards include a smart card to cryptographically sign transactions

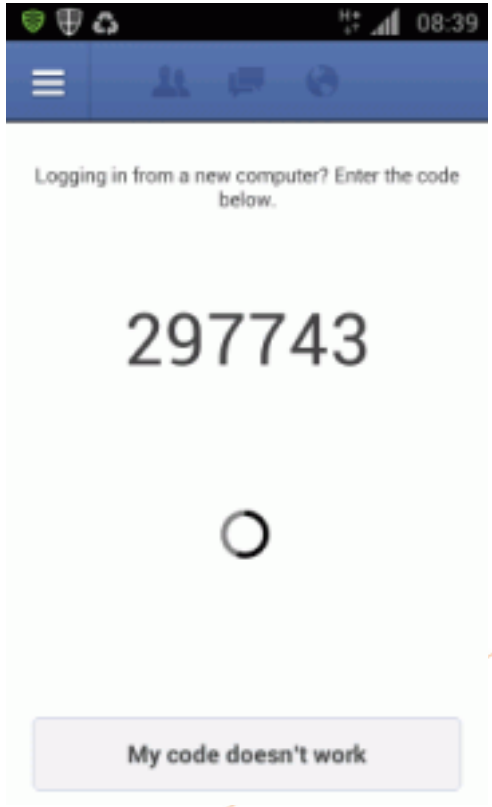
Passwords :: Multi-factor authentication

Popular sites have MFA available:

- Google: 2-step verification
- Facebook: login approvals
- Microsoft: two-step verification
- Dropbox: two-step verification
- AWS: AWS Multi-Factor Authentication
- Twitter: Verification code

Source: https://www.eff.org/deeplinks/2013/05/howto-two-factor-authentication-twitter-and-around-web





endres
IT Security

QUESTIONS

Pablo Endres <epablo@pabloendres.com>
Twitter: @epablosensei
Blog: http://www.PabloEndres.com

THANK YOU FOR YOUR TIME

endres
IT Security