Welcome to 2nd Beer-Talk

iPhone Security

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Who am I ?

Riccardo Trombini, B.Sc. FHO in Computer Science

Business

- Working in IT Security since 2000
- Study Information Technologies at FH in Rapperswil SG
- IT Security Analyst, with Compass since 2009

Private

- In a relationship with …
- Apple follower, always in the first row
- iOS Developer
- Social Media enthusiast (fb, twitter, foursqure, instagram ..)

iPhone Security

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

An Ideal World

Centralized management with a MDM solution, to

- Enforce security policies
- Monitor status of devices
- Real-time incident handling

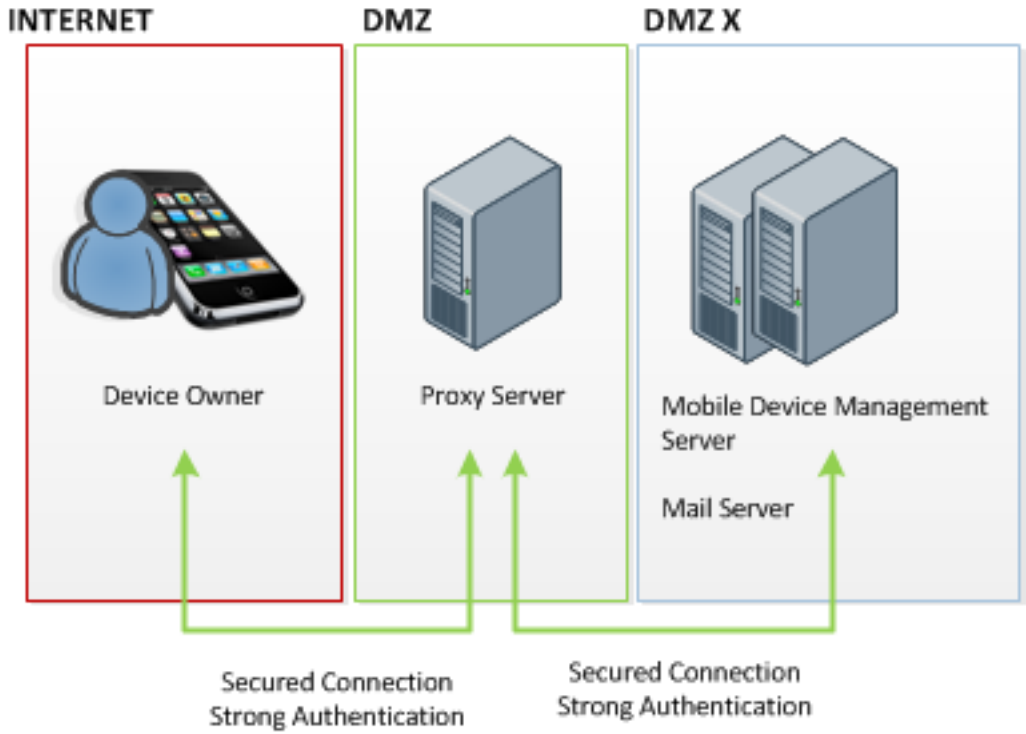
Synchronization

- Encrypted channel
- Strong authentication

Fully Protected Device

- Access Control
- Strong Encryption
- Vulnerabilities

Fully Aware Users



Sadly there is no such thing

Centralized management with a MDM solution, to

- Enforce security policies
- Monitor status of devices
- Real-time incident handling

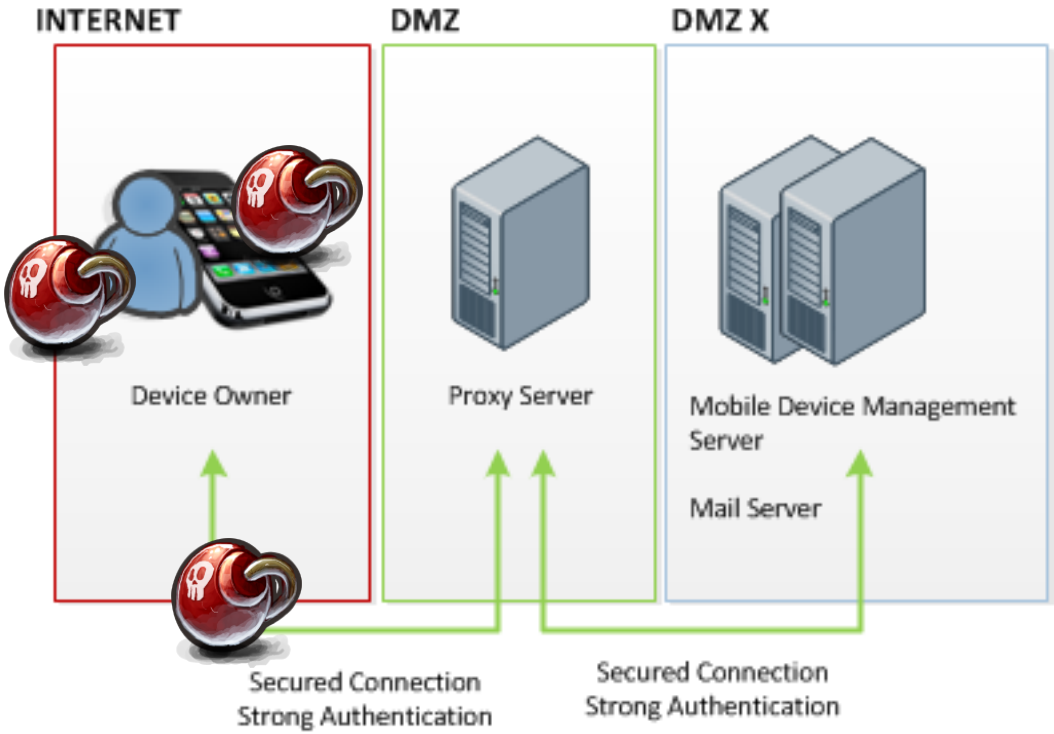
Synchronization

- Encrypted channel
- Strong authentication

Fully Protected Device

- Access Control
- Strong Encryption
- Vulnerabilities

Fully Aware Users



What is MDM?

- **M**obile **D**evice **M**anagement
- Centralized Management of mobile devices

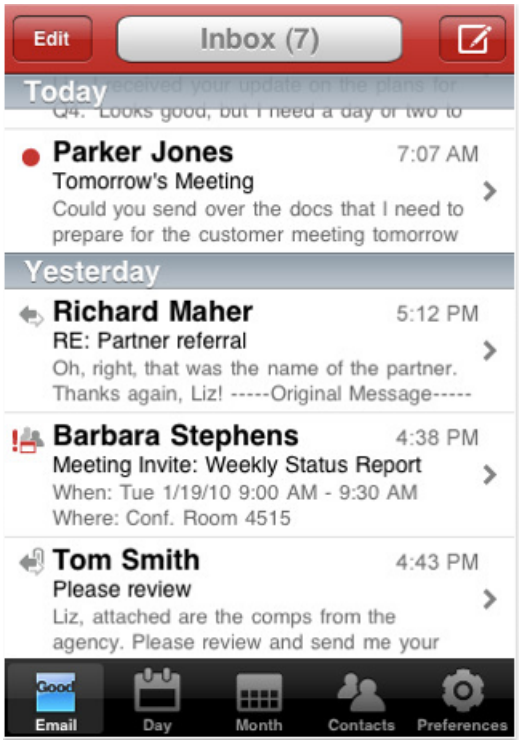
Functionality

- OTA „Over The Air“ enrollment and profile distribution (config)
- Easy synchronisation of Emails, Calendar, Contacts, ...
- Enforce compliance policy
- Monitor device status for inventory and compliance
  - Device Information (UDID, iOS Version, Modem Version ..)
  - Network Information (Carrier Settings, Data roaming status ..)
  - Compliance & Security (Installed profiles, certificates, passcode status ..)
- Remote administration like
  - Remote wipe
  - Remote lock
  - Passcode reset
  - Locate device

MDM != MDM – iOS Integration

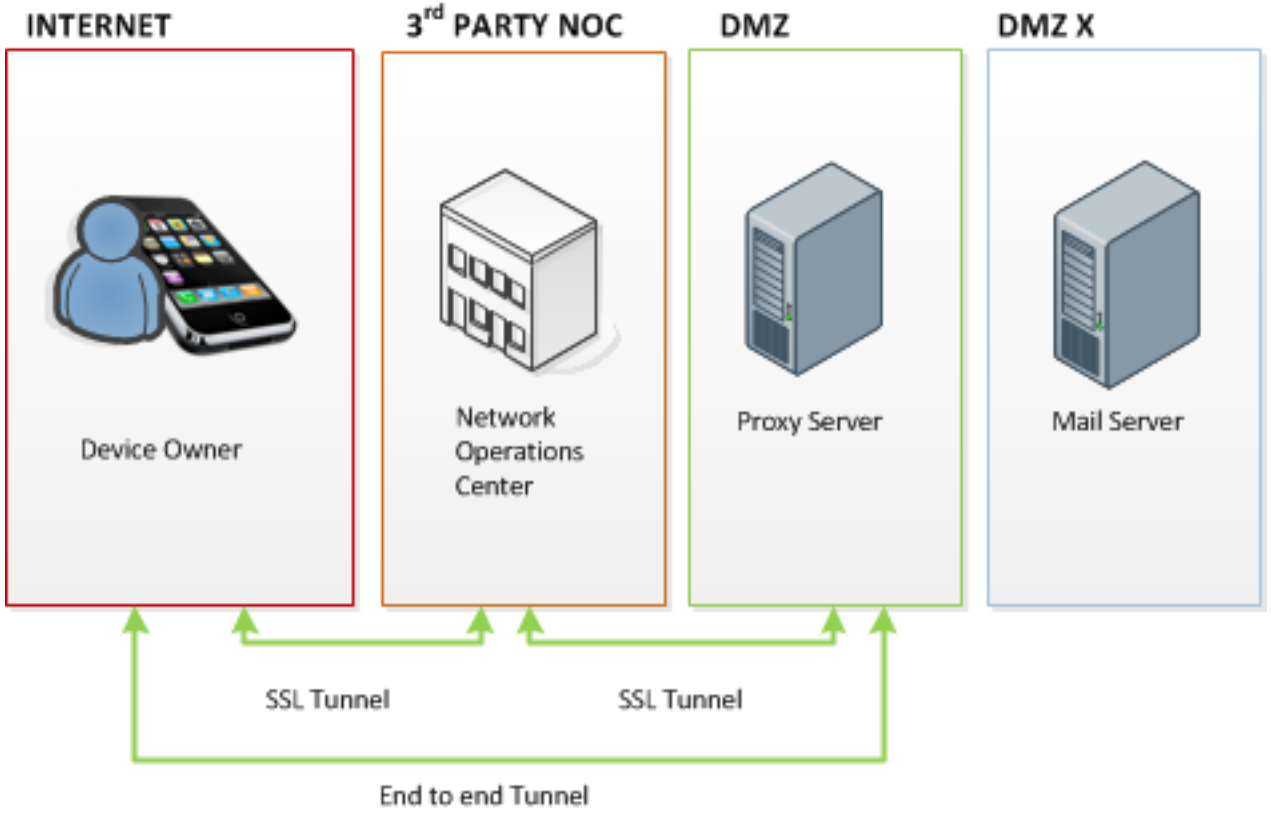
Nativ iOS Apps

Sandbox Client



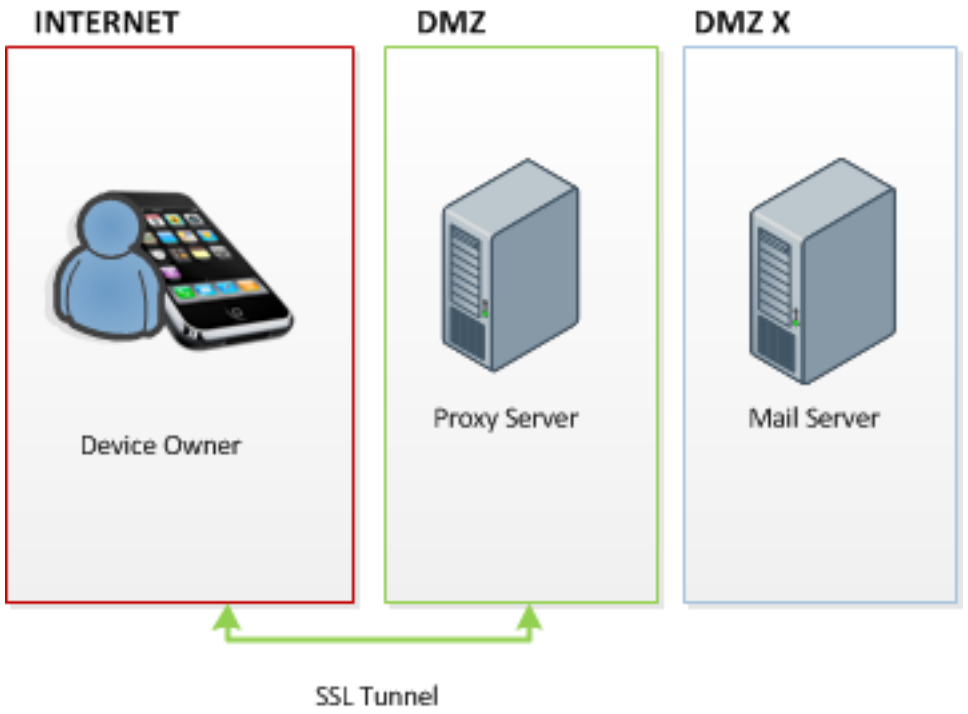
MDM != MDM – Network Design

NOC (Network Operation Center)



MDM != MDM – Network Design

Direct Access to DMZ



Demo #1

Break Passcode Protection

Break File Encryption on iPhone

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

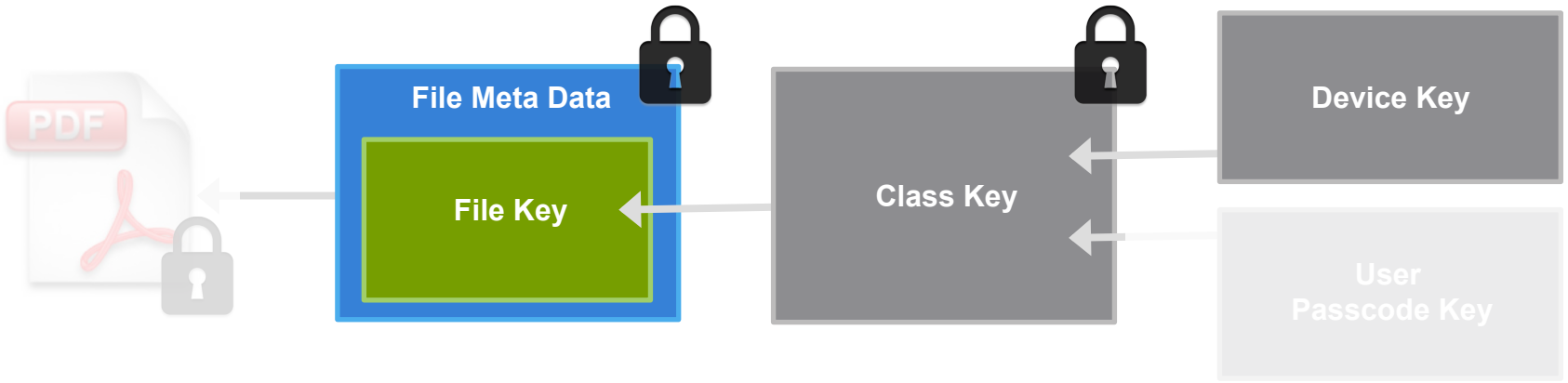
iOS Security Controls

Encryption

- Full Disk Encryption
  - Since iPhone 3GS
  - AES CBC 256 bit
  - does only provide one reason: Rapid device wiping
  - FDE pretty useless. Kernel transparently decrypts requested files
- Data Protection API
  - Introduced with iOS 4
  - Additional level of encryption
  - File encryption can be tied to the Passcode

iOS Security Controls

Encryption - Data Protection API



BootRom-Attack

Summary

- User Awareness - Always know where your device is !
- Enforce strong Passcode Policy with MDM!
  - Length
  - Alphanumeric
  - Special characters
  - C0mpa$$ … don't !
  - Usability?

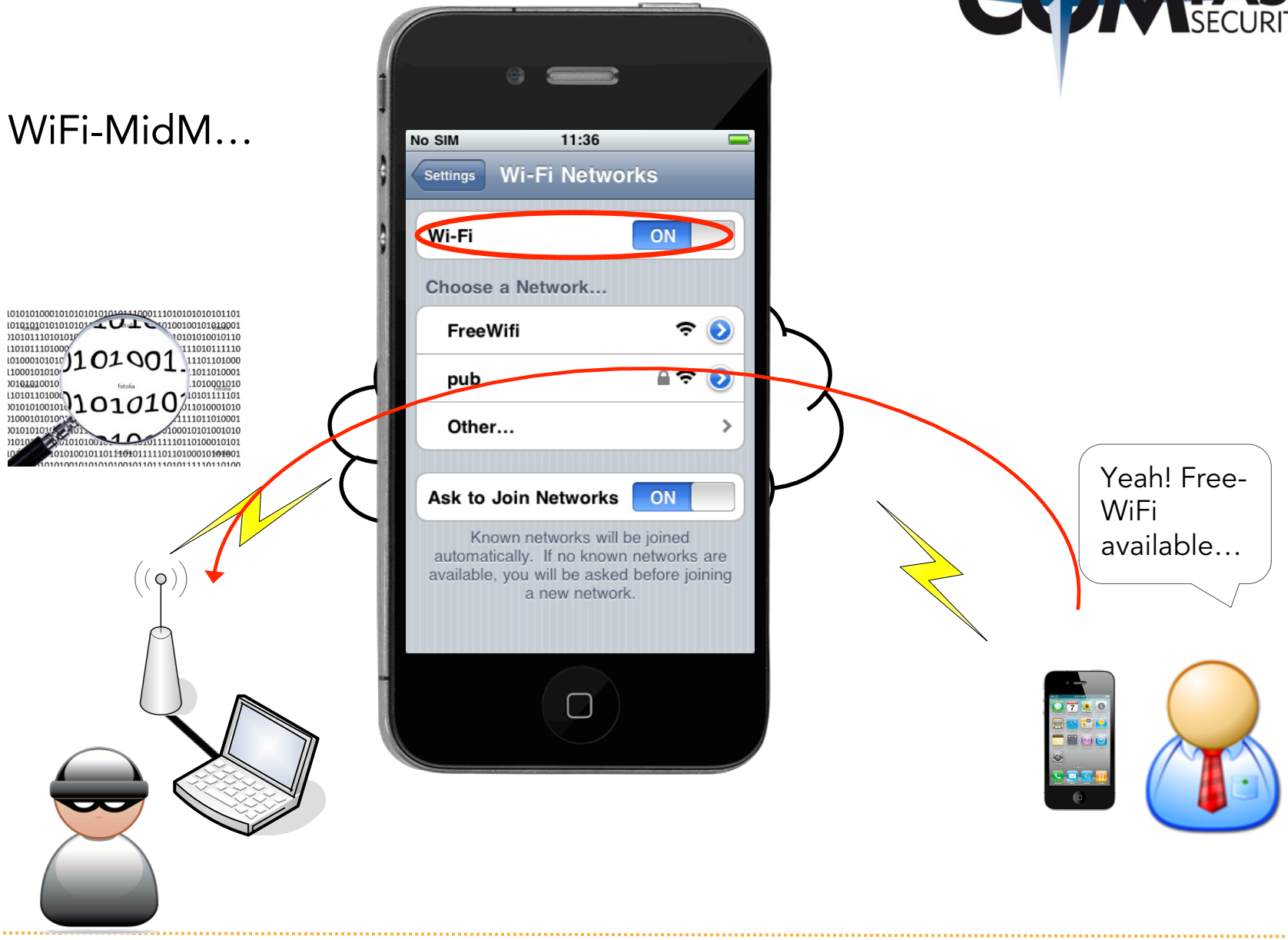
LiveDemo [Free-WiFi-CertPush-Attack]

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

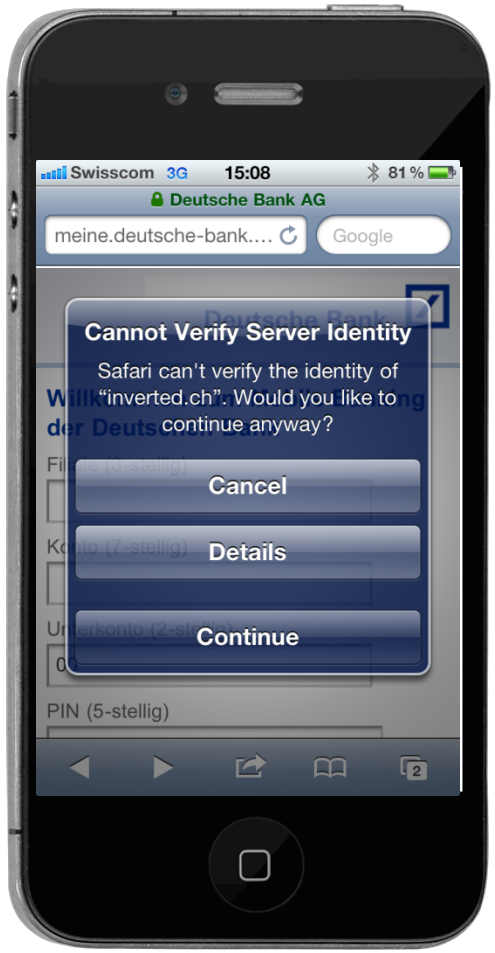
Free-WiFi-Cert-Push-Attack

WiFi-MidM…



Free-WiFi-Cert-Push-Attack

The Problem with the Certificate….



Free-WiFi-Cert-Push-Attack

The Solution ;-)

Free-WiFi-Cert-Push-Attack

Behavior of the iPhone …

www.apple.com/library/test/success.html

HTTP GET request

OK

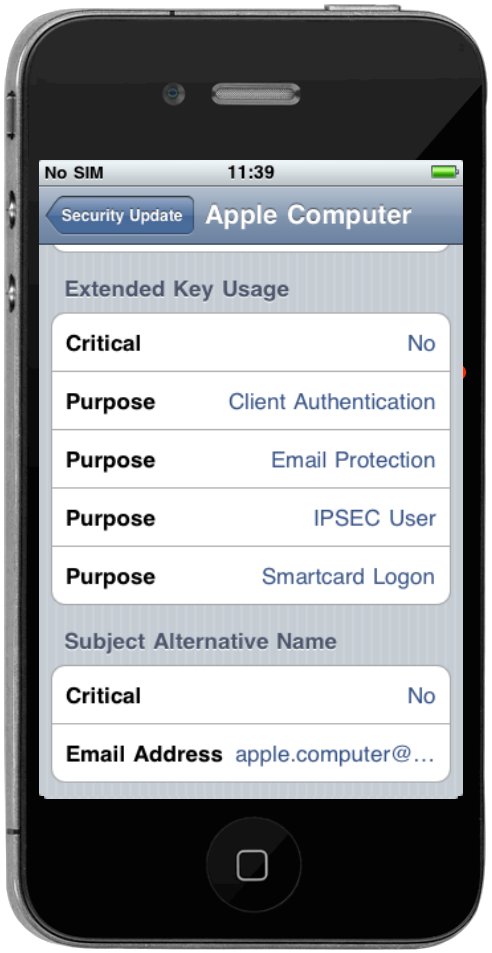
Redirect

Hotspot Login-Site

Hotspot Management

Free-WiFi-Cert-Push-Attack

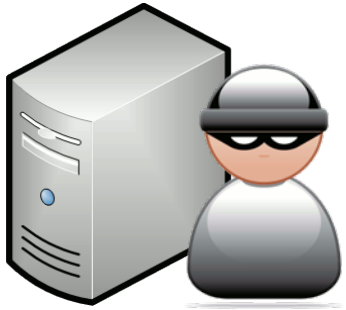
Cert-Push …



www.apple.com/library/test/success.html

HTTP GET request

Redirect



Mobile Conficuration

Attacker Host

Free-WiFi-Cert-Push-Attack

Make your own Apple Certificate

Posteingang - apple.computer@anonmails.de

Benutze SSL-Verbindung / Language: de , en

Einstellungen | Posteingang

Betreff:	**Your TC Internet ID request no. 401127285 has been approved**
Datum:	31.08.2011 15:51
Von:	certificate@tctrustcenter.com
An:	apple.computer@anonmails.de
Sender:	certificate@tctrustcenter.com
Dateien:	smime.p7s 2.72 KB

Dear Apple Computer,

You have requested a TC Internet ID with the following data:

Name:..... Apple Computer
Country:..... Switzerland

We confirm your request with the order ID 401127285.

Issuance of the Certificate
****
To issue your certificate you have to generate a respective key pair on the order status webpage.

The required password to access the order status webpage will be provided to you in a separate email.

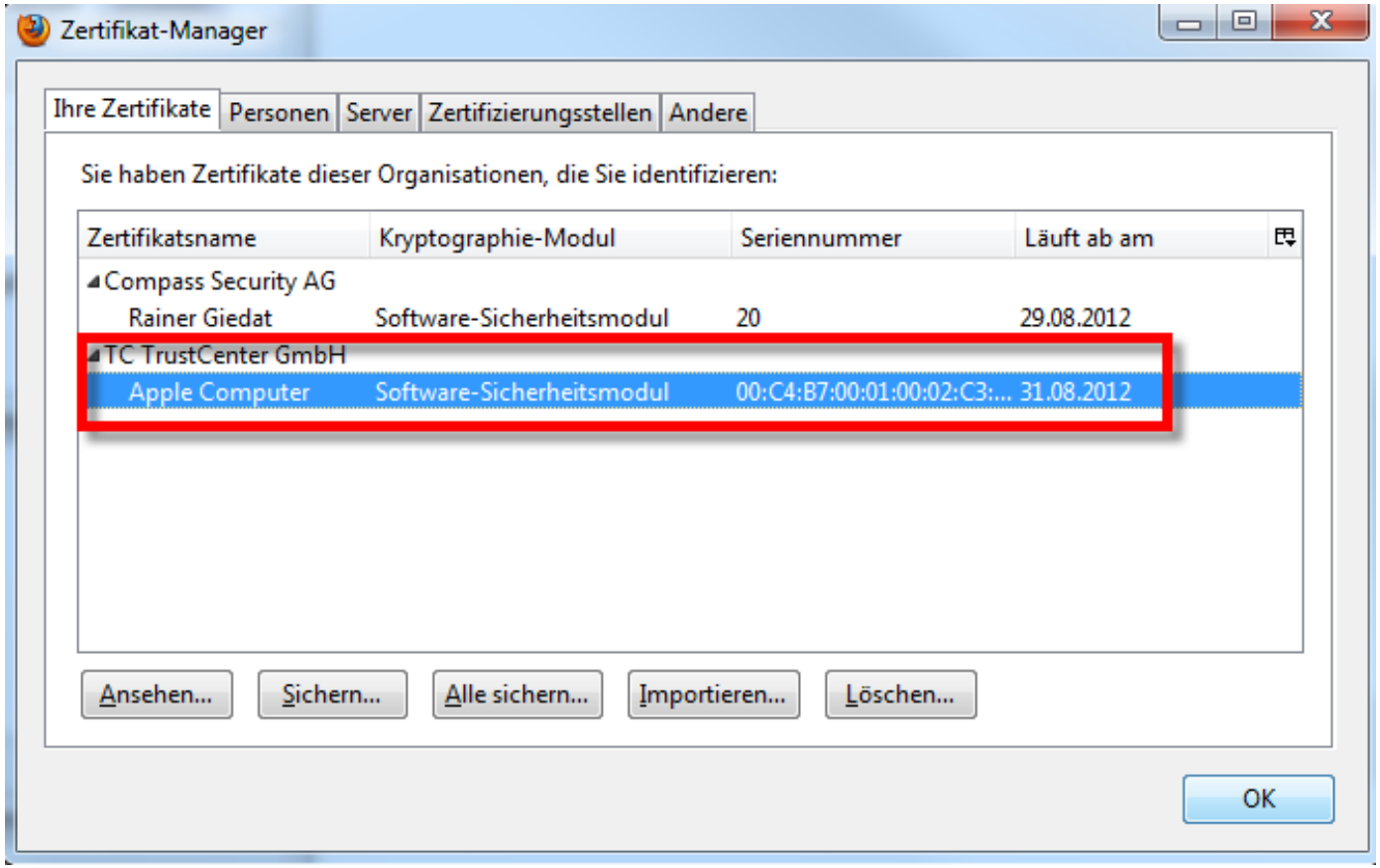
Order status webpage:
https://www.trustcenter.de/RetailStore/cid/Login.action?loginName=mFZkAcRCvS

After key generation the certificate will be issued and installed in your browser instantly.

Please Note: After you have successfully installed your certificate, we highly
recommend to backup your personal security environment (PSE). Otherwise in case of loss of the private

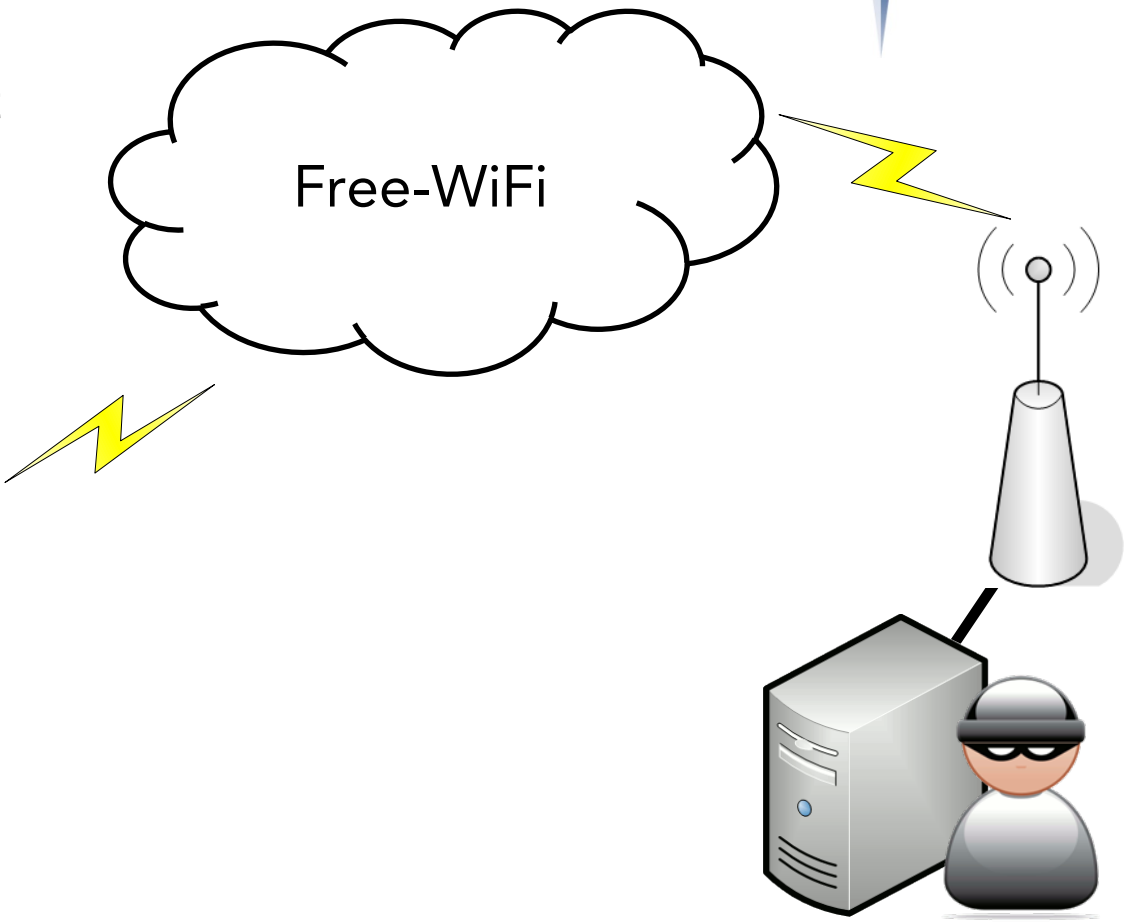
Free-WiFi-Cert-Push-Attack

Result…



Free-WiFi-Cert-Push-Attack

MitM with valid Cert



Summary

- User Awareness
  - Think before accepting configurations
  - Be suspicious
- Apple should improve certificate validation for mobile configuration
- Synchronization should be protected with two-way authentication

Questions ?


COMPASS
SECURITY