

Welcome to 2nd Beer-Talk

iPhone Security

Werkstrasse 20 Postfach 2038 CH-8645 Jona

Compass Security AG 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

13

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

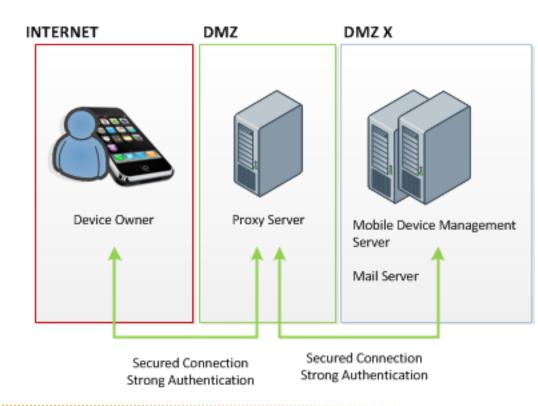
Synchronization

- Encrypted channel
- Strong authentication

Fully Protected Device

- Access Control
- Strong Encryption
- Vulnerabilities

Fully Aware Users



Centralized management with a MDM solution, to

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

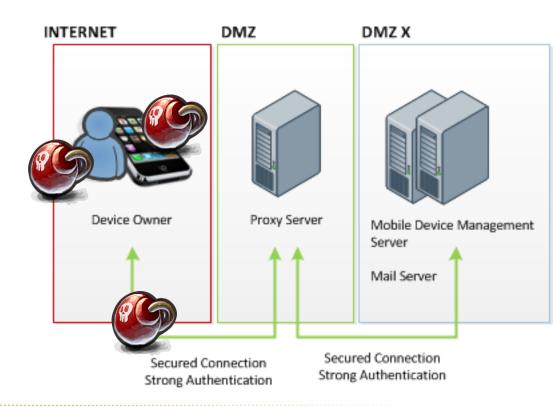
Synchronization

- Encrypted channel
- Strong authentication

Fully Protected Device

- Access Control
- Strong Encryption
- Vulnerabilities

Fully Aware Users





What is MDM?



- Mobile Device Management
- Centralized Management of mobile devices



www.csnc.ch

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



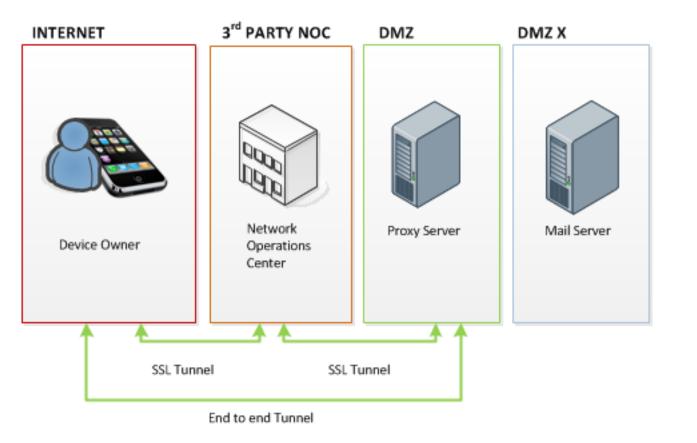
CEPASS SECURITY

Sandbox Client

Edit	Inbox (7)	
Today	oks good, but i nee	e on the plans to ed a day or two t	0
Tomore Could y	er Jones row's Meeting rou send over the c e for the customer r		>
Yestero	lay		
RE: Pa Oh, righ	ard Maher artner referral nt, that was the nar again, Liz!Ori		>
Meetin When:	ara Stephens g Invite: Weekly S Tue 1/19/10 9:00 A Conf. Room 4515	status Report	РМ >
Liz, atta	Smith review ached are the comp . Please review and		⊳м >
Good Email	Day Month	Contacts Prefe	erences



NOC (Network Operation Center)



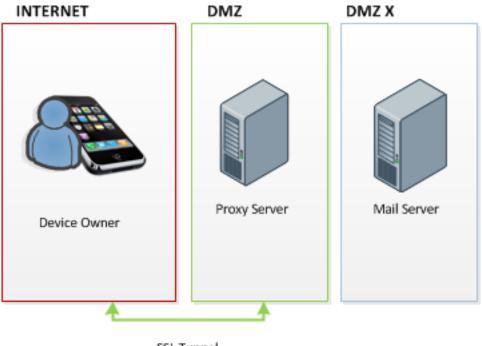




MDM != MDM – Network Design



Direct Access to DMZ



SSL Tunnel







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

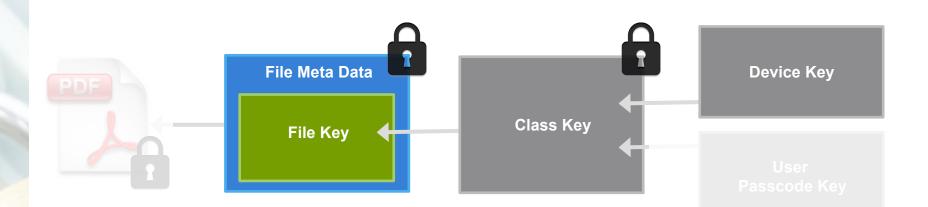


- Full Disk Encryption
 - Since iPhone 3GS
 - AES CBC 256 bit
 - does only provide one reason: Rapid device wiping
 - FDE pretty useless. Kernel transparently decrypts requested files
- Data Protection API
 - Introduced with iOS 4
 - Additional level of encryption
 - File encryption can be tied to the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

iOS Security Controls

Encryption - Data Protection API





BootRom-Attack





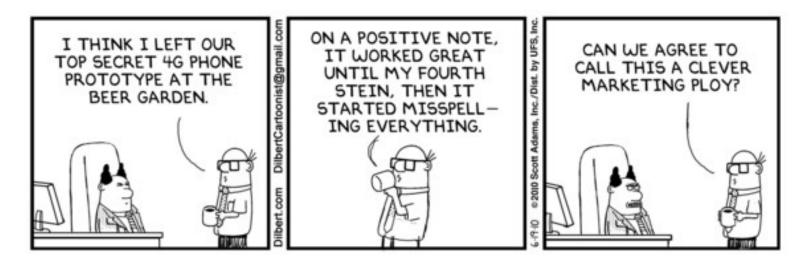




- User Awareness Always know where your device is !
- Enforce strong Passcode Policy with MDM!
 - Length

Summary

- 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 **CAN PASS** SECUDITY WiFi-MidM... No SIM 11:36 Wi-Fi Networks Settings Wi-Fi ON Choose a Network... FreeWifi ŝ \bigcirc)10101110101010 0101010010110 101011101000 111010111110 101000101010)1010100 11101101000 1011010001 1 ? 🕖 1000101010 pub 1010001010 00101010010 110101101000 10101111101)1000101010 1111011010001 Other... 00010101001010)0101010 111110110100010101 10100101101110101010001010101001 0110111010111111011010 Yeah! Free-Ask to Join Networks ON WiFi Known networks will be joined available... automatically. If no known networks are available, you will be asked before joining a new network.



The Problem with the Certificate....



www.csnc.ch

The Solution ;-)



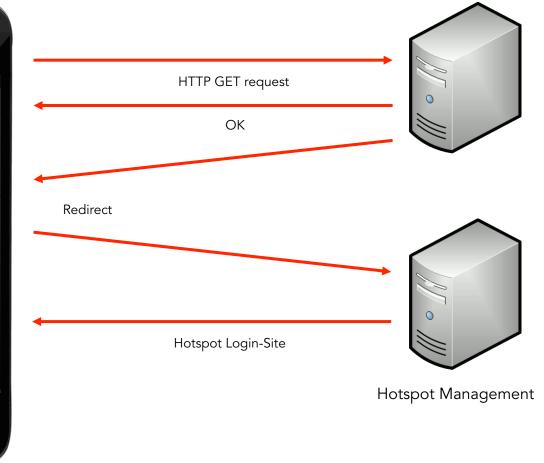
© Compass Security AG

www.csnc.ch

COMPASS

Behavior of the iPhone ...

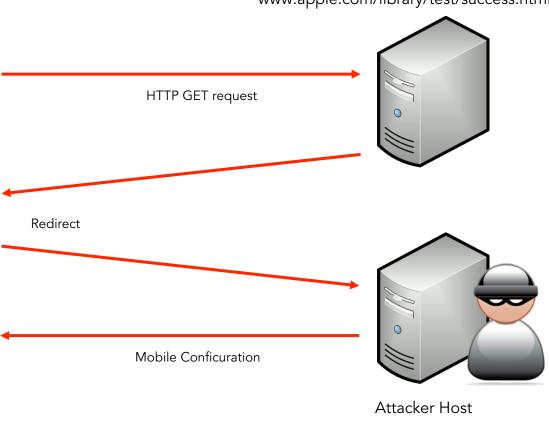




www.apple.com/library/test/success.html

Cert-Push ...





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

COMPASS SECUDITY



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

www.csnc.ch

Result...

hre Zertifikate Personen	Server Zertifizierungsstellen And	dere		
Sie haben Zertifikate die	ser Organisationen, die Sie identif	izieren:		
Zertifikatsname	Kryptographie-Modul	Seriennummer	Läuft ab am	C,
Compass Security AG Rainer Giedat	Software-Sicherheitsmodul	20	29.08.2012	
TC TrustCenter GmbH				
Apple Computer	Software-Sicherheitsmodul	00:C4:B7:00:01:00:02:C3:	31.08.2012	
Ansehen Siche	rn Alle sichern Impor	tieren		

CEPASS SECURITY

Free-WiFi-Co	ert-Push-Attack	CC PASS
MitM with value	Free-WiFi	SECURIT



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?







www.csnc.ch