

Cnlab / CSI 2011

Demo

Smart-Phone: Ein tragbares Risiko?

Agenda – Demo 45'

Schutz der Smart-Phones:

- **Angriffsszenarien**
- **«Jailbreak»**
- **Was nützt die PIN?**
- **Demo: Zugriff auf Passwörter iPhone**

Bekannte Schwachstellen auf Smart-Phones:

- Überblick und Klassifizierung der aktuellen Schwachstellen
- Demo: SSL-Schwachstelle

Angriffsszenarien

Szenario	iPhone			ANDROID			Windows Phone		
	ohne PIN	mit PIN	Jailbroken	ohne PIN	mit PIN	«rooted»	ohne PIN	mit PIN	«unlocked»
Physischer Zugriff auf Smart-Phone -> Zugriff auf Daten									
Installation von Malware durch User -> Zugriff auf Daten anderer Anwendungen									

«Jailbreak»: Software-Modifikation des Gerätes

Smart-Phone	Bezeichnung
iPhone	Jailbreak
Android	Root (rooten)
Windows Phone 7	Unlock (ChevronWP7)

iPhone Jailbreak

- Motivation:
 - Ausführen von Anwendungen die nicht von Apple freigegeben wurden
 - Ausschalten von SIM-Lock
- Was wird gemacht:
 - Anwendungsprüfung ausgeschaltet
 - Einschränkungen im File-System ausgeschaltet
- Methoden:
 - Ausnützen einer Schwachstelle im Gerät oder OS
 - www.jailbreakme.com (PDF Exploit) (fixed in iOS 4.3.4)
 - SHAtter, limer1n (Boot-ROM Exploits, fixed in iPad 2)

Android Root

- Motivation:
 - Hochprivilegierter Zugang «root» zu Smart-Phone
 - Funktionelle Anpassungen am OS
 - Einfaches Backupen des gesamten Smart-Phones
 - Installation von «Custom ROM»
- Was wird gemacht:
 - Code von «su» wird installiert. «su» erteilt Apps root Privilegien auf Anfrage.
- Methoden:

Durch Ausnutzung von Schwachstellen im OS

 - Abhängig vom Brand
 - Via App (SuperOneClick, Universal Androot, Z4Root): fixed in Android 2.3
 - GingerBreak für Android 2.3

Windows Phone 7: ChevronWP7

- Durch einen Exploit im OS konnte WP7 in den Developer-Modus versetzt werden.
- Exploit wurde im Feb. 2011 durch MS behoben.
- Microsoft plant zusammen mit dem Entwickler-Team von ChevronWP7 einen öffentlichen Unlock-Dienst anzubieten.



Was nützt die PIN?

- Schutz vor Verwendung des GUI
- Schutz gegen unberechtigte Installation von Apps
- Teilweise Verschlüsselung von gespeicherten Daten

Was nützt die PIN?

iPhone

iPhone: Verschlüsselung von gespeicherten Daten

Hardware Encryption

- Ab 3GS sind alle Daten verschlüsselt abgespeichert. Als Schlüssel wird ein Device Key verwendet.

Data Protection

- Zusätzlich können Dateien mit dem Passcode geschützt werden. Dazu werden sie mit einem Schlüssel verschlüsselt welcher aus dem Passcode abgeleitet ist.
- Data Protection kann auch für Einträge in der Keychain verwendet werden.
- Data Protection ist eine offene Schnittstelle, die von allen Anwendungen verwendet werden kann.
- Zurzeit verwendet Apple die Data Protection nur bei der Anwendung Mail zum Schutz von E-Mails und Attachements.

Was nützt die PIN?

iPhone

iPhone: Data Protection Classes

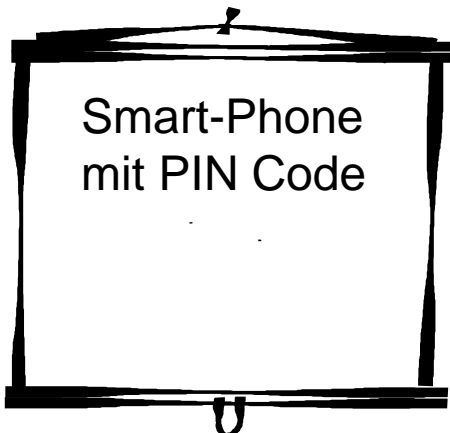
Alle Dateien und alle Einträge in der KeyChain sind einer Data Protection Class zugewiesen. Diese definiert wie die Daten verschlüsselt werden und in welchem Zustand sie von Anwendungen auf dem iPhone gelesen werden können.

Aktive Data Protection Class: File System	Aktive Data Protection Class: KeyChain	Daten sind verfügbar im iPhone-Zustand:
...ProtectionComplete	...WhenUnlocked	Nicht gesperrt
	...AfterFirstUnlock	Nach erster Passcode Eingabe
...ProtectionNone	...Always	Jedem

iPhone-Demo: Zugriff auf Passwörter in der Keychain



1. Jailbreak
2. SSH Server installieren
3. Keychain Datenbank anpassen
4. Passwörter auslesen



iPhone-Demo: Bruteforce auf die PIN



1. Jailbreak
2. SSH Server installieren
3. Bruteforce auf die PIN



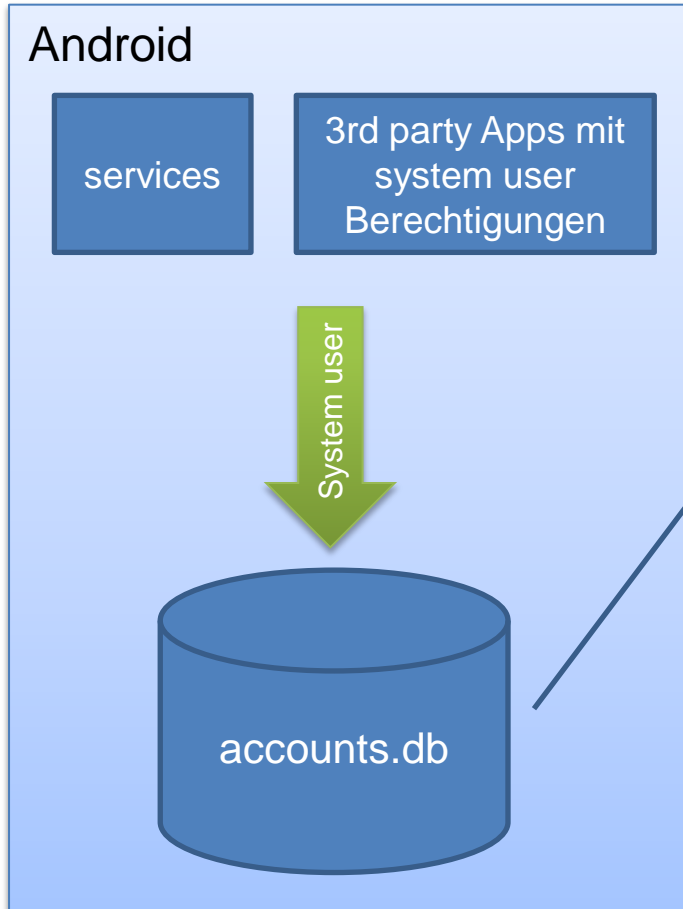
Bruteforce speed

Device	Time to try 10000 passcodes
iPad 1	~16min
iPhone 4	~20min
iPhone 3GS	~30min

Tools: <http://code.google.com/p/iphone-dataprotection/>

Was nützt die PIN?

Android: Fehlende Verschlüsselung



Accounts.db:
Unverschlüsselt, einzelne
Hersteller (z.B. HTC) haben
Schutzmechanismen
implementiert

Benutzernamen
Passwörter
Authenticationtokens (z.B. Gmail)

Was nützt die PIN? Windows Phone 7:



- Schutz vor Verwendung des GUI
- Windows Phone 7 bietet keine «Volume Encryption» Option an.

Was nützt die PIN? – Fazit

Schutz vor...	iPhone	Android	WP 7
Verwendung des GUI	✓	✓	✓
Zugriff auf Passwörter	(✓)	(✗)	✗
Zugriff auf Daten	(✓)	✗	✗
Netzwerkzugriffen	✗	✗	✗
Jailbreak ohne Datenverlust	✗	✓	✓
Installation von Anwendungen	(✓)	✓	✓

Agenda – Demo 45'

Schutz der Smart-Phones:

- Angriffsszenarien
- «Jailbreak»
- Was nützt die PIN?
- Demo: Zugriff auf Passwörter iPhone

Bekannte Schwachstellen auf Smart-Phones:

- **Überblick und Klassifizierung der aktuellen Schwachstellen**
- **Demo: SSL-Schwachstelle**

Bekannte Schwachstellen auf Smart-Phones

Schwachstelle	iPhone	Android	WP7
Fehler bei der Prüfung von X.509 Zertifikaten	< iOS 4.3.5	OK	OK
Code Execution via Adobe Flash	n/a	Flash Player <10.1.95.1	n/a
Auslesen ActiveSync Passwort	alle iOS	Kein Schutz	Kein Schutz
Umgehung der PIN Eingabe	iOS 4.1	OK	OK
PDF Exploit	< iOS 4.3.4	OK	OK
Device Encryption	OK	Kein Schutz	Kein Schutz
DigiNotar Zertifikate	Kein Schutz	Keine Schutz	Patch ist angekündigt.

Prüfung von Zertifikaten

The screenshot shows a certificate inspection tool with the following components:

- Zertifikat** window with tabs: Allgemein, Details, Zertifizierungspfad.
- Zertifizierungspfad** tree view:
 - StartCom Certification Authority
 - StartCom Class 2 Primary Intermediate Server CA
 - *.cnlab.ch
- Detail window 1** (for StartCom Class 2 Primary Intermediate Server CA):

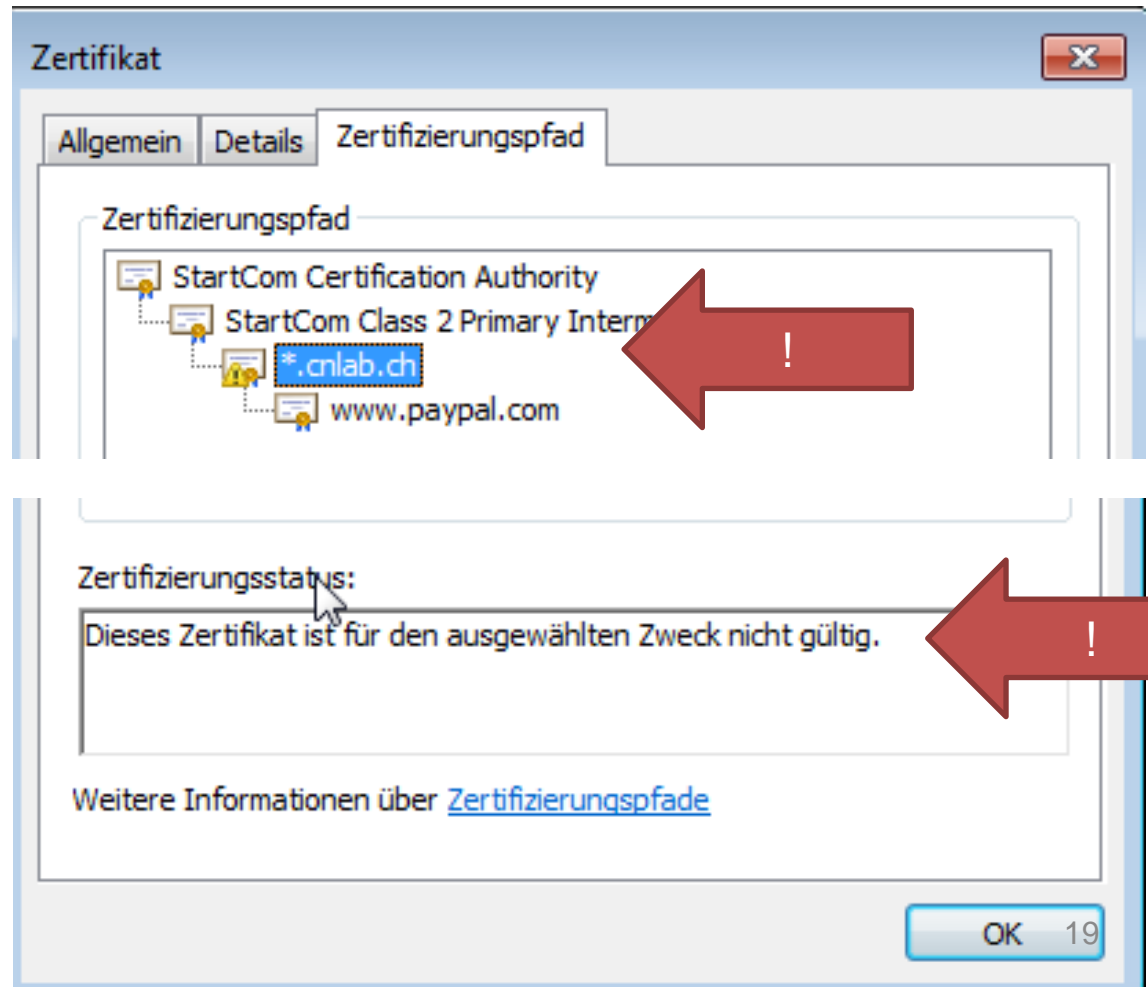
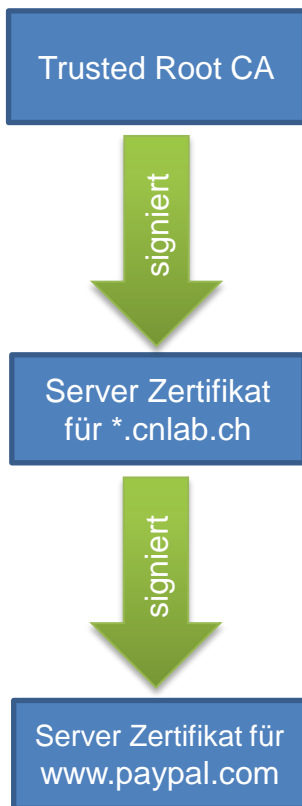
Basiseinschränkungen	Typ des Antragstellers=Zertif...
Schlüsselverwendung	Zertifikatsignatur, Offline Signi...
Fingerabdruckalgorithmus	sha1
Typ des Antragstellers=Zertifizierungsstelle Einschränkung der Pfadlänge=0	
- Detail window 2** (for *.cnlab.ch):

Basiseinschränkungen	Typ des Antragstellers=Endei...
Fingerabdruckalgorithmus	sha1
Fingerabdruck	8d 4a 4a d8 52 05 9f a8 40 81
Typ des Antragstellers=Endeinheit Einschränkung der Pfadlänge=Keine	

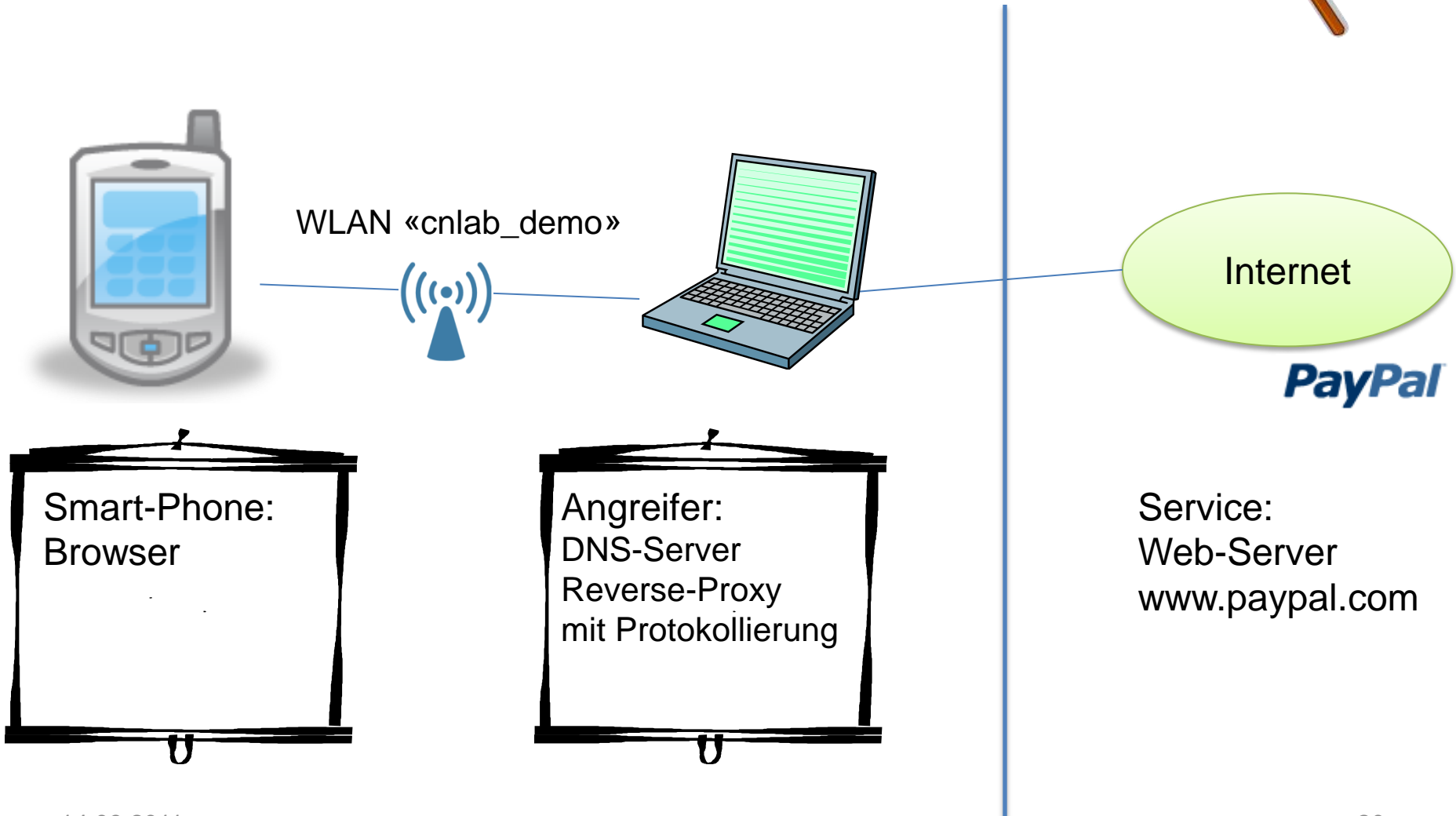
- Angaben im Zertifikat (Basic Constraints) definieren ob ein Zertifikat als CA verwendet werden darf.
- Bei der Prüfung der Zertifikate müssen diese Angaben geprüft werden.
- Fehler ist auch bei Microsoft IE aufgetreten (MS02-050)

Demo: SSL-Schwachstelle

- Verlängerung der Zertifikatskette



Demo: SSL-Schwachstelle - Aufbau



Fazit: Aktuelle Schwachstellen

- Schwachstellen die vor Jahren auf dem PC aktuell waren, treten nun auch auf den Smart-Phones auf
- iPhone:
 - Behebung einer Schwachstelle nur durch eine neue Version des IOS
 - Installation immer über iTunes, ab IOS 5 auch «over the air»
- Android:
 - Patches werden «over the air» verteilt
 - Verschiedene Brands
- Windows Phone 7:
 - Nur wenige Patches bis anhin
 - Installation via Zune, kleine Patches auch «over the air»

Angriffsszenarien (ohne Hardware-Modifikation)

Szenario	iPhone			Android			Windows Phone		
	ohne PIN	mit PIN	Jailbroken	ohne PIN	mit PIN	«rooted»	ohne PIN	mit PIN	«unlocked»
Physischer Zugriff auf Smart-Phone -> Zugriff auf Daten	☒*	☒*	n/a	☒	☑	n/a	☒	☑	n/a
Installation von Malware durch User -> Zugriff auf Daten anderer Anwendungen	☑	☑	☒*	☑	☑	☒*	☑	☑	☑

* Schutz der Daten durch Apps möglich

Danke

Folien von heute: <http://www.cnlab.ch/docs>

Christian Birchler

christian.birchler@cnlab.ch

+41 55 214 33 40

Thomas Lüthi

thomas.luethi@cnlab.ch

+41 55 214 33 41