IT-Ermittler Tagung ostpol Herbst 2014

cnlab - Mobile Security

iOS, Android

Chur, 25. September 2014

Christian Birchler, René Vogt

Folien: www.cnlab.ch → Publikationen → Tagung ostpol

Agenda

- Vorstellung cnlab

Mobile Security

- Sicherheitsmechanismen
  Geräte PIN, Speicherverschlüsselung, Update-Funktionen
- Zugriff auf Geräte
  Umgehung der Sicherheitsmechanismen, Zugriff auf E-Mail-Daten, «Back-Doors»
- Demo
- Ausblick iOS8/Android 5

Unterstützung durch cnlab

- Was cnlab kann
- Was cnlab nicht kann

https://www.cnlab.ch/de/security

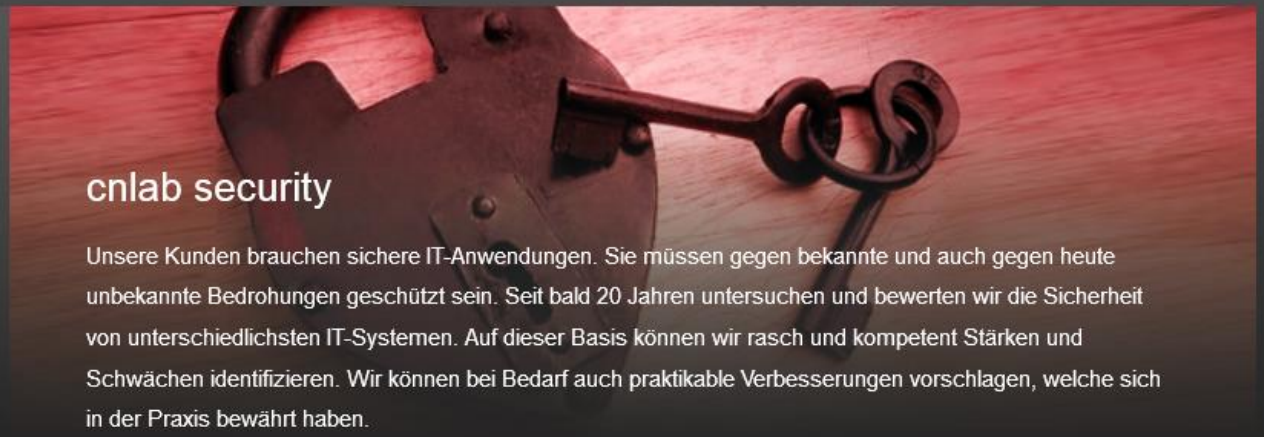
Contact | Sitemap | SFT Suche nach... DE EN

cnlab

information technology research performance software security

Security

- Produkte und Dienstleistungen
  - Application-Security
  - Mobile-Security
  - Netzwerk-Security
  - Secure File Transfer (SFT)
- Publikationen
- Über cnlab security
  - Mitarbeiter
  - Kunden
  - Kontakt



cnlab security

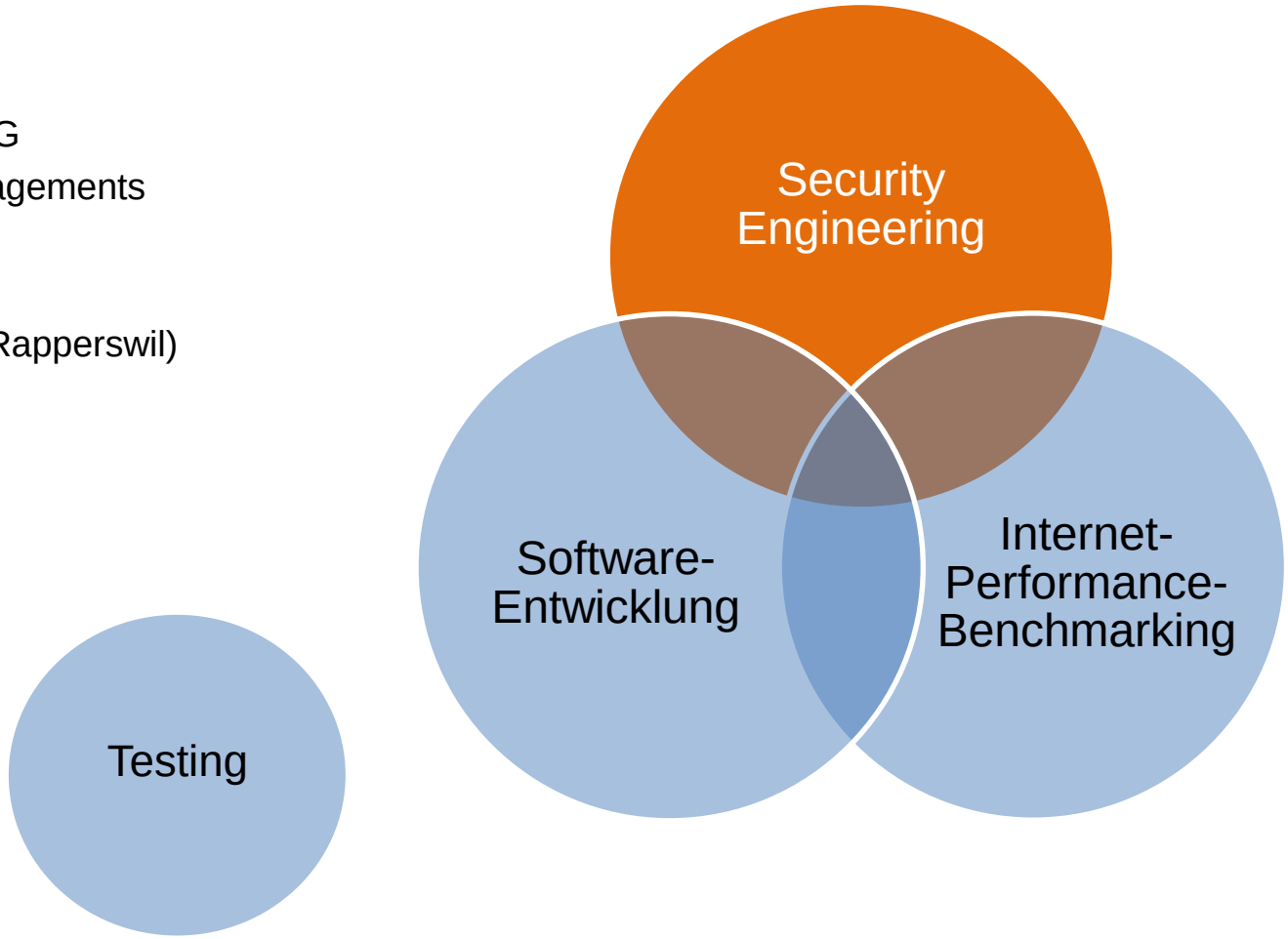
Unsere Kunden brauchen sichere IT-Anwendungen. Sie müssen gegen bekannte und auch gegen heute unbekannte Bedrohungen geschützt sein. Seit bald 20 Jahren untersuchen und bewerten wir die Sicherheit von unterschiedlichsten IT-Systemen. Auf dieser Basis können wir rasch und kompetent Stärken und Schwächen identifizieren. Wir können bei Bedarf auch praktikable Verbesserungen vorschlagen, welche sich in der Praxis bewährt haben.

News

cnlab

cnlab Organisation
- 14 Ingenieure
- Sitz Rapperswil / SG
- Im Besitz des Managements

cnlab Partner
- HSR (Hochschule Rapperswil)
- ETH Zürich



Mobile Security Erfahrungen von cnlab

Prüfungen iOS- und Android-Konfiguration

- Mobile Device Management (MDM) Setup
- VPN-Konfiguration

Prüfungen Mobile-Apps

- Polizei-Apps
- Apps für Finanzdienstleister (E-Banking)

Prüfungen Applikationen und IT-Infrastrukturen

- Netzwerk-Architekturen
- OS- und DB-Hardening
- Web-Anwendungen

Kunden
im Sicherheits-Bereich

Financial Services:
- Credit Suisse
- Migros Bank
- Raiffeisenbank
- SGKB
- SIX
- ZKB

IT-Betreiber:
- Swisscom
- Inventx

Verwaltungen, Öffentliche Dienste:
- Kantonale Verwaltungen
  (BE, BL, SG, SZ, TG, VD, ZG, ZH)
- Kantons- und Stadtpolizeien

Software- und Komponenten-Anbieter:
- Crealogix
- Kobil

Weitere Referenzen können auf Anfrage bekannt gegeben werden.

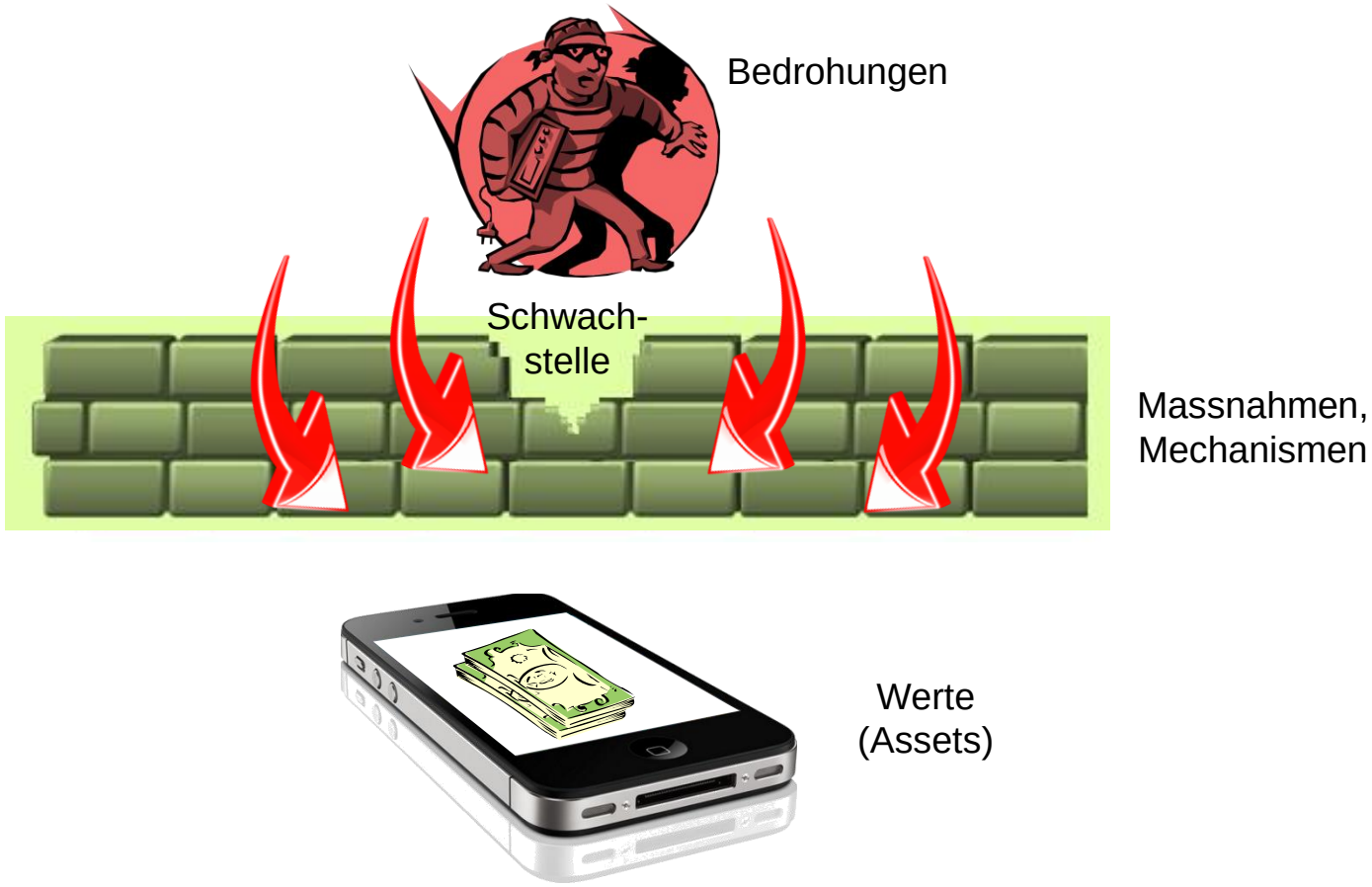
Agenda

Vorstellung cnlab

Mobile Security
- Sicherheitsmechanismen
  Geräte PIN, Speicherverschlüsselung, Update-Funktionen
- Zugriff auf Geräte
  Umgehung der Sicherheitsmechanismen, Zugriff auf E-Mail-Daten, «Back-Doors»
- Demo
- Ausblick iOS8/Android 5

Unterstützung durch cnlab
- Was cnlab kann
- Was cnlab nicht kann

Einführung Risiken und Sicherheitsmechanismen



Risiko = Eintrittswahrscheinlichkeit * Schadensausmass

Sicherheitsmechanismen

- Geräte-PIN
- Speicherverschlüsselung
- Rechtesteuerung
- «Sandbox»
- Kontrolle der Apps im Store
- Update-Funktionalität

Sicherheits-Mechanismen erschweren forensische Untersuchungen!

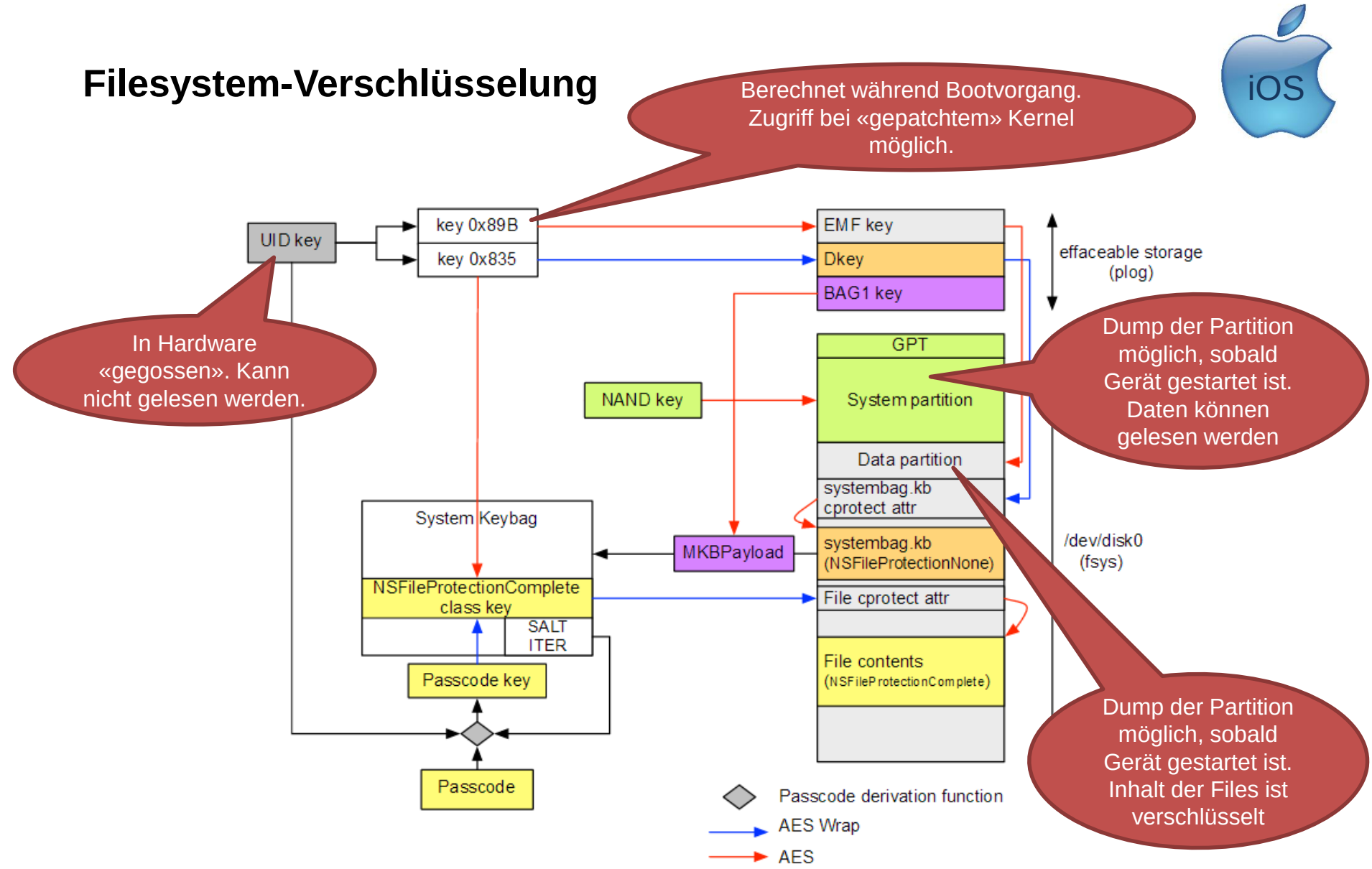
Geräte-PIN

- Verhindert Verwendung des Gerätes
- Verhindert Zugriff auf Daten via Schnittstellen (z.B. USB)
- Verhindert ausgeschaltetes Gerät zu booten (nur bei Android mit verschlüsseltem Gerätespeicher)

Ohne PIN ist kein Zugriff auf Geräte möglich*

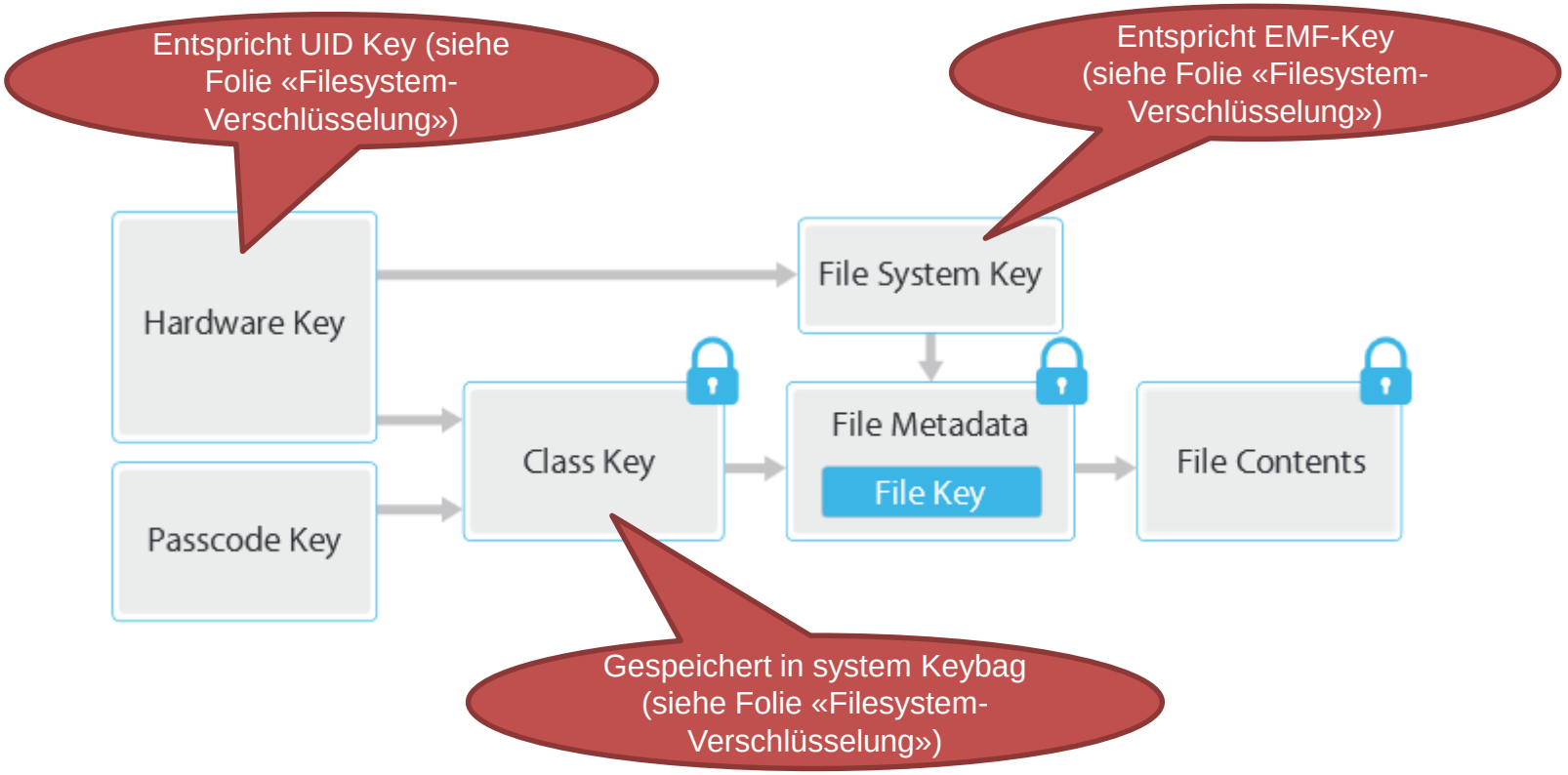
*Ausnahme: Zugriff auf Speicherkarte, «gepairte» Geräte, Geräte mit Jailbreak

Filesystem-Verschlüsselung



Quelle: http://code.google.com/p/iphone-dataprotection/wiki/EncryptionKeys

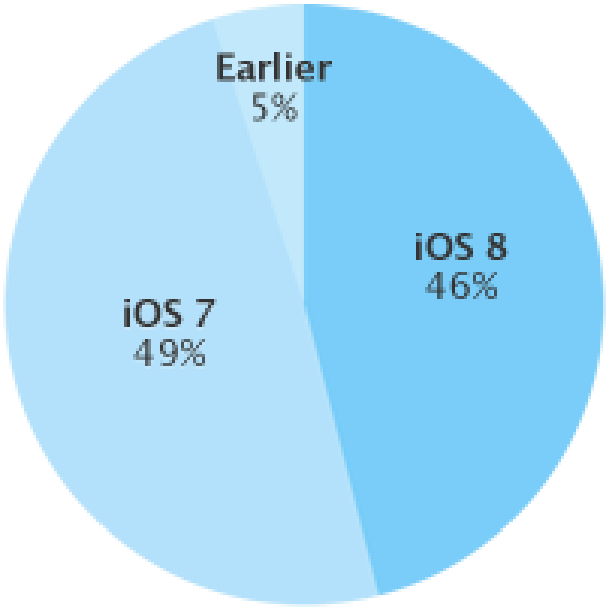
File-Verschlüsselung



Quelle: http://images.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf

Update-Funktionalität – Verteilung installierter OS-Versionen

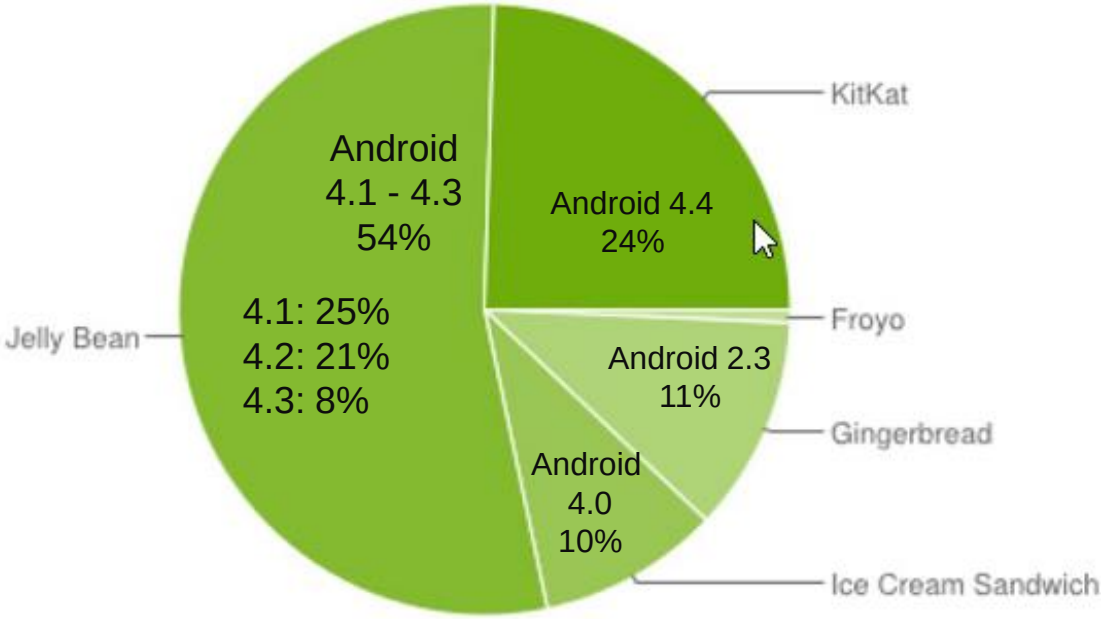
iOS



Stand 21. September 2014

Quelle: https://developer.apple.com/support/appstore/

Android



Stand 9. September 2014

Quelle: http://developer.android.com/about/dashboards/index.html

Übersicht iOS-Gerätegenerationen

Generation	Verfügbar seit	Gerätebezeichnungen
Legacy-Geräte (<A4)	07/2007	iPhone3, iPhone3GS
A4-Geräte	07/2010	iPhone4, iPad
A5-Geräte	04/2011	iPhone4S, iPad mini (1st gen), iPad2
A5X-Geräte	04/2012	iPad (3rd gen)
A6-Geräte	09/2012	iPhone 5, iPhone 5C
A6X-Geräte	11/2012	iPad (4th gen)
A7-Geräte (64-Bit)	10/2013	iPhone 5S
A8-Geräte (64-Bit)	09/2014	iPhone 6, iPhone 6 plus

«Alte» Geräte

«Aktuelle» Geräte

Jailbreak/Rooting

- iOS → Jailbreak, Android → Rooting
- Installation erfolgt meist durch Ausnutzung einer Schwachstelle
- Für aktuelle Geräte verfügbar
- Gespeicherte Daten gehen im Normalfall nicht verloren
- Deaktiviert Sicherheitsmechanismen

Jailbreak und Rooting-Vorgang nimmt Änderungen am Gerät vor!
Für forensische Untersuchungen nur bedingt geeignet.
Auf Geräte mit einem Jailbreak oder Root-Zugang kann für Untersuchungen besser zugegriffen werden.

Datenvorkommen / Zugänglichkeiten

Smartphone

Cache (flüchtig)	Speicher auf wechselbaren Medien (nicht flüchtig)
Interner Speicher (flüchtig)	Interner Speicher (nicht flüchtig)

Schlüsselspeicher
(z.B. UID bei iOS-Geräten)

Cloud-Speicher
(z.B. iCloud, Google Drive, Dropbox)

Anwendungsserver
(z.B. E-Mail-Server)

Sicherungskopie
(Backup)

Speicherung der Daten unterschiedlicher E-Mail-Dienste

	Exchange (ActiveSync)	Gmail (IMAP)	Yahoo (POP)	Outlook.com (via App)
Daten auf E-Mail-Server	X	X	(X)	(X)
Daten in Cloud-Backup	-	-	-	(X)
Daten im lokalen Backup	-	-	-	(X)
Daten auf Gerät	X	X	X	X
Zugriff auf gelöschte E-Mails auf dem Gerät	(X)	(X)	(X)	(X)

X - Trifft zu
(X) - Trifft beschränkt zu

Backup von E-Mails auf iOS-Geräten

- Mail-Accounts (Benutzername und Passwort) sind im lokalen Backup und im iCloud-Backup gespeichert.

- Mails werden weder im lokalen Backup noch im iCloud-Backup gespeichert.

Speicherung der Daten unterschiedlicher E-Mail-Dienste

	Exchange (ActiveSync)	Gmail (IMAP)	Yahoo (POP)	Outlook.com (via App)
Daten auf E-Mail-Server	X	X	(X)	(X)
Daten in Cloud-Backup	-	-	-	(X)
Daten im lokalen Backup	(X)	(X)	(X)	(X)
Daten auf Gerät	X	X	X	(X)
Zugriff auf gelöschte E-Mails auf dem Gerät	(X)	(X)	(X)	(X)

X - Trifft zu
(X) - Trifft beschränkt zu

E-Mail-Dienste (Datenspeicherung)

- E-Mails bleiben häufig auf dem E-Mail-Server gespeichert (z.B. IMAP, ActiveSync Exchange)
- Lokale Kopie der E-Mails sind in einer Datenbank auf dem Mobilgerät gespeichert. Attachments sind im Filesystem abgelegt
- Beim Löschen von E-Mails wird der Eintrag in der Datenbank als gelöscht markiert. Attachments werden nicht (unmittelbar) gelöscht.
- E-Mails sind typischerweise nicht in Backups.

E-Mails und Attachments sind auch nach dem Löschen noch für eine unbestimmte Dauer auf dem Gerät gespeichert und können ausgelesen werden. Manipulationen am Gerät können aber dazu führen, dass diese Daten überschrieben werden.

Vorgehen - Auslesen von E-Mails

Problemstellung: Auf aktuellen iOS-Geräten lassen sich E-Mails mit gängigen Forensik-Tools (z.B. XRY) nicht auslesen

- Über USB besteht keine Möglichkeit diese Daten auszulesen

Demo

Zusammenfassung - Auslesen von E-Mails

Vorgehen:

- Jailbreak installieren
- Direkter Zugriff auf Gerät via SSH
- Kopieren der E-Mail-Datenbank
- Auswertung der E-Mail-Datenbank

«Back-Doors» in iOS

- White Paper: Identifying back doors, attack points, and surveillance mechanisms in iOS devices (2014) (Jonathan Zdziarski, http://www.zdziarski.com/blog/?p=3705)
- iOS-Geräte bieten Schnittstelle auf diverse Dienste
  - Zugriff auf Photos, SMS, Adressbuch, Geolocation-Cache
    - Auch ohne das iTunes-Passwort bekannt sein muss!
  - Sniffen von Netzwerkverkehr
  - Verwendung der Schnittstellen setzen keinen Jailbreak voraus
- Zugriff via USB und Netzwerk (TCP-Port 62078)
- Definition gemäss Apple: «Diagnose»-Schnittstelle
- Wird vermehrt durch Forensic-Tools (z.B. Oxygen) verwendet
- Verwendung stark eingeschränkt in iOS8
  - Meist nur noch Zugriff via USB

Zugang zu iOS-Gerät und «gepairtem» System erlaubt Lesen von einigen Daten ohne Kenntnisse der Geräte-PIN und des iTunes-Passwortes.

Verfügbarkeit des «gepairten» Systems (PC) ist häufig relevant.

Was erwarten wir von iOS8

- Verfügbar seit 17.9.2014
- Schnelle Verteilung auf Geräten
- Diverse Schwachstellen behoben
- Keine fundamentalen Änderungen gegenüber iOS7
- Jailbreak «in Kürze» verfügbar

iOS 8 hat auf forensische Auswertungen beschränkten Einfluss

Was erwarten wir von Android L (5)

- Verfügbar im Herbst 2014
- Vorabversion für Entwickler verfügbar
- Langsame Verteilung auf Geräten
- Per Default Datenpartition verschlüsselt
- Rooting wird weiterhin möglich sein

Android L hat auf forensische Auswertungen beschränkten Einfluss.
Es braucht Anpassungen durch die Forensik SW-Lieferanten.

Agenda

Vorstellung cnlab

Mobile Security

- Sicherheitsmechanismen
  Geräte PIN, Speicherverschlüsselung, Update-Funktionen
- Zugriff auf Geräte
  Umgehung der Sicherheitsmechanismen, Zugriff auf E-Mail-Daten, «Back-Doors»
- Demo
- Ausblick iOS8/Android 5

Unterstützung durch cnlab

- Was cnlab kann
- Was cnlab nicht kann

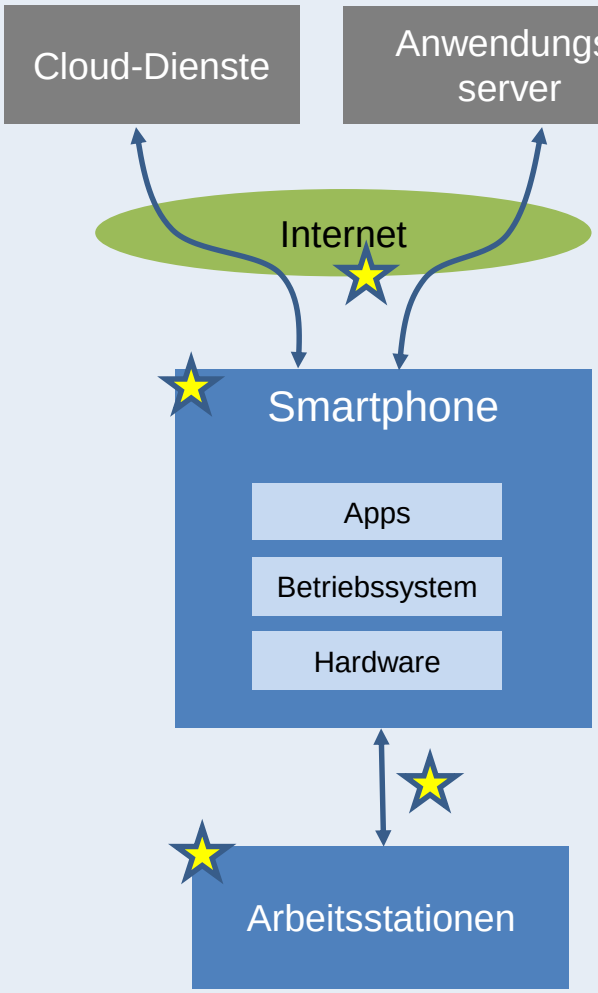
Unterstützung durch cnlab 1/2

Forensische Tools nützen Schwachstellen der Geräte aus.

Wir kennen die Schwachstellen und können dadurch

- beurteilen, weshalb gewisse Dinge funktionieren und andere nicht
- eine Aussage machen, in welchen Fällen Daten ausgelesen werden können und in welchen nicht
- gezielt Daten von den Geräten auslesen

Unterstützung durch cnlab 2/2



Sicherheitsprüfungen von Diensten

Analyse Netzwerkverkehr

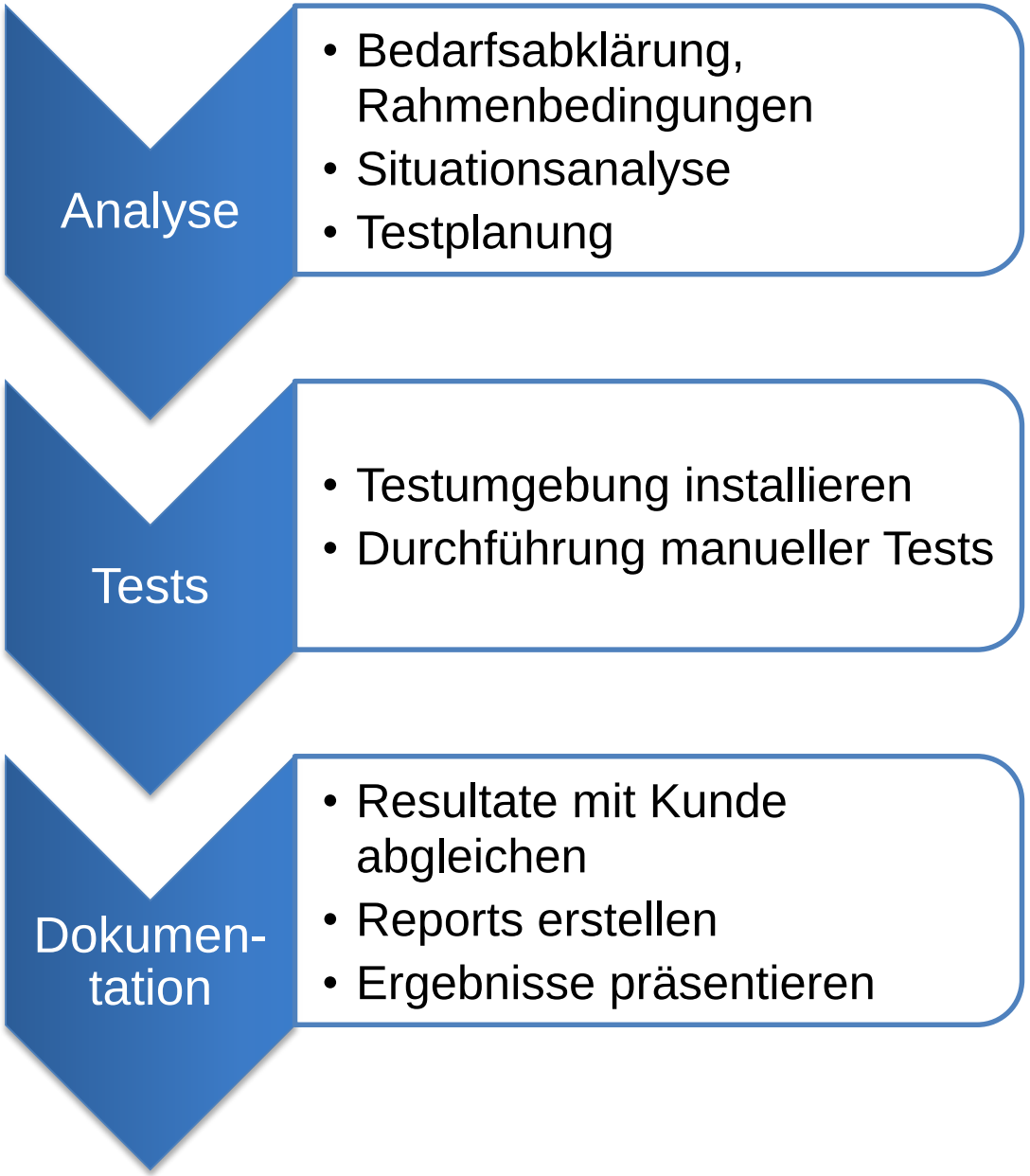
Daten-Analyse von Smartphones

Sicherheitsprüfungen von Apps

Sicherheitsprüfungen von Smartphones

Sicherheitsprüfungen von Arbeitsstationen

Standardvorgehen



Was cnlab nicht kann

- Wir können keine Hardware-Manipulationen an Geräten durchführen.

- Wir können keine Untersuchungen an Geräte vornehmen und dabei sicherstellen, dass keine Änderungen an den Geräten stattfinden.

Danke

Christian Birchler
christian.birchler@cnlab.ch
+41 55 214 33 40

René Vogt
rene.vogt@cnlab.ch
+41 55 214 33 31