ITMC Jahresabschluss 2014

cnlab - Mobile Security

iOS, Android

Zürich-Regensdorf, 4. Dezember 2014

Christian Birchler, René Vogt

Folien: www.cnlab.ch → Publikationen

Agenda

- Vorstellung cnlab

Verbreitung der Smartphones

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

cnlab

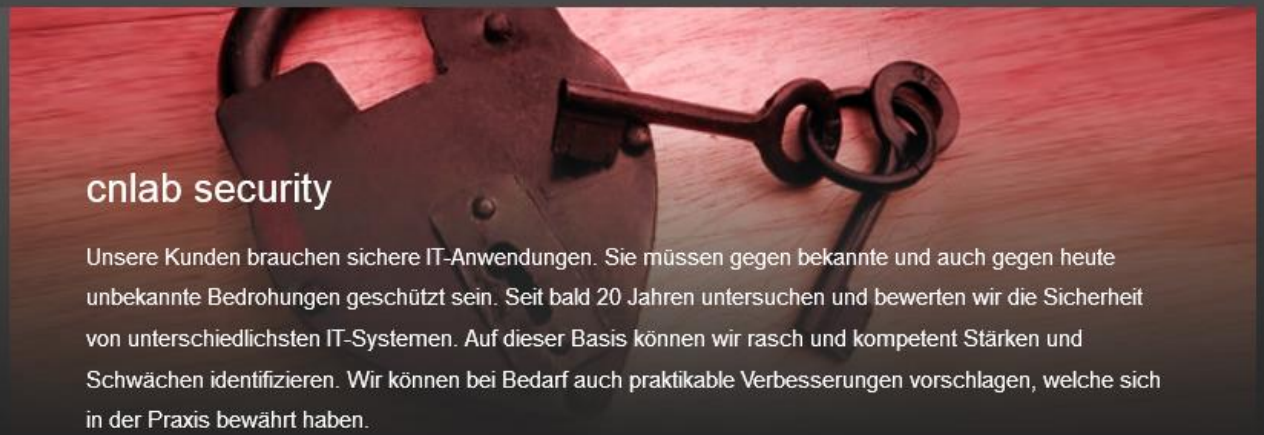
information technology research performance software security

Security

Produkte und Dienstleistungen
- Application-Security
- Mobile-Security
- Netzwerk-Security
- Secure File Transfer (SFT)

Publikationen

Über cnlab security
- Mitarbeiter
- Kunden
- Kontakt



cnlab security

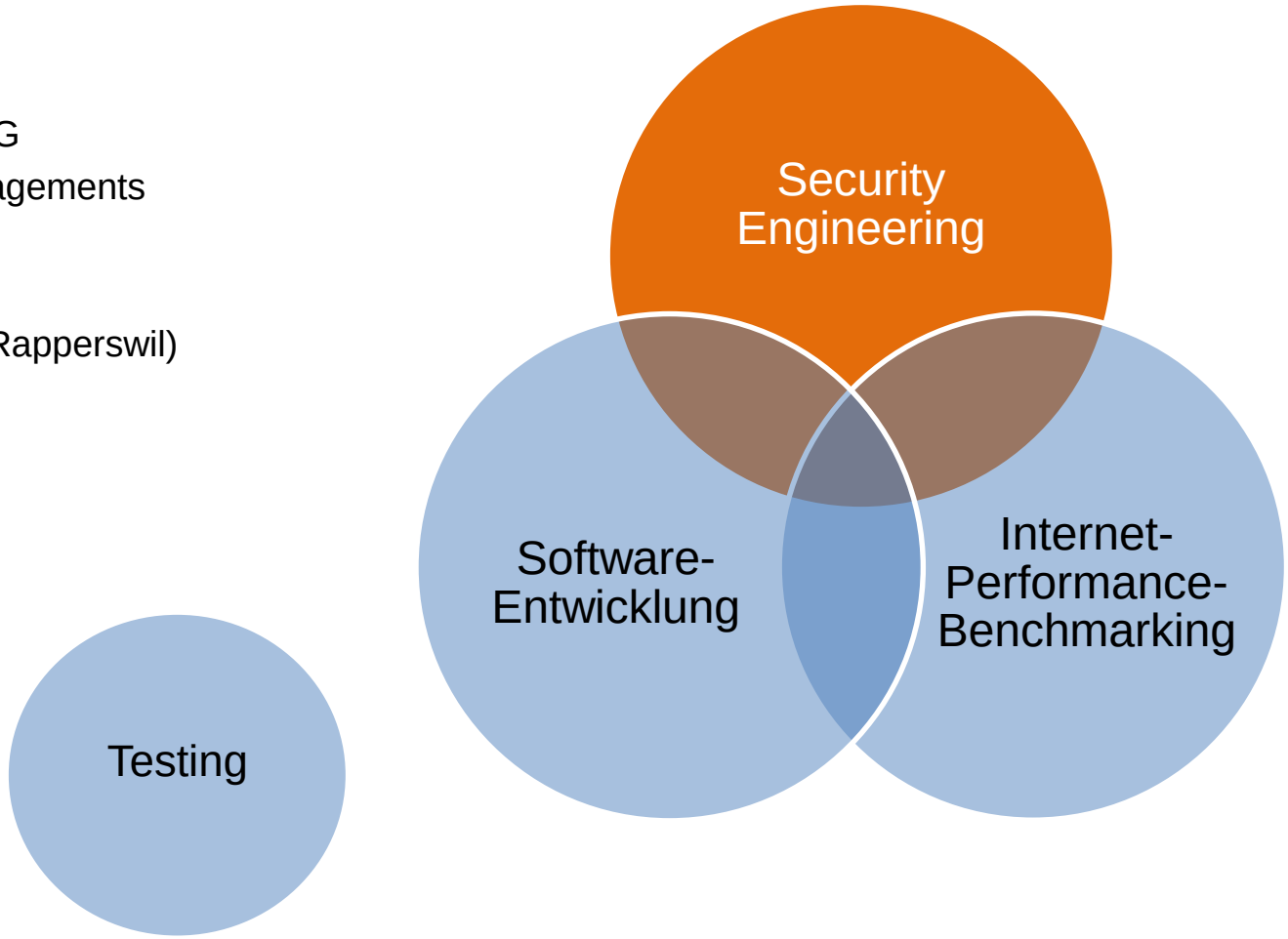
Unsere Kunden brauchen sichere IT-Anwendungen. Sie müssen gegen bekannte und auch gegen heute unbekannte Bedrohungen geschützt sein. Seit bald 20 Jahren untersuchen und bewerten wir die Sicherheit von unterschiedlichsten IT-Systemen. Auf dieser Basis können wir rasch und kompetent Stärken und Schwächen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

News

cnlab

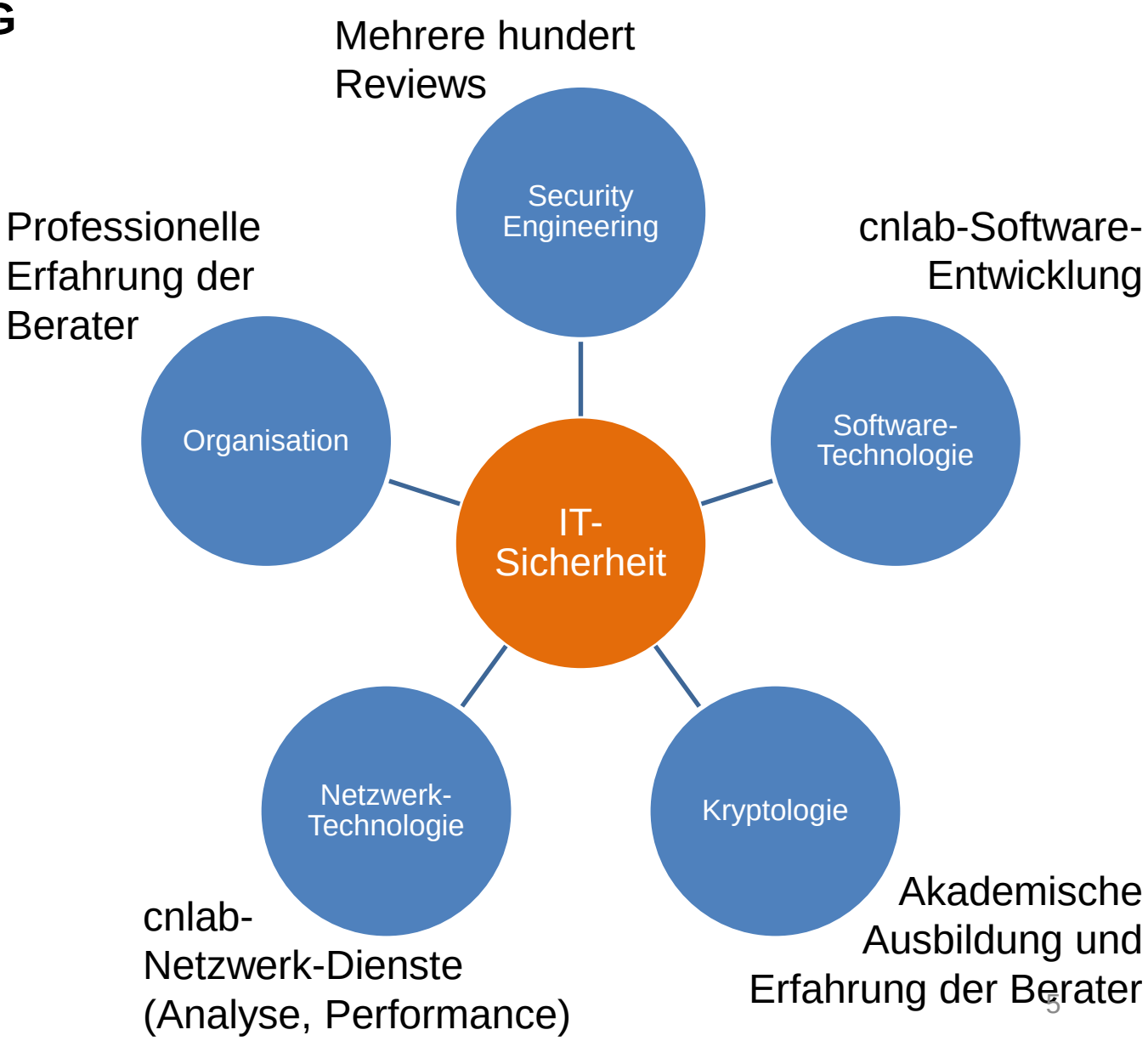
cnlab Organisation
- 14 Ingenieure
- Sitz Rapperswil / SG
- Im Besitz des Managements

cnlab Partner
- HSR (Hochschule Rapperswil)
- ETH Zürich



Cnlab security AG

Sicherheit im Mittelpunkt



Typische Prüfungen im Mobile Umfeld

Apps

- Sicherheit der App (Authentisierung, Autorisierung, Session-Management), bekannte Schwachstellen, OWASP Top Ten Risks
- Schutz der Daten
- Prozesse (Betrieb, Verteilung, Aktualisierung)

Smartphone-Konfigurationen

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

IT-Infrastrukturen

- Middleware (Web-Services und Anwendungen)
- OS- und DB-Sicherheit
- Netzwerk-Architekturen

Agenda

Vorstellung cnlab

Verbreitung der Smartphones

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

Verbreitung Smartphones – Welt

Weltbevölkerung 2014: 7.2 Milliarden

66% der Mobile Phones sind Smartphones

Worldwide Device Shipments by Segment (Thousands of Units)

Device Type	2013	2014	2015
Traditonal PCs (Desk-Based and Notebook)	296,131	276,221	261,657
Ultramobiles, Premium	21,517	32,251	55,032
PC Market Total	**317,648**	**308,472**	**316,689**
Tablets	206,807	256,308	320,964
Mobile Phones	1,806,964	1,862,766	1,946,456
Other Ultramobiles (Hybrid and Clamshell)	2,981	5,381	7,645
Total	**2,334,400**	**2,432,927**	**2,591,753**

Source: Gartner (June 2014)

Anteil Windows Phones
2014: 4%
2018: 10%

Android zu iOS = 4 zu 1

Worldwide Device Shipments by Operating System (Thousands of Units)

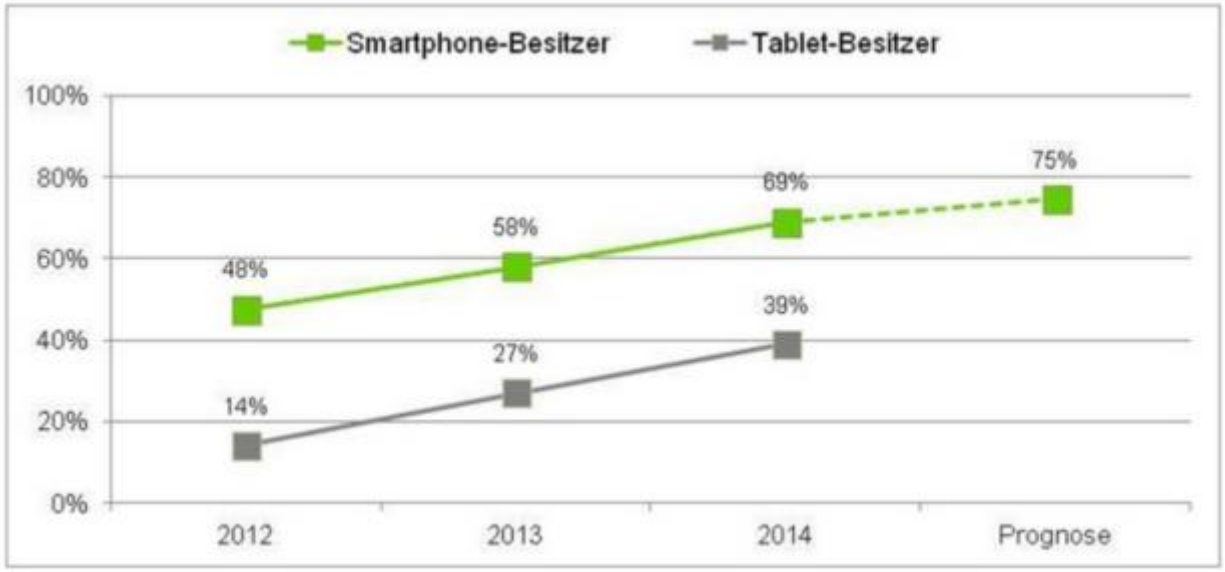
Operating System	2013	2014	2015
Android	898,944	1,168,282	1,370,893
Windows	326,060	333,419	373,694
iOS/Mac OS	236,200	271,115	301,349
Others	873,195	660,112	545,817
Total	**2,334,400**	**2,432,927**	**2,591,753**

Shipments include mobile phones, ultramobiles (including tablets) and PCs

Source: Gartner (June 2014)

Quelle: Gartner

Verbreitung Smartphones – CH



Anzahl Besitzer in der Schweiz, Quelle: Comparis.ch

OS Verteilung CH
Android: 39%
iOS: 56%

Verwendete Clients im E-Banking Umfeld:
80% Desktop
15% iOS
5% Android

Quelle: verschiedene CH-Banken

Agenda

Vorstellung cnlab

Verbreitung der Smartphones

Mobile Security

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

Eingebaute Sicherheitsmechanismen «Hardware»

Geräte-PIN

- Schutz gegen interaktive Verwendung des Gerätes
- Schutz gegen Zugriff über andere Schnittstellen (z.B. USB)

Schlüsselspeicher (Keychain)

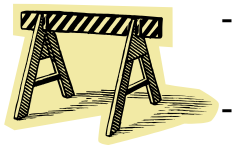
- Sichere Ablage von «sensitiven» Informationen
- Schutz gegen unberechtigten Zugriff auf dem Gerät, im Backup, usw.

Speicherverschlüsselung

- Schutz gegen physischen Zugriff auf den Speicher
- Schutz gegen Zugriff mit modifiziertem Betriebssystem

Eingebaute Sicherheitsmechanismen «Betriebssystem»

Zugriffskontrolle auf OS-Stufe



- Optimale Trennung von Anwendungen auf Betriebssystem-Stufe
- Einsatz von Betriebssystem-Benutzern mit eingeschränkten Rechten

Update-Funktionalität

- Schnelle Aktualisierung von Betriebssystem und Apps

Integritätskontrolle auf OS-Stufe

- Schutz gegen «Rooting» / «Jailbreaking»
- Sicherstellen, dass alle Sicherheitsmechanismen intakt sind

Einagebaute Sicherheitsmechanismen «Apps»

Sandbox

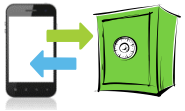
- Logische Trennung (Separierung) von Apps
- Zugriffe auf Betriebssystem-Funktionen und Hardware einschränken

Integritätskontrolle Apps

- Inhaltliche und technische Kontrolle der Apps im Store
- Verwendung von digitalen Signaturen

Rechtesteuerung

- Vergabe von Zusatzrechten durch Benutzer (z.B. Zugriff auf GPS, Internet)



Backup

- Regelmässige Erstellung von Backups mit einfacher Restore-Möglichkeit
- Sichere Ablage der Backup-Daten

App Store - Integritätskontrolle Apps

Apple

- Prüfung:
  - Verwendete API, Methoden, Funktionen
  - Angeforderte Berechtigungen (Sensoren und Daten)
  - Inhalte
- Genaue Prüftätigkeit nicht bekannt
- Prüfung dauert typischerweise 10 Tage (bevor App im Store verfügbar ist)

Google (Play-Store)

- Automatisierte Prüfung
- Genaue Prüftätigkeit nicht bekannt
- Prüfung dauert typischerweise wenige Stunden (nachdem App im Store verfügbar ist)

Geräte-PIN

- Verhindert Verwendung des Gerätes
  - Blockierung nach einer Anzahl Fehlversuchen

- Verhindert Zugriff auf Daten via Schnittstellen (z.B. USB)

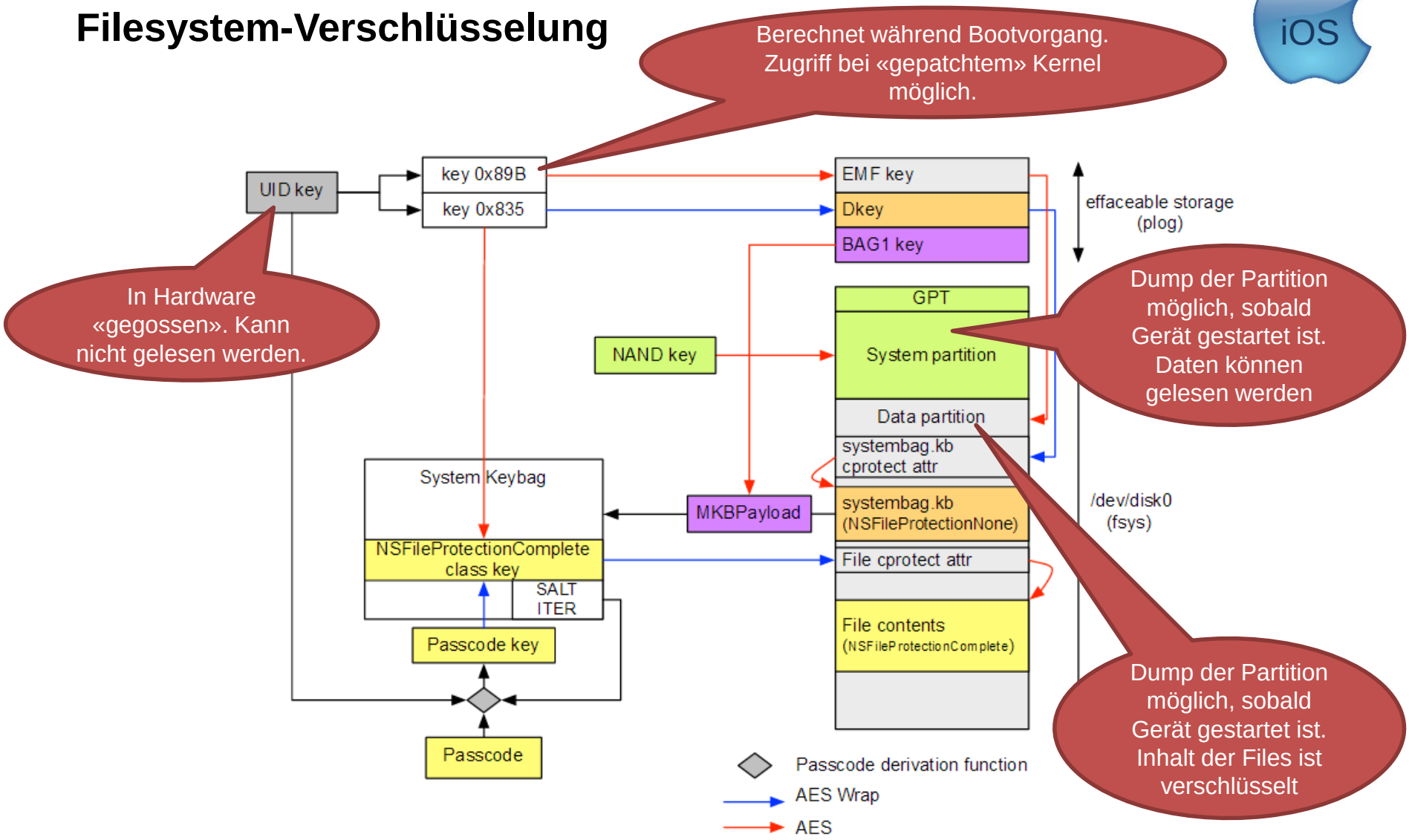
- Verhindert ausgeschaltetes Gerät zu booten (nur bei Android mit verschlüsseltem Gerätespeicher)

Ohne PIN ist kein Zugriff auf Geräte möglich*

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

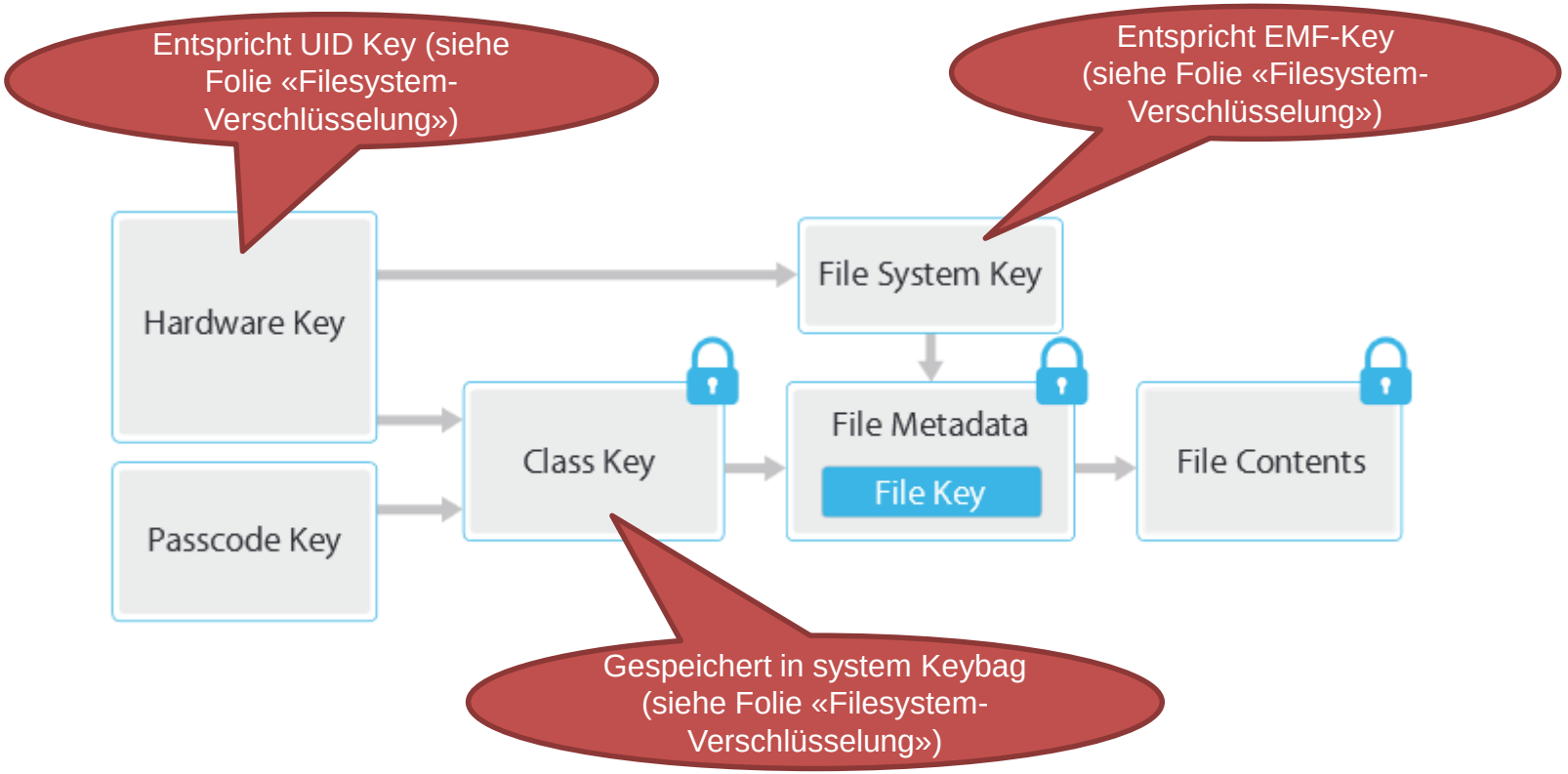
Filesystem-Verschlüsselung

iOS



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

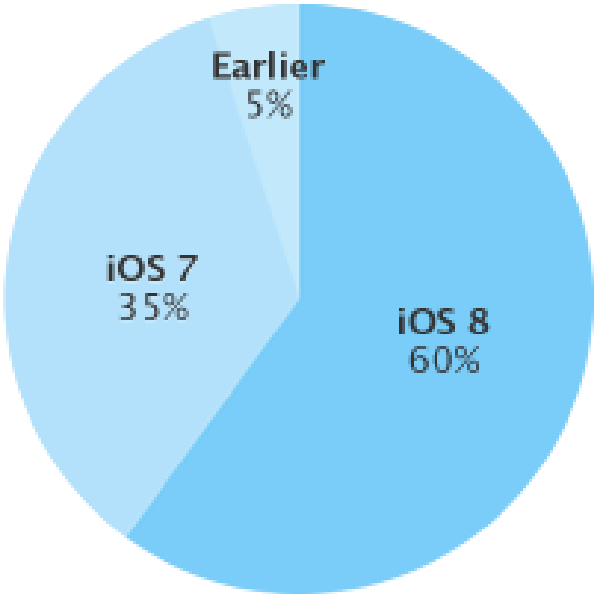
File-Verschlüsselung



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

Update-Funktionalität – Verteilung installierter OS-Versionen

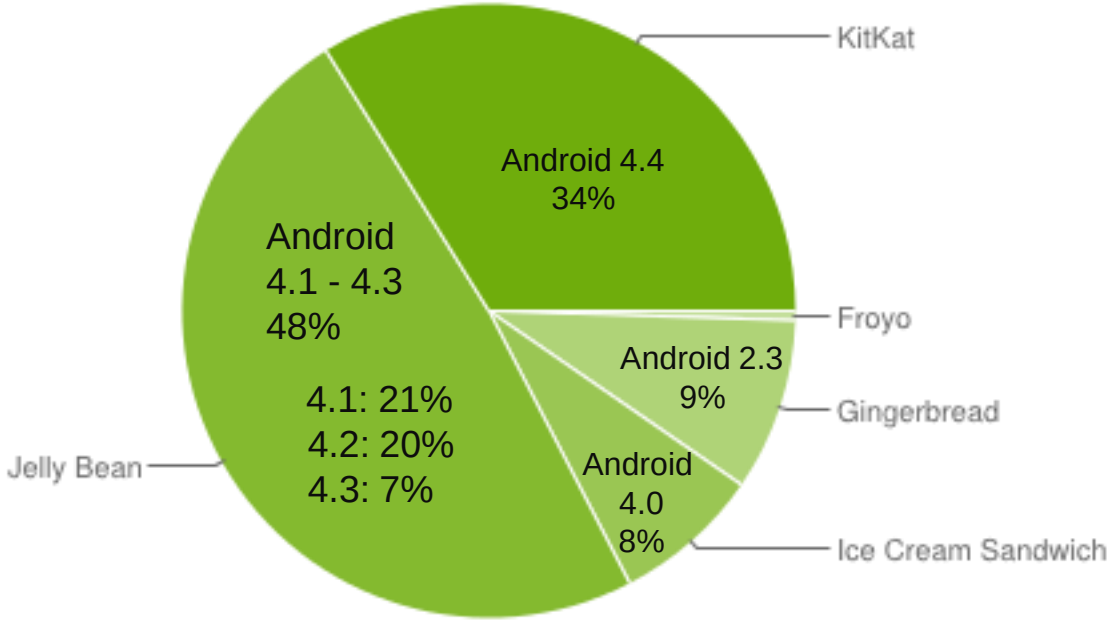
iOS



Stand 24. November 2014

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

Android



Stand 3. November 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 (via USB) 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

Backup von E-Mails auf Android-Geräten

- Es werden keine Mail-Accounts (Benutzername und Passwort) und keine Mails im Google-Cloud-Backup gespeichert.
  - Ausnahme bei GMail
- Lokale Backups (via USB) sind bei Android nur beschränkt möglich und können Mail-Accounts und Mails enthalten.

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.

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.

«Masque Attack» – Bekannte Schwachstellen

- Idee: Ersetzen einer bereits installierten App (z.B. E-Banking-App) mit einer «Fake»-App
  - Unter Verwendung eines fremden «Bundle-Identifiers»
- «Fake»-App hat Zugriff auf bestehende App-Daten (z.B. Schlüssel)
  - Kein Zugriff möglich auf bestehende Keychain-Einträge
- «Fake»-App kann Phising-Seite präsentieren
- Angriff benötigt Sideloading
  - Möglich mit Enterprise-Zertifikat oder Entwickler-Zertifikat (Beschränkt auf bekannte UUIDs)
- Bisher (iOS8.1.1) nicht gepatched

Keine Apps aus fremden Quellen installieren

Android-«Signaturen» – Bekannte Schwachstellen

- Signaturprüfung bei Android
  - Alle Apps müssen signiert sein
  - Beim Update einer App muss dasselbe Zertifikat verwendet werden
- Schwachstelle in Signaturprüfung (Paket-Installer)
  - Modifikationen an App-Dateien werden nicht detektiert
  - Erlaubt das Ersetzten von Systemanwendungen (-> höhere Berechtigungen)
- Angriff benötigt Sideloading
- In vielen Geräten nicht gepatched

Keine Apps aus fremden Quellen installieren

Ausblick iOS8

- Verfügbar seit 17. September 2014
- Schnelle Verteilung auf Geräten
- Diverse Schwachstellen behoben
- Keine fundamentalen Änderungen gegenüber iOS7
- Jailbreak verfügbar

iOS 8 hat auf forensische Auswertungen beschränkten Einfluss

Ausblick Android 5

- Verfügbar seit Oktober 2014
- Langsame Verteilung auf Geräten
- Sicherheitstechnische Neuerungen
  - Datenpartition per Default verschlüsselt
  - Einsatz von SELinux
  - Data separation («container»-Lösung)
  - Mehrbenutzer Unterstützung
  - Kill Switch
- Rooting wird erschwert, aber wird weiterhin möglich sein

Android 5 hat auf forensische Auswertungen beschränkten Einfluss.
Es braucht Anpassungen durch die Forensik SW-Lieferanten.

Fazit - Würden Sie?

beunruhigt sein, wenn Sie Ihr Smartphone im Zug liegen gelassen haben?

eine App installieren, welche nicht über den offiziellen App-Store publiziert wurde?

Ihr Smartphone an einer öffentlichen Ladestation anschliessen?

Sie wollen ein sicheres Smartphone –
Entscheiden Sie sich für ein Apple oder Android Gerät?

Ein **aktuelles und gut konfiguriertes** Smartphone bietet einen guten Schutz gegen unberechtigte Datenzugriffe.

Danke

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

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