

Cnlab / CSI 2011

Das Sicherste

Agenda

- Was heisst sicher?
- Wie funktionieren die Smart-Phones?
- Der Vergleich

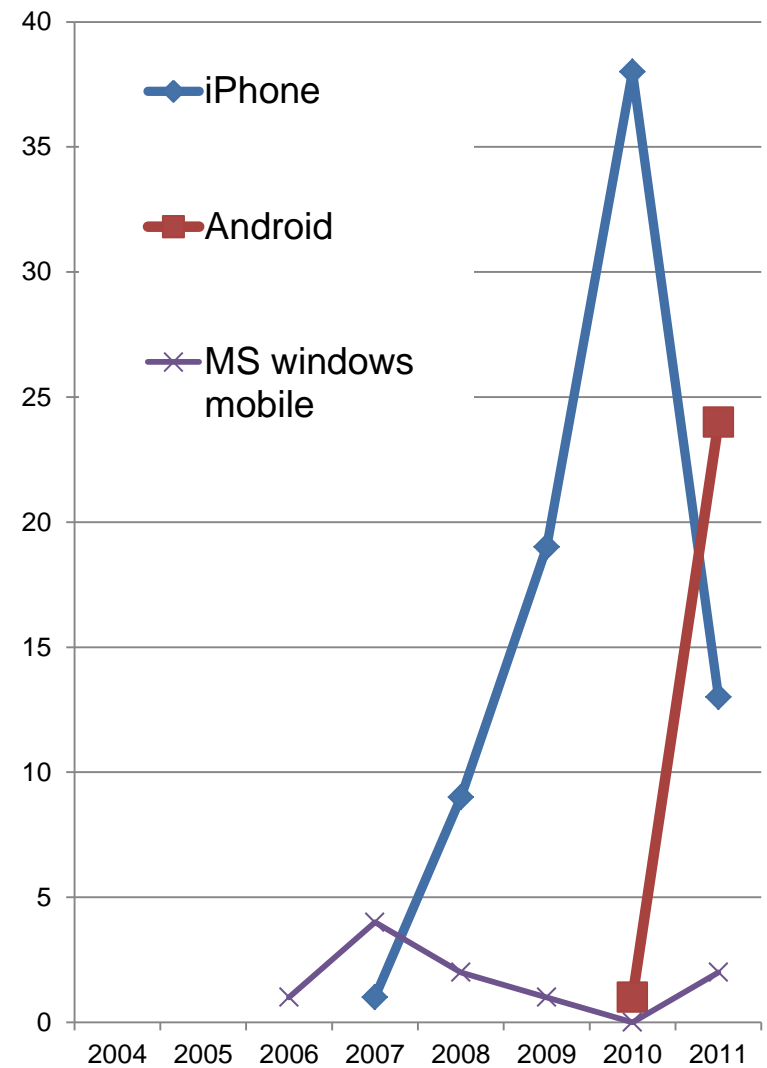
Was heisst sicher

Vulnerability-Statistik

Quelle:

<http://nvd.nist.gov/>

(Stand 12.8.2011)



OWASP Mobile-Projekt

Top 10 Mobile Risks Draft 0.1

- Insecure or unnecessary client-side data storage
- Lack of data protection in transit
- Personal data leakage
- Failure to protect resources with strong authentication
- Failure to implement least privilege authorization policy
- Client-side injection
- Client-side DOS
- Malicious third-party code
- Client-side buffer overflow
- Failure to apply server-side controls

Quelle: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

ISO 27002 als Sicherheits-Referenz

1. Weisungen und Richtlinien zur Informationssicherheit
2. Organisatorische Sicherheitsmassnahmen und Managementprozess
3. Verantwortung und Klassifizierung von Informationswerten
4. Personelle Sicherheit
5. Physische Sicherheit und öffentliche Infrastruktur
6. Netzwerk- und Betriebssicherheit (Daten und Telefonie)
7. Zugriffskontrolle
8. Systementwicklung und Wartung
9. Umgang mit Sicherheitsvorfällen
10. Notfallvorsorgeplanung
11. Einhaltung rechtlicher Vorgaben, der Sicherheitsrichtlinien und Überprüfungen durch Audits

Welche Daten sind eigentlich heikel in einem Smart-Phone?

Komponenten	Private Anwender	Professionelle Anwender
E-Mails, SMS	H	H
Termine	M	H
Kontakte	M	H
Daten von Apps (Geo, Notizen, Fotos)	M	H
Synchronisierte Daten	T	H
Passwörter		
- iPhone	T	T
- Private Konten (z.B. Shop)	M	M
- Firmenkonten (z.B. AD-Login)	(H)	H
Backup-Dateien	M	H

Sensibilität
Hoch
Mittel
Tief

Wie funktionieren die Smart- Phones (Fokus Sicherheit)

5. Physische Sicherheit und öffentliche Infrastruktur

- Viren und Malware
 - Noch **weniger Schadcode** als im PC-Umfeld
- Verwendung im öffentlichen Raum
 - **Ausspähen** von Eingaben (Passwort) und Ausgaben
- Zugang zu laufenden Geräten
 - Angreifer kann auf **Speicherinhalt** zugreifen
 - Transparente Schutzmechanismen sind «**offen**»

6. Netzwerk- und Betriebssicherheit (1): Active-Sync-Policing

Einstellung	iPhone	Windows Phone 7	Android 2.2
AllowNonProvisionableDevices	Green	Green	Yellow
AlphanumericDevicePasswordRequired	Green	Yellow	Green
AttachmentsEnabled	Yellow	Yellow	Yellow
DeviceEncryptionEnabled	Green	Green	Green
RequireStorageCardEncryption	Yellow	Yellow	Yellow
DevicePasswordEnabled	Green	Green	Green
PasswordRecoveryEnabled	Yellow	Yellow	Yellow
DevicePolicyRefreshInterval	Green	Yellow	Yellow
AllowSimpleDevicePassword	Green	Green	Yellow
MaxAttachmentSize	Yellow	Yellow	Yellow
WSSAccessEnabled	Yellow	Yellow	Yellow
UNCAccessEnabled	Yellow	Yellow	Yellow
MinDevicePasswordLength	Green	Green	Green
MaxInactivityTimeDeviceLock	Green	Green	Green
MaxDevicePasswordFailedAttempts	Green	Green	Green
DevicePasswordExpiration	Green	Green	Yellow
DevicePasswordHistory	Green	Green	Yellow
AllowStorageCard	Yellow	Yellow	Yellow
AllowCamera	Green	Yellow	Yellow
RequireDeviceEncryption	Green	Yellow	Yellow
AllowUnsignedApplications	Yellow	Yellow	Yellow
AllowUnsignedInstallationPackages	Yellow	Yellow	Yellow

Einstellung	iPhone	Windows Phone 7	Android 2.2
AllowWiFi	Yellow	Yellow	Yellow
AllowTextMessaging	Yellow	Yellow	Yellow
AllowPOPIMAPEmail	Yellow	Yellow	Yellow
AllowIrDA	Yellow	Yellow	Yellow
RequireManualSyncWhenRoaming	Green	Yellow	Yellow
AllowDesktopSync	Yellow	Yellow	Yellow
AllowHTMLEmail	Yellow	Yellow	Yellow
RequireSignedSMIMEMessages	Yellow	Yellow	Yellow
RequireEncryptedSMIMEMessages	Yellow	Yellow	Yellow
AllowSMIMESoftCerts	Yellow	Yellow	Yellow
AllowBrowser	Green	Green	Green
AllowConsumerEmail	Yellow	Yellow	Yellow
AllowRemoteDesktop	Yellow	Yellow	Yellow
AllowInternetSharing	Yellow	Yellow	Yellow
AllowBluetooth	Yellow	Yellow	Yellow
MaxCalendarAgeFilter	Yellow	Yellow	Yellow
MaxEmailAgeFilter	Yellow	Yellow	Yellow
RequireSignedSMIMEAlgorithm	Yellow	Yellow	Yellow
RequireEncryptionSMIMEAlgorithm	Yellow	Yellow	Yellow
AllowSMIMEEncryptionAlgorithmNegotiation	Yellow	Yellow	Yellow
MinDevicePasswordComplexCharacters	Yellow	Yellow	Yellow
MaxEmailBodyTruncationSize	Yellow	Yellow	Yellow
MaxEmailHTMLBodyTruncationSize	Yellow	Yellow	Yellow
UnapprovedInROMApplicationList	Yellow	Yellow	Yellow
ApprovedApplicationList	Yellow	Yellow	Yellow
AllowExternalDeviceManagement	Yellow	Yellow	Yellow

6. Netzwerk- und Betriebssicherheit (2)

- Netzwerkstrategien

- Technologie beeinflusst Verfügbarkeit
- Fail-over-Strategien bei “schwachen” Zellen

- Integration in Office

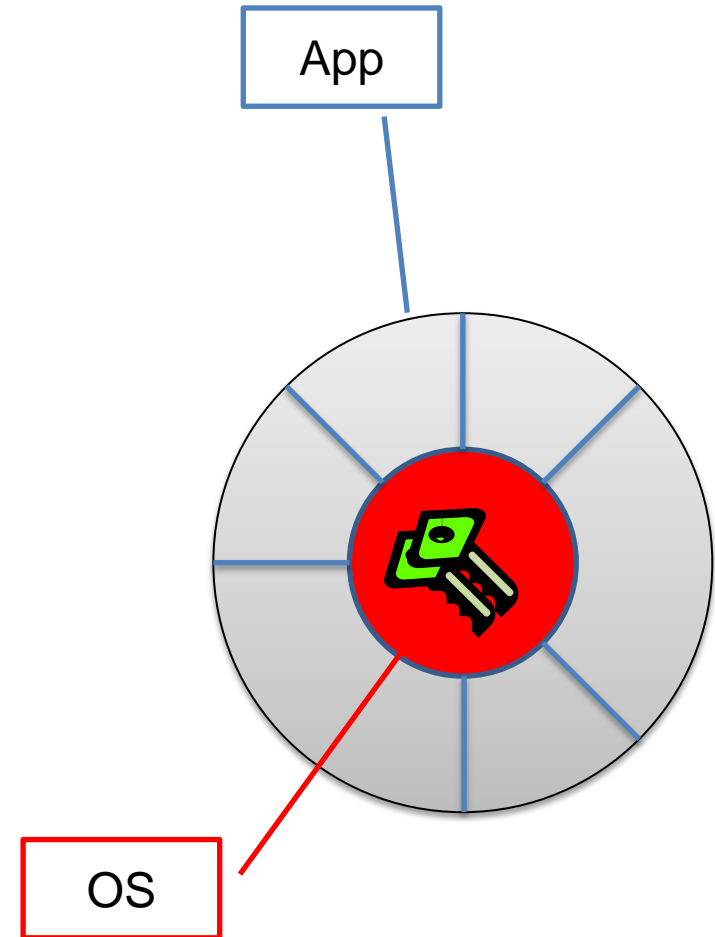
	iPhone	WP7	Android
Exchange	ActiveSync	Outlook	ActiveSync
Office	Viewer	Office Hub	Viewer
File-System	iTunes	Zune Sharepoint	Explorer

Abdeckung
Gut
partiell

7. Zugriffskontrolle (1): Schutzfunktionen im Smart Phone

Grundsatz:

- Apps haben eigene **Speicherbereiche** im File-System
- OS erlaubt Zugang auf den gesamten Speicher, aber Apps «dürfen» nur kontrollierte Zugangsfunktionen verwenden.
- Falls sich eine App nicht an die Vorschrift hält, so hat sie weitgehend Zugang.
- OS bietet Mechanismen zum Schutz von **Credentials** (z.B. KeyChain im IOS)
- Apps haben eigene Speicherbereiche.
- OS erlaubt Zugang auf den gesamten Speicher, aber Apps «dürfen» nur kontrollierte Zugangsfunktionen verwenden.
- Falls sich eine App nicht an die Vorschrift hält, so hat sie weitgehend Zugang.



	iPhone	WP7	Android
Rooter	JailBreak	Chevron	Super user tools Custom bootloader

7. Zugriffskontrolle (2): Datenverschlüsselung im iPhone

User Passcode ist optional
(Bildschirm-PIN)

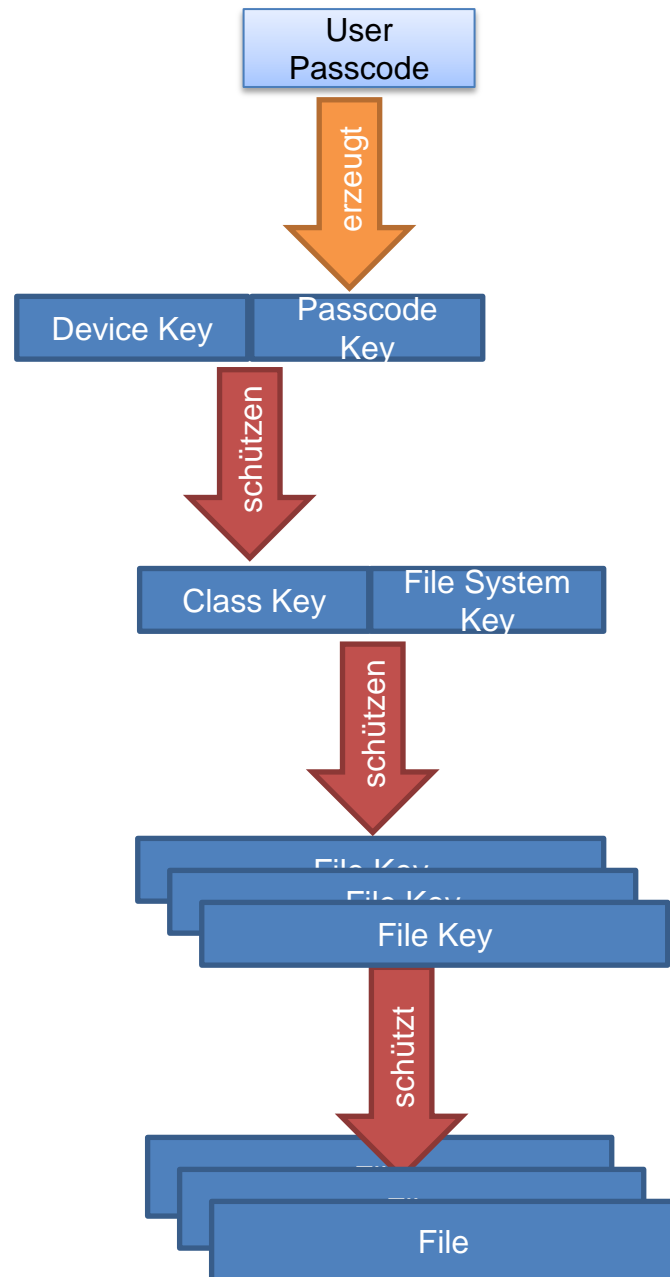
Verschlüsselungen: AES

Data protection

- Mail-Anwendung (Inhalte und Anhänge)
- KeyChain-Inhalte

Device-Key ist in der HW abgelegt
(nicht zugänglich)

Remote Wipe löscht den File
System Key



7. Zugriffskontrolle (3): Backup-Schutz

iPhone

- Ohne Backup-PW
 - Keychain ist mit device key geschützt.
 - Daten sind ungeschützt.
 - Recovery ist nur auf das Original-Gerät möglich.
- Mit Backup-PW
 - Alle Daten sind mit PW geschützt.
 - Recovery auf alle Geräte ist möglich.

Android und WP7

- Keine generischen Schutzmechanismen bekannt

8. Systementwicklung und Wartung: Programmintegrität

	iPhone	WP7	Android
Public Apps	AppStore	Marketplace	Market (Google) div. Shops
Enterprise Apps	«provisioning profiles»	unbekannt	Unsignierte Apps
User-ID	Apple ID	Live ID	div. User IDs
App-Schutz	Signatur	Signatur	Signatur (opt.)
App-Prüfung	Apple	MS	Abh. vom Shop
App-Updates	AppStore	Marketplace	Abh. vom Shop
Prüfungs- Umfang	Technik, Inhalt	Technik	Identität des Lieferanten
Anzeige von Updates	Automatisch	Automatisch	Abh. vom Shop

	Abdeckung
	OK
	mangelhaft

9. Umgang mit Sicherheitsvorfällen: OS-Updates

	iPhone	WP7	Android
Werkzeug	iTunes	Zune	«over the air»
Anbieter	Apple	Microsoft	Geräte-Hersteller via Carrier
Konzept	Volle Images	Volle Images	Inkrementell
Reaktionszeit	Tief	tief	unterschiedlich
Zeitbedarf	Hoch	Hoch	Tief
Update-Stand im Feld	Hoch	Hoch	tief

Abdeckung

Gut

partiell

10. Notfallvorsorgeplanung: Backup

	iPhone	WP7	Android
Backup-Werkzeug	iTunes	Zune	Google (Cloud) Third-Party-Tools
Automatismen	Beim Synchronisieren	Bei Updates	Google Over the Air
Zentralisierung	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Abdeckung

Gut

partiell

11. Rechtliches: App-Verteilung

	iPhone	WP7	Android
Prüfungsautorität	Apple	MS	Abh. vom Shop
Prüfungskriterien	Technik, Inhalt	Technik	Abh. vom Shop
Lizenz-Anteil des Shops	30%	30%	30%
Transaktions-Anteil des Shops	30%	n/a (30%)	n/a (30%)
Garantierte Response Time	Keine	Keine	«Sofort»

Abdeckung
OK
mangelhaft

Die Bedeutung von Apps wird sinken mit verbesserten Funktionen im Browser (HTML5)

Der Vergleich

Vergleich anhand ISO 27002

Abdeckung	1	2	3	4	5	6	7	8	9	10	11
Gut											
Mittel											
mangelhaft											
	Weisungen	Organisation	Verantwortung, Klassifizierung	Personelle Sicherheit	Physische Sicherheit	Netzwerk und Betrieb	Zugriffskontrolle	Entwicklung und Wartung	Sicherheitsvorfälle	Notfallvorsorge	Rechtliche Vorgaben
iPhone											
Android											
Windows Phone 7											
Windows 7 Notebook											

Weitere Quellen

OWASP Mobile Security Project:

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

National Vulnerability Data Base: <http://nvd.nist.gov/>

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

Danke

Paul Schöbi

paul.schoebi@cnlab.ch

+41 55 214 33 33