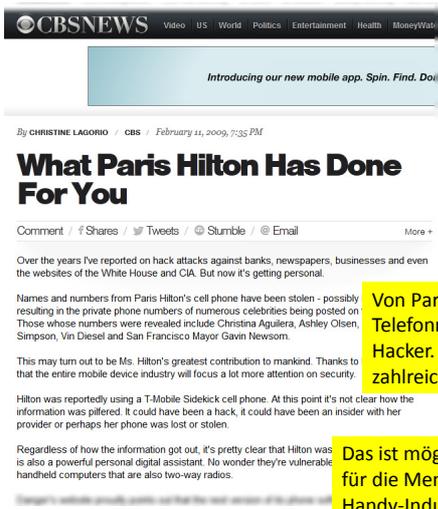


Smartphone-Sicherheit: Welches Handy-OS ist das sicherste?

Prof. Dr. Rainer W. Gerling
IT-Sicherheitsbeauftragter
Max-Planck-Gesellschaft



Was Paris Hilton für uns getan hat



Von Paris Hiltons Handy wurden Namen und Telefonnummern gestohlen – vermutlich von einem Hacker. Dadurch sind die privaten Telefonnummern zahlreicher Berühmtheiten im Internet verfügbar.

Das ist möglicherweise Frau Hiltons größter Beitrag für die Menschheit. Inretwegen wird die gesamte Handy-Industrie dem Sicherheitsaspekt sicherlich mehr Bedeutung beimessen.

nach S. Gerling

MAX-PLANCK-GESSELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 2

Smartphones: lohnende Ziele

Wir tragen sie **immer** bei uns ... viele Daten können **LIVE** verfolgt werden ...

Wen kennen wir:
Personen, Adressen,
Telefonnummern

Was machen wir
demnächst:
Termine (... mit wem?)

Fotos, Videos (inkl.
Ton, die Geräte haben
Mikrophone)

Telefongespräche

GPS: Wo sind wir
gerade, wohin bewegen
wir uns

Weitere Apps erweitern
die Möglichkeiten noch
(z.B. Online-Banking)

SMS/E-Mails: unsere
Komplette
Kommunikation
(idR. unverschlüsselt)

Was beschäftigt uns
gerade? - Ideen,
Erinnerungen, Notizen

Quelle: S. Gerling

MAX-PLANCK-GESSELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 3

Was ist daran so besonders?

- Paradigmenwechsel bei der Softwareinstallation
 - Viele kleine Apps von unbekanntem Entwicklern
 - Amateure vs. professionelle Softwareentwickler schwer unterscheidbar
- Fehlende Sicherheitsinfrastruktur
 - Virens Scanner
 - Firewalls
 - Datensicherheit / Diebstahlschutz
- Sicherheitsupdates kommen nicht schnell genug
 - z.B. bei einigen Android Smartphones
- Fehlendes Problembewusstsein bei Anwendern
 - Komfort ↔ Sicherheit
- zentrales Management möglich
 - Google Apps Device Policies / Apple Configurator
 - Sicherheitsvorgaben
 - Detailliertere Nutzer-/Rechte-Verwaltung erforderlich
- Umfassende Sicherheitslösungen fehlen noch

Quelle: S. Gerling

MAX-PLANCK-GESSELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 4

Sicherheitsaspekte



- iOS, Android, Windows, Mac OS X und Linux bieten die Möglichkeit ein Login-Passwort/PIN zu nutzen ☺
- Auf Smartphones ist der Default kein Passwort/PIN ☹
 - Wenn PIN dann 4 Ziffern
- Es ist nervig vor (!) jeder Nutzung (ausgehendes Telefonat) die PIN einzugeben.
 - Die Annahme eingehender Gespräche und Notrufe sind ohne PIN-Eingabe möglich

MAX-PLANCK-GESSELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 5

iPhone Anmeldebildschirm





4 Ziffern (Default)
15 Min.



mehr als 4 Ziffern
2,5 Jahre (9 Ziffern)

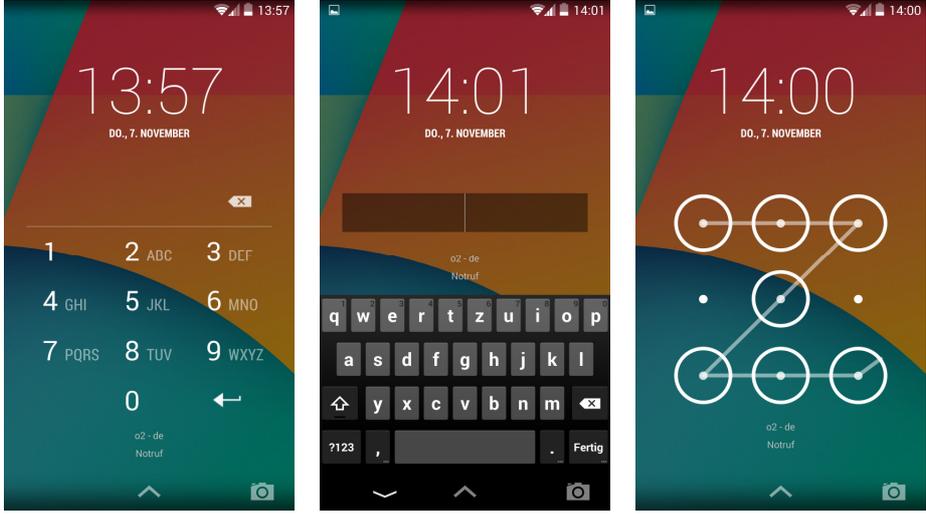


beliebige Zeichen
5,5 Jahre (6 a..z, Ziffern)

MAX-PLANCK-GESSELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 6

0,08 sec

Android 4 Anmeldebildschirm



The image displays three sequential screenshots of the Android 4 lock screen. The first screenshot shows a numeric keypad with the time 13:57 and date DO., 7. NOVEMBER. The second screenshot shows a full QWERTY keyboard with the time 14:01 and date DO., 7. NOVEMBER. The third screenshot shows a pattern lock interface with the time 14:00 and date DO., 7. NOVEMBER. Each screenshot includes a status bar at the top with signal, Wi-Fi, and battery icons.

nur Ziffern
Mind. 4

beliebige Zeichen
Mind. 4

Muster

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 7

Mustererkennung



The image shows a close-up of a hand touching a glass surface, likely a tablet or smartphone screen. The fingers are positioned as if they are about to touch or have just touched the surface, illustrating the concept of fingerprint recognition.

- Wette bei „Wetten das“
 - Ein Spiel auf einem iPad an den Fingerspuren erkennen

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 8

Windows Phone 8 & Firefox OS



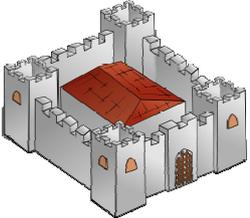
- Mindestens 4 Ziffern
- Nur Ziffern

- 4 Ziffern

MAX-PLANCK-GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 9

Walled Garden

- Ein abgeschottetes IT-System mit einem zentralen System, um „Inhalte“ in das System zu bringen.
 - Spielkonsolen:   
 - Betriebssysteme:    
 - Betriebssysteme (Zukunft):  
- Voraussetzungen:
 - Konzeptionell sauberes System
 - Keine Hintertür
 - Fehlerfreies System
 - Gute, transparente und faire Kontrolle am Eingang
- Motivation des Herstellers?
 - Systemsicherheit
 - Einkommenssicherung



MAX-PLANCK-GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 10

Appstore



MAX-PLANCK-GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 11

Playstore

Unbekannte Herkunft
Installation von Apps aus anderen
Quellen als dem Play Store zulassen

Apps mit unbekannter Herkunft können gefährlich für Ihr Telefon und Ihre persönlichen Daten sein. Sie stimmen zu, dass Sie die Verantwortung für alle Schäden an Ihrem Telefon und jegliche Datenverluste tragen, die aus der Verwendung dieser Apps entstehen können.

Abbrechen OK



MAX-PLANCK-GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 12

Playstore

Unbekannte Herkunft
Installation von Apps aus anderen Quellen als dem Play Store zulassen

amazon apps
AndroidPIT
apk

Google

Dropbox
BoxCryptor
OPENVPN

„sideloading“

MAX-PLANCK-GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 13

Playstore

Unbekannte Herkunft
Installation von Apps aus anderen Quellen als dem Play Store zulassen

Apps verifizieren
Installation schädlicher Apps blockieren oder Warnung senden

Benachrichtigungszugriff
1 App kann Benachrichtigungen lesen

ANMELDEDATENSPEICHER

Speichertyp
Hardware-gestützt

Vertrauenswürdige Anmeldedaten
Vertrauenswürdige CA-Zertifikate ansehen

Von Speicher installieren
Zertifikate von Speicher installieren

MAX-PLANCK-GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 14

- Neuerungen mit Android 4.2
 - Google scannt apk-Dateien im Netz
 - Alle Apps können gegen eine Black/White-List abgeglichen werden
 - Apps verifizieren ist per default aktiv
 - In den Einstellungen jederzeit änderbar
 - Bei einer Installation per „sideloading“ wird nachgefragt

Apps verifizieren?

Darf Google alle auf diesem Gerät installierten Apps auf schädliches Verhalten prüfen?

Weitere Informationen finden Sie unter "Einstellungen" > "Sicherheit".

Nicht zustimmen Zustimmen

Sicherheit

GERÄTEVERWALTUNG

Geräteadministratoren
Geräteadministratoren abrufen oder deaktivieren

Unbekannte Herkunft
Installation von Apps aus anderen Quellen als dem Play Store zulassen

Apps verifizieren
Installation schädlicher Apps blockieren oder Warnung senden

Benachrichtigungszugriff
1 App kann Benachrichtigungen lesen

ANMELDEDATENSPEICHER

Speichertyp
Hardware-gestützt

Vertrauenswürdige Anmeldedaten
Vertrauenswürdige CA-Zertifikate ansehen

Von Speicher installieren
Zertifikate von Speicher installieren

Programme Starten



- Alle vier Betriebssysteme starten Apps nur nach Prüfung einer Digitalen Signatur
 - iOS: Signatur von Apple
 - Android: Signatur des Autors
 - Windows Phone: Signatur von Microsoft
 - Blackberry: Signatur von Blackberry

- Jailbreak (iOS) oder Rooten (Android)
 - Anwendungen ohne Signatur starten

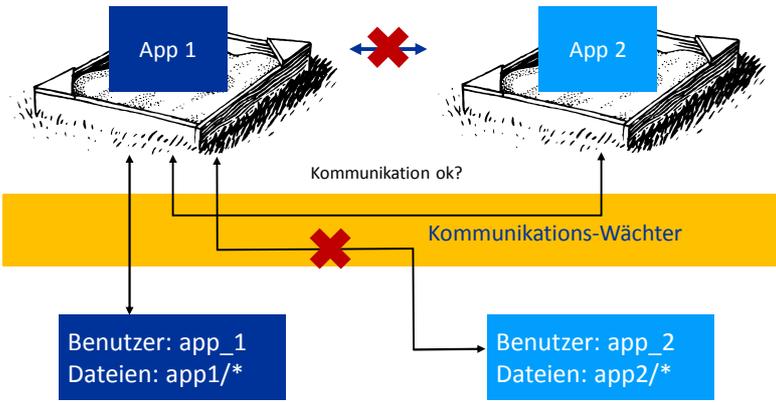
- Sicherheitslücken werden positiv wahrgenommen

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 15

Sicherheitsmodell



- Anwendungs-Isolation



Quelle: S. Gerling

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 16

Apple's iOS

- Sichere Boot Kette
 - Durchbrechen der Kette wird als „Jailbreak“ bezeichnet
- Der komplette Flash-Speicher ist verschlüsselt („Festplattenverschlüsselung“)
 - Der Schlüssel hängt von der Hardware ab (File System Key)
 - Dient dem schnellen Löschen des Handys
- Dateien in der Data Partition können zusätzlich mit individuellen Schlüsseln verschlüsselt werden
- Für das Schlüsselmanagement gibt es weitere Schlüssel

- Installation von Enterprise Anwendungen auf Firmengeräten

Quelle: Apple iOS Security

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 17

Key Handling iOS

Key Class	Schutz des Schlüssels		User Log-Off
Complete Protection:	user passcode	UID	Wird gelöscht
• Mail, App Launch Images, Location data, some Apps			
Protected Unless Open:	user passcode	UID	Kann nur nach Login wieder geöffnet werden
• Mail Download when locked			
Protected Until First User Authentication:	user passcode	UID	Wird nicht gelöscht
No Protection:	-	UID	-

Anmeldezeit
Verzögerungen

GUI

▪ Knacken der PIN per Brute Force geht nur auf dem Gerät

Crypto
Hardware

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 18

Google's Android



- Ab Android Version 3 kann der Flashspeicher verschlüsselt werden
 - Bekanntes Verfahren dmccrypt aus der Linux Welt
 - Benutzer-Passwort geht in den Schlüssel ein
 - Preboot Authentication
 - Verschlüsselung der SD-Karte möglich (App)
 - Funktioniert nicht immer
- Anwendungen können von verschiedenen Orten installiert werden
 - Google PlayStore
 - Beliebiger anderer Store z.B. Amazon App Store, AndroidPit
 - Vom Datenträger (SD-Karte)
- Rechte einer App stehen in der zugehörigen Manifest-Datei

Microsoft's Windows Phone 8



- Windows Phone 8 nutzt das United Extensible Firmware Interface (UEFI) Boot-Protokoll
- Der Flash-Speicher kann mit einer vom Bitlocker abgeleiteten Verschlüsselung vollständig verschlüsselt werden
 - Im wesentlichen ist das Schlüsselmanagement anders
- Unternehmens-Hub erlaubt die Installation von unternehmenseigenen Anwendungen

Exchange ActiveSync Richtlinien

Funktion	Einstellung	iOS ab 3.x	Android ab 2.2	WP 7/8
AllowNonProvisionableDevices	\$false	●	-	●
DevicePasswordEnabled	\$true	●	●	●
AlphanumericDevicePasswordRequired	\$true	●	●	-
MaxInactivityTimeDeviceLock	'00:15:00'	●	●	●
MinDevicePasswordLength	'4'	●	●	●
PasswordRecoveryEnabled	\$false	-	-	-
RequireDeviceEncryption	\$true	○	●	●
AttachmentsEnabled	\$true	-	-	-
AllowSimpleDevicePassword	\$true	●	-	●
DevicePasswordExpiration	'30.00:00:00'	●	●	●
DevicePasswordHistory	'3'	●	-	●
Remote Wipe		●	●	●

Quelle: <http://refraction.co.uk/blog/wp-content/uploads/2010/11/Exchange-ActiveSync-Policies.pdf>

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 21

Apple Configurator

▪ Neues Tool im Mac App Store zur Verwaltung von iDevices

Prepare Devices
Prep your iOS devices for mass deployment.
Configure your organization's devices. Quickly update them to the latest iOS version, install profiles, install free and volume purchased apps, or restore a device backup. [Learn more](#)

Supervise Devices
Enforce a standard configuration on your iOS devices.
Maintain control over groups of devices that share common apps, settings, and profiles. Automatically restore devices to the specified configuration when reconnected. [Learn more](#)

Assign Devices
Assign iOS devices to users in your organization.
Create and manage users and groups. Assign supervised devices to individual users, back up and restore users' content and settings, and distribute and retrieve users' documents. [Learn more](#)

Welcome to Apple Configurator
iOS device configuration, supervision and assignment made easy.

Start Preparing Devices

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 22

Google Apps Device Policy




- Verwaltung der Geräte mit ActiveSync über eine Web-Anwendung bei Google
 - Auf Android-Geräten muss die Device Policy-App installiert sein
 - Google-Sync-Geräte: iOS, Windows Phone (müssen Microsoft Exchange ActiveSync verwenden)
 - Google Apps for Business, Google Apps for Education oder Google Apps for Government erforderlich
- Geräte werden bei Google gemanagt

Mobile settings

Org Settings Activation **Devices**

Search Approve Block Remote Wipe Export All 1 - 30 of 38 State

Device ID	Name	Email	Model	OS	Type	Last Sync	Status
AppL-XUDT9Y	Juan DalFinaire	juandalfinaire@iabostrat.com	iPhone 4	iOS 9	Google Sync	11/01/11	Approved
AppL-S8899Q	Emma Zuriz	emmazuriz@iabostrat.com	iPhone 3GS	iOS 5	Google Sync	11/01/11	Approved
AppL-8C339S	Ricardo Domercq	ricardodomercq@iabostrat.com	iPhone 3Gs	iOS 4.0	Google Sync	11/04/11	Approved
AppL-8L339S	Ricardo Domercq	ricardodomercq@iabostrat.com	iPhone 4	iOS 5	Google Sync	11/04/11	Approved
AppL-8L339S	Ricardo Domercq	ricardodomercq@iabostrat.com	Windows Phone 7	Windows Phone 7	Google Sync	11/04/11	Approved
AppL-3YX108	Evansom	averror@iabostrat.com	iPhone 3G	iOS 4.2	Google Sync	11/01/11	Approved
3806-379607	Suarez Miranda	suarezmiranda@iabostrat.com	Nexus S	Android 2.3.6	Android	10/29/11	Approved
AppL-39G6AT	Lazana Merrill	suarezmiranda@iabostrat.com		3.5	Google Sync	10/29/11	Approved
AppL-28V092	Hanni Buchhalter	suarezmiranda@iabostrat.com		3.5	Google Sync	10/29/11	Approved
AppL-2TTAAT	Doctor Books	suarezmiranda@iabostrat.com		3.5	Google Sync	10/29/11	Approved
AppL-DUG6AT	Herbert Quast	86753098075300		3.5	Google Sync	10/20/11	Approved
AppL-JFX6AT	Isidoro Paredi	419111826		3.5	Google Sync	10/20/11	Approved
AppL-JG66AT	Jacques Reboul	1902611228		3.5	Google Sync	10/15/11	Approved
AppL-FF1AAS	Victor Moon	suarezmiranda@iabostrat.com		3.5	Google Sync	10/15/11	Approved
AppL-EVD3NS	Tom Castro	tomcastro@iabostrat.com	iPhone 3Gs	iOS 4.3	Google Sync	10/14/11	Approved
AppL-SGX6AT	Gervasio Montenegro	gervasiomont@iabostrat.com	iPhone 4	iOS 4.3	Google Sync	10/13/11	Approved
3c99-4a7a08	Erik Lorenz	eriklorenz@iabostrat.com	Liquid MT	Android 2.3.5	Android	10/13/11	Wiping
AppL-WD66AT	Beatriz Viterbo	beatrizviterbo@iabostrat.com	iPhone 4	iOS 4.3	Google Sync	10/8/11	Blocked

On mouseover hovercards

Approve Block Remote Wipe View Details

MAX-PLANCK | SEITE 23

Microsoft & Blackberry



- Microsoft System Center Configuration Manager
 - Die identischen Management Werkzeuge wie für Desktops
 - Nutzt Exchange Active Synch (EAS)
 - Unterstützt auch andere Geräte (Symbian, iOS, und Android)
- BlackBerry Enterprise Service 10
 - Verwaltet Balance
 - Unterstützt BlackBerry OS, BlackBerry 10, Android und iOS
 - Unterstützt mehrere Geräte pro Nutzer
 - Dienstliches und privates Gerät

MAX-PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 24

Sicherheitsprobleme beim Business Einsatz

- zentrales Management ist heute möglich und sollte auch eingesetzt werden!
 - Sicherheitsvorgaben
 - Detailliertere Nutzer/Rechte-Verwaltung erforderlich
- Umfassende Sicherheitslösungen fehlen noch



- Nutzer (und manchmal auch IT-Abteilungen) neigen zu Komfort
 - Nur keinen zusätzlichen Stress|Fehler|Probleme durch Sicherheit
- Plattformübergreifend: nur Dritthersteller
 - Teilweise mit eigenen Klienten für mehr Funktionalität
 - Z.B. Airwatch, Good Technology, MaaS360, MobileIron, SAP, ZenPrise, ...

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 25

Andere Lösungen

- Trennung durch Sicherheitsdomänen
 - Beispiele für Desktop:
 - Qubes, Sirrix TrustedDesktop, (Citrix XenClient)
 - Beispiele für Smartphones:
 - BizzTrust, Sirrix TrustedMobile
 - Blackberry Balance
 - Secure Work Space für iOS und Android angekündigt
 - „Privater Teil“ abschaltbar
 - Samsung Knox (SE Android)
 - Teil von SAFE
- Anwendungssicherheit vs. Devicesicherheit
 - Moxier Mail
 - Touchdown von Nitrodesk
 - ActiveSync-Policy wird nur auf Anwendung angewandt
 - PIN, Wipe usw.

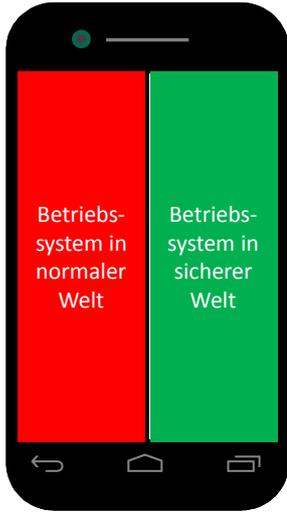
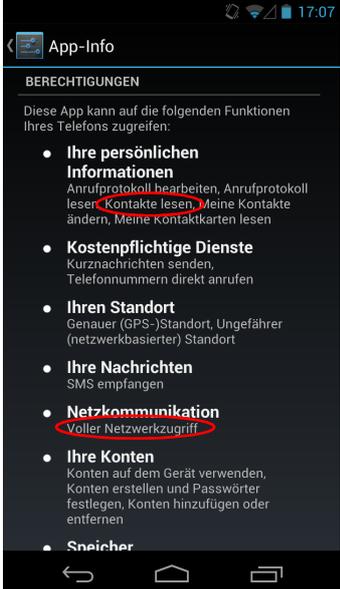


Abbildung: S. Gerling

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 26

Rechte einer Anwendung



App-Info

BERECHTIGUNGEN

Diese App kann auf die folgenden Funktionen Ihres Telefons zugreifen:

- Ihre persönlichen Informationen**
Anrufprotokoll bearbeiten, Anrufprotokoll lesen, Kontakte lesen, Meine Kontakte ändern, Meine Kontaktkarten lesen
- Kostenpflichtige Dienste**
Kurznachrichten senden, Telefonnummern direkt anrufen
- Ihren Standort**
Genauer (GPS-)Standort, Ungefährer (netzwerkbasierter) Standort
- Ihre Nachrichten**
SMS empfangen
- Netzwerk**
Voller Netzwerkzugriff
- Ihre Konten**
Konten auf dem Gerät verwenden, Konten erstellen und Passwörter festlegen, Konten hinzufügen oder entfernen
- Speicher**

- Was ergibt sich aus diesen Rechten?

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 27

WhatsApp

▪ Bei jedem Start der Software werden die Telefonnummern aus dem Adressbuch an den Anbieter übertragen.



0160-88012345
0161-12345678
0183-23456789
...



WhatsApp

...

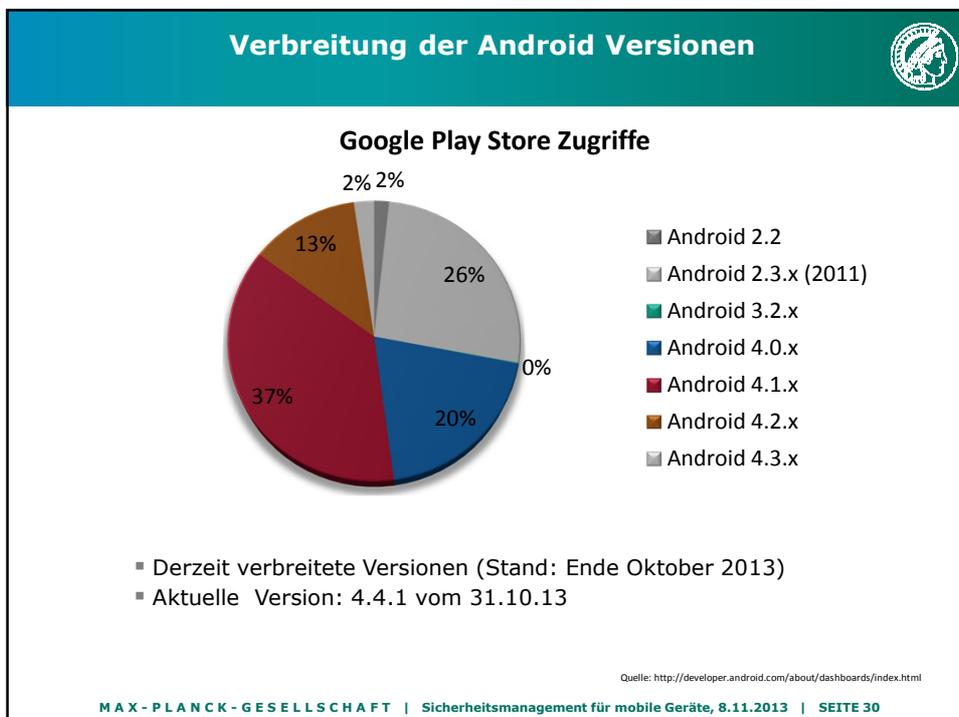
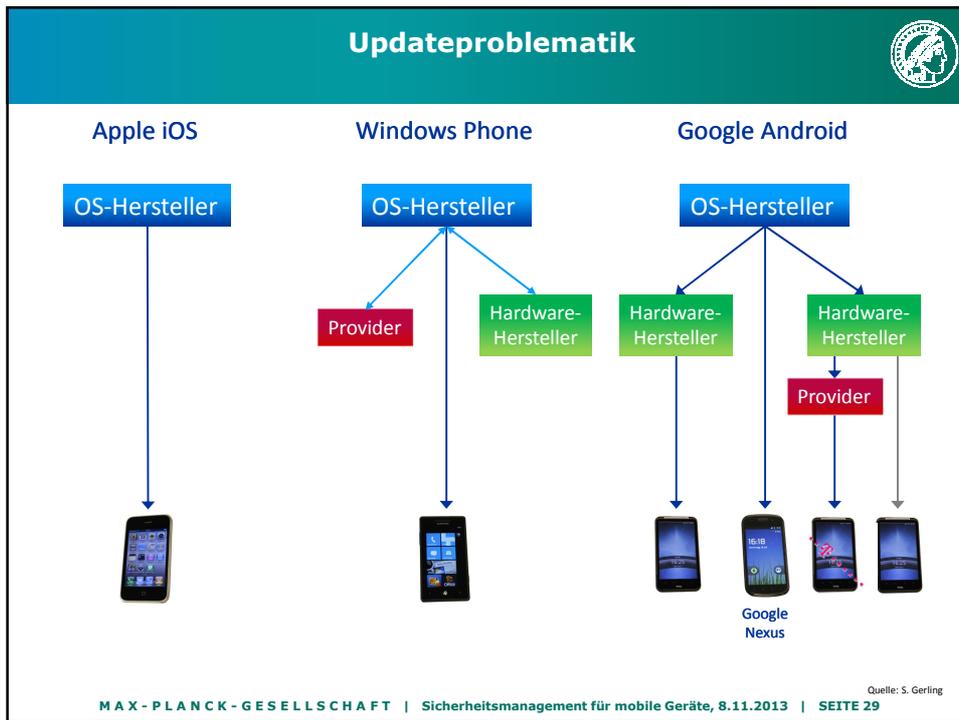
0160-88012345
0161-12345678
0170-45678923
0171-67891234
...



0161-12345678
0160-88012345
0172-23456789
...

iPhone,
BlackBerry, Nokia,
Android, Windows
Phone

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 28



Updatedauer



07.04.2012 11:55 dt « Vorige | Nächste »

Android-Updates kommen zu langsam

vorlesen / MP3-Download

Wenn Google eine neue Version seines mobilen Betriebssystem Android herausbringt, dauert es im Schnitt ein Dreivierteljahr, bis es auf den Smartphones ankommt. Das ist das Resultat einer [Erhebung](#), über die c't in der aktuellen Ausgabe 9/2012 berichtet. Von 29 Android-Smartphones, die die fünf größten Hersteller 2009 und 2010 auf den Markt gebracht haben, wurden fünf zweimal aktualisiert, 17 bekamen nur ein verspätetes Update, sieben Geräte gingen ganz leer aus. Das im November gestartete Android 4.0 läuft erst auf 1,6 Prozent aller Geräte.



Hersteller	Update-Dauer (Monate)
HTC	5,6
Samsung	8,6
Motorola	8,8
Sony Ericsson	9,1
LG	10,5

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 31

Sicherheitsfunktionalitäten



	iOS v7.x	Android v4.x	Windows Phone 8	Blackberry 10
Passwortschutz	Ja	Ja	Ja	Ja
Device Encryption	Immer	(Ja)	Bitlocker (Enterprise)	Ja (Balance)
File Encryption	Ja	Nein	Nein	
S/Mime	Ja	(Nein)	Nein	Ja
Sandboxing	Ja	Ja	Ja	Ja
Sideloadung	Nein	Ja	Nein	(Nein)
Herstellerupdates	Ja	(Nein)	(Ja)	Ja
Enterprise Apps	Ja	(Nein)	Ja	Ja
Custom Launcher	Nein	Ja	Nein	Nein
VPN	IPsec, SSLvpn	IPsec, SSLvpn	-	IPsec
OpenVPN	Nein	Ja	Nein	Nein
Jailbreak/Rooting	Ja	Ja	Nein	Nein

MAX - PLANCK - GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 32

Welches Smartphone ist das Sicherste?



- Android ist das unsicherste, aber offenste Betriebssystem!
- Review Prozess beim Einbringen in den Walled Garden
 - Apple hat viel Erfahrung, ist aber intransparent
 - Microsoft hat die besseren Werkzeuge
- Verschlüsselung
 - Apple hat ein rundes Konzept für alle iOS Geräte
 - Microsoft verschlüsselt nur Firmenhandys/-tablets
 - Blackberry nutzt Verschlüsselung zur Trennung der Workspaces bei Balance
- Firmenunterstützung
 - Apple: Firmenaccount mit eigenem Shop nur mit DUNS-Nummer
 - Microsoft: Unternehmens-Hub kann einfach eingerichtet werden
- Management-Funktionen vergleichbar
- Apple, Microsoft und Blackberry fast gleich auf
 - Microsoft und Blackberry aber noch zu neu

MAX-PLANCK-GESELLSCHAFT | Sicherheitsmanagement für mobile Geräte, 8.11.2013 | SEITE 33

**Vielen Dank für Ihre
Aufmerksamkeit !**

www.mpg.de/datenschutz