IS-BREMEN Information Security

Bring your own device (BYOD)

Gefahren und Risiken bei der Nutzung mobiler Endgeräte

Dr. Thomas Kemmerich
thomas.kemmerich@tgt-it.de
Tel.: 0170 2300573

IS-BREMEN Information Security

BYOD - Informationssicherheit

Netze

Internet

Cyber Crime

Soziale Netzwerke

Datenschutz

Das Netz vergisst nichts

Soziale Medien

Nachvollziehbarkeit

Spuren

Second Life

Informationssicherheit

Viren / Würmer / Trojaner

Cyber Mobbing

BYOD - Informationssicherheit

Wir betrachten IOS und Android und (Windows Phone - nicht)

BYOD - Informationssicherheit

kurzer, unvollständiger Vergleich der Plattformen Android und IOS

Apple IOS

- properitär, nicht öffentlich
- nur auf Apple HW
- keine Virtualisierung durch Drittanbieter
- Download der Apps nur über Appstore möglich
- App Store relativ abgesichert (Apps werden geprüft)*
- ...

Android

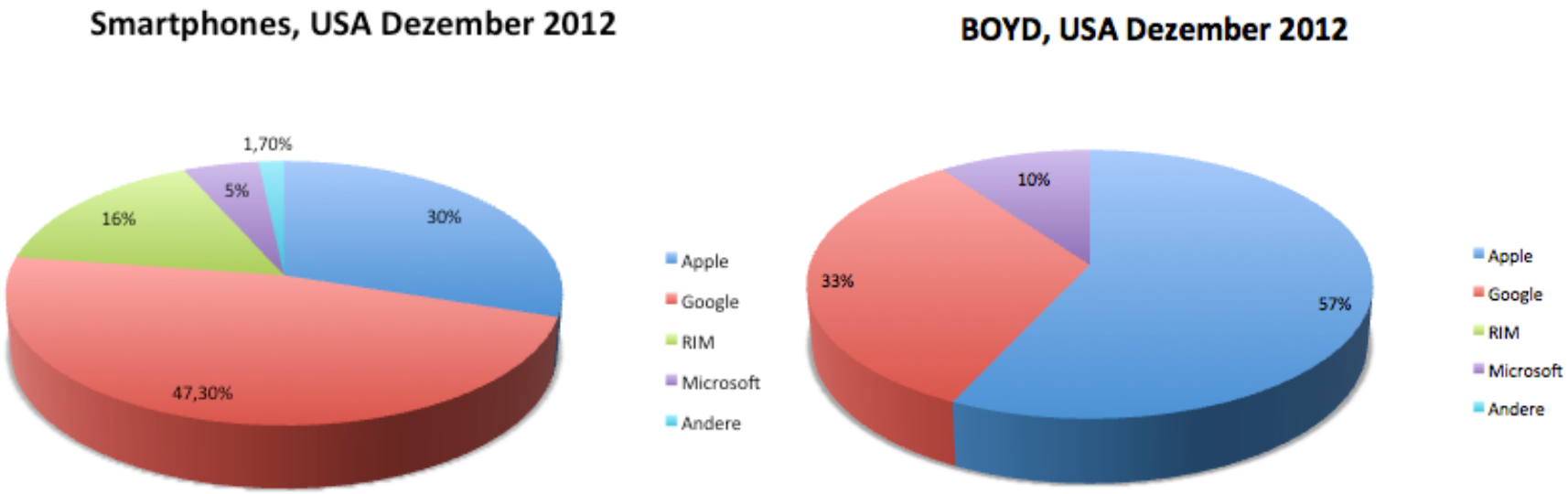
- Code offen
- läuft auf unterschiedlichen Plattformen
- Virtualisierung durch Drittanbieter
- Download von Apps auch über andere Anbieter als Google möglich
- Apps werden nicht immer geprüft*
- ...

* Tests sind nicht 100% sicher, da nur bestimmte Eigenschaften abgefragt werden

Blackberry bietet viele dieser Features, aber als „Own Device“ in DE nicht attraktiv

BYOD - Informationssicherheit

Verteilung von Smartphones in den USA Dez. 2011



insgesamt 97,9 Millionen Nutzer, über 13 Jahre alt, von 234 Mio. Mobil-Nutzern

nach comScore (www.comscore.com)

BYOD - Informationssicherheit

Wie viel Papier benötigt man, um den Code von Android aus zu drucken (8pt, Zeilenabstand 1)

BYOD - Informationssicherheit

Problem der Software-Sicherheit

„Trinity of Trouble“: Software wird immer **erweiterbarer**, **vernetzter** und vor allem **komplexer**

- Windows XP (ca. 40 Mio. Lines of Code),
- Vista (> 50 Mio. Lines of Code),
- Windows 7 (unbekannt…)
- Linux Kernel 2.6 (ca. 13 Mio. Lines of Code)
- Android (ca. 15 Mio. Lines of Code)

Wachsende Anzahl von Software-Schwachstellen
Sicherheitslücken in SW als Haupteinstiegspunkt für Angreifer

Wie können wir diese Masse an Code vom Standpunkt der Sicherheit her verstehen?

BYOD - Informationssicherheit

Wir benötigen:

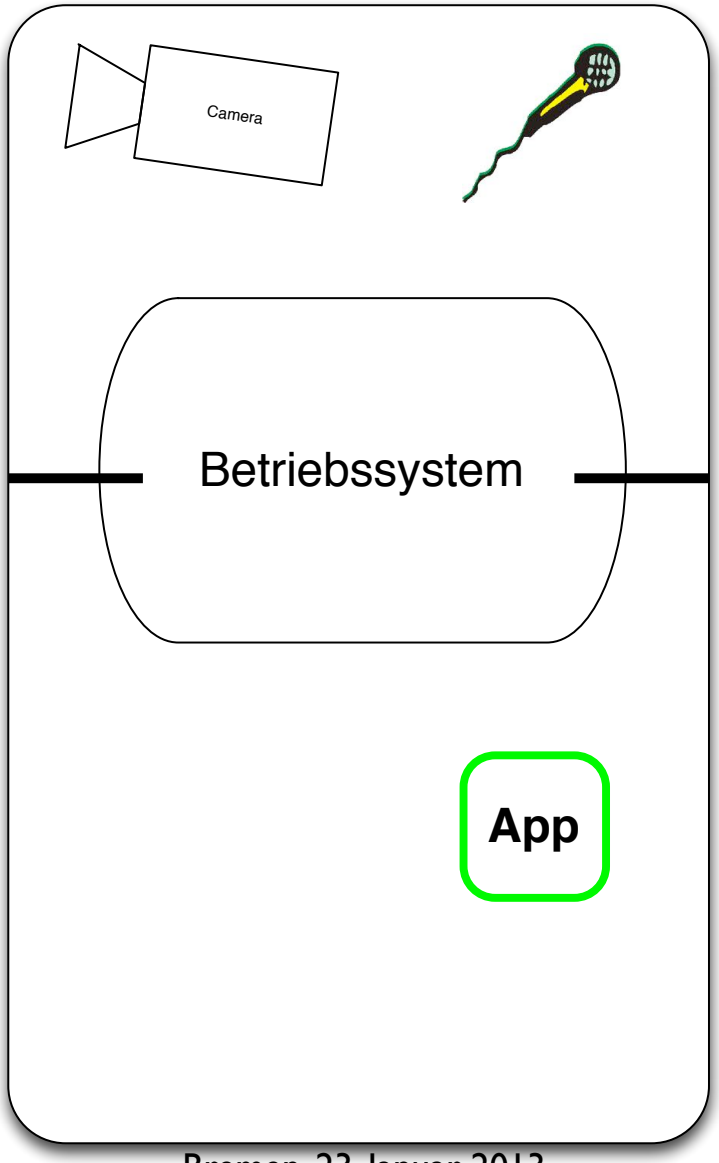
- Tools zur Überprüfung der Apps bezüglich IT-Security, Code-Analyse:
  - statische Code-Analyse
  - dynamische Code-Analyse
- Standardisierte Testverfahren zur Prüfung von Apps
- Zertifizierung von Apps hinsichtlich Ihrer IT-Security, Verfahren und eine Zertifizierungsstelle
- Einen sicheren App-Store für alle betroffenen PLattformen

BYOD - Informationssicherheit

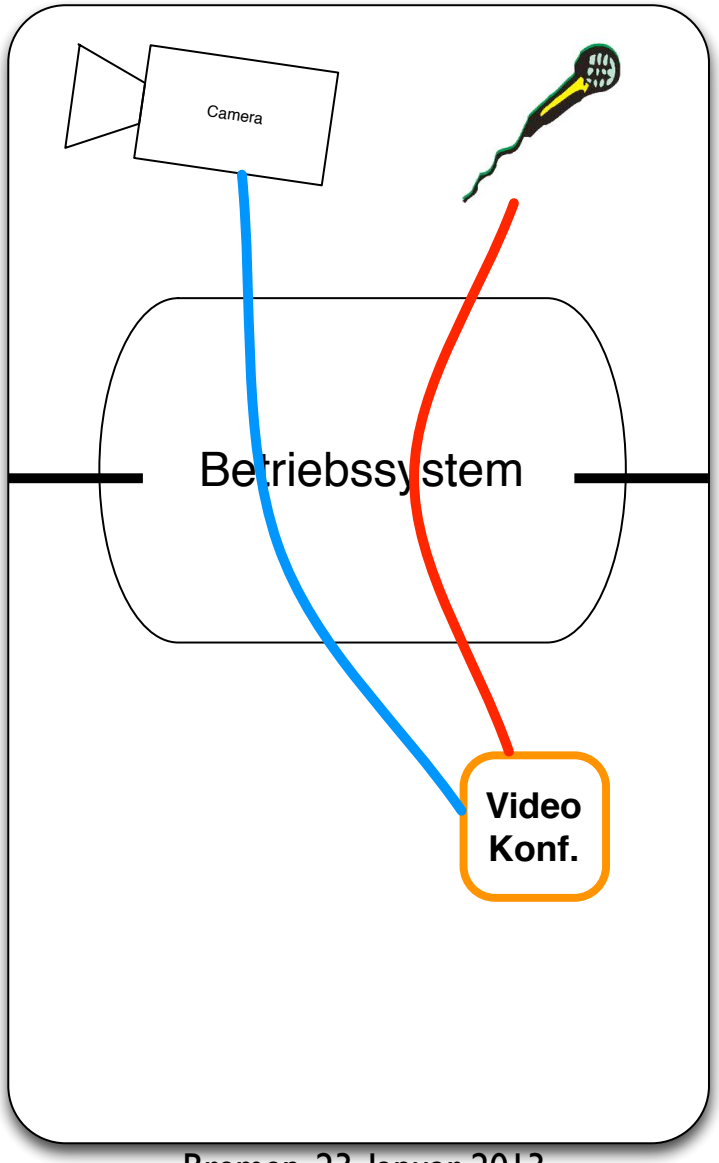
Typische Gefährdungen bei der Nutzung von Smartphones?

- Maleware
  - Trojaner, Viren, Würmer
- Remote Control durch Dritte
- Datendiebstahl
- Mithören von Kommunikationsverbindungen
- Diebstahl des Geräts
- Verfügbarkeit stören
- Daten fälschen
- Denail of Service
- Nutzung durch Unbekannte / nichtauthorisierte Bekannte
- ...

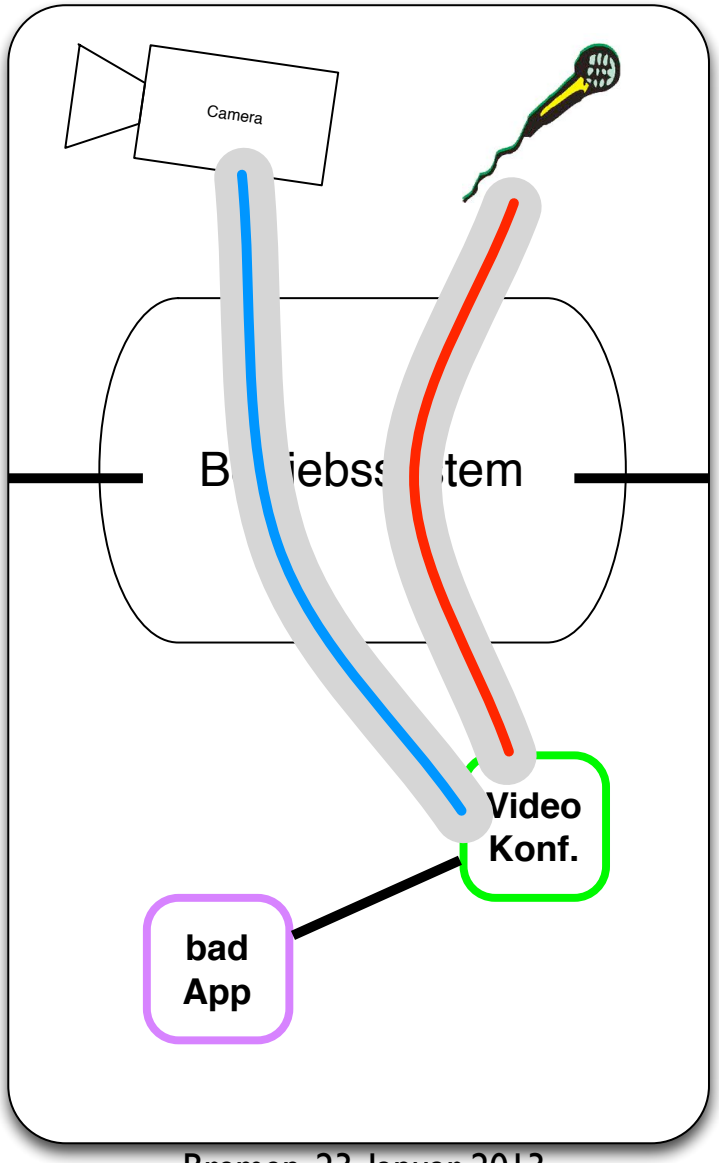
BYOD - Informationssicherheit



BYOD - Informationssicherheit

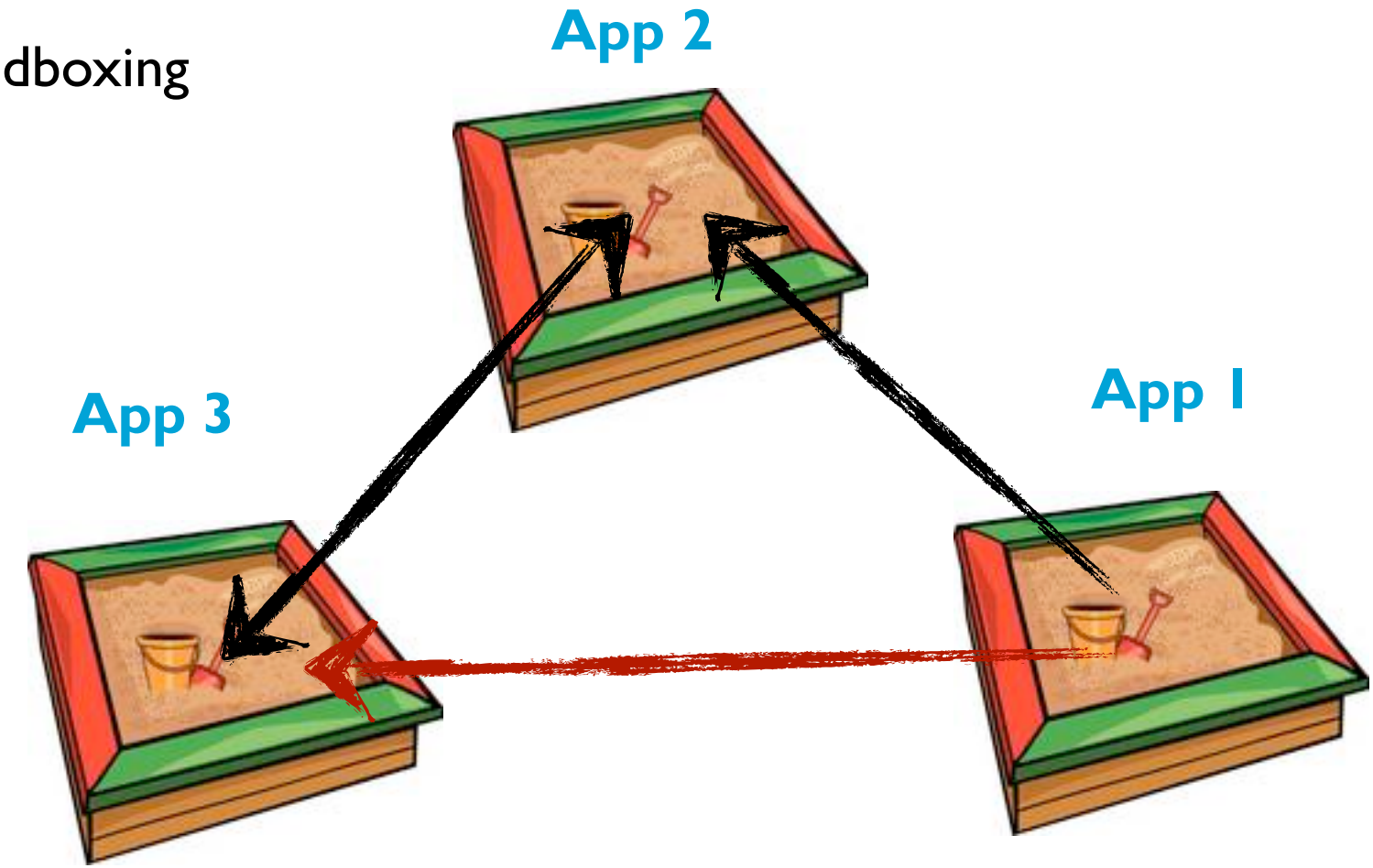


BYOD - Informationssicherheit



BYOD - Informationssicherheit

Sandboxing



BYOD - Informationssicherheit

Mobile Device Management (MDM)

Optimierung der Funktionalität und Sicherheit mobiler Geräte im Unternehmen

- Device Deployment
- Software Update (OS and Apps)
- Diagnose der Geräte (prüfen ob Jailbrake, unzulässige Apps etc.)
- Device tracking
- Backup and Restore
- Remote Löschen der Daten
- Netznutzung und Betriebsüberwachung
- Protokollierung und Reporting
- Firmware over the Air - Distribution
- Trobleshooting and User Support
- .....

BYOD - Informationssicherheit

Mobile Device Management (MDM)

Figure 1. Magic Quadrant for Mobile Device Management Software

Source: Gartner (May 2012)

siehe auch:

Market Overview: On-Premises Mobile Device Management Solutions, Q3 2011

Hier sind die Leistungsmerkmale der bezeichneten MDM-Systeme beschrieben

Es fehlen aber in allen MDMs derzeit die für BYOD notwendigen Strategien und rechtlichen sowie persönlichen Richtlinien

BYOD - Informationssicherheit

Virtualisierung

Drei wesentliche Aspekte der Virtualisierung:

- CPU-Vitualisierung
- Speicher-Virtualisierung
- I/O-Virtualiserung (Ports und Devices)

BYOD - Informationssicherheit

Virtualisierung

Type 2 Hypervisor:
basiert auf Anwendungsebene --> App

Type 1 Hypervisor:
basiert auf Hardwareebene --> Unterstützung durch HW-Hersteller

Derzeit noch im Entwicklungszustand, Gegenstand der Forschung

siehe auch:

Joo-Young Hwang et.al., Xen on ARM: System Virtualization using Xen Hyoervisor for ASM-based Secure Mobile Phones
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4446362&isnumber=4446298&tag=1

Xiaoyi Chen et.al., Smartphone Virtualisation: Status and Challanges
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6066716

BYOD - Informationssicherheit

Virtualisierung

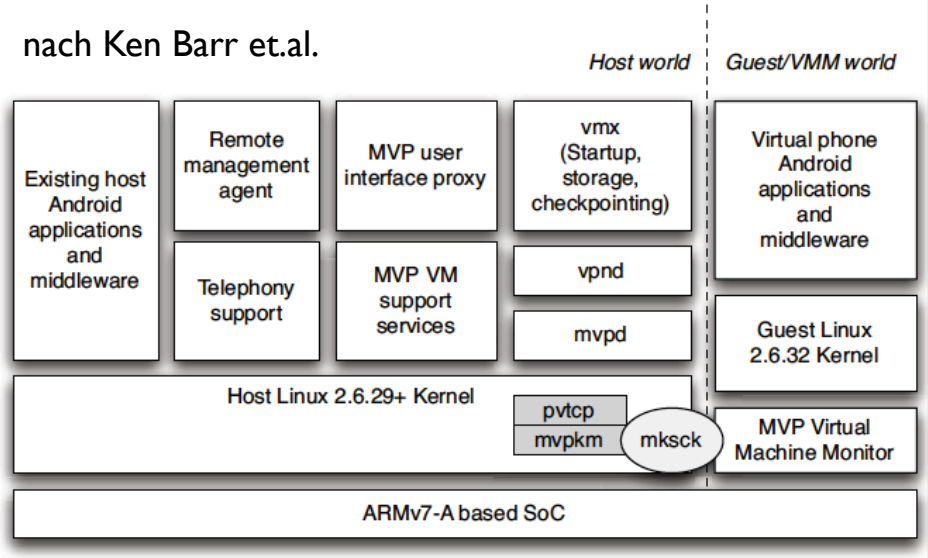
Beispiele:

Mobile Virtualization Platform (MVP) von VMware:

Type 2 hypervisor : hosted hypervisor

erlaubt den Betrieb eines Gastbetriebssystems neben dem Host-Betriebssystem

nach Ken Barr et.al.



siehe auch:

Ken Barr et.al. The VMware Mobile Virtualization Platform: is that a hypervisor in your pocket
http://dl.acm.org/citation.cfm?id=1899945

BYOD - Informationssicherheit

Virtualisierung

Beispiele:

Xen-on-ARM *(ARM: Advanced RISC Machines)*

Type 1 Hypervisor : direkt auf der Hardware

erlaubt mehrere Betriebssysteme nebeneinander zu betreiben

Projekt Zen und Samsung *

* siehe auch:
http://www.xen.org/products/xen_arm.html

BYOD - Informationssicherheit

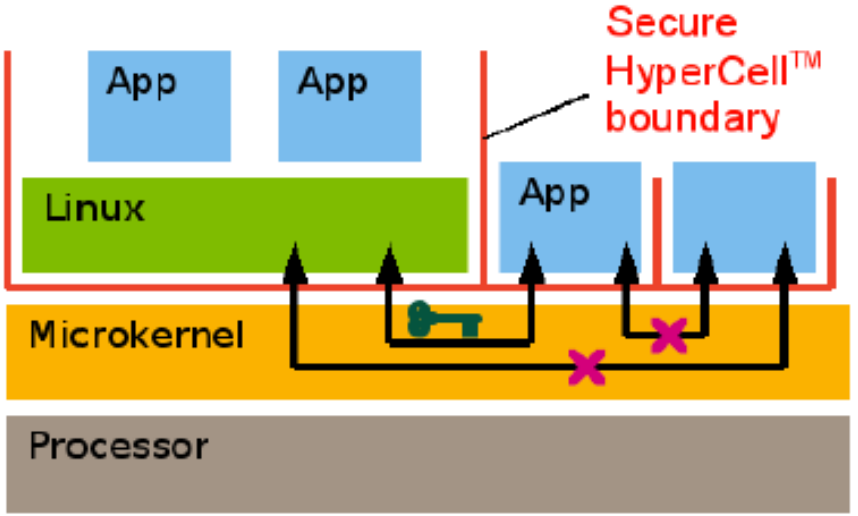
Virtualisierung

Beispiele:

Type I Hypervisor : Microkernel als Hypervisor

Apps laufen direkt auf dem Microkernel

Microkernel liefert Security Level



* siehe auch:

Hypervisor for consumer electronics
http://ssrg.nicta.com.au/publications/papers/Heiser_09.abstract

BYOD - Informationssicherheit

Virtualisierung

ARM-Virtualisierung
(ARM: Advanced RISC Machines)

Entwicklung von Hardware Virtualisierung

→ HW-Hersteller unterstützen nur noch Hypervisor

Hypervisor Security steht im Fokus der Sicherheitsfachleute

und der Angreifer

siehe auch:
www.arm.com

BYOD - Informationssicherheit

Virtualisierung

Derzeit bestehende Probleme bei der Virtualisierung von SPs:

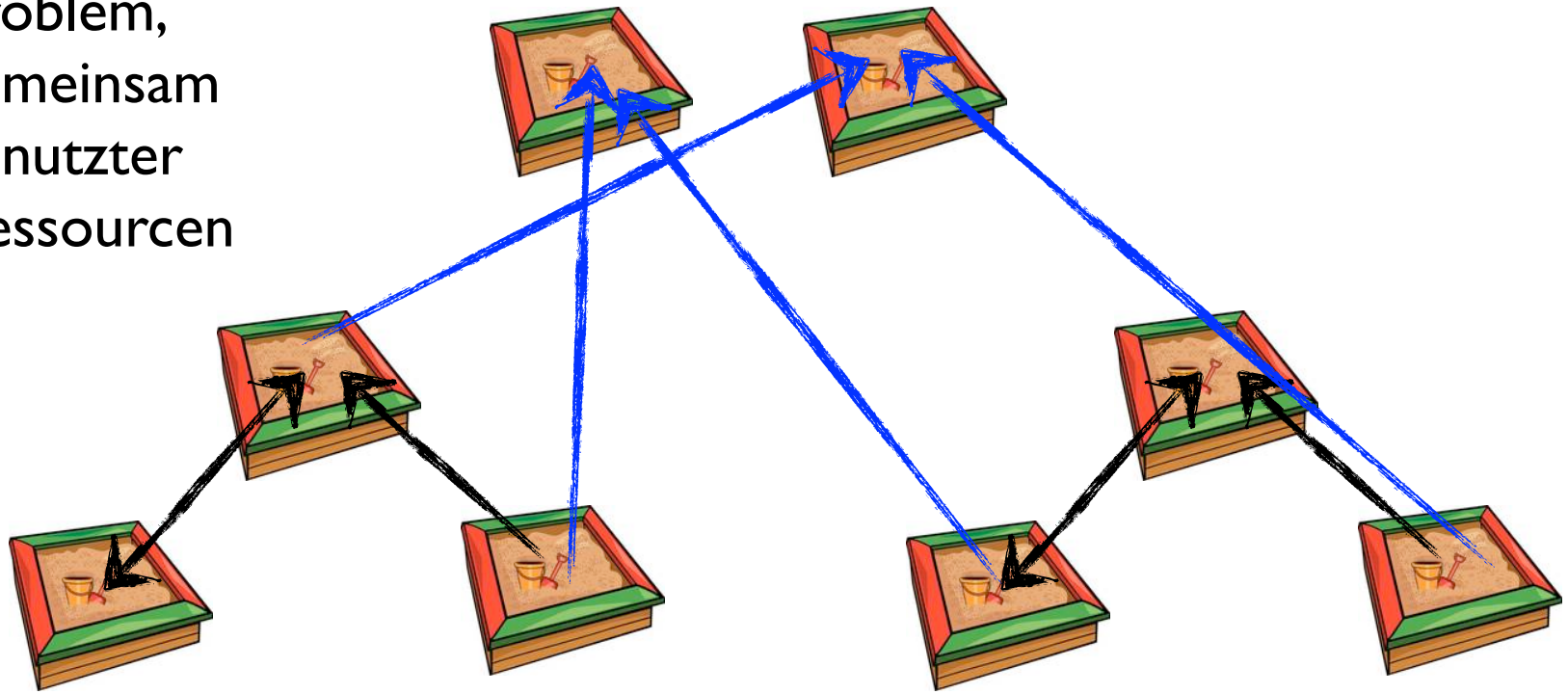
- Abhängigkeit von Hardware-Herstellern und Netzprovidern
- Energieverbrauch und Speicherplatz sind wesentliche Faktoren beim Design von Smartphones
- Hypervisor vom Typ 2 beinhalten eine Reihe von Unsicherheiten
- Hypervisor Security steht künftig im Fokus (bei Herstellern und Angreifern

BYOD - Informationssicherheit

Virtualisierung

Kamera  Mikro 

Problem, gemeinsam genutzter Ressourcen

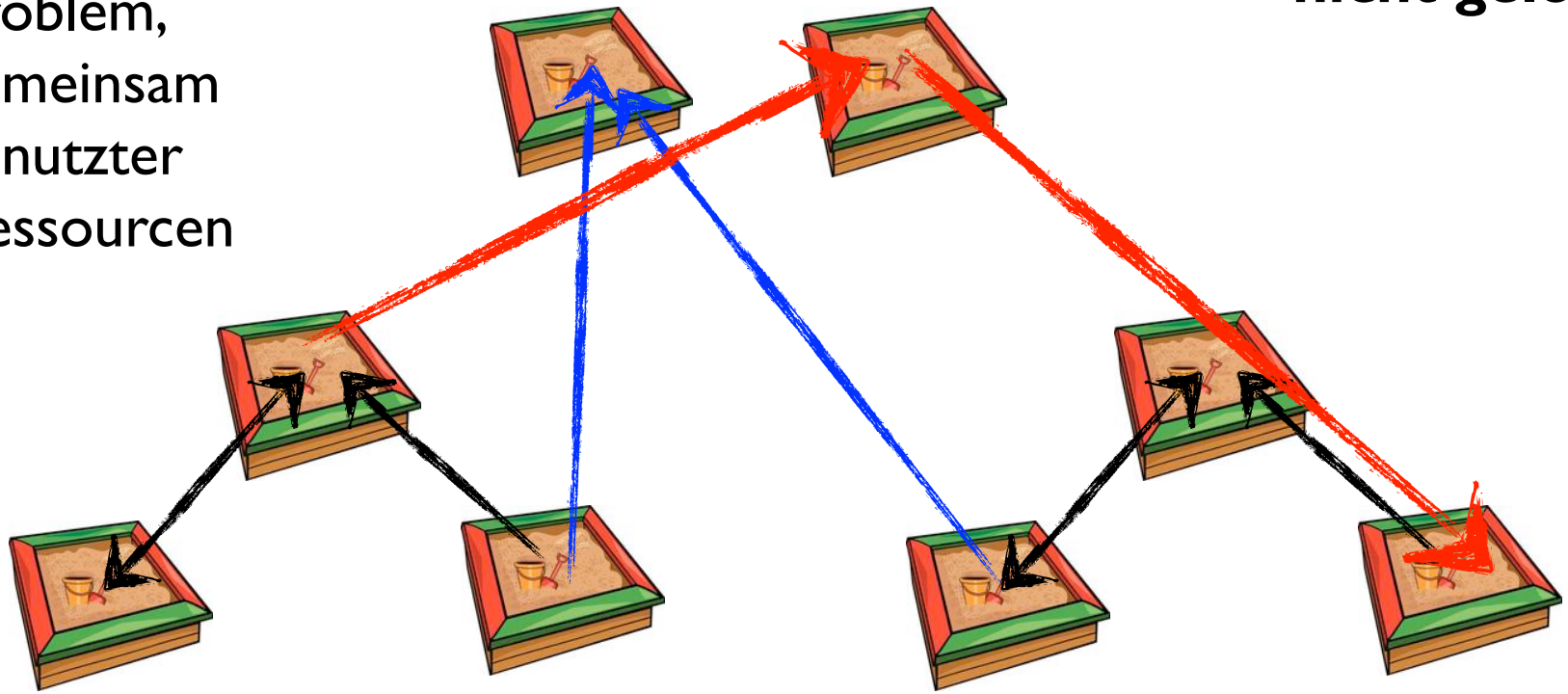


BYOD - Informationssicherheit

Virtualisierung

Kamera  **Mikro** 

Problem, gemeinsam genutzter Ressourcen



nicht gelöst

BYOD - Informationssicherheit

Technische Informationssicherheit

Firewalls:

Packetfilter: --> Sperren von Web-Seiten (URI)
--> Sperren von Zugängen, Ports (z.B. für Spiele)
--> zeitliches Sperren von Netzzugriffen
--> Nur bestimmte Rechner dürfen auf das Internet zugreifen

Zugriffskonzepte: rollenbasiert

--> erfordert technischen Sachverstand, ist aufwändig und löst nur ca. 50% der Probleme

BYOD - Informationssicherheit

Technische Informationssicherheit

vs.

Organisatorische Informationssicherheit

BYOD - Informationssicherheit

Organisatorische Informationssicherheit

<u>Standardkonforme Maßnahmen:</u>

Sicherheitsstrategie
Sicherheitsleitlinien
Sicherheitsorganisation
Bewusstsein für Informationssicherheit schaffen
Qualifizierungs- und Schulungsmaßmahmen
Penetrationstests
Audits

BYOD - Informationssicherheit

Organisatorische Informationssicherheit

Standardkonforme Maßnahmen:

Sicherheitsstrategie

Sicherheitsleitlinien

Was gehört wohl in eine Sicherheitsstrategie und in eine Sicherheitsleitlinie hinein?

BYOD - Informationssicherheit

Maßnahmen zum Schutz von **Android Smartphones**

1. **Nutzen Sie die eingebauten Android-basierten Sicherheitsfunktionen.**
   Diese Einstellungen sind unter *Settings* und *Location & Security* zu finden. Es empfiehlt sich auch, die etwas zeitaufwändige Möglichkeit zu nutzen, das Gerät im inaktiven Zustand zu sperren, um dann mithilfe des Kennworts das Gerät wieder zu aktivieren. Des weiteren gibt es mit der Fingerabdruck-Option den wohl sichersten Schutz vor fremdem Zugriff.
2. **Deaktivieren Sie die automatische Wi-Fi-Verbindung.**
   Der automatische Zugang zu offenen drahtlosen Netzen öffnet Tür und Tor für jeden, und lässt die Daten vom Smartphone frei durch den drahtlosen Router fließen.
3. **Lassen Sie nur Apps aus Android Market zu.**
   Dies liefert zwar keine hundertprozentige Garantie gegen gefälschte Apps, doch ist der offizielle Android-Store vertrauenswürdiger als die Dritter.
4. **Vergeben Sie keine Berechtigungen, deren Sinn Sie nicht verstehen.**
   Die meisten Schädlinge wollen Zugriffsrechte auf eine ganze Reihe von Informationen auf dem Smartphone. Auf diese Weise kann die Malware als Backdoor-Programm aktiv werden und auf dem Gerät Anruf-Logs ändern, Textnachrichten überwachen und abfangen und anderes mehr.
5. **Installieren Sie zusätzlich eine effektive mobile Sicherheits-App.**
   Ein solcher zusätzlicher Schutz ist nötig, weil die Cyberkriminellen immer neue Wege finden, die vorhandenen Schutzmechanismen der Geräte auszuhebeln.

BYOD - Informationssicherheit

Maßnahmen zum Schutz - klare Benutzungsregelungen

1. **Gerätesperre per PIN**
   automatisch aktiviert nach z.B. 2 Min., ausreichend lange PIN (> 4 Zeichen)
2. **Nutzung von VPN-Verbindungen beim Austausch von Unternehmensdaten**
3. **Verschlüsselung der gespeicherten Daten auf dem Smartphone**
4. **Keine Weitergabe des Smartphones an Dritte (Familienmitglieder, Freunde?)**
5. **Smartphones niemals unbeaufsichtigt liegen lassen**
6. **Bei Verlust, sofortige Information der Firmen-IT** (Hotline einrichten)
7. **Apps nur aus vorher festgelegten Quellen downloaden**
8. **Apps nur minimale und absolut notwendige Rechte vergeben**
   im Zweifelsfall immer die IT-Abteilung fragen/benachrichtigen
9. **Es sind sofort alle Updates für das Betriebssystem und alle Apps zu installieren**
10. **Ein Jailbrake des Smartphones ist unter keinen Umständen zulässig**

BYOD - Informationssicherheit

Maßnahmen zum Schutz - klare Benutzungsregelungen

11. Sicherheitsrichtlinien innerhalb der Organisation veröffentlichen und die Mitarbeiter die Kenntnis und deren Einhaltung abzeichnen lassen

12. Regelmäßige Schulungen über Gefahren bei der Nutzung mobiler Geräte durchführen
Schulungsmaßnahmen interessant gestalten, gegebenenfalls Erfolgskontrolle durch einen Test durchführen

13. Trennung von privaten und geschäftlichen Daten auf dem Smartphone realisieren

14. Diese Benutzerregelung betrifft auch und insbesondere die private Nutzung der Smartphones, Tablet-PCs und Notebooks

15. Es ist der IT-Abteilung der Organisation zeitnah zu melden, welche neuen Apps installiert wurden und welche Zugriffsrechte vergeben worden sind

BYOD - Informationssicherheit

Maßnahmen zum Schutz - **klare Benutzungsregelungen**

Würden Sie das mit Ihrem eigenen Smartphone, Tablet-PC oder Notebook akzeptieren?

BYOD - Informationssicherheit

Organisatorische Informationssicherheit

Bewusstsein für den sicheren Umgang mit IT schaffen

- Gefährdungen identifizieren
- Nutzungsregeln festlegen
- Netiquette
- Privatsphäre sichern auf unterschiedlichen Plattformen

--> erfordert Überzeugungsarbeit, teils umfangreichen Sachverstand und ist aufwändig