Bring Your Own Daemons - Mobility und Sicherheit

René Pfeiffer

DeepSec GmbH
https://deepsec.net/, rpfeiffer@deepsec.net

5. mobility summit austria 2014
Florido Tower Wien, Österreich.

DEEPSEC

Vorstellung

- Studium der Physik
- Benutzer mobiler Arbeitsplätze seit 1997
- selbstständig seit 1999 in der Informationstechnologie
- seit 2001 Lehrtätigkeit bei Firmenschulungen und dem Technikum Wien
- seit 2008 in der Geschäftsführung der DeepSec In-Depth Security Konferenz
- seit 2010 in der Geschäftsführung der Crowes Agency OG

Motivation – Warum?

- Verbreitung mobiler Endgeräte und “Cloud” Nutzung
- extrem kurze Produktzyklen mobiler Geräte
- verändertes Perimeterparadigma
- Sicherheitsrichtlinien als Tagesmenü
- Wie behält man Daten, Überblick und Verstand?

Informationssicherheit

- *Information* ist alles, was sich speichern / drucken / aufschreiben / merken läßt.
- *Sicherheit* ist ein Kompromiß zwischen Gruppen mit verschiedenen Agenden.
- *Informationssicherheit*
  - ist nicht wohldefiniert;
  - ist eine komplexe/periodische Tätigkeit, kein Zustand, kein Objekt, keine Ware;
  - ändert sich (im mobilen Bereich) ständig.

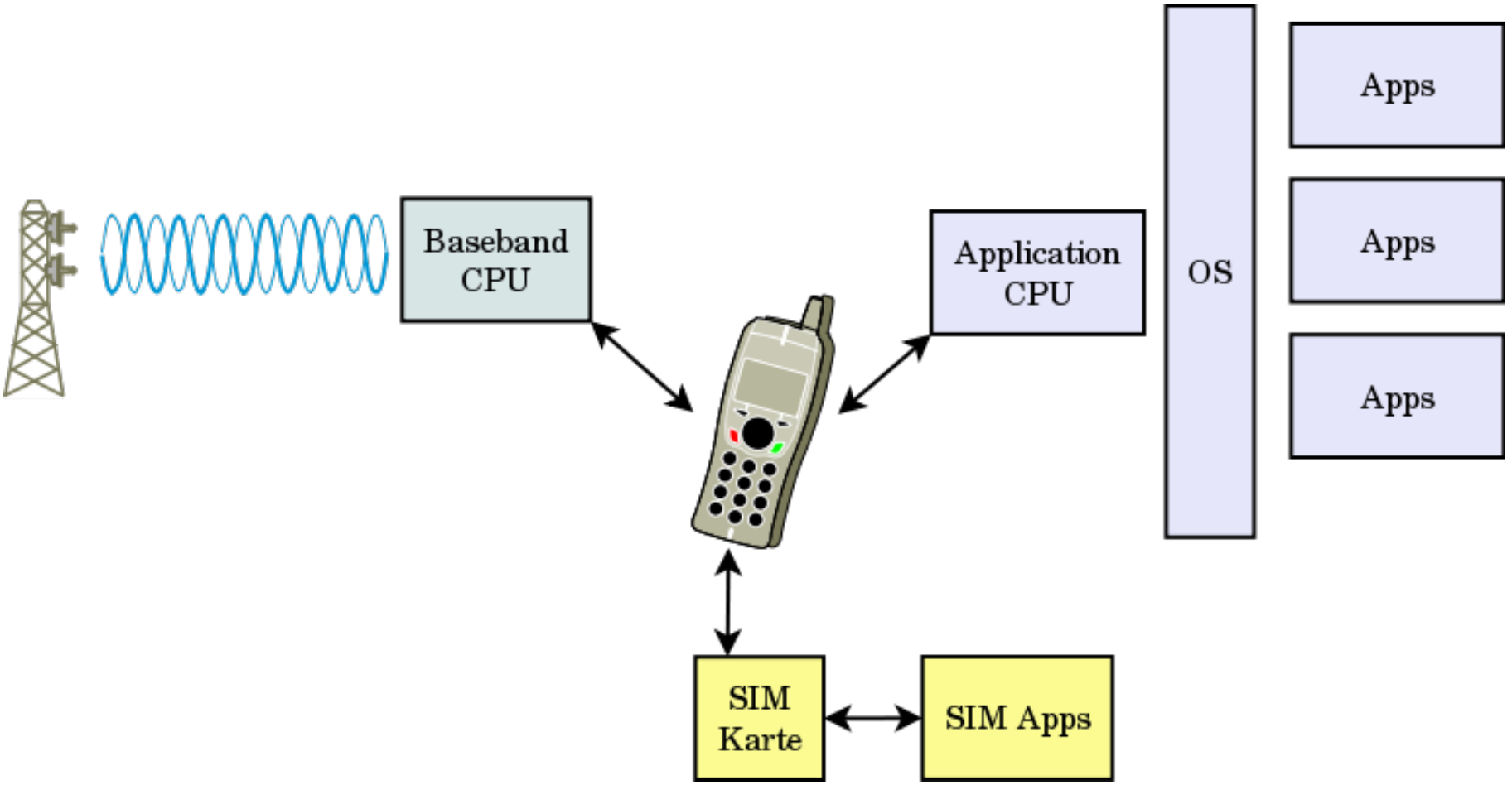
Internet

- Geburt am 29. Oktober 1969 mit zwei Knoten
- offenes Design
  - textbasierte Protokolle
  - offene Standards
- Sicherheit ist optional
  - Entwickler dürfen naiv sein (siehe z.B. WhatsApp, . . .)
  - Verschlüsselung und Authentisierung wahlweise
- Vertrauensstatus des Netzwerks ist *unbekannt* – großer Vorteil!

Mobilfunknetzwerke - Infrastruktur

- Vertrauensmodell in Mobilfunknetzwerken
  - Netzwerk ist Autorität und bedingungslos vertrauenswürdig
  - Client vertraut immer automatisch dem Netzwerk
  - “interessant” bei Roaming
- Verschlüsselung auf Luftschnittstelle ist
  - knackbar (A5/1, A5/2),
  - nicht vorhanden (A5/0, je nach Land)
  - noch nicht vorhanden (A5/3 bei 3G) oder
  - verbessert (4G/LTE/SAE/EPS/3GPP)
- Mittelsmannattacken möglich – stärkster Sender gewinnt
- Client (=Telefon) versteckt Informationen
  - eigenen Status und Aktivitäten im Mobilfunknetzwerk
  - Lokalisierungsanfragen (z.B. “stille” SMS)

Mobilfunknetzwerke



Smartphones & Tablets

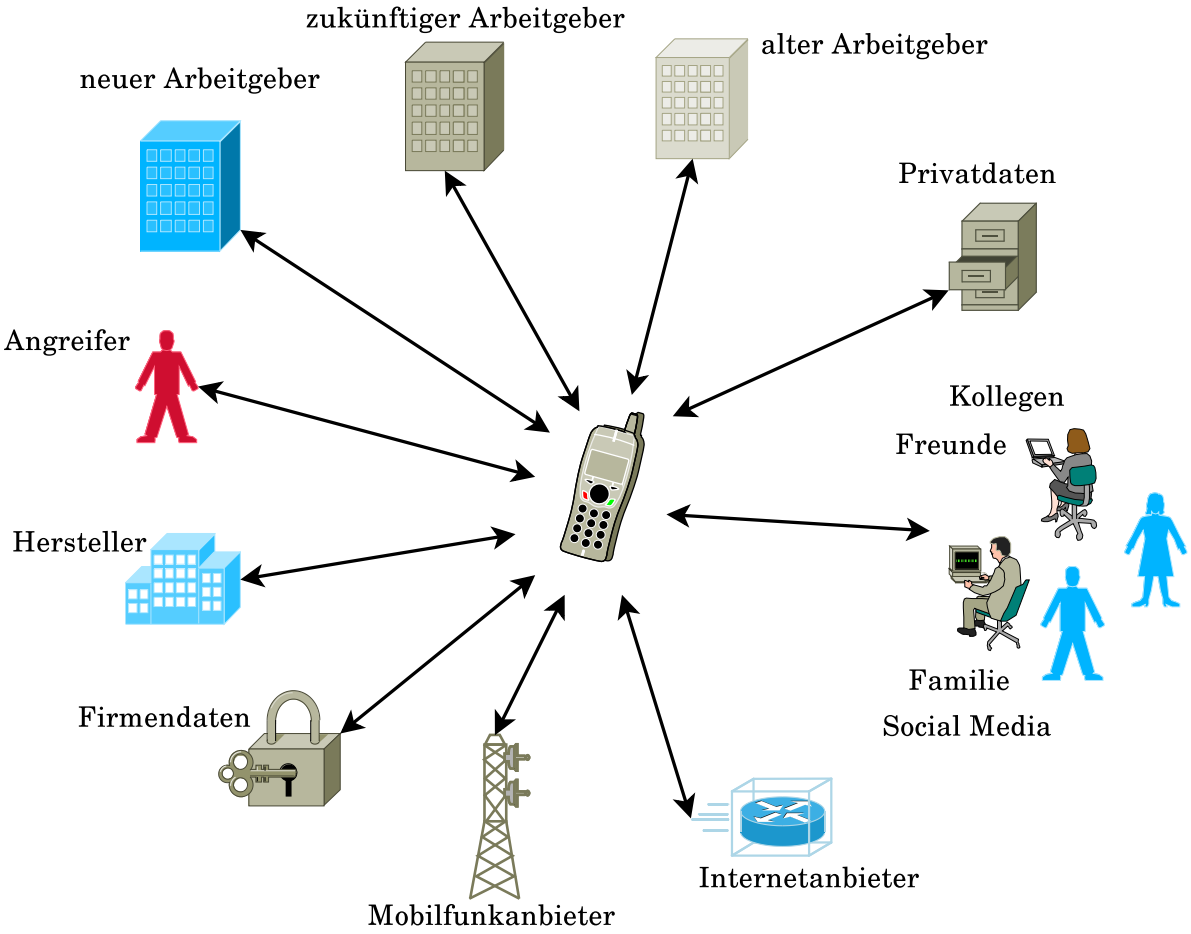
- schwerer zu kontrollieren als PC Plattform
  - Hardware zu unterschiedlich
  - schlecht anzupassen / vorzukonfigurieren
  - Produktzyklen noch kürzer
- reichhaltige Schnittstellen
  - Bluetooth
  - Mobilfunk
  - Near Field Communication (NFC)
  - WLAN

  Telefone kündigen sich *ständig* an
- ändern Funktionalität stetig durch *Apps*

Bring Your Own Device (BYOD)

- Angestellte bringen eigene Hardware mit – Telefon, PC, Tablet, Kaffeemaschine, Laptop, . . .
- Verbindund von Unterhaltungselektronik mit Arbeitswerkzeugen
  - Bonus für Hardware-Hersteller
  - Bonus für BYOD Integratoren
- BYOD ist ein *loses Konzept!*
  - BYOD bedarf wohlüberlegter Umsetzung
  - BYOD erfordert BYOD-taugliche Infrastruktur
- BYOD ist Outsourcing an eigene Mitarbeiter

End Node Problem



App Store Problem

- App Stores sind sicher – pures Wunschdenken
- Sicherheitsüberprüfungen der Stores unbekannt
  - Apple prüft Apps nur wenige Sekunden
  - Fake Tor app . . . in Apple's App Store for months
  - Malware Scanner for Google Play Store Apps
- Apples App Store verwendet SSL/TLS (HTTPS) erst seit März 2013 (!)
- eigene App Stores möglich, aber
  - erfordern Infrastruktur und
  - Vorbereitung

Herstellerproblem

- Geräte kommen mit Zoo vorinstallierter Apps, z.B.
  - Apps des Mobilfunkanbieters
  - Office Pakete
  - Multimediaplayer
  - Social Media Apps
- Apps teilweise nicht löschbar
  - Südkorea hat dies rechtlich verboten
- IT Security Grundsatz: *Minimierung von Software*
  - zwingend notwendig zur Absicherung
  - nur möglich per Jailbreak & Neuinstallation

App Permission Problem

- App Entwickler beherrschen Berechtigungen – pures Wunschdenken
- Berechtigungen zu weitläufig oder mißbraucht
  - Taschenlampen-App verfolgt Nutzer per GPS
  - Swype Keyboard App fragt Ort 4000+/Tag ab
  - Facebook App benutzt Kamera eigenständig
  - Skype nimmt Smartphone komplett in Besitz
- Berechtigungen werden nach/vor Installation nie kontrolliert
- Updates können Berechtigungen ändern

Security Management

- Security Management schließt Infrastruktur & Geräte mit ein
- IT Security Prinzipien analog zu anderen Technologien
  - Klassifikation von Daten
  - Kompartimentierung
- Existenz von BYOD Policy ist Grundbedingung!
- Implementation BYOD Policy = BYOD

Mobile Umgebungen definieren (1)

Mobile Umgebungen definieren (2)

Startpunkt: End Point Ansicht

- Anlehnung an Data Loss Prevention
  - Welche Daten darf End Point sehen?
  - Wie darf End Point mit Daten verbunden sein?
  - Wie werden End Points *korrekt* ausgeschieden?
- BYOD Geräte registrieren
  - Modelle/Hersteller einschränken
  - unregistrierte Geräte blockieren
- Auswahl Apps und Berechtigungen festlegen
- Softwareupdates automatisieren
- Sicherheits-Software installieren
  - Berechtigungen überwachen
  - Apps sperren

Mehrschichtiger Schutz

- *defence in depth* – mehrschichtiger Schutz
  - nicht alleine auf Hersteller verlassen
  - nicht alleine auf Schutzsoftware verlassen
  - nicht alleine auf Verschlüsselung verlassen
- Trennen von Zugangsdaten
  - eigene Zugänge nur für mobilen Bereich
  - spezielle Netzwerkbereiche nur für mobilen Bereich
- Erwartungshaltungen
  - Endgerät geht verloren
  - Endgerät wird kompromittiert
- *Versagen mit Stil* – ganz wichtig!

Zusammenfassung

- alle Netzwerke sind nicht vertrauenswürdig
- Mobilität & BYOD erhöhen Gefahren für Unternehmen
- Mobilkonzept auf sinnvolle Szenarien einschränken
- eigene IT aus Sicht der Endpunkte absichern
- eigenes IT Security Konzept flexibel gestalten

Fragen?


WARNING
You are now entering a top secret lair.
The area is patrolled regularly by
psychotic henchmen, rabid guard dogs,
sadistic killer clowns, insane minions,
genetically engineered super soldiers,
flesh eating zombies, evil lackeys
heavily armed titanium-robots and
super villains in training.

Kontakt

Informationen über die DeepSec und DeepINTEL Konferenzen erhält man über die folgenden Wege:

- https://deepsec.net/ & https://deepintel.net/
- E-Mail (PGP/GPG) 0x8531093E6E4037AF oder 0xE1170EDE22860969
- Videos http://www.vimeo.net/deepsec
- Twitter https://twitter.com/deepsec
- RedPhone & TextSecure: +43.676.5626390

Obligatorische geheime Botschaft

```
--BEGIN PGP MESSAGE--
Version: GnuPG v1.4.12 (GNU/Linux)

jA0EAwMCWyPontkww4RgycEAk47QuXBPkckVahSHlwmuFj7EYT21eyz9g4gtzDMD
67vohgWPYFi6tdCkEXE9yp/SeR8JxrR73bmukrY9779lkZ+vEWFaFNd+CdlQio6Q
DSLdayq57pd/E7jdvbhfkLzGpu/oAVGTsMcLRWWjTvSlVL65PRPZNBu0Ce22uMhr
4mFiBJCmL8+vTUXuuDo09QDu5CIxVbBWnJ9JN6Y4tJuiBykFgo0gVftmFmjJqVX6
GMs4ygxCdcdv6JEczXd53D7glIlFTeYEEk44rNCZDnVRpnQ9ByT3mgJBfp9g6nSg
3Z8hXPw1A5z12m3v8elCCt8jFbtQ4HSKsRW41oOGJ1JG8bHH5dGtYOTbNxrdPNuM
df7G1Emzd/vFWE5wKW8xoCP4V9oWLBdGZsyQejq13A6z92neR8uqpyZs5EjhUdYA
U0tClauFgkhu23eenRALlUQFKfhbmmCqvrfyR6OsH4k2+5Rxm05wn9YitdD6uTx+
3CiSEQYDkzjWb0PFl8jrJRbmu/1OfjSpcrZFtywyzOD2MmUFWG5NP/q/32wDOc61
DD0IBF2cUsmpL1AspjOiRStJuLPz5Bqa5WzUXzFTKT8H3Q==
=F7ea
--END PGP MESSAGE--
```

Hinweis: GnuPG kann auch symmetrische Verschlüsselung.