DECOIT

D•A•CH Security 2011

Sichere Plattform zur Smartphone-Anbindung

auf Basis von Trusted Network Connect (TNC)

Prof. Dr.-Ing. Kai-Oliver Detken
Geschäftsführer
DECOIT GmbH
URL: http://www.decoit.de
E-Mail: detken@decoit.de

Consultancy & Internet Technologies

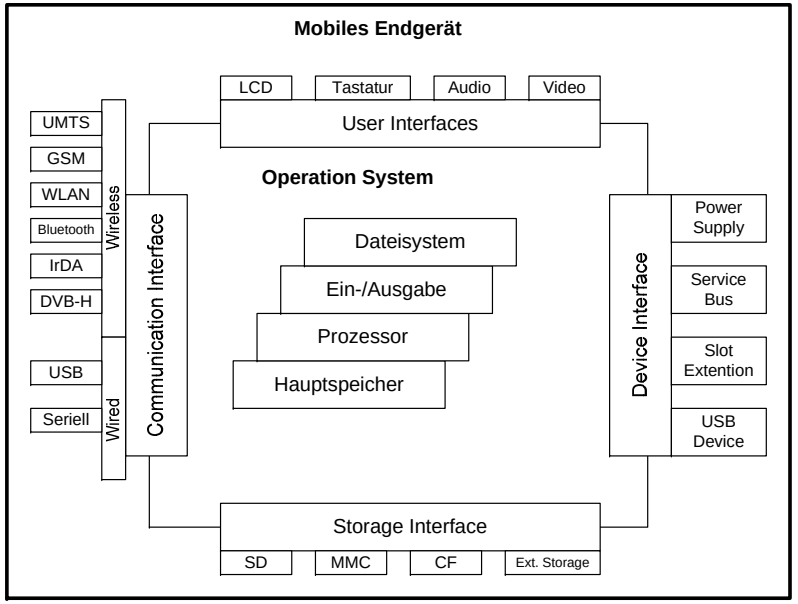
DECOIT

Smartphone-Vielfalt

- Google hat mit dem Android-Betriebssystem Nokia als Marktführer abgelöst
- Apple und Blackberry folgen auf den nachfolgenden Plätzen
- Der Smartphone-Markt wuchs um mehr als 88% weltweit (Android teilweise sogar um 600%)
- Verlierer im Smartphone-Markt im Vergleich zum Vorjahr ist Microsoft mit einem Marktanteil um 5%
- Der Handy-Kampf um den Verbraucher wird von Plattformen beherrscht und nicht mehr von Gerätefunktionen dominiert

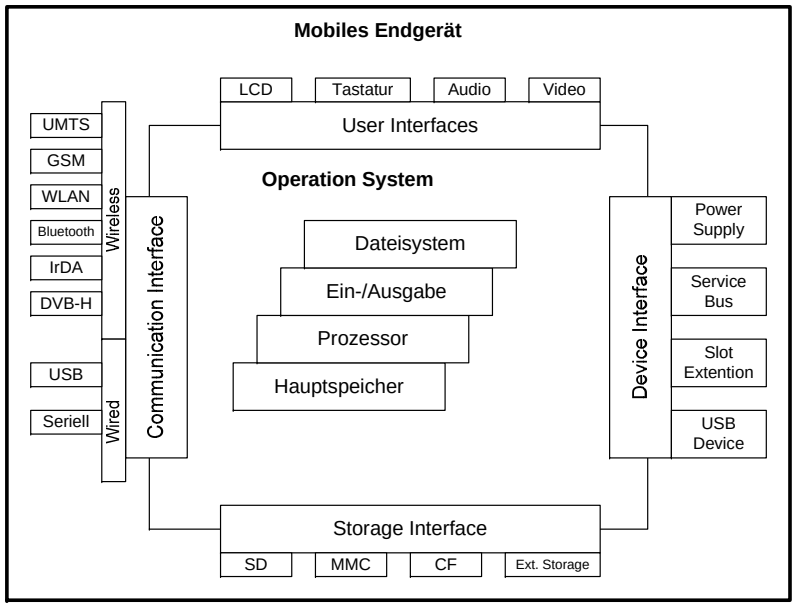
Eigenschaften mobiler Endgeräte (1)

- Mobile Endgeräte:
  - Zunehmende Integration von Funktionalitäten und Schnittstellen in mobile Endgeräte
  - Zusammenführung ursprünglich verschiedener Geräteklassen (Handy und PDA)
  - Leistungsfähigere Endgeräte
  - Mobile Endgeräte werden zudem als digitale Assistenten eingesetzt



Eigenschaften mobiler Endgeräte (2)

- Dienste:
  - Verstärkte Verbreitung von echten mobilen Diensten
  - Spezifischen Eigenschaften und Fähigkeiten der mobilen Endgeräte werden genutzt
  - Neue Benutzungsparadigmen wie „Digital Lifestyle“ oder „Ubiquitous Computing“ verändern die Anforderungen an mobile Dienste
  - Bedienbarkeit und Kommunikationsfähigkeit ist wichtig
  - Der Wunsch nach aktuellen und ständig verfügbaren Informationen führt zum mobilen Internet

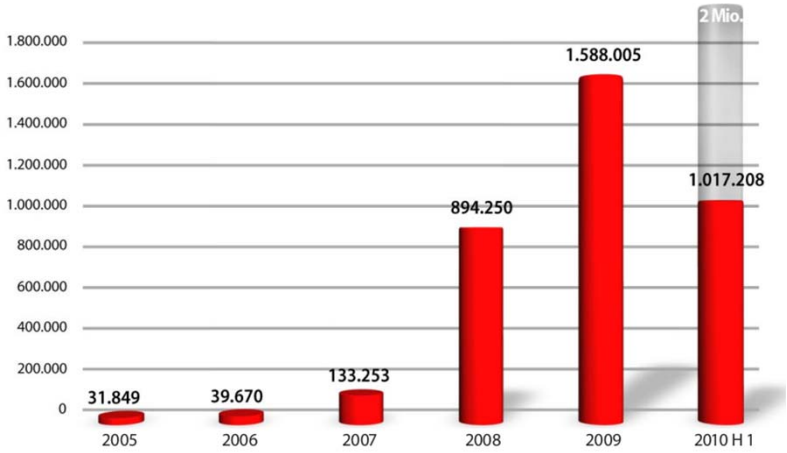


Neue Sicherheitsrisiken

- Fehlerhafte Konfiguration
  - Fehlkonfigurationen in Sicherheitskomponenten wie Firewalls, VPN-Gateways etc.
  - Betriebssystemfehler der Handys
- Offene mobile Endpunkte
  - Zugriff und Verwaltung von kritischen Geschäftsdaten
  - Keine Integritätsüberprüfung der Hardware ist möglich
  - Wachsender Malware-Markt für Smartphones
  - Verwendung von mobilen Endgeräten in unsicheren Netzen

Anstieg von Malware

- Laut den Prognosen von Sicherheitsexperten wird es in den kommenden Jahren zu einem sprunghaften Anstieg von Schadsoftware (Malware) kommen
- Dabei rücken vor allem Smartphones und andere mobile Endgeräte (z.B. Tablet-PCs) zunehmend in den Fokus der Angreifer



GData Malware Report 2010

VOGUE (www.vogue-project.de)

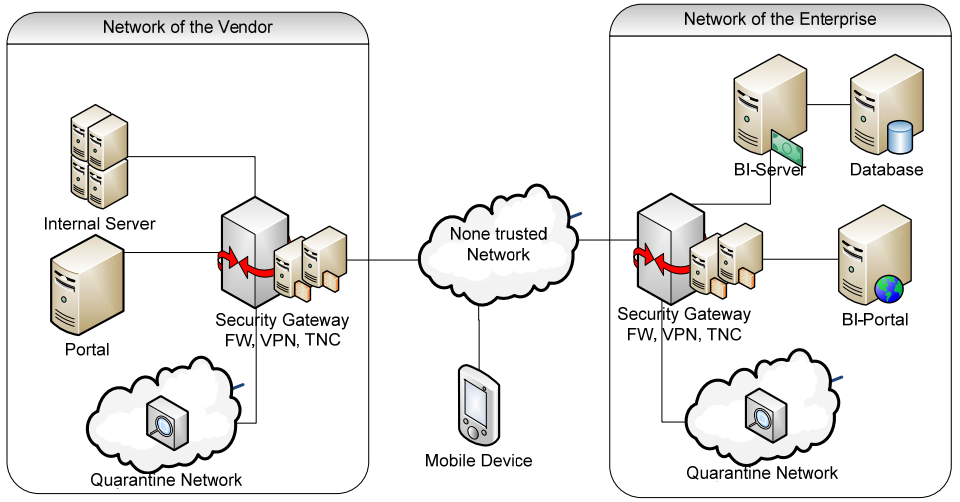
- Das VOGUE-Projekt ist ein nationales BMBF-Projekt
- Es startete im Oktober 2009 und endet im September 2011
- Folgende Partner sind in diesem Projekt involviert:
  - DECOIT GmbH (Konsortialführer)
  - Fraunhofer SIT (Darmstadt)
  - Mobile Research Center (Bremen)
  - NCP engineering GmbH (Nürnberg)
  - OTARIS (Bremen)

Ziele des VOGUE-Projektes

- Erschließen des aufkommenden Marktes von TPM-basierten Lösungen im mobilen Bereich für die deutsche Wirtschaft
- Entwicklung einer Basis zur Erprobung von TPM-basierten Lösungen unter Verwendung eines Emulators der KMUs den Einstieg in dieses neue Geschäftsfeld ermöglicht
- Ermöglichen von sicherheitskritischen und mobilen Geschäftsprozessen durch die Etablierung einer vertrauenswürdigen Plattform für mobile Endgeräte. Hierdurch wird bereits möglichen Angriffen vorgebeugt bzw. deren Schaden drastisch reduziert
- Demonstration auf der Basis einer verbreiteten Plattform für mobile Endgeräte

Generisches Anwendungsszenario

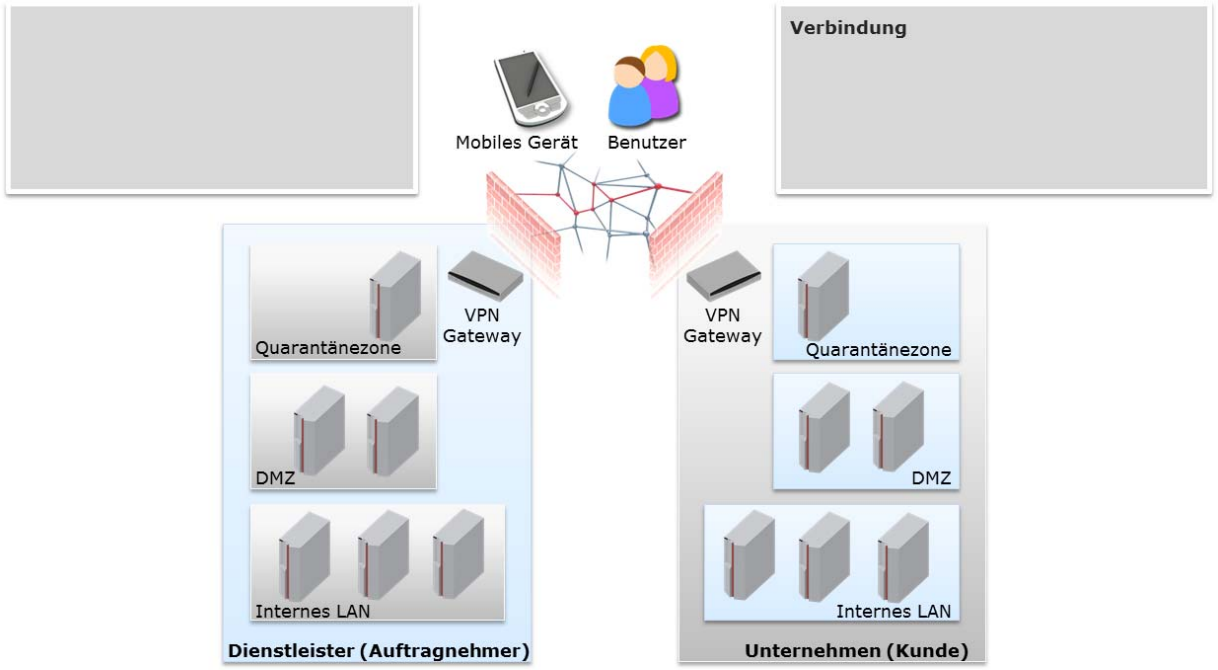
- Folgendes Sicherheitsniveau haben wir heute:
  - Keine Sicherheitsüberprüfung der Software (Patches)
  - Keine Hardware-Kontrolle verfügbar
  - Kein Support für verschiedene Security Policys
- Es wurde daher im ersten Arbeitspaket ein generisches Szenario aus unterschiedlichen Anwendungsfällen entwickelt
- Zwei verschiedene Netze werden mit unterschiedlichen Sicherheitsrichtlinien verwendet
- Kleine Demonstration: animiertes Szenario



Einwahl-Szenario von VOGUE

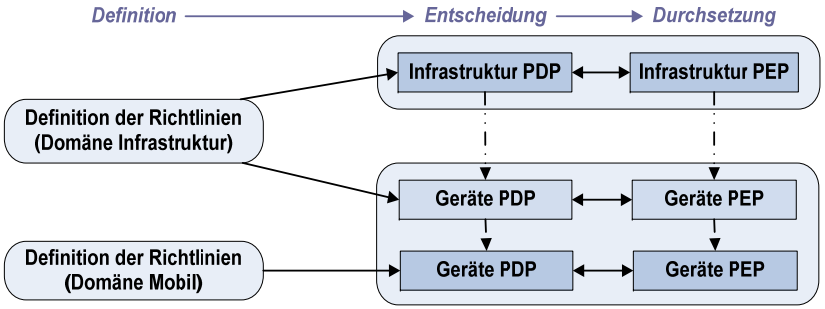
Animiertes Szenario

VOGUE



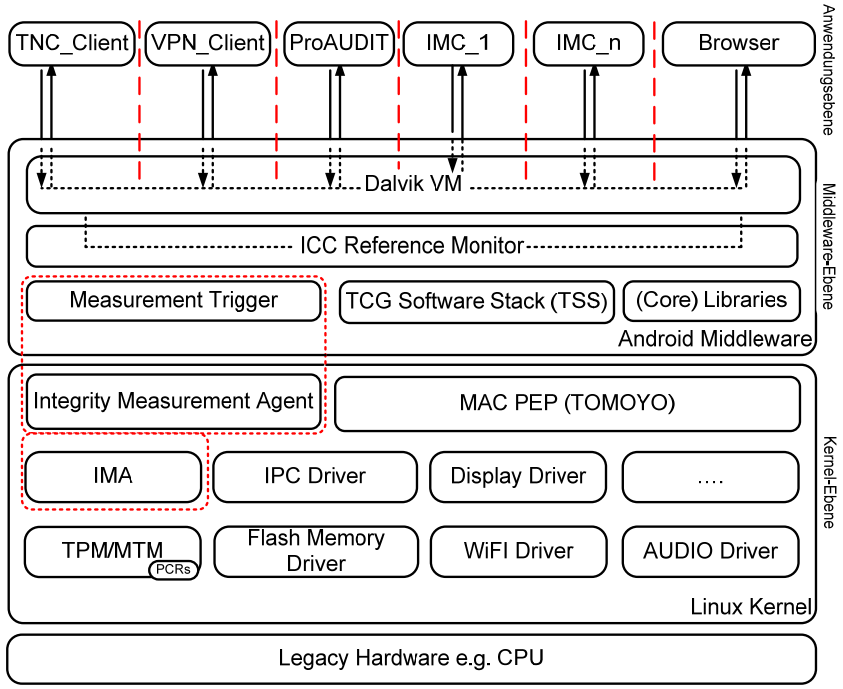
Teilung der Richtliniendomänen in Infrastruktur und Gerät

- Der Policy Decision Point (PDP) erhält die Informationen und prüft diese gegen die Richtlinie
- Die Durchsetzung der Richtlinie wird durch die Policy Enforcement Points (PEP) erreicht, die außerdem zum Sammeln der nötigen Information dienen
- Die Entscheidung und Durchsetzung von Richtlinien bzgl. Infrastrukturressourcen muss auf Infrastrukturseite geschehen
- Entsprechend müssen die Richtlinien der mobilen Domäne auf dem mobilen Gerät entschieden und durchgesetzt werden
- Im Falle des Einsatzes von Software und Daten auf dem mobilen Gerät, müssen Richtlinienentscheidungen der Infrastrukturdomäne auch auf dem Gerät repräsentiert sein



Mobile VOGUE-Plattform unter Android

- Mobile Betriebssysteme wie Android ermöglichen die Entwicklung von Anwendungen (offene Plattform)
- Root-of-Trust Implementierung ist durch das Mobile Trusted Module (MTM) möglich
- MTM/TPM-Software- Emulation wurde für die Entwicklung eingesetzt
- Es wird die Integrity Measurement Architektur (IMA) als Kernel-Erweiterung eingesetzt, um die Integrität weiterer Kernel-Module, Middleware mit ausführbaren Codes, Konfigurationsdateien, Skripte, dynamische Bibliotheken vor der Ausführung messen zu können
- TOMOYO wird als Referenzmonitor eingesetzt, der nicht erlaubte Interaktionen bzw. nicht autorisierte Zugriffe auf Gerätressourcen auf Kernel-Ebene unterbindet



Projektergebnisse von VOGUE

- Die Definition der Anforderungen und mobiler Szenarien wurde beendet und in ein generisches Szenario überführt
- Eine Analyse mobiler Betriebssysteme wurde vorgenommen, um die Basis für die Entwicklung festzulegen
- Während des Projektes standen Software-Emulationen für die Verwendung von TPM- oder MTM-Chips zur Verfügung
- Innerhalb des Projektes wurde eine VOGUE-Architektur entwickelt
- Es sind die verschiedenen Module der VOGUE-Plattform (OpenVPN, FreeRADIUS, LDAP, TNC-Client/-Server) erweitert, zusammengeführt und getestet worden
- Ein erster Demonstrator wurde bereits im November 2010 fertiggestellt
- Die Plattform wurde verfeinert und Android-Versionen kontinuierlich angepasst
- Abschließend wird es noch eine Analyse des Prototypen geben

Fazit und Ausblick

- Mobile Endgeräte erweitern die vorhandene IT-Infrastruktur von Unternehmen
- Sie müssen deshalb in die vorhandenen IT-Sicherheitsrichtlinien bzw. das Sicherheitskonzept integriert werden
- Das BSI gibt aufgrund der wachsenden Malware-Probleme inzwischen die Empfehlung heraus Smartphones (speziell iPhone und Blackberry) nicht mehr im Unternehmen einzusetzen
- Ausnahmen sollten nur zugelassen werden, wenn die Endgeräte Simko-2-Verschlüsselungstechniken nutzen können
- Simko 2 beinhaltet: digitale Identität, sichere Authentifizierung, Verschlüsselung der Daten, sichere Datenkommunikation, abgesicherter Boot-Prozess, kontrollierter Prozess für Zusatzsoftware
- Grundsätzlich sollten mobile Endgeräte wie vollwertige Rechnersysteme behandelt und eingesetzt werden

DECOIT

Vielen Dank für ihre Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
info@decoit.de

Consultancy & Internet Technologies