

Sicherheitsfälle mobile Endgeräte

Keynote KSÖ Sicherheitskongress Panel III

31. Mai 2011, 16:00

Messe Wien

Prof. (FH) Priv.-Doz. DI Dr. René Mayrhofer

Fachhochschule Hagenberg (Mobile Computing)

eSYS GmbH (Security Consultant)

rene.mayrhofer@fh-hagenberg.at

The most profound technologies are those that **disappear**. They weave themselves **into the fabric of everyday life** until they are **indistinguishable** from it.

Mark Weiser, 1991, „The Computer for the 21st Century“

Arten von mobilen Endgeräten



Arten von mobilen Endgeräten



Problemfelder

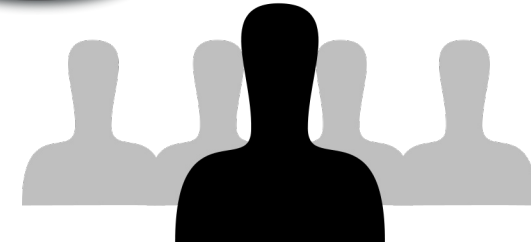
Sicherheit für wen?

- mobiles Gerät
- Infrastruktur
- Benutzer



Sicherheit wofür?

- (auf dem Gerät gespeicherte) Daten
- (drahtlose) Kommunikation
- Privatsphäre (des Benutzers)





Datensicherheit auf mobilen Geräten

Bedrohungen

- mobile Endgeräte sind vollständige Computer, aber mit mehr Schnittstellen
- Malware
- physischer Zugriff
- Verlust und Rückruf
- drahtlose Netzwerke
- (derzeit) kaum Sicherheitsmaßnahmen



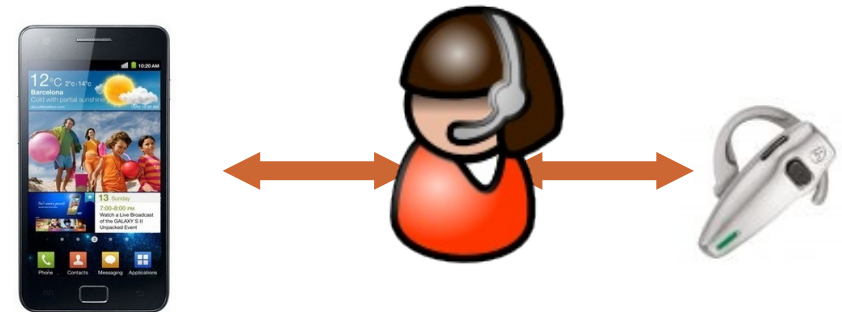
⇒ **Datensicherheit am Gerät nur sehr schwierig und nur mit großem Aufwand oder großen Einschränkungen der Endanwender zu gewährleisten**



Drahtlose Kommunikation

Bedrohungen

- Abhören (eavesdropping)
- Wiederholen (replay)
- Verändern (modification, fabrication)
- Vortäuschen eines Absenders (faking, spoofing)
- Blockieren (denial of service)
- Man-in-the-Middle
- Angriffe auf Lücken im Endgerät
- Überwinden von Kommunikationssperren und Überwachungsmaßnahmen durch verschiedene Netzwerkanbindungen und Anonymisierungstechniken



⇒ **Drahtloskommunikation muss als nicht vertrauenswürdig angenommen werden**



Privatsphäre mobile Benutzer

Bedrohungen

- viele persönliche Daten auf dem Endgerät
 - Kontakte
 - Kalender
 - Nachrichten (Email, SMS, Instant Messaging)
 - aufgenommene Bilder, Videos
 - Historie (Anwendungen, Web-Browser, Suchbegriffe)
- detailliertes Profiling von Endbenutzern möglich und wirtschaftlich reizvoll
- Social Engineering durch Informationen auf dem Endgeräte sehr einfach
- zunehmende Zahl von sicherheitskritischen Anwendungen
 - Kreditkarten- und Bankdaten
 - Gesundheitsdaten
 - Bewegungs- und Kommunikationsmuster



Proliferation mobiler Plattformen

- Symbian OS
- Windows Mobile / CE / Windows Phone 7
- Linux
 - LiMo, EZX, etc.
 - Android
 - Maemo / MeeGo
 - bada
- Apple iPhone
- Blackberry
- Java 2 Micro Edition (J2ME)



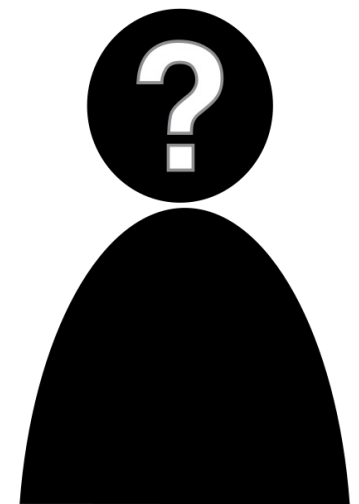
Vergleich mobiler Plattformen

	Android	iOS	Blackberry	Symbian
Einschränkung auf App Store	nein	ja	nein	nein
Sandbox für Anwendungen	ja	ausgewählte (Safari)	nein (unbekannt)	nein
Signierte Anwendungen	ja	ja	ja	ja
Capabilities für Anwendungen	ja (Alles-oder-Nichts)	nein	ja (konfigurierbar)	ja (konfigurierbar)
Garbage Collection	ja (Java)	nein (Objective C)	ja (Java)	nein (C++)
Absicherung gegen Exploits	kein NX kein ASLR	NX Stack+Heap kein ASLR	unbekannt	kein NX kein ASLR
Daten-verschlüsselung	nein	ja, aber Lücken	ja	nein

Sichere mobile **benutzbare** Kommunikation

Aufmerksamkeit ist eine eingeschränkte Ressource

- Vision von Pervasive Computing: Verwendung **Hunderter** Services täglich, nahtlose Einbettung in tägliches Leben, **spontane** Verwendung, unterschiedliche administrative Domänen
- Ständige Sicherheitsabfragen und viele verschiedene, „gute“ Passwörter **funktionieren in der Praxis nicht!**
- Benötigt Sicherheitsmaßnahmen
⇒ **unaufdringlich**, aber **nicht unsichtbar**



Sicherheit vs. Privatsphäre

Herausforderungen für Gesetzgebung

- Treffsichere Überwachungsmaßnahmen und Interventionsmöglichkeiten
- **und**
- Wahrung der Grundrechte von Bürgern

Problematik des Digital Divide

- Organisierte Kriminalität kann **Überwachung trivial umgehen**
(bspw. Vorratsdatenspeicherung und Zugriff per Sicherheitspolizeigesetz)
 - Verschiedene Netzwerke, WLAN Hotspots, Pre-Paid SIM Karten, etc.
 - Anonymisierung
- Trifft daher oft nur breite Bevölkerungsschicht

Problematik der Datensicherheit

- **Mobile Geräte** erzeugen bisher unbekannte **Datenflut**
- **Einmal aufgezeichnete Daten** erzeugen nicht abschätzbares **Missbrauchspotenzial**

Forschungslabor **Mobile Security**

Offene Fragestellungen in Forschung und Entwicklung

- **Grundlagenforschung:** Hardware, Kryptographie, mobile Betriebssysteme
- **Angewandte Forschung:** Einbettung in Plattformen und Unternehmen
- **Soziale Einbettung:** Besseres Benutzerverständnis

Konsortium

- **Laborleitung:** Fachhochschule Hagenberg
- Secure Business Austria
- NXP Semiconductors
- underground-8
- ?



Danke für Ihre Aufmerksamkeit!

Folien: <http://www.mayrhofer.eu.org/presentations>
Spätere Fragen: rene.mayrhofer@fh-hagenberg.at
rene@mayrhofer.eu.org

OpenPGP key: 0x249BC034 und 0xC3C24BDE
717A 033B BB45 A2B3 28CF B84B A1E5 2A7E 249B C034
7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE