



# Mobile Security

## Sicherheit mobiler Endgeräte

Manuel Atug

in Vertretung für **Randolf Skerka**

SRC Security Research & Consulting GmbH

- Arten mobiler Endgeräte
- Sicherheitsaspekte beim Einsatz mobiler Endgeräte
- Exkurs: Bluejacking
- Schutzmöglichkeiten
  - ▶ *Diebstahlschutz*
  - ▶ *Datenverschlüsselung*
  - ▶ *Zugriffskontrolle*
  - ▶ *Datensicherung*
- Nutzungspolitik mobiler Endgeräte

*«During the lead-up to the Gulf War, a senior British military officer had his laptop computer stolen from the back seat of his car while it was parked. What was significant about this theft was that the laptop contained files, which documented the allies' plans for the gulf war. After news reports about the incident aired - the computer was returned by the recalcitrant thief. His comment was that he was a "thief and not a bloody spy."»*

**<http://eiminc.net/clientsecurity2.htm>**

*«A British spy lost a security services laptop after drinking too much and losing track of it. The £2,000 computer was reported to contain details of British secret agents working abroad.»*

**THE TIMES 1990** *"Laptop stolen from the back of a Ministers car", "The laptop contained details of the Desert Storm invasion plans"*

- Mobile Endgeräte enthalten immer mehr sensible Informationen.
- Kosten der „Geräte“ sind hierbei der geringere Schaden.
- Durch die „Größe“ der Geräte entstehen zusätzliche Risiken.
- Sensibilisierung ist ein wesentlicher Schutz.

# Arten mobiler Endgeräte



# Arten mobiler Endgeräte

- Laptops
- Notebooks
- Personal Digital Assistants (PDA)
  - ▶ **PalmOS based:** *PalmPilots, Handspring*
  - ▶ **EPOC based:** *Psion*
  - ▶ **WindowsCE based:** *HP Jornada*
  - ▶ **Symbian OS (Smart-Handys):** *SiemensSX1, Nokia7650*
- Smart-Phones
  - ▶ *Nokia 6220, Siemens S55*
- Bluetooth-Handys
  - ▶ *Nokia 6220, SonyEricsson T630, Siemens S55*

- Mobile Endgeräte
  - ▶ werden in unsicheren Umgebungen betrieben.
  - ▶ sind gegen direkte Angriffe stärker verwundbar als Systeme, die in einer Büroumgebung betrieben werden.
  - ▶ sind gegen Diebstahl, Manipulation, Zerstörung etc. besonders verwundbar.
  - ▶ beinhalten und verarbeiten sensible Daten.
- Verlust oder Offenlegung vertraulicher Daten kann einen Vertrauensverlust zur Folge haben.
- Mobile Endgeräte enthalten Einrichtungen für kabellose Kommunikation (IrDA, Bluetooth, WLAN).

- **Offenlegung (Disclosure)**

Bekannt werden der auf dem Gerät gespeicherten (sensiblen) Daten.

- ▶ *Schwache Software und Betriebssysteme*
  - Jeder, der Zugang zum Gerät erhält, kann auf die Daten zugreifen.
- ▶ *Auswirkungen von Malware (Spyware, Viren etc.)*
  - Unbewußt installiert
  - Ausreichender Schutz ist unabdingbar
- ▶ *Gedankenlosigkeit und Nachlässigkeit von Anwendern*

Das System muß einfach zu bedienen und zuverlässig sein

  - Installation unbekannter Software
  - „Shoulder Sniffing“
  - Mangelnde Aufsicht des Geräts

- **Private Benutzung**

Nutzung von Firmeneigentum für private Zwecke

- ▶ *Kinder*

- Installieren Spiele, die aus dem Internet geladen werden
- Führen „aktive Inhalte“ auf Webseiten aus
- Installieren Software, die mit Freunden getauscht wurden

- ▶ *Nutzung zum Surfen im Internet*

- Infizierung mit Malware aus dem Internet
- Zugriff auf Webseiten mit aktiven Inhalten (ActiveX, Java, JavaScript ...)

- ▶ *Der „Uuups“ Effekt*

- Versehentliche Löschung / Zerstörung von Daten
- Batterie / Akku vergessen rechtzeitig auszuwechseln

- **Remote access**

Risiken beim Fernzugriff auf vertrauliche Daten

- ▶ *Offenlegung (Disclosure)*

- Unverschlüsselte Übertragung vertraulicher Daten
- Versand vertraulicher Daten an den falschen Empfänger

- ▶ *Höhere Anfälligkeit gegen Angriffe*

- Zugriff auf das Internet über öffentliche POPs
- Zugriff auf das Internet über öffentliche WLAN Access Points
- Keine Absicherung über Firmen-Firewall

- **Physikalische Angriffe**

Angriffe, die durch physikalische Einwirkung Schaden verursachen

- ▶ *Diebstahl*

- Diebstahl des gesamten Geräts oder Teile hiervon

- ▶ *Zeitweiser Zugriff auf das Gerät*

Jemand erhält zeitweise Zugriff zum Gerät

- Manipulation
- Zerstörung
- Kopieren von Daten
- Offenlegung von Daten

***Physikalischer Zugriff kann genutzt werden, um softwarebasierte Zugangskontrollen zu umgehen!***

- **Zusammenfassung**

- ▶ Finanzieller Verlust
- ▶ Verlust von Geräten (Verlust der Verfügbarkeit)
- ▶ Manipulation der Geräte (Verlust der Integrität)
- ▶ Verlust der Daten (Verlust der Verfügbarkeit)
- ▶ Manipulation der Daten (Verlust der Integrität)
- ▶ Offenlegung der Daten (Verlust der Vertraulichkeit)

# Exkurs: Bluejacking

- **Der Begriff**

- ▶ *Abgeleitet aus „Bluetooth“ und „Hijacking“*
- ▶ *Bluejacking ist die Möglichkeit, an bluetoothfähige Endgeräte Nachrichten zu schicken, ohne dass man dazu autorisiert wurde.*

- **Bluetooth**

- ▶ *Industriestandard (Bluetooth Special Interest Group), 1998*
- ▶ *Funknetz für kurze Distanzen*
  - Klasse 3 -> Niedrigste Leistungsklasse (1 mW, 0 dBm), max. Entfernung 10m*
  - Klasse 2 -> Mittlere Leistungsklasse (ca. 2 mW, 4 dBm), max. Entfernung 20m*
  - Klasse 1 -> Höchste Leistungsklasse (100 mW, 20 dBm), max. Entfernung 100m*
- ▶ *730 kbit/s Netto-Übertragungsrate (11 x schneller als ISDN)*

- **Die Gefahren**

- ▶ *Vergleichbar mit einem „Klingelstreich“*

- **Die Lösung:**

- ▶ *Bluetooth am Handy abschalten oder*
- ▶ *Discover-Funktion deaktivieren*





- **Hintergrundinfos**

- ▶ The world's first website dedicated to bluejacking  
<http://www.bluejackq.com/>
- ▶ The Official Bluetooth® Wireless Info Site  
<http://www.bluetooth.com/>
- ▶ Bluetooth™ Security White Paper  
[http://www.bluetooth.com/upload/24Security\\_Paper.PDF](http://www.bluetooth.com/upload/24Security_Paper.PDF)
- ▶ An Overview of Bluetooth Security  
[http://www.giac.org/practical/gsec/Nikhil\\_Anand\\_GSEC.pdf](http://www.giac.org/practical/gsec/Nikhil_Anand_GSEC.pdf)
- ▶ Bluejacking schürt Angst vor Handy-Viren  
<http://www.sophos.de/virusinfo/articles/bluejack.html>
- ▶ Heise Bluetooth FAQ  
<http://www.heise.de/mobil/bluetooth/faq>
- ▶ PC-WELT: "Bluejacking" - Ihr Handy wird gekapert  
<http://www.pcwelt.de/news/vermishtes/35598/>
- ▶ Bluetooth Security  
<http://www.niksula.cs.hut.fi/~jiitv/bluesec.html>

- **Benutzersensibilisierung**
  - ▶ *Richtlinien, Policies, Leitfäden, ...*
- **Diebstahlschutz**
  - ▶ *Befestigung an einem festen Gegenstand*
  - ▶ *Ständige Beaufsichtigung des Geräts*
  - ▶ *Diebstahlversicherung*
- **Datensicherung**
  - ▶ *Regelmäßige Speicherung der Daten auf Wechselmedien (CDR)*
  - ▶ *Sicherung der Daten auf einem Backup-Server*

- **Datenverschlüsselung**

Soviel wie möglich verschlüsseln!

- ▶ *Datenbankverschlüsselung (PalmOS Systeme)*
- ▶ *Festplattenverschlüsselung*
  - Hardwarebasiert
  - Softwarebasiert
- ▶ *Dateisystemverschlüsselung*
  - Virtuelle Festplatten (z.B. PGPDisk, E4M, Scramdisk, loopAES [linux], )
  - Partitionsverschlüsselung
- ▶ *Explizite Dateiverschlüsselung*

***Auch temporäre Dateien können sensible  
Informationen enthalten!***

- **Zugangskontrolle**

- ▶ *Vorhandene Möglichkeiten ausreizen*
  - Verwendung starker Kennworte
  - Regelmäßige Passwortänderung
  - Token-basierte Authentifizierung

- **Richtlinien für physikalischen Schutz:**

- ▶ *Lassen Sie mobile Geräte nie unbeaufsichtigt*
- ▶ *Markieren Sie mobile Geräte verdeckt*
- ▶ *Lassen Sie mobile Geräte nie sichtbar im Auto liegen*
- ▶ *Rauchen, essen und trinken Sie nicht, während Sie das mobile Gerät nutzen*
- ▶ *Reinigen Sie mobile Geräte nur mit zulässigen Mitteln*
- ▶ *Inventarisieren Sie alle mobilen Geräte, die Sie verwenden*
- ▶ *Versichern Sie mobile Geräte gegen Diebstahl*

- **Richtlinien für softwarebasierten Schutz:**

- ▶ *Verwenden Sie Paßworte*

- Power-On Passwort (Einschalt-Passwort)
- BIOS Paßwort
- Festplatten Paßwort

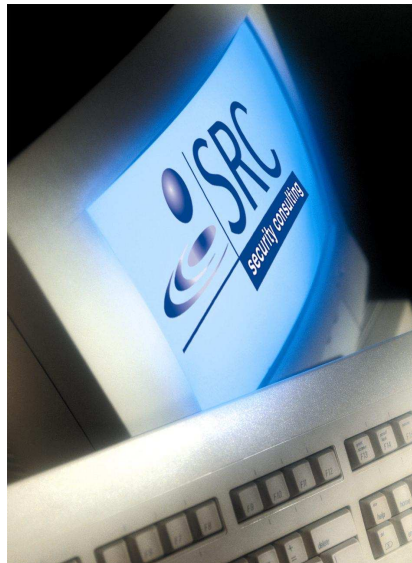
- ▶ **Verwenden Sie unterschiedliche Paßworte!**

- ▶ *Konfigurieren Sie Ihren Laptop so, dass er nur von der internen Festplatte bootet.*
- ▶ *Installieren Sie Anti-Virus Software und aktualisieren Sie diese regelmäßig*
- ▶ *Aktivieren Sie eine Personal-Firewall, wenn Sie das Internet nutzen*
- ▶ *Verwenden Sie keine Auto-Login Möglichkeiten*
- ▶ *Verschlüsseln Sie soviel wie möglich*
  - Interne Datenbanken (PalmOS)
  - Aktivieren Sie die auto-unmount-Funktion verschlüsselter Filesysteme
  - Verschlüsseln Sie Ihre Kommunikationsverbindungen

- **Sonstige Richtlinien**

- ▶ *Private Nutzung von Firmengeräten ist untersagt*
- ▶ *Sichern Sie die Daten regelmäßig*
- ▶ *Behandeln Sie Daten auf mobilen Geräten vertraulich*
- ▶ *Achten Sie in der Öffentlichkeit darauf, dass niemand Einsicht in Ihre Arbeit nehmen kann*

- **Wireless Insecurity**  
<http://www.computerworld.com/industrytopics/financial/story/0,10801,49371,00.html>
- **Palm has arrived – the hackers attack**  
[http://www.it-director.com/article\\_pf.php?articleid=7781](http://www.it-director.com/article_pf.php?articleid=7781)
- ***Defcon 1*™ protection cables with alarm**  
<http://www.laptopguardian.com>
- **Security Tracking System**  
<http://www.nissetowa.com/Property.htm>
- ***Privacy.FILE* file encryption**  
<http://www.digital-privacy.com/privacy.htm>
- **KeyDrive**  
<http://www.keydrive2.com/pages/620683/index.htm>
- ***Private Eye*™**  
<http://www.forsites.com>
- ***Encryption for the Masses (E4M)***  
<http://www.e4m.net>
- ***PDA Defense***  
<http://www.pdadefense.com>
- ***Symbian Tools***  
<http://smartsam.de>
- ***PDA Tools***  
<http://www.pdassi.de>



**SRC**  
**Security Research & Consulting GmbH**  
Graurheindorfer Str. 149a  
53117 Bonn

Tel. +49-(0)228-2806-0  
Fax: +49-(0)228-2806-199  
E-mail: [info@src-gmbh.de](mailto:info@src-gmbh.de)  
WWW: [www.src-gmbh.de](http://www.src-gmbh.de)