Wir stehen für **Wettbewerb** und **Medienvielfalt**.

Rundfunk & Telekom Regulierungs-GmbH
RTR

Aktuelle Bedrohungsszenarien für mobile Endgeräte

Ulrich Latzenhofer

RTR-GmbH

Inhalt

Allgemeines

- Gefährdungen, Schwachstellen und Bedrohungen mobiler Endgeräte
- Maßnahmen gegen Gefährdungen

Aktuelle Beispiele

- Überwachung mittels Remote Administration Toolkits
- SS7: Sicherheit von mTAN und Handy-Signatur auf dem Prüfstand
- Gemalto: Schlüssel aus SIM-Karten von Geheimdiensten gestohlen?

Allgemeines

Gefährdungen, Schwachstellen und Bedrohungen

Mobilnetz
- Missbrauch von Komponenten (z.B. SIM-Karten, Signalisierungsnetz)

Hardware
- Verlust, Diebstahl

Betriebssystem
- Angriffe über Schnittstellen (z.B. Vortäuschung von bekanntem WLAN)
- Missbräuchlicher Zugriff auf Systemdaten nach Rooten bzw. Jailbreak

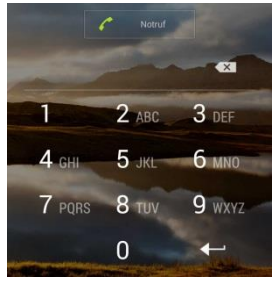
Apps
- Zugriff auf private Daten
- Missbrauch privater Daten

Nutzer
- Bequemlichkeit vs. Sicherheit
- Social Engineering

Maßnahmen zum Schutz der Hardware

Authentifizierung aktivieren

- PIN für Zugriff auf SIM-Karte
- PIN oder Passwort zur Bildschirmsperre (geringerer Schutz durch Gesichtserkennung und Lock-Screen-Pattern)



Speicher verschlüsseln

Diebstahlschutz einrichten

- Ortung des Telefons
- Löschung sensibler Daten aus der Ferne
- Auslösung einer Alarmsirene aus der Ferne

Maßnahmen zum Schutz des Betriebssystems

Nicht benötigte Schnittstellen deaktivieren

- NFC
- Bluetooth
- WLAN
- Mobiler Internetzugang bzw. Daten-Roaming

Automatisches Verbinden nur mit abgesicherten WLANs

Vorsicht bei offenen WLANs, auch mit vertrautem SSID

- Keine Übermittlung vertraulicher Daten (z. B. Passwörter) im Klartext
- Vorsicht vor Access Points, die vertrautes WLAN vortäuschen

Verzicht auf Rooten oder Jailbreak

Maßnahmen zum Schutz vor bösartigen Apps

Vorsicht beim Installieren von Apps

- Je weniger Apps, desto besser
- Apps nicht einfach ausprobieren, sondern Bewertungen lesen
- Apps nur aus vertrauenswürdigen App-Stores installieren
- Auf Plausibilität der Berechtigungen achten

Antivirus-Software einsetzen

Gerät in heiklen Situationen ausschalten

Zwei-Faktor-Authentifizierung nur auf unterschiedlichen Geräten

- Online-Banking mit mTAN
- Handy-Signatur

Andere Maßnahmen

Datenverkehr nach Möglichkeit verschlüsseln (WPA2, VPN, TLS)

Sichere Passwörter sicher verwenden

- Auswahl langer, komplexer Passwörter aus großem Zeichenvorrat
- Keine Passwörter auswählen, die sich erraten lassen
  (z. B. persönliche Daten, Wörterbucheinträge)
- Passwörter nicht aufschreiben, sondern in Passwort-Safe speichern
  (z. B. KeePass, auch für mobile Endgeräte verfügbar)
- Passwörter nach Möglichkeit nur verschlüsselt übertragen
- Vorsicht vor Social Engineering, Phishing etc.

Aktuelle Beispiele

Beispiel 1: Überwachung mittels Remote Administration Toolkits

AndroRAT: Open-Source-Werkzeug für Zugriff auf mobile Endgeräte

- Abrufen von Kontakten (und all ihren Informationen)
- Abrufen von Anrufprotokollen
- Abrufen von Kurznachrichten
- Ortung über GPS/Netzwerk
- Live-Überwachung des Telefonstatus (eingehend, ausgehend, versäumt)
- Aufnahme von Fotos mit Kamera
- Streaming von Ton mit Mikrophon (oder anderen Quellen)
- Senden von Textnachrichten
- Tätigen eines Anrufs
- Öffnen von Seiten im Webbrowser

Beispiel 1: Architektur von AndroRAT

Client-Server-Applikation

- Server = Java-fähiger Rechner
- Client = mobiles Endgerät unter Android

Installation der Client-Komponente auf dem Zielgerät

- Als Open-Source-Software in andere Apps integrierbar (Trojaner)
- Varianten
  (a) Opfer wird dazu gebracht, Client-Komponente freiwillig zu installieren
  (b) Client-Komponente wird ohne Wissen des Opfers installiert
- Sicherheit von Android nicht ausgehebelt, sondern viele Berechtigungen

Verbindungsaufbau vom Client zum Server

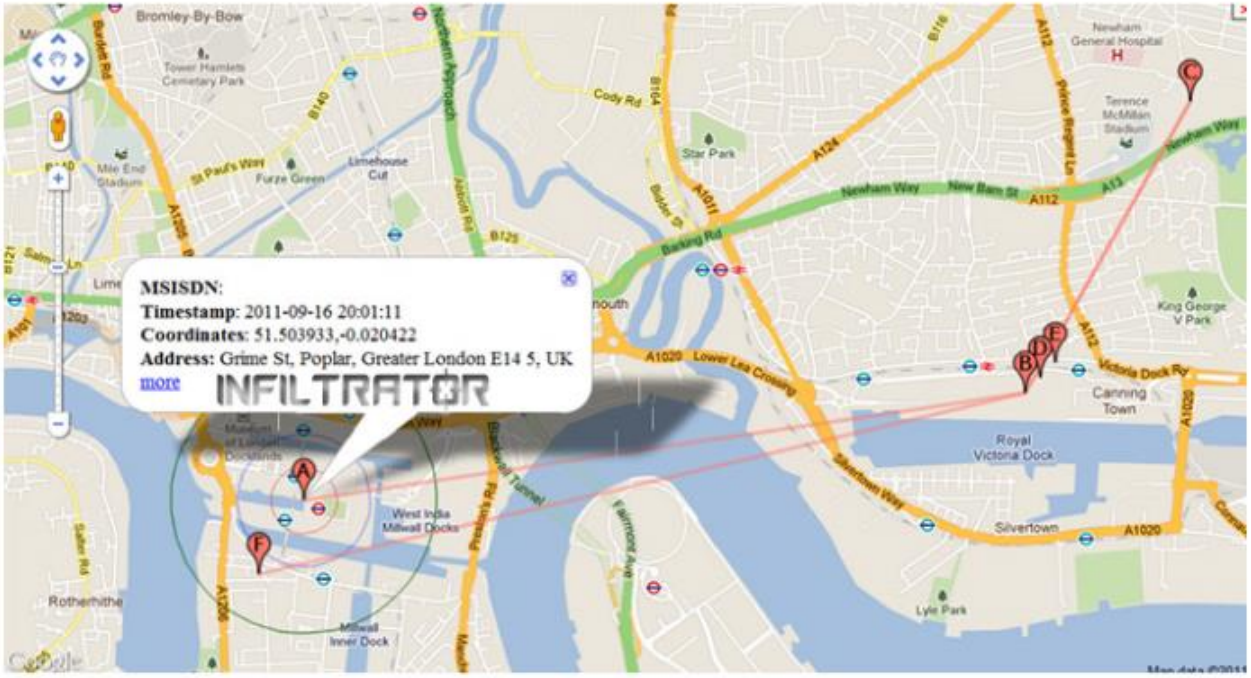
- Auslösung durch Anruf oder SMS von bestimmtem Absender

Beispiel 2: Signalling System #7 (SS7)

- Als Nachfolger älterer Signalisierungssysteme 1975 entwickelt, 1981 standardisiert
- Seit 1990 durch zusätzliche Protokolle zur Unterstützung von Mobiltelefonen ergänzt
- Immer noch gängiger Standard zur Signalisierung in Fest- und Mobilnetzen
- Signalisierung nicht über Nutzkanal, sondern eigenen Signalisierungskanal
- Austausch von Signalisierungsinformation zwischen Betreibern mittels Signalisierungsnetz
- Keine Authentifizierung im Signalisierungsnetz
  ⇒ Missbrauch für jeden mit Zugang zum Signalisierungsnetz möglich

Beispiel 2: Ortung von Geräten mittels SS7

The **Infiltrator Real-Time Tracking System** will provide the location (GPS coordination) at a Cell-ID level. The input will be the target mobile number or the IMSI and the result will show the BTS coordination, where the target is registered on any map.



- The location of all subscribers that belong to all the GSM service providers in the country.
- The location of local subscribers outside their network (roamers in other networks).
- The location of roamers in the local network
- Status of the target phone
- Last place of registration (if offline)

Beispiel 2: Missbrauchsmöglichkeiten von SS7

Ortung von Geräten zwecks Überwachung

- Auch als kommerzielle Dienstleistung

Umleitung von Gesprächen und SMS zu anderem Ziel

- Beispiel: TAN bei Online-Banking oder Handy-Signatur

Umleitung von Gesprächen und SMS über Proxy

- Aufzeichnung von Inhalten

Abrufen temporärer kryptographischer Schlüssel

- Dechiffrieren von Inhalten

Beispiel 3: Stehlen Geheimdienste Schlüssel von SIM-Karten?

Bericht von „The Intercept“ unter Berufung auf Edward Snowden

Gemalto: Herstellung von rund 2 Mrd. SIM-Karten jährlich für rund 450 Mobilnetzbetreiber (Weltmarktführer)

Schlüssel von Gemalto-SIM-Karten angeblich systematisch erkundet und zur unbemerkten Überwachung von Kommunikation missbraucht

Kolportierte Vorgangsweise von NSA und GCHQ

- Überwachung der privaten Kommunikation von Gemalto-Mitarbeitern („Cyber-Stalking“)
- Angriff auf interne Netze und Installation von Malware auf Rechnern von Gemalto
- Angriff auf Mobilnetzbetreiber zum Ausspähen von Kundendaten und Netzplänen

Fazit

- Mobile Endgeräte bieten heute eine Vielfalt an Möglichkeiten, bergen aber auch Gefahren, deren man sich manchmal nicht bewusst ist

- Durch bewussten und sorgsamen Umgang mit mobilen Endgeräten lässt sich manche Gefährdung abwehren

Wir stehen für **Wettbewerb** und **Medienvielfalt**.

Rundfunk & Telekom Regulierungs-GmbH

RTR

Aktuelle Bedrohungsszenarien für mobile Endgeräte

Ulrich Latzenhofer

RTR-GmbH