Malware Detection on Mobile Clients

Michael Gröning
INET RG - HAW Hamburg

December, 11th 2010

Hochschule für Angewandte
Wissenschaften Hamburg
Hamburg University of Applied Sciences

Gliederung

- Einleitung
- Motivation
- Schadprogramme auf Mobiltelefonen
- Erkennung von Malware
- Ziele des Projektes

Glossar

Malware: Programm, welches Schaden anrichtet

Exploit: Programmroutine zum Ausnutzen einer Schwachstelle

Featurephone: Telefon, welches nicht den Funktionsumfang eines Smartphones hat (z.B. Kein Appstore...)

Angriffsvektor: Weg, den ein praktischer Angriff auf ein System nehmen könnte.

Rootkit: Malware, die dem Angreifer den Zugriff auf das System mit Adminrechten erlaubt.

Gliederung

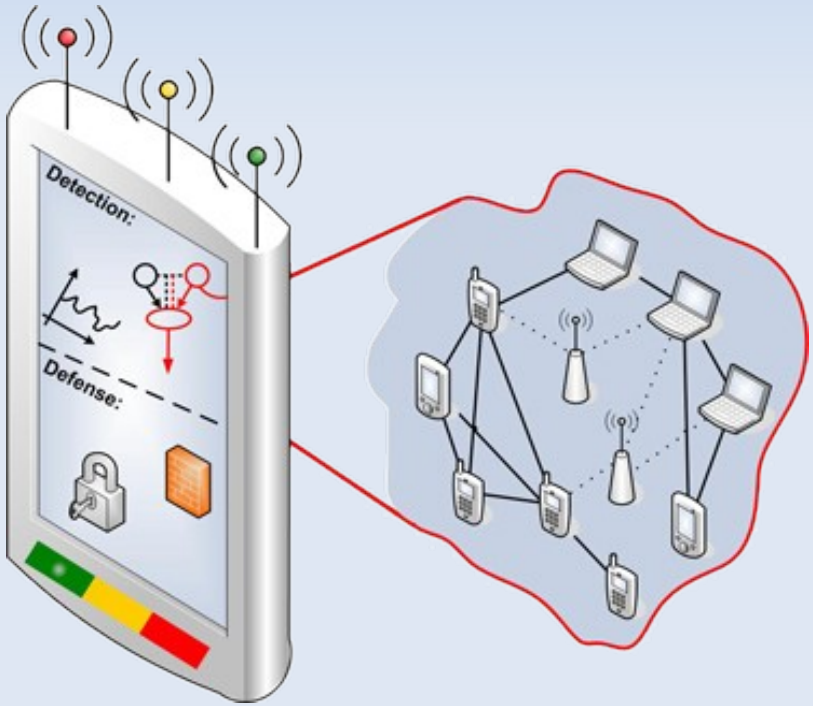
- Einleitung
- **Motivation**
- Schadprogramme auf Mobiltelefonen
- Erkennung von Malware
- Ziele des Projektes

Motivation

Über mich:

- 10 Jahre Interesse an IT-Sicherheit
- 2 Jahre SysAdmin @ Uni Hamburg
- 4 Jahre Incident Response Team @ DFN-CERT
  - Codeanalyse
  - Bearbeitung von Sicherheitsvorfällen
- Daneben viele Projekte und ehrenamtliche Tätigkeiten im ITSec Bereich.

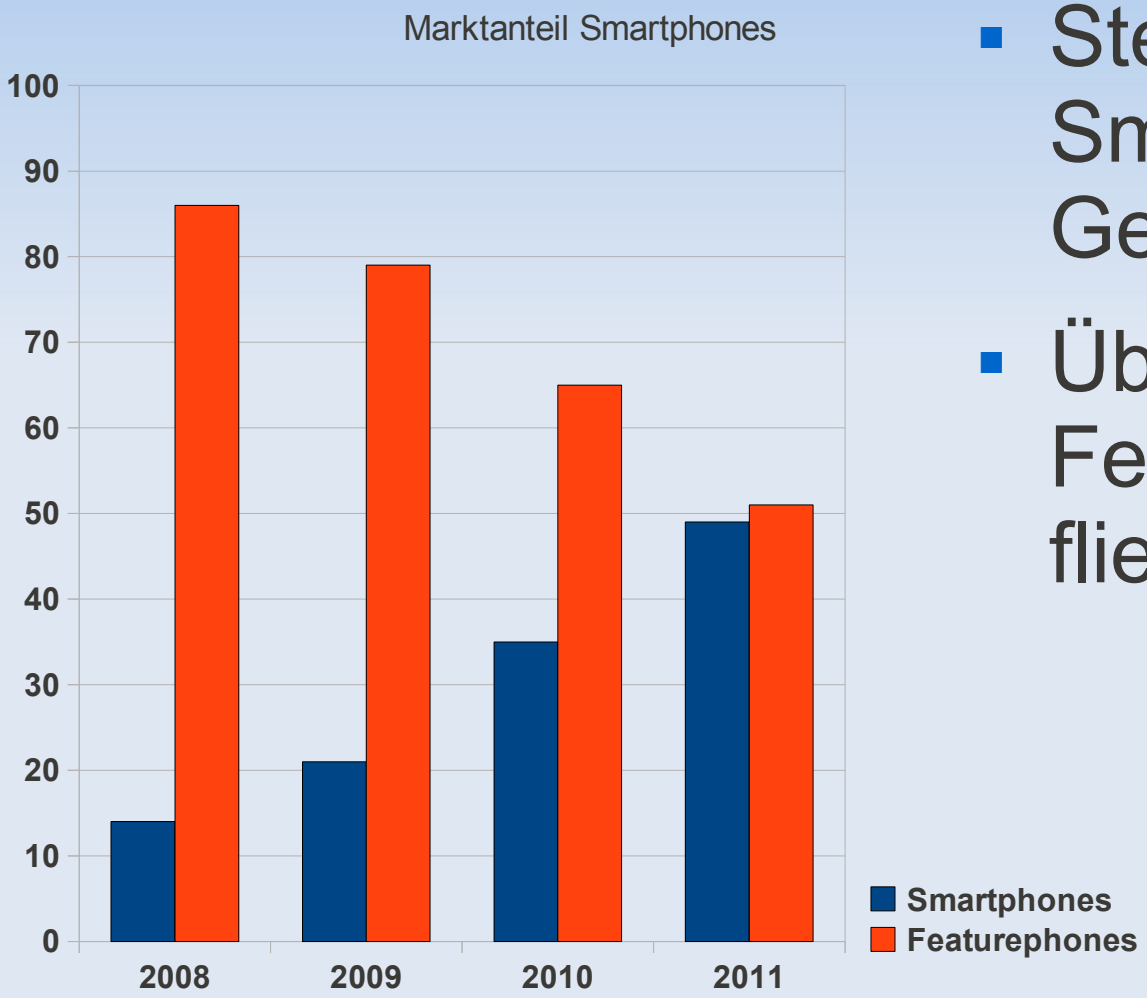
Motivation



- Telefone werden heute anders benutzt als vor wenigen Jahren
  - Facebook, Twitter, Banking, E-Mail....
- Deutlich mehr Ressourcen imTelefon
- Erhöhte Sicherheit auf Desktop-PCs

→ langweilige Ziele?

Motivation



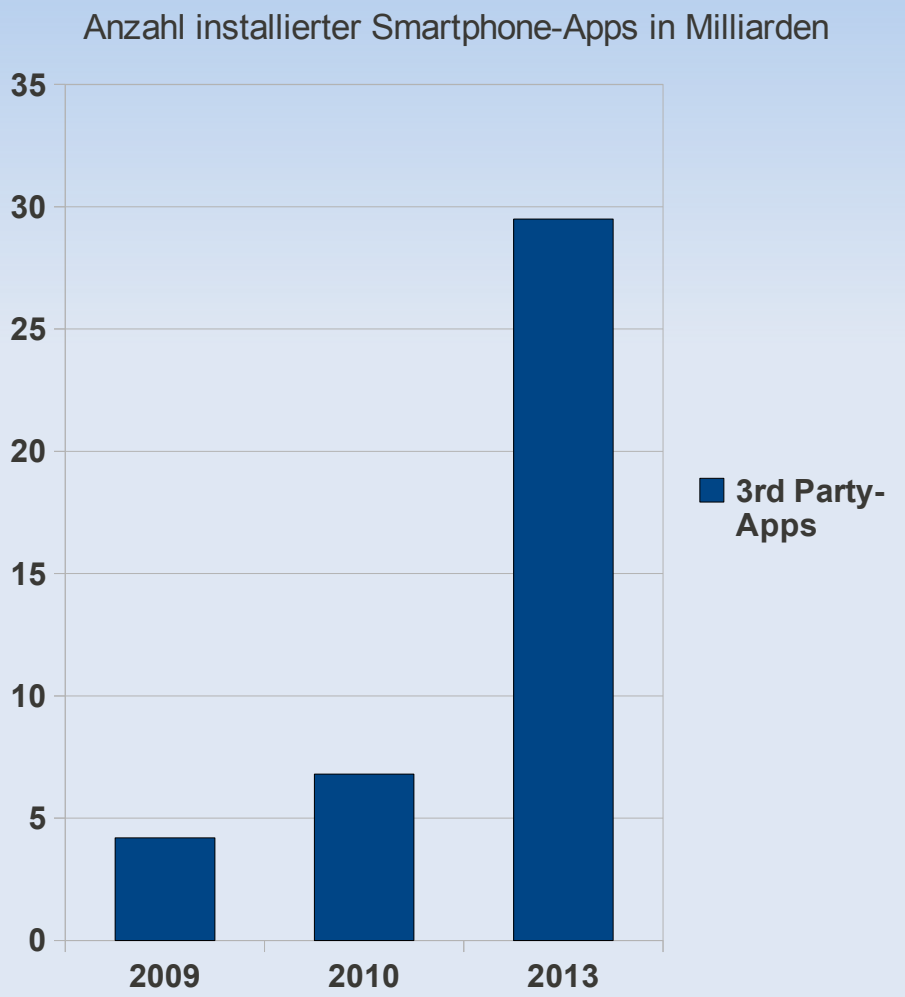
Quelle: The Nielsen Company, 2010

- Steigende Anzahl von Smartphones am Gesamtmarkt
- Übergang zu den Featurephones wird fließender

iNET

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Motivation



Quelle: Gartner, 2010

- Stark wachsender Markt für Smartphone Anwendungen

iNET

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Motivation

- Stark wachsender Markt führt zwangsläufig zur Malware-Entwicklung

  → Verdopplung von Malware auf Android Plattform innerhalb von 6 Monaten.

Quelle: Lookout Mobile, 2010

Gliederung

- Einleitung
- Motivation
- **Schadprogramme auf Mobiltelefonen**
- Erkennung von Malware
- Ziele des Projektes

Schadprogramme auf Mobiltelefonen

Smartphones im Jahr 2010:

- 1 GHz Cortex A8 CPU
- 512 MB Ram
- 802.11bgn-Wireless
- 7.2 MBps HSDPA
- 32 GB Flash-Memory
- 132g
- Desktop-Related OS:

  (Linux, OS X/iOS)

iNET

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Schadprogramme auf Mobiltelefonen

- Personalisierte Daten
- Kostenpflichtige Dienste
- Gezielte Angriffe auf bestimmte Personen/Gruppen
- Tracking von Benutzern über Geolocation
- Überwachung des Kommunikationsverhaltens

Schadprogramme auf Mobiltelefonen

Angriffsvektoren

- Bösartige Apps (dialer, spyware...)
- Mobilfunk Baseband (SMS,MMS, Basisstationen..)
- WiFi Baseband/Services (Bluetooth,WLAN)
- OS / 3rd Party Libraries (Linux, OS X, PDF, SQL, Drivers...)
- Browser (Webkit, Gecko,)
- Angriffe über IP-Layer (z.B. XMPP, Bonjour)
- Mehrstufige Angriffe(z.B. Zuerst bösartiges *.pdf, dann lokaler root-Exploit)

Gliederung

- Einleitung
- Motivation
- Schadprogramme auf Mobiltelefonen
- **Erkennung von Malware**

Malware-Erkennung auf Smartphones

Übersicht:

- Bestehende Verfahren
  - **Signaturbasierte Erkennung**
  - Verhaltensüberwachung
  - Serverbasierte Erkennung
- Neue Ansätze?

Malware-Erkennung auf Smartphones

Übersicht:

- Bestehende Verfahren
  - Signaturbasierte Erkennung
  - **Verhaltensüberwachung**
  - Serverbasierte Erkennung
- Neue Ansätze?

Malware-Erkennung auf Smartphones

Übersicht:

- Bestehende Verfahren
  - Signaturbasierte Erkennung
  - Verhaltensüberwachung
  - **Serverbasierte Erkennung**
- Neue Ansätze?

Malware-Erkennung auf Smartphones

Wie arbeiten echte Anti-Malware Programme?

Zwei Anti-Malware Programme für Android:

- Kein hoher Verbrauch von Ressourcen:
  - → Keine Große Datenbank
  - → Keine Überwachung laufender Prozesse
- Greifen stark auf Cloud-Services zu
  - → Kooperativer/zentralisierter Ansatz?
- Fokus auf bösartige Apps, kein Scan des Netzwerkverkehrs oder der gespeicherten Daten!

Gliederung

- Einleitung
- Motivation
- Schadprogramme auf Mobiltelefonen
- Erkennung von Malware
- **Ziele des Projektes**

Ziele

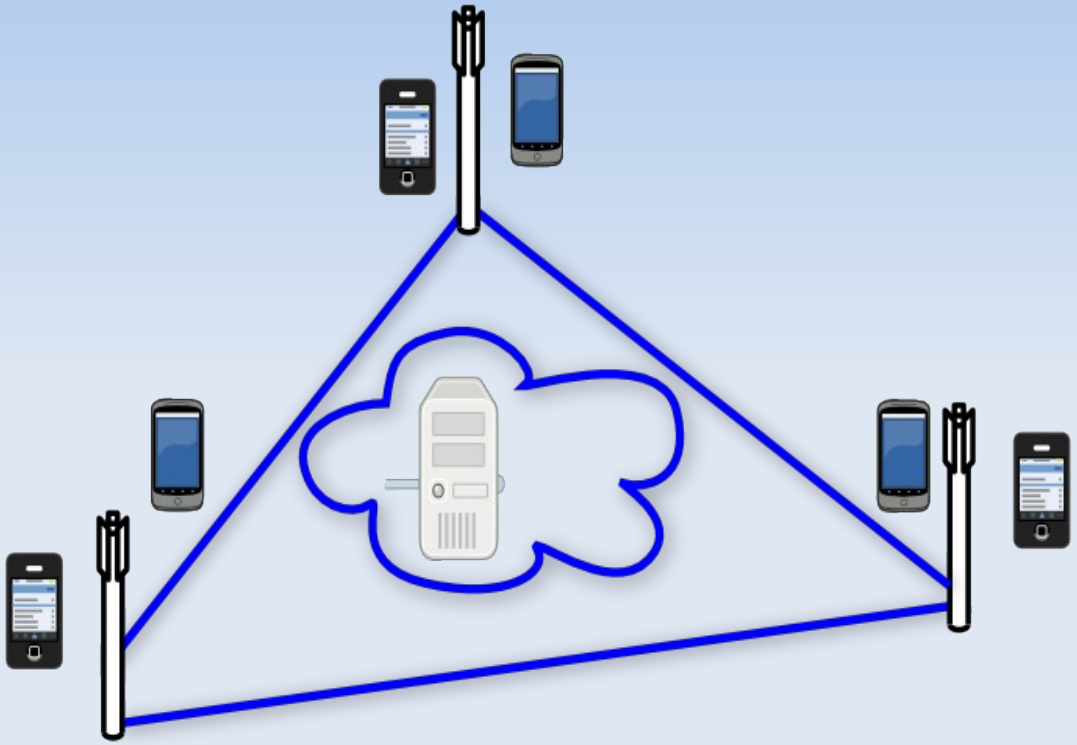
Leichtgewichtige Malwareerkennung:

- Keine hohe Rechenlast
- Spezialisierung auf Mobile Malware
- Fokus über Apps hinaus (z.B.: Kernel-Rootkits)
- Überwachung von Netzwerkinteraces
- Mehrstufiger Ansatz/Cloud-Services:

  → Erste Stufe erlaubt False Positives

  → Komplexere zweite Stufe arbeitet genauer

Ziele



Kooperativer Ansatz:

- Handy to Handy
- Einbeziehung von Servern im Netz/VMs
- Selbsorganisation der Cloud

Vorgehensweise

- Zuerst Konzeption von leichtgewichtiger Malware-Erkennung
  - Evaluation von Erkennungstechniken:

    z.B.: Anomalie-Erkennung in Datenströmen
- Prüfung des Einsatzes von OpenSource Komponenten.

  → Sicherheitsgewinn ggü. Closed-Source

  → Nachprüfbarkeit gibt Vertrauen

Risiken

- Zu hohe Komplexität des kooperativen Ansatzes
- Probleme in anderen Teilprojekten
- Neue Malware-Designs die nicht berücksichtigt werden.
- Neue Techniken der Malware-Verschleierung

References

- Oberheide et al.: CloudAV: N-Version Antivirus in the Network Cloud, Proc. of the 17th USENIX Security Symposium . San Jose, CA, July 2008
- Liang Xie et al.: pBMDS: a behavior-based malware detection system for cellphone devices. Proc. of the 3rd ACM conference on Wireless network security. (WiSec '10), pp. 37-48, March 2010.
- Conti et al.: Automated mapping of large binary objects using primitive fragment type classification. Proc. of the Tenth Annual DFRWS Conference, pp S3-S12, August 2010
- Oberheide et al.: When Mobile is Harder Than Fixed (and Vice Versa): Demystifying Security Challenges in Mobile Environments, Proc. of the 11th Workshop on Mobile Computing Systems and Applications (HotMobile 2010), Annapolis, MA, February, 2010.
- Mulliner et al.: Injecting SMS messages into smart phones for security analysis, Proc. of the 3rd USENIX conference on Offensive technologies, Montreal, Canada, 2009
- Harald Welte: Anatomy of contemporary GSM cellphone hardware, Berlin, 2010 http://laforge.gnumonks.org/papers/gsm_phone-anatomy-latest.pdf

Vielen Dank!

Hochschule für Angewandte
Wissenschaften Hamburg
Hamburg University of Applied Sciences

Fragen?

iNET

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Approaches on Malware Detection

Verhaltensbasierte Malwareerkennung:

- Verhalten von Anwendung:

  → Zugriffe auf Datenbestände

  → Verdächtiger über Netzwerk/SMS etc.

- Verhalten des Telefons:

  → z.B.: Aktivität bei gleichzeitig aktivierter Tastensperre

  → Aktivierte Schnittstellen (z.B.: Bluetooth, GPS)

Approaches on Malware Detection

Signaturbasierte Malware Erkennung

- Vergleich von Datei-Fingerprints mit bestehenden Signaturen

  → Erkennt keine unbekannte Malware

  → Regelmäßige Updates sind nötig

- Unzuverlässig gegen versteckte Malware

Approaches on Malware Detection

Server/Cloud basierter Ansatz:

- Verlagerung der Arbeit vom Mobiltelefon weg:

  → erhöhte Batterielaufzeit

  → keine Updates auf dem Telefon

- Kooperativer Ansatz:

  → Andere Knoten profitieren sofort von Ergebnissen

  → Proaktiver Schutz ist möglich