Steganographie und Steganalyse auf Smartphones

Ulrich Viefhaus

FernUniversität in Hagen

16. und 17. September 2016

Inhalt

Bedeutung

Definition

Das Wort Steganographie setzt sich aus den beiden altgriechischen Wörtern στεγανός (bedeckt) und γράφειν (schreiben) zusammen. Sinngemäß bedeutet es „geheimes Schreiben“.

Abgrenzung Kryptographie

Kryptographie und Steganographie haben unterschiedliche Ziele.

- Kryptographie: Nachrichten werden durch Verschlüsselung geschützt, aber offen versendet.
- Steganographie: Existenz von Nachrichten wird verborgen.

Es ist durchaus möglich eine Nachricht erst zu verschlüsseln und sie dann durch Steganographie zu verstecken.

Kerckhoffs' Prinzip

Definition

Die Sicherheit eines Verschlüsselungsverfahrens darf nur von der Geheimhaltung des Schlüssel abhängen, nicht jedoch von der Geheimhaltung des Algorithmus.

- Wurde bei Steganographie lange nicht beachtet.
- Optische Unerkennbarkeit war entscheidend.
- Findet in neueren Algorithmen Anwendung.

Tarnmedium

Definition

Ein Tarnmedium (engl. cover medium) ist ein Medium, in dem eine geheime Nachricht versteckt wird.

Beispiel: Bild im jpeg Format.

Verdeckter Kanal

Definition

Ein verdeckter Kanal (engl. hidden channel) dient dem Übermitteln von Informationen über ein Protokoll auf eine Art, die in dem Protokoll nicht vorgesehen ist.

Beispiel: Nutzung des „Options“ Feldes im TCP Header zur Datenübertragung.

Stegoschlüssel

Definition

Ein Stegoschlüssel (engl. stegokey) ist ein Schlüssel, mit dem die Verteilung der Bits der geheimen Nachricht in dem Tarnmedium festgelegt wird.

Beispiel: Vereinbarter Schlüssel wird als Seed für einen PRNG genutzt, der bestimmt in welchen Pixeln eines Bildes die geheime Nachricht versteckt wird.

Analog zu kryptografischen Schlüsseln gibt es zwei Arten von Stegoschlüsseln:

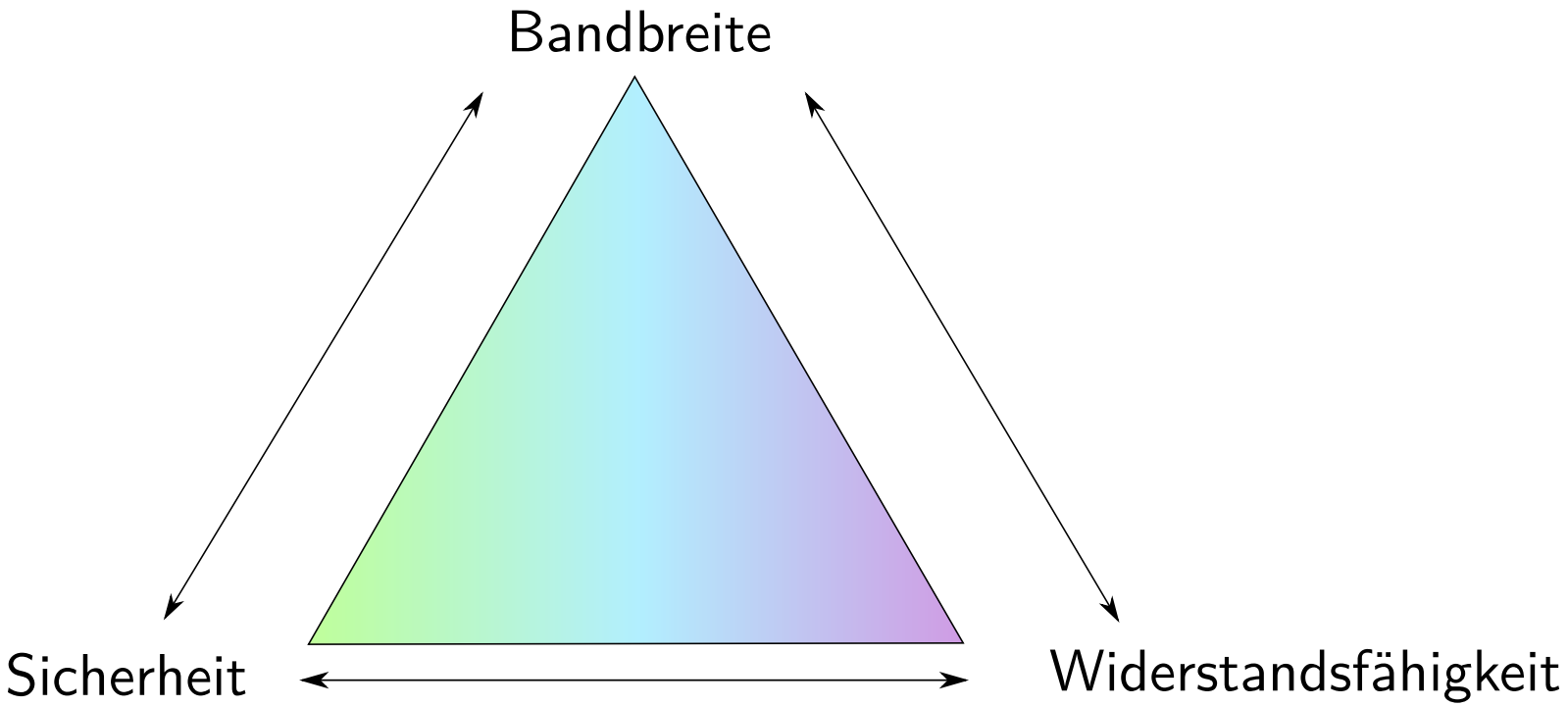
- Symmetrische Stegoschlüssel
- Asymmetrische Stegoschlüssel

Notwendige Eigenschaften

Bei der verdeckten Kommunikation müssen drei notwendige Eigenschaften gegeneinander abgewogen werden:

- Bandbreite (engl. steganographic bandwidth)
- Unerkennbarkeit (engl. security)
- Widerstandsfähigkeit (engl. robustness)

Magisches Dreieck



Inhalt

Besonderheiten auf Smartphones

- Energieverbrauch ist von großer Bedeutung
- Vielzahl an Sensoren und Netzwerkschnittstellen
- Große Anzahl sensibler Daten

Arten von verdeckten Kanälen auf Smartphones

- Lokale Kanäle
- Objektkanäle
- Netzwerkkanäle

Lokale Kanäle

Lokale Kanäle werden durch steganographische Verfahren erzeugt, die auf Systemresourcen angewandt werden. Sie ermöglichen die verdeckte Kommunikation zwischen Prozessen auf dem selben Gerät. Beispiele:

- Vibrationseinstellungen
- Lockfiles
- Prozessorauslastung

Objektkanäle

Objektkanäle werden durch steganographische Verfahren erzeugt, die auf virtuelle Objekte wie Dateien angewandt werden. Objekte eignen sich sowohl zum Speichern von geheimen Informationen als auch zum Versand über andere Dienste. Beispiele:

- Multimediadateien in diversen Formaten (z.B. JPEG, Gif, MPEG, mp3)
- Textdateien (z.B. PDF und Word)

Netzwerkkanäle

Netzwerkkanäle werden durch steganographische Verfahren erzeugt, die auf Netzwerkprotokolle- und Anwendungen. Netzwerkdienste eignen sich zur verdeckten Kommunikation mit anderen Geräten. Beispiele:

- HTTP mittels URLs
- Videostream mit spezifischen Abständen zwischen Frames
- Einfügen von energiearmen Töne in GSM-kodierte Sprachübertragung

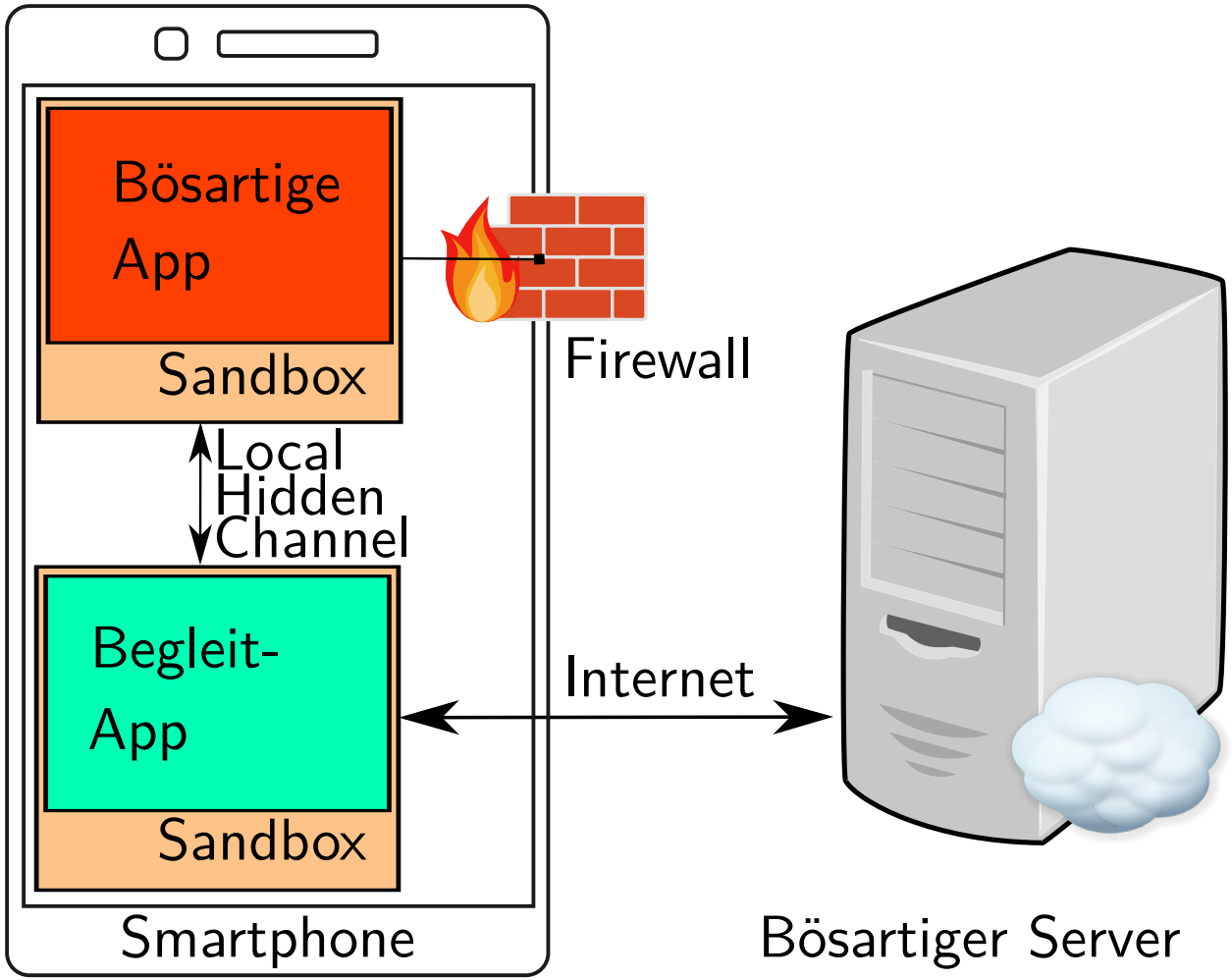
Inhalt

Gefahren von Steganographie auf Smartphones

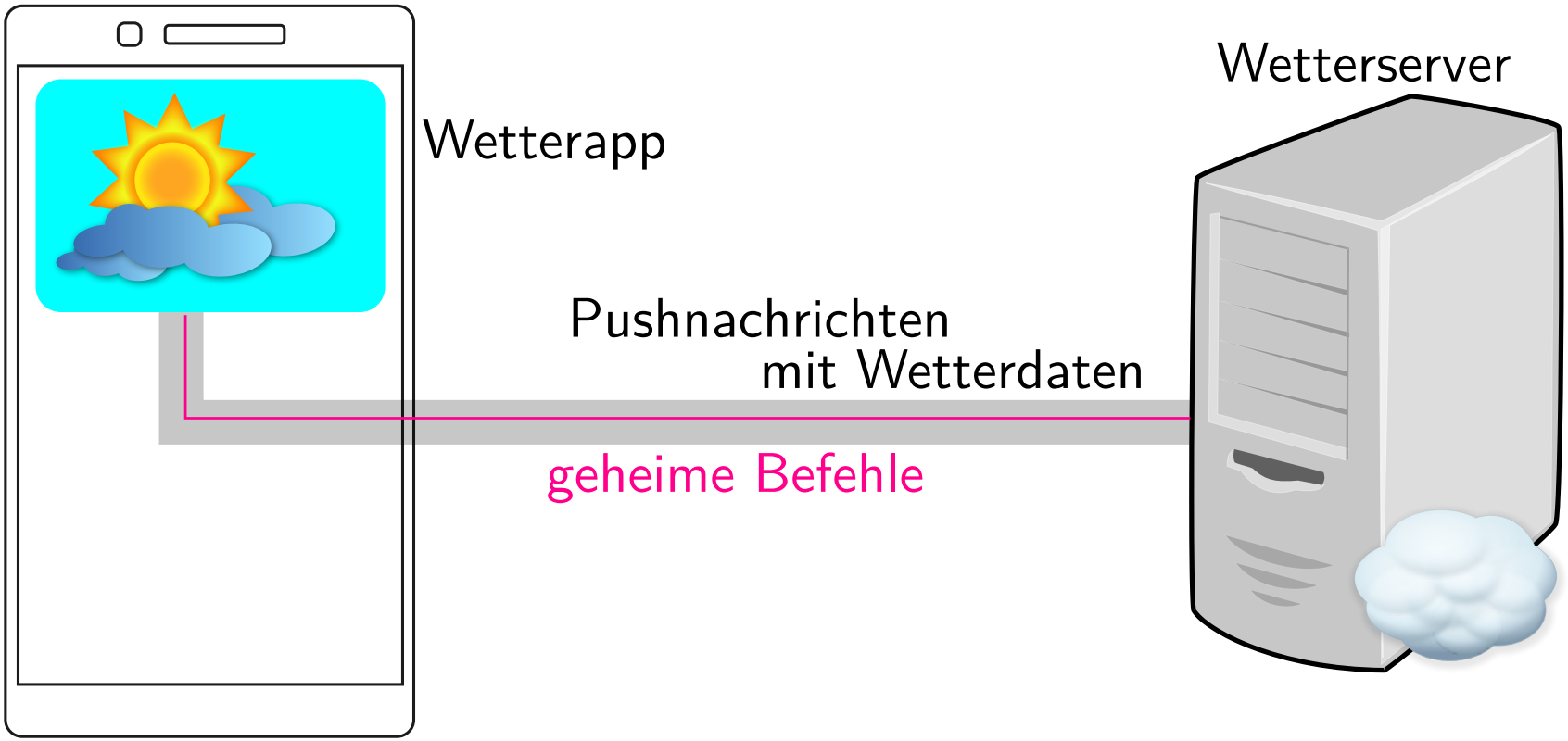
Durch Steganographie entstehen auf Smartphones zwei weitere Gefahren für den Nutzer, die nur schwer zu erkennen sind.

- Unbemerktes Ausleiten von sensiblen Informationen.
- Unbemerktes Empfangen von Befehlen.

Schema für das Ausleiten von Informationen



Schema für das Empfangen von Befehlen



Inhalt

Gegenmaßnahmen

Gegenmaßnahmen sind in drei Bereiche gegliedert:

- Erkennung (Stegoanalyse)
- Beseitigung
- Reduktion der Bandbreite

Maßnahmen gegen lokale Kanäle

Erkennen von Steganographie durch:

- Taint tracking
- Überwachung von API-Aufrufen
- Überprüfung auf Grenzwerte

Falls ein Zugriff auf lokale Ressourcen als bösartig eingeschätzt wird, kann dieser unterbunden werden.

Maßnahmen gegen Objektkanäle

Erkennen von Steganographie durch:

- Signaturen
- Statistischen Methoden

Nach der Erkennung kann die versteckte Nachricht aus dem Tarnmedium entfernt werden.

Maßnahmen gegen Netzwerkkanäle

Erkennen oder Entfernen von Steganograhie durch

- Network traffic normalizer
- Statistischen Methoden
- Maschinelles Lernen

Danke für Ihre Aufmerksamkeit! Fragen?