Grenzen der Anonymität

Crypto-Workshop VHS Tübingen

Kurt Jaeger, pi@opsec.eu

http://cccs.de/

Tübingen, 15. März 2014

Übersicht

- Anonymität und Pseudonymität
- Schutz der Privatsphäre
- Gegen wen ?
- Gegen welche Angriffe ?
- Der Faktor Zeit
- Kosten
- Empfehlungen

Anonymität und Pseudonymität

- eine Person
- eine Gruppe
- eine Institution
- eine agierenden Struktur

die nicht identifiziert werden kann
Quelle: Wikipedia
Pseudonymität: Ein Dritter entscheidet
Datenschutz

Um was geht es bei Datenschutz ? 1

- Nicht Schutz von Daten
- Schutz der Privatsphäre (privacy)
- Gesellschaft für Informatik: Ein Bit über die Lebenszeit eines Menschen (80-100 Jahre) vertraulich halten

Um was geht es bei Datenschutz ? 2

Menschen verhalten sich...

- entsprechend dem, was sie wissen
- anderen gegenüber, je nachdem was sie über diese anderen wissen
- anderen gegenüber, je nachdem was sie denken, dass andere über sie wissen
- unter Überwachung anders

weniger frei

Um was geht es bei Datenschutz ? 3

Preisdifferenzierung

- Kosten der Informationsverarbeitung sind radikal gesunken
- Preisdifferenzierung wird einfacher
- **Privatsphäre des Bürgers hat einen Wert** $>> 0$
- Statistischer Wert, nicht individuell
- Nicht der einzelne Vorgang "Verlust eines Factoids"

Mechanism Design

Was ist Preisdifferenzierung (1) ?

Was ist eine Transaktion ?

- Akteure
- Vertrag
- Dauer (!)
- Ein Akteur bekommt Produkt oder Dienstleistung
- Ein Akteur bekommt Geld

Naives Marktmodell: Vollständige Information

- Akteure kennen sämtliche Umweltzustände
- können die Handlungen ihrer Vertragsparteien beobachten
- Informationen sind kostenlos verfügbar
- Verträge sind vollständig
- ihre Erfüllung kann kostenlos beobachtet werden...
- ...und kann vollständig durchgesetzt werden

Was ist Preisdifferenzierung (2) ?

Der Verkäufer kennt den Kontext der Transaktion

- Ort
- Zeit
- Nachfrager
- Präferenzhierarchie
- Angebotssituation

und legt daraufhin einen **individuellen** Preis fest

Preisdiskriminierung

Andrew Odlyzko, 20030727

Privacy, Economics and Price Discrimination on the Internet

- Ansporn, Preise zu differenzieren (Ertrag)
- einfachere Mittel, das auch zu tun

Evolution der Ökonomie

- In bestimmten Märkten: Hohe Fixkosten, niedrige variable Kosten
- Dem Käufer wird ein Preis nahe seinen Möglichkeiten abverlangt
- Eine Frage von Ökonomie, Recht und Politik
- Die Leute mögen keine "dynamischen" Preise
- Wie kann man Preisdiskriminierung erkennen ?

Schutz gegen wen ?

- Nachbarn
- Arbeitgeber
- Andere Unternehmen
- Grosse Unternehmen
- Staatliche Stellen
- Behörden mit Sicherheitsaufgaben (BOS)
- Kriminelle
- Terroristen
- Andere Organisationen
- Infrastrukturbetreiber
- Die NSA
- Andere Länder

Netzwerke

Was sind die Kommunikationswege ?

- Telefonieren
- Internet-Surfen
- E-Mail
- Autofahren
- Bilderkennung
- Stromzähler
- Plastik-Geld
- Gesundheitskarte
- ...

Was sind die Angriffswege ? 1

- Leitungen
- Netzknoten
- Rechner
- Rechenzentren
- Netzbetreiber
- Websites
- E-Mail
- Auch ohne Netzverbindung

Was sind die Angriffswege ? 2

- Mobiltelefone
- Infrastruktur
- Sicherheitslücken
- USB
- Verschlüsselungssysteme und deren Spezifikationen
- Logistikketten
- Chips, Zufallszahlen
- Strom

Alles, was Chips hat: Michael Hastings

Welche Datenspuren fallen im Netz an ? 1

- Metadaten
- Informationen über einen Kommunikationsvorgang
- Nicht die Inhalte!

Welche Datenspuren fallen im Netz an ? 2

- Die IP-Adresse, mit der man ins Netz geht
- HTTP, browser fingerprint
- Lightbeam https://www.mozilla.org/en-US/lightbeam/
- Mail: Von wem, wann erhalten, wann gelesen, wann/wem geantwortet
- Inhalte der Mail: Gmail reads your mail
- DNS-Queries
- Domains, Whois-Daten
- Bei Telefonie: VoIP
- MACs bei WLANs
- Username bei DSL
- ...

Mein IT-ler kümmert sich...

- Ist genauso Ziel von Angriffen
- z.B. Angriff auf Belgacom Netzverwaltung

Snowden zeigte: Universalität der Angriffe

Was ist ein Computer ?

- CPU, Central Processing Unit
- Speicher
- Ein/Ausgabe: Bildschirm, Tastatur, Netzverbindung, Sensoren

Beispiele

- Desktop
- Laptop
- Smartphone
- Baseband-Prozesser im Smartphone
- USB-Stick
- SD-Speicher

Wieviele Computer sind im Auto ? ca. 100

Was ist ein Sensor ?

- Geräusch
- Bewegung/Beschleunigung
- Temperatur
- Anwesenheit diverser Stoffe (Wasser osä)
- Längen
- GPS
- ...

Abschätzung über Kosten

- was kostet es, alles zu speichern über eine Person ?
- alles, was sie schreibt ?
- alles, was sie sagt ?
- alles, was sie hört ?
- alles, was sie sieht ?

Technologieentwicklung

Handlungsoptionen

- Verschlüsselung hilft
- Anonymität für Sie und andere (!): in der Masse verstecken
- Bargeld
- Online-Shopping vermeiden, speziell für Elektronik
- Betreiben Sie Ihren eigenen Mailserver
- Nutzen Sie keine sozialen Netzwerke
- Nur Open Source kann geprüft werden
- IETF perpass
- Digitale Stromzähler und andere Sensoren vermeiden
- Politisch: Etatkürzungen für Geheimdienste

Grenzen der Anonymität ?

Welche Anonymität ?