Anonymität im Internet

Technische und rechtliche Aspekte

Gliederung

- Politische Motivation
- Technische Grundlagen
- Die CCC-Kaskade
- Rechtliche Rahmenbedingungen
- Erfahrungen mit Strafverfolgern u.Ä.

Warum? (technisch)

- Internet ist grundsätzlich transparent
- Inhalte werden mitgelesen
- Verschlüsselung versteckt Inhalte
- Metadaten bleiben sichtbar (Wer mit wem wann, wie lange, wie oft)
- Wegen effizienter Auswertbarkeit für Angreifer sehr aufschlussreiche Information

Warum? (politisch)

- Politische Großwetterlage
- Data Retention
- Data Mining
- Zensur (islamische Staaten, China, Büssow)
- Umkehr der Unschuldsvermutung
- Informationelle Selbstbestimmung
- Verhaltensänderungen von Individuen

Verschlüsselung

- Alice und Bob
- Schlüsseltausch
- Alice verschlüsselt mit Schlüssel von Bob
- Alice sendet das Chiffrat an Bob
- Bob entschlüsselt mit seinem Schlüssel
- Dritte können den Inhalt nicht mitlesen
- Eve sieht aber den Kommunikationsvorgang

Lösungsansatz: Stellvertreter

- Alice und Bob sprechen über Peter miteinander (Eilbote)
- Eve sieht Kommunikation zwischen Peter/Alice ODER Peter/Bob
- Kann Eve beides gleichzeitig beobachten, ahnt sie, dass Alice und Bob kommunizieren
- Peter sammelt Nachrichten und verteilt verspätet (Briefträger-Prinzip)
- Problem: Peter kennt alle Kommunikationsvorgänge (Postkontrolle DDR)

Mehrere Stellvertreter

- Vertrauen wird auf mehrere Boten verteilt
- Alle Boten müssen zusammenwirken, damit Anonymität aufgehoben werden kann
- Zwiebelschalenprinzip (Viele Briefumschläge ineinander)
- Sofern auch nur ein Bote vertrauenswürdig ist, bleibt der Zusammenhang zwischen Alice und Bob verborgen

JAP / TOR

- JAP: Java Anonymisier Proxy (BMWA)
- TOR: The Onion Router (US-Navy / EFF)
- Unterschiedlicher Ansatz (feste Routen, flexible Reihenfolge der Stellvertreter)
- Starke Verschlüsselung
- Rauschquellen zwischen den Knoten (bei Jap)

Motivation

- Metadatenanalyse funktioniert nicht mehr
- Unbeobachtete Informationsbeschaffung (Information über Krankheiten, Gewerkschaften, Presse)
- Unbeobachtete Kommunikation
- Whistle-Blower (Informant)
- Entfaltung von bürgerlicher Selbstverantwortung braucht Freiräume. In überwachter Gesellschaft schwierig bis unmöglich (DDR, China ...
- .... Europa 2010?

Installation

- https://www.ccc.de/anonymizer/
- http://www.anon-online.de/
- http://tor.eff.org/

Installation als lokaler Proxy

(How-to auf der Webseite, kinderleicht ;-)

Haftung von Anbietern

- Kein Täterschaft / Teilnahme
- Haftungsprivilegierungen in §8-11 TDG (keine Haftung für fremde Inhalte, sofern man keine konkrete Kenntnis hat)
- Telefonnetzbetreiber haftet auch nicht für Inhalte die über sie kommuniziert werden

Aufdeckung von Anonymität

- Grundsätzlich möglich, wenn alle Betreiber zusammenwirken
- Bei JAP sind feste Kaskaden festgelegt, so dass eine Aufdeckung möglich ist.
- Bei TOR schwierig bis unmöglich
- Verteilung von Kaskaden über verschiedene Gesetzgebungen.

Bestandsdatenherausgabe

- Name / Adresse / Bankverbindung
- Herausgabeanspruch nach TKG

- Bei einem Anonymisierdienst fallen derartige Daten nicht an.
- Folglich kann auch nichts herausgegeben werden

Verbindungsdatenherausgabe

- Wer hat wann mit wem kommuniziert
- Verbindungsdatenherausgabeanspruch nach §100g/h StPO
- Aufklärung von Straftaten, die mit Hilfe von Kommunikationseinrichtungen begangen wurden
- Richterprivileg, bei Gefahr im Verzug Staatsanwaltschaft
- Anspruch grundsätzlich gegeben, doch fallen derartige Daten nicht an.

TK-Überwachung I

- Telefonüberwachung nach §100a/b StPO
- Ist ein Anonymisierdienst überhaupt eine TK-Anlage?
- In die Zukunft gerichtet.
- Anschlüsse: Konkrete URLs.

TK-Überwachung II

- Katalogstraftat (nur sehr schwere Straftaten)
- Richtervorbehalt
- Bei Gefahr im Verzug auch Staatsanwaltschaft (dann nur 3 Tage)
- Auf 90 Tage begrenzt
- Beschränkte Verwertung von Zufallsfunden

TK-Überwachung III

- CCC arbeitet mit Strafverfolgern zusammen, überprüft jedoch die Voraussetzungen genau.
- Wichtiges Argument gegen Vorwurf der Begünstigung von Straftaten
- Mehrfache Kontrolle (StA, Richter, Betreiber)
- Alle Betreiber müssen zusammenwirken
- Zukunftspläne: Verbesserung der Anonymität der Abhörschnittstelle (Zusammenwirkung)

Statistik 2005

- Ca. 10 Anfragen von Privaten.
  Diese sind die schwierigsten Fälle.
- Ca. 6 Anfragen von Polizeidienststellen
  Diese brauchen meist nur eine Bestätigung für ihre Akten.
- Ungefähr 4 Anfragen der StA.

Statistik II

- 1 Vorladung der Polizei Hamburg an das Chaos Cafe Ellerbrook
- 1 Überwachungsanordnung nach §100a StPO.
  StA hat jedoch die Formulierung der Anfrage verplant ....
- Bislang keine Datenherausgabe.

Vorratsdatenspeicherung

- Totale Überwachung des gesamten Internetverkehrs
- Widerspricht dem Wesen eines Anonymisierdienstes
- Lösung: weg von festen Institutionen, p2p-Ansatz
- Nationale Umsetzung ungewiss ...

Zukunft

- Wir brauchen viele viele neue Anonymisierdienste!
- Spenden Willkommen!
- Kto: 59 90 90-201 bei der Postbank Hamburg, BLZ 200 100 20