Kryptographische Missbrauchssicherungen für die Vorratsdatenspeicherung

Heiko Stamer

Universität Kassel
Fachbereich Elektrotechnik/Informatik
Wilhelmshöher Allee 71-73, 34109 Kassel

stamer@theory.informatik.uni-kassel.de

76F7 3011 329D 27DB 8D7C 3F97 4F58 4EB8 FB2B E14F

7. Krypto-Tag der GI-Fachgruppe „Angewandte Kryptologie“
b-it Bonn, 9. November 2007

UNIKASSEL VERSITÄT

Inhalt

Vorratsspeicherung von Daten

Problematik der Vorratsspeicherung

Missbrauchsszenarien und Anforderungen

Kryptographische Lösungen

Vorratsspeicherung von Daten

- Begriff aus dem Datenschutz- und Telekommunikationsrecht
- Speicherung personenbezogener Daten für eine *spätere Verarbeitung*, wobei der *Verarbeitungszweck* zum Zeitpunkt der Speicherung noch *nicht (klar) feststeht*

Betroffene Kommunikationsdienste: Telefon (Sprachdienste, Konferenzschaltungen, Sprachspeicherung, Rufumleitung, etc.), Mitteilungsdienste (z. B. SMS, MMS), Internet (E-Mail, VoIP)

Bestandsdaten	Verkehrsdaten, Verbindungsdaten
Name, Adresse, Bankverbindung, etc.	Zeitstempel (Beginn und Ende), Dauer, eindeutige Teilnehmerkennungen (z. B. Rufnummer, IMEI, IP-Adresse), ggf. Standortdaten (z. B. Funkzelle)

EU-Richtlinie 2006/24/EG

Vorratsspeicherung von Daten, die bei *öffentlich zugänglichen* Kommunikationsdiensten erzeugt oder verarbeitet werden

Hintergrund: Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten (insb. Terrorismus)

Zweck: Unterschiedliche nationalen Vorschriften harmonisieren

Inhalt der Richtlinie: (ändert 2002/58/EG, Datenschutzrecht)

- Gegenstand (Kommunikationsdienste) und Anwendungsbereich (juristische und natürliche Personen)
- Vorratsspeicherungspflicht des Anbieters
- Zugangsberechtigungen (Ausgestaltung Mitgliedsstaat)
- Kategorien von Daten, die gespeichert werden (keine Inhalte)
- Speicherungsfristen (mindestens 6, höchstens 24 Monate)

Klage (Irland) vor dem Europäischen Gerichtshof anhängig

Deutscher Regierungsentwurf (April 2007)

Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur . . . (TKG-E)

- Verpflichtet Anbieter von Telekommunikationsdiensten zur Vorratsspeicherung von Verkehrs- und ggf. Standortdaten für

  Telefon- und Mitteilungsdienste, E-Mail, Internetzugang

- Speicherfrist: 6 Monate (keine unverzügliche Löschungspflicht)
- Zugriffsrechte:
  1. Strafverfolgungsbehörden bei „erheblichen“ Straftaten und auch bei mittels Telekommunikation begangenen Straftaten; zusätzlich zur Gefahrenabwehr
  2. Nachrichtendienste (BND, Verfassungsschutz, MAD) zur Erkenntnisgewinnung im Rahmen ihrer gesetzlichen Aufgaben

Agenda:

- Verabschiedung im Bundestag: 9. November 2007 (Heute!)
- Inkrafttreten: geplant zum 1. Januar 2008

Problematik

Sachverständigenanhörung im Rechtsausschuss am 21.9.2007:
überwiegend negative Beurteilung des vorgelegten Entwurfs

- *Überschießende* Richtlinienumsetzung im Regierungsentwurf:
  - Speicherpflicht für Anoymisierungsdienste
  - ~~Identifizierungszwang zur Einrichtung von E-Mail-Konten~~
  - Zugriffsrechte sind zu weit gefasst (unklare Zweckbindung)
  - ~~Verfrühte Einführung der Internetprotokollierung~~
  - Fehlende Entschädigungsregelung für Anbieter
- *Zugriffsbefugnisse* werden im Nachhinein oft ausgeweitet (z. B. Verwendung der LKW-Mautdaten zur Strafverfolgung)
- Zugriff auch für *Drittstaaten* (Cybercrime-Konvention)
- Gespeicherte Daten sind *Missbrauch* ausgesetzt („Hacker“- bzw. Insider-Angriffe, unbefugte Verwendung)

Alternativen: Einzelfallbezogenes Quick-Freeze-Verfahren

Missbrauch von Verbindungsdaten

1. Missbrauch durch Zugriffsbefugte
   - **(a)** Private Zwecke (vgl. BND-Vorfall, Berliner Zeitung 31.08.2007)
   - **(b)** Dienstliche Zwecke (vgl. Cicero-Affäre, BVerfG. 1 BvR 538/06)
   - **(c)** Weitergabe/Abfrage von Daten an/von Drittstaaten mit unzureichender rechtsstaatlicher Kontrolle
2. Missbrauch durch Unbefugte
   - Verkauf von Bewegungs- bzw. Kommunikationsprofilen
   - Wirtschaftsspionage (vgl. Angebotsverfahren ICE vs. TGV)
   - Erpressung, Schmutzkampagnen, Schmähkritik etc.

Problematik zu 1(b):

- Richterliche/Parlamentarische Kontrolle oft unzureichend (vgl. Studien MPI 2003, Backes/Gusy 2003)
- Benachrichtigung der Betroffenen unterbleibt häufig

Anforderungen: ETSI Dokumente

Technical Specification ETSI DTS/LI00039 V0.2.1 (2007-06)
Requirements of Law Enforcement Agencies for handling Retained Data.

4.8. Availability constraints

d) "After a lawful authorization has been issued, provision of the results *shall as soon as possible* (service level agreement are a national issue)."

e) "CSP will retain data in such a way that the data retained and any other necessary information relating to such data can be delivered upon request to the competent authorities *without undue delay*."

Anforderungen: ETSI Dokumente

Technical Specification ETSI DTS/LI00039 V0.2.1 (2007-06)
Requirements of Law Enforcement Agencies for handling Retained Data.

4.9. Information transmission and protection requirements

a) "the need to *protect information on which and how many requests are or were made* on retained data and the periods during which the information was requested"

- Organisatorische Missbrauchssicherungen, Übergabeschnittstelle
  - beschränkter Personenkreis, Authentifizierung LEA etc.

i) "confidentiality measures to *protect the transmission* of the results *may be* required. The *use of encryption* shall be possible"

j) "in order to prevent or trace misuse of the technical functions integrated in the telecommunication installation, *requests shall be fully recorded*, including any application caused by faulty or unauthorized input."

l) "all national regulations, procedures and processes *shall be followed and are not replaced or superseded* by requirements in the present document."

Kryptographische Lösungen

1. Verschlüsselte Übertragung der abgefragten Daten
   - Infrastruktur oft bereits vorhanden (TKÜV): SINA-Boxen
2. Erweiterung: Schlüsselverteilung als Missbrauchssicherung
   - Zusätzliche Kontrollinstanz: BfDI, ULD, RegTP etc.
   - Hybride Verschlüsselung mit Sitzungsschlüssel $k = k_1 \oplus k_2$

$$\mathrm{Sym}_k(\texttt{Data}),\ \mathrm{Asym}_{\mathsf{PK:BKA}}(k_1),\ \mathrm{Asym}_{\mathsf{PK:BfDI}}(\texttt{Req} \parallel k_2)$$

   oder

$$\mathrm{Sym}_k(\texttt{Data}),\ \mathrm{Asym}_{\mathsf{PK:BND}}(k_1),\ \mathrm{Asym}_{\mathsf{PK:BfDI}}(h(\texttt{Req}) \parallel k_2)$$

3. Verschlüsselte Speicherung der Verbindungsdaten
   - Probleme: Durchsuchbarkeit (Zeitfenster), Effizienz
4. Erweiterung: Schlüsselverteilung, wie in Punkt 2
5. Oblivious Transfer bzw. Private Information Retrieval
   - Aufwendig, aber auch für Nachrichtendienste interessant

Vielen Dank!