Kryptographische Missbrauchssicherungen für die Vorratsdatenspeicherung

Heiko Stamer

Universität Kassel, Fachbereich Elektrotechnik/Informatik
Wilhelmshöher Allee 71-73, D-34109 Kassel
stamer@theory.informatik.uni-kassel.de

Auf Grundlage der EU-Richtlinie 2006/24/EG hat die Bundesregierung im April 2007 einen umstrittenen Gesetzentwurf [BT07a] vorgelegt, welcher alle Telekommunikations- und Internetanbieter verpflichtet, die Kommunikationsverbindungsdaten ihrer Kunden für mindestens 6 Monate auf Vorrat zu speichern. Bei der Sachverständigenanhörung im Rechtsausschuss des Deutschen Bundestages [BT07b] ist kürzlich sehr deutlich geworden, dass nicht nur verfassungs- und datenschutzrechtlich *große Bedenken* bestehen, sondern das auch viele technische Fragen noch ungeklärt sind.

Zwar gab es auf europäischer Ebene bereits verschiedene Expertentreffen [AKV1] und das Europäische Institut für Telekommunikationsnormen (ETSI) hat mittlerweile ebenfalls in Form von Standardisierungsbestrebungen [ETSI1, AKV2, ETSI2] reagiert, jedoch sind bisher kaum *datenschutzfreundliche Lösungen* für die Speicherung der sensiblen Verbindungsdaten öffentlich bekannt geworden. Das ist im Zusammenhang mit der Brisanz von Telekommunikationsverbindungsdaten mehr als erstaunlich, da diese Daten ein *enormes Missbrauchspotential* in sich bergen.

Im Vortrag werden verschiedene Speicher- und Zugriffsszenarien sowie entsprechende Implementierungsansätze diskutiert, die mit Hilfe von Kryptographie (Verschlüsselung, PIR u. ä.) eine „datenschutzfreundlichere Vorratsdatenspeicherung“ ermöglichen könnten. Diese *konstruktive* Herangehensweise soll jedoch nicht darüber hinweg täuschen, dass ich persönlich *jegliche* Vorratsspeicherung prinzipiell für unverhältnismäßig, ineffizient und datenschutzrechtlich gefährlich halte.

Literatur

[BT07a] Gesetzentwurf der Bundesregierung. *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG.* BT-Drucksache 16/5846. Online verfügbar unter http://www.bundestag.de/ausschuesse/a06/anhoerungen/24_tkue_vorratsdatenspeicherung/01_Bundestagsdrucksachen/1605846.pdf

[BT07b] Zusammenfassung der Stellungnahmen der Sachverständigen im Rechtsausschuss. *Telefonüberwachung und Datenspeicherung umstritten.* Online verfügbar unter http://www.bundestag.de/aktuell/archiv/2007/telekom_kw38/index.html

[AKV1] Arbeitskreis Vorratsdatenspeicherung. *Protokoll des Expertentreffens zu Implementierungsfragen der Vorratsdatenspeicherung vom 16. Mai 2007.* Online verfügbar unter: http://wiki.vorratsdatenspeicherung.de/Protokoll_des_Expertentreffens_zu_Implementierungsfragen_der_Vorratsdatenspeicherung_vom_16._Mai_2007

[AKV2] Arbeitskreis Vorratsdatenspeicherung. *ETSI-Dokumente.* Online verfügbar unter: http://wiki.vorratsdatenspeicherung.de/ETSI-Dokumente

[ETSI1] European Telecommunications Standards Institute. *Retained data requirements law enforcement.*

[ETSI2] European Telecommunications Standards Institute. *Security framework in Lawful Interception and Retained Data environment.* Ref. DTR/LI-00044, Start of work on 2007-04-25.