Vorratsdatenspeicherung

Überwachung, Auswertung, Gegenmaßnahmen

Stefan Schumacher

Magdeburger Institut für Sicherheitsforschung

23.04.2015, Uni Bremen



Über Mich



Über Mich

- Bildungswissenschaft/Psychologie
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Geek, Nerd, Hacker seit knapp 20 Jahren
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`



Forschungsprogramme des MIS

- Psychologie der Sicherheit
  - Social Engineering
  - Security Awareness, Sicherheit in Organisationen
  - Didaktik der Sicherheit
  - Didaktik der Kryptographie
  - Lernfelder: Fachinformatiker IT-Sicherheit
  - Lernfelder: IT-Sicherheit für Kaufleute
  - Lernfelder: IT-Sicherheit für Elektroberufe



Informationstechnologie und Sicherheitspolitik

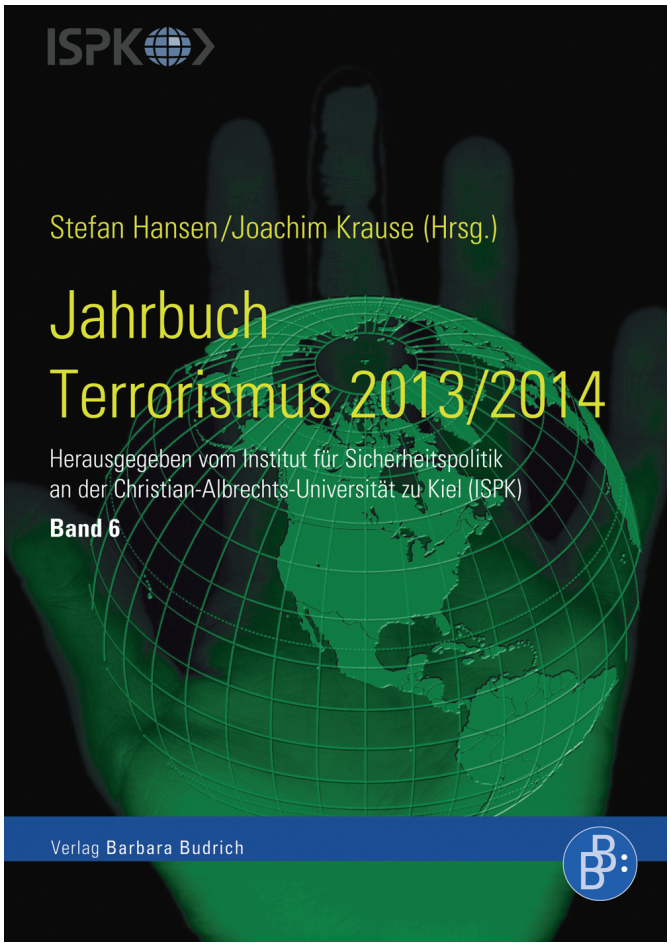
Sambleben, J. und Schumacher, S. (Herausgeber)



http://www.sicherheitsforschung-magdeburg.de/buecher.html

Jahrbuch Terrorismus 2013/2014

Hansen, S. und Krause, J. (Herausgeber, Institut für Sicherheitspolitik Kiel)



Stefan Schumacher:
Cyber-Terrorismus:
Reale Bedrohung oder Mythos?
S. 159 – 180

Inhaltsverzeichnis

1 Rasterfahndung

2 Vorratsdatenspeicherung

Rasterfahndung

- Durchsuchung von Datenbeständen
- Eingrenzung von Eigenschaften
- keine bekannte/konkrete Zielperson bekannt
- Bsp: Judenkarteien im Dritten Reich
- händische Auswertung und Zusammeführung
- aufwändig, schlechte Effizienz

Rasterfahndung

- 1979: Weiterentwicklung durch Horst Herold, BKA-Präsident
- konspirative Wohnungen in Frankfurt/Main identifizieren
  - Stromrechnung bar bezahlt
  - entferne legale Namensträger aus Menge der Barzahler
    - gemeldeten Einwohner
    - Kfz-Halter
    - Rentner
    - Bafög-Bezieher
    - im Grundbuch verzeichnete Eigentümer
    - Brandversicherten
    - gesetzlich Krankenversicherten
  - noch sehr viel Handarbeit nötig



Rasterfahndung

- verschnitt von Datenbeständen
- nach bestimmten Kriterien
- IT mehr Rechenleistung verfügbar
- bessere Datenbanken verfügbar
- immer mehr Daten ...



Inhaltsverzeichnis

1 Rasterfahndung

2 Vorratsdatenspeicherung



Vorratsdatenspeicherung

- Speicherung personenbezogener Daten
- durch oder für Behörden
- für den Fall einer späteren Nutzung
- hier: Telekommunikationsverbindungsdaten
- Speicherung der Verbindungsdaten durch Telkos
- Metadaten



Vorratsdatenspeicherung

- bessere Verhütung von Straftaten
- bessere Verfolgbarkeit von Straftaten
- Analyse des Kommunikationsverhaltens möglich
- Analyse der Persönlichkeit und des sozialen Netzes möglich
- elektronische Kommunikation wächst

Technik

- Fräulein vom Amt steckt Verbindung und protokolliert
- Elektromechanische Wähler eingeführt, keine Protokollierung möglich
- Fangschaltung notwendig
- digitale Vermittlungsstellen in den 1980ern eingeführt
- umfassende Protokollierung möglich
- Einzelverbindungsnachweis möglich
- Fangschaltung nicht mehr notwendig



Speicherung

- Telkos dürfen nur abrechnungsrelevante Daten speichern
- BDSG verbietet Speicherung von personenbezogenen Daten
- es sei denn sie sind notwendig oder per Gesetz verlangt
- Forderung aus Politik und Strafverfolgern: zusätzliche Daten speichern



Forderungen

- Daten min. 6 Monate speichern
- Standortdaten
- eindeutige Geräteidentifikation (IMEI, MAC)
- Verkehrsdaten: eingehende Verbindungen, Handystandort, IP-Adressen, E-Mailverkehr



Verkehrsdaten

§3 Nr. 30 TKG

- der in Anspruch genommene Telekommunikationsdienst
- die Nummer oder die Kennung der beteiligten Anschlüsse (Anrufer und Angerufener)
- personenbezogene Berechtigungskennungen
- die Kartennummer (bei Verwendung von Kundenkarten)
- eventuelle Standortdaten (bei Mobiltelefonen)
- Beginn und das Ende der jeweiligen Verbindung (Datum und Uhrzeit)
- die übermittelten Datenmengen



Daten heute

- massive Ausbreitung des Internets in den letzten 20 Jahren
- massive Ausbreitung der IT in viele Lebensbereich (Smart Meter, Smart Home, Iphones, KFZ ...)
- Internet der Dinge dank RFID
- Bewegungsprofile im GSM/GPS
- massive Ausweitung der anfallenden Daten
- Sammlung und Auswertung der Daten um politische und wirtschaftliche Ziele umzusetzen



Daten - Information - Wissen

- Daten: 27.04.2011, 2011-04-27, 04/27/2011
- Information: Daten müssen gelesen und interpretiert werden
- Computer kann schnell interpretieren, *wenn* ein Interpretationsrahmen vorgegeben ist

Beispiel Rasterfahndung

- Alle muslimischen, männlichen Studenten zwischen 20 und 30 Jahren, die Ingenieur- oder Naturwissenschaften studieren und im letzten Jahr in Afghanistan oder Pakistan waren, sind Terroristen.
- Payback erfasst Einkaufszettel: Gib mir alle schwangeren Frauen/Mütter mit Säuglingen in Magdeburg, die Grüne wählen und in Zahlungsschwierigkeiten sind.
- Facebook: Gib mir alle ungeouteten, latent homosexuellen, konservativen Studenten.



Knowledge Discovery in Databases

- Computer können Rechnen, mehr nicht. Sie sind stumpfsinnig.
- maschinelles Lernen: Generierung von Wissen aus Erfahrung, erkennt Gesetzmäßigkeiten in den Lerndaten (Handschriftenerkennung, Bilderkennung)
- Data Mining: neue Muster in großem Datenbestand erkennen (Rasterfahndung, Fraud Detection)
- Online Analytical Processing: Hypothesen als Anfragen (Business Intelligence)
- Hardware und Software wird besser und billiger



Problematisch: IP-Adresse

- IP-Adresse: Hausnummer des Rechners im Internet
- z.B. 141.44.1.1; 192.168.1.1, 127.0.0.1, www.Kaishakunin.com
- identifiziert ein Gerät im Internet, wird **immer** übertragen
- ISP (T-Online, Alice, AOL, Kabel Deutschland) kann die IP einer Person (Vertragspartner) zuordnen $\rightsquigarrow$ Identifizierbarkeit
- IP taucht auf in jeder E-Mail, in Weblogs, FTP-Logs etc.pp.
- Gateways und Proxies (VPN-Client, anyone)
- Protokollierung und Zusammenführung $\rightsquigarrow$ Profil
- Probleme: IP-NAT, UMTS, Gerichtsverwertbarkeit



Problematisch: Zusammenführung

- Zusammenführung der Daten: Facebook + Payback + Amazon + GSM + Ebay
- Personalisierung der Daten, d.h. Zuordnung auf eine Person
- Daten werden verkauft
- validierte E-Mail-Adresse von Wissenschaftlern: 1-2$, Datensätze von Patienten bis zu 5.000$
- Ziehen von (falschen) Schlüssen
- Identitätsdiebstahl (vorrangig in den USA dank SSN)
- Umgehung nationaler Gesetze durch Kooperationen (NSA-UK, GCHQ-USA)



Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte

Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte



Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte



Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte die Dihydrogenmonoxid enthalten und kleiner als 5kb sind



Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte die Dihydrogenmonoxid enthalten und kleiner als 5kb sind
- gib mir alle Handies die am 24.12. in der selben Funkzelle waren



Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte die Dihydrogenmonoxid enthalten und kleiner als 5kb sind
- gib mir alle Handies die am 24.12. in der selben Funkzelle waren
- gib mir alle Handynummern aller E-Mailkontakte



Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte die Dihydrogenmonoxid enthalten und kleiner als 5kb sind
- gib mir alle Handies die am 24.12. in der selben Funkzelle waren
- gib mir alle Handynummern aller E-Mailkontakte
- gib mir alle schwangeren Single-Frauen aus Hamburg die FDP wählen und Coldplay mögen sowie eine Katze haben



Datensammlung und -auswertung

- gib mir alle Kontakte
- gib mir alle Kontakte der Kontakte
- gib mir alle Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte
- gib mir alle E-Mails der Kontakte der Kontakte der Kontakte die Dihydrogenmonoxid enthalten und kleiner als 5kb sind
- gib mir alle Handies die am 24.12. in der selben Funkzelle waren
- gib mir alle Handynummern aller E-Mailkontakte
- gib mir alle schwangeren Single-Frauen aus Hamburg die FDP wählen und Coldplay mögen sowie eine Katze haben

Bewegungsprofil Malte Spitz

http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten

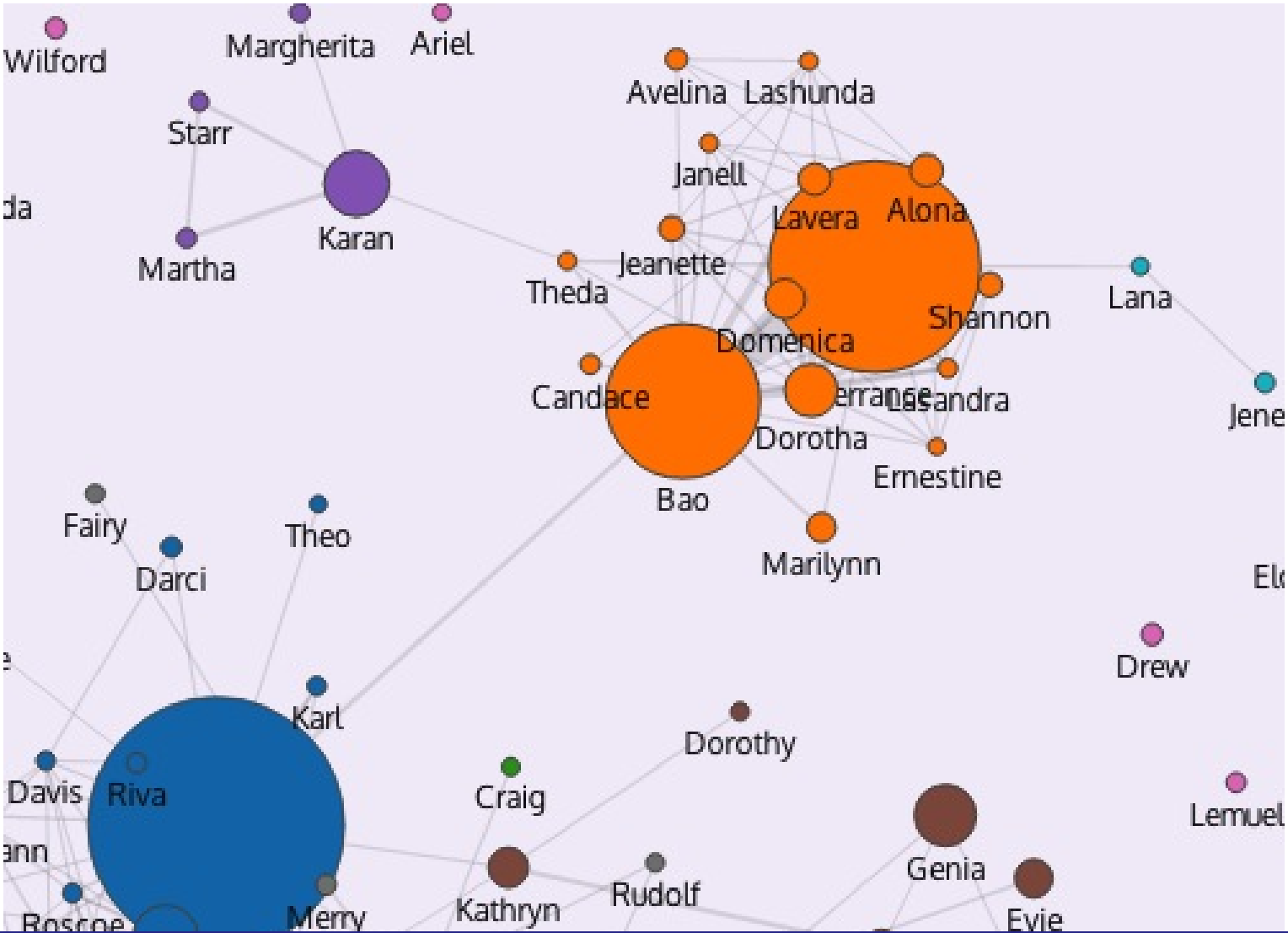


Bewegungsprofil Malte Spitz

http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten



Kommunikationsnetz TechCrunch



Aufklärung

- großflächige Überwachung sozialer Netzwerke
- Erkennung von sich entwickelnden Revolutionen
- Kommunikationsaufkommen steigt massiv an
- Metadaten zur Analyse der Situation
- Braut sich was zusammen?

Daten verschneiden

- Kommunikationsdaten (Wer mailt/telefoniert mit wem?)
- Bewegungsdaten Handy
- Bewegungsdaten Bahn, Flugverkehr
- Zahlungsverkehr (SWIFT)
- gezielte Angriffe (Trojaner, etc.)
- Kombination zum Lagebild

Kritik

- keine Anonymität mehr möglich z.B. für Beratungsangebote
- Salami-Taktik, Ausweitung der Kommunikationsdaten
- Vergangenheitsbezogen, nur nachträglich Wirksam
- Abschreckungswirkung gering insbesondere gegen OK und Terrorismus

Kritik

- AK Vorrat: Aufklärungsquote steigt von 55% auf 55,006%
- Bundeskriminalamt, Polizeiliche Kriminalstatistik 2006:
- durchschnittliche Aufklärungsquote 55,4%
- 78,5% Verbreitung pornographischer Schriften via Internet
- 86% Internetbetrug
- 85,5% der Straftaten gegen Urheberrechtsbestimmungen im Internet aufgeklärt



Kritik

- Missbrauchsrisiko
- Verfolgung von Whistleblowern
- Teuer



Daten kontrollieren

- angefallene Daten lassen sich nicht kontrollieren oder sicher löschen
- wir liefern unsere Daten freiwillig ab (Facebook)
- wir liefern unsere Daten freiwillig aus (Apple, Google, DRM)



Gegenmaßnahmen

- Kryptographie nutzen
- SSL/TLS: https://www
- E-Mails verschlüsseln
- Anonymisierungsdienste wie Tor nutzen
- Off the Record



- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher