Grundbegriffe

Jens Lechtenbörger

Kommunikation im Fediverse 2018/19

1 Einleitung

1.1 Lernziele

- Grundlegende Begriffe Vertrauen, Privatsphäre, Dezentralisierung und Fediverse mit ihren Zusammenhängen erklären
- Eigenschaften wie Privatsphäre und Rechte des User Data Manifesto an exemplarischem Projekt untersuchen (Seminarteil)

2 Grundlegende Begriffe

2.1 Vertrauen

- Trust im Sinne von CACS?

2.1.1 Vertrauen und Trusted Computing

- Video „Trusted Computing“ (2005) von Benjamin Stephan und Lutz Vogel
  - `https://www.lafkon.net/tc/`

2.2 Privatsphäre

- Privacy im Sinne von CACS?

2.3 Informationelle Selbstbestimmung

- Deutsches Grundrecht seit Volkszählungsurteil, 1983
  - „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. [...]

> Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“

2.4 Autonomie und Privatsphäre

- Selbstbestimmung auf voriger Folie
- Eben Moglen über das verworrene Netz: Privatsphäre besitzt ökologische Dimension
- Daniel Solove [Sol07] unterscheidet orwellsche und kafkaeske Phänomene (meine Interpretation)
  - Orwellsch: In Anlehnung an Roman *1984*, Überwachung unterdrückt abweichendes Verhalten
  - Kafkaesk: In Anlehnung an Roman *Der Prozess*, Hilflosigkeit und Verwundbarkeit angesichts fehlender Transparenz und Kontrolle

2.5 Mehrparteienprivatsphäre (MP)

- Siehe [SC18]
  - „Multiparty privacy (MP) aims to facilitate the coordination of collectively held privacy boundaries by all individuals that co-own a data item online, as the privacy of all of them may be at stake depending on with whom the co-owned data item is shared. MP particularly focuses on supporting the detection and resolution of multiparty privacy conflicts (MPCs), when individuals whose privacy may be affected by the same co-owned data item have conflicting privacy preferences.“
- Heutige Mechanismen
  - Tagging
  - Reporting

2.5.1 MP-Ansätze

- Klassifikation aus [SC18]
  - Manuell
  - Auktion
  - Aggregation
  - Adaptiv
  - Spieltheoretisch
  - Feingranular
- Ihr Projekt?

2.6 Privatsphäre und Kommunikation

- Gibt es noch Vier-Augen-Gespräche?
  - Über welche (Sicherheits-) Eigenschaften verfügen sie? (Jahrtausende alter Standard)
- Online
  - Off-The-Record-Kommunikation
    - Vertraulichkeit, Authentizität, Abstreitbarkeit
    - (Perfect) Forward Secrecy
  - OMEMO als Weiterentwicklung auch für Gruppen-Chat
- Ihr Projekt?

2.7 Dezentralisierung und Föderation

- Dezentral laut Duden: „auf verschiedene Stellen oder Orte verteilt, nicht von einer Stelle ausgehend“
- Dezentralisierung laut Duden: „Übertragung von Funktionen und Aufgaben auf verschiedene [untergeordnete] Stellen“
- Föderation: „Zusammenschluss von Organisationen“

2.8 Freie Software

- Erinnerung
  - „Frei“ wie in Freiheit, nicht Freibier
  - Vier Freiheiten
    1. Software ausführen (auch geänderte Versionen)
    2. Software untersuchen
    3. Kopien weitergeben
    4. Veränderte Versionen weitergeben

3 Dezentralisierte IT-Systeme

3.1 IT-Bezug

- Dezentralisierung von IT hat lange Tradition
  - Übersichtsartikel [Kin83] von 1983 zu Dezentralisierung als Managemententscheidung im Unternehmen
    - „The fundamental question, when one looks carefully at the issue of whether to centralize or decentralize computing, is who will have control over procurement, use, and management?“
    - Drei Aspekte
      - De-/Zentralisierung von Kontrolle

        - De-/Zentralisierung physischer Orte
        - De-/Zentralisierung von Funktionen
    * Vor- und Nachteile
        - Bürokratisch und langsam oder flexibel und passgenau?
        - Skaleneffekte oder Einzellösungen?
        - Standard oder durcheinander?
        - Top-down oder grass roots?

3.2 Weitere IT-Bezüge

- Internet mit dezentralen Ansätzen
  - Keine zentrale Instanz, deren Ausfall zum Totalausfall führt
    * Autonome Systeme als dezentral verwaltete Teilnetze
  - **Aber** zentralisierte Kontrolle über IP-Adressen und DNS-Namen
- Web und E-Mail sind dezentral
  - Web könnte noch dezentraler sein: Decentralized Web FAQ
- Git ist dezentral
- Peer-To-Peer-Netze sind dezentral
  - Zuerst File Sharing, heute Blockchain
  - Peer to peer (P2P) in Reinform: Jede/r kann mit gleichen Rechten teilnehmen

3.3 User Data Manifesto 2.0

- Manifest für Grundrechte zu eigenen Daten im Internetzeitalter
  - [Lesezeit]

  1. Kontrolle über Datenzugriff
     - Zugriffsrechte und Lizenzen unter Nutzerkontrolle
     - Keine Sonderrechte für Provider/Dritte
  2. Wissen, wie Daten gespeichert werden
     - Informationen zu Server-Orten und Rechtslage
     - Keine zentralisierten Dienste, sondern P2P; freie Software
  3. Freie Wahl der Plattform
     - Extraktion der Daten ohne Vendor-Lock-In
     - Offene Standards und freie Software
- Ihr Projekt?

4 Fediverse

4.1 Das Fediverse

- https://fediverse.party/en/fediverse/
  - Kofferwort: Federated Universe
  - Föderierte soziale Netze mit freier Software
    - Und mehr: https://gitlab.com/fediverse/fediverse.gitlab.io/issues/11
- Zentrale Argumente
  - Freie Software notwendig für Vertrauen
  - Föderation ermöglicht Autonomie und Wahl vertrauenswürdiger Anbieter
  - Vermeidung von Monopolen
  - Mehr?

4.2 Kritik an Fediverse und Föderation

- Zufälliger Blog-Artikel
  - Nachrichten sind im Regelfall Klartext
  - Serverbetreiber können alles überwachen
- Aussagen aus Signal-Blog
  - Signal (freie WhatsApp-Alternative) ist zentralisiert
    - Innovative Lösungen erfordern zentrale Kontrolle
  - XMPP als föderierte Alternative ist nicht massentauglich
    - Standardisierung macht langsam (in sich bewegendem Ökosystem)
    - Erweiterungen führen zu Inkonsistenz
  - Föderation führt früher oder später zu monopolähnlichem Anbieter
    - Netzwerkeffekte

4.3 Unser Verständnis (erste Version)

- Charakteristika?
- Vor- und Nachteile?
- Ihr Projekt?

5 Schluss

5.1 Zusammenfassung

- User Data Manifesto definiert Rechte für Privatsphäre
- Dezentralisierung und Förderation eröffnen Autonomie, stärken Vertrauen
- Freie Software ermöglicht Transparenz und Kontrolle, reduziert Bedarf an Vertrauen
- Fediverse kombiniert obige Aspekte

Quellenangaben

[Kin83] John Leslie King. "Centralized Versus Decentralized Computing: Organizational Considerations and Management Options". In: *ACM Comput. Surv.* 15.4 (Dec. 1983), pp. 319–349. ISSN: 0360-0300. DOI: 10.1145/289.290. URL: https://doi.org/10.1145/289.290.

[SC18] Jose M. Such and Natalia Criado. "Multiparty Privacy in Social Media". In: *Commun. ACM* 61.8 (July 2018), pp. 74–81. ISSN: 0001-0782. DOI: 10.1145/3208039. URL: https://cacm.acm.org/magazines/2018/8/229766-multiparty-privacy-in-social-media/fulltext.

[Sol07] Daniel J. Solove. "I've got nothing to hide and other misunderstandings of privacy". In: *San Diego Law Review* 44 (2007), p. 745. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565.

Lizenzangaben