Grundbegriffe *

Jens Lechtenbörger

VM Neuland im Internet 2021

Inhaltsverzeichnis

1 Einleitung

1.1 Lernziele

- Erste Schritte in Solid gehen
- Grundlegende Begriffe Kontrolle, Vertrauen, Privatsphäre, Dezentralisierung und Solid mit ihren Zusammenhängen erklären

2 Solid

2.1 Das Projekt Solid

- Social Linked Data, `https://solidproject.org/`
  - Als MIT-Projekt vom Web-Erfinder Tim Berners-Lee gestartet
  - Freie Software und offene Standards auf GitHub
- Pod = Personal online data store

*Dieses PDF-Dokument ist eine minderwertige Version einer OER-HTML-Seite; freies Repository mit Org-Mode-Quelltexten.

  - Dezentrale Web-Server mit freier Software
    * Verwaltung von Identitäten und Daten mit **Web-Standards**
    * Z. B. öffentliche Instanz oder eigener Solid-Server

2.2 Argumente

- Aus [Cap+17]
- (Dokieli als dezentrales Authoring- und Annotation-Werkzeug; in Solid integriert)
  - "independence of centralised platforms is a necessity for ownership of published ideas, and to establish a relation of trust"
    * "any author can say anything about anything"
    * "others are free to selectively (dis-)trust certain sources"
    * "technical reasons of scalability and resilience"
    * "societal need for freedom of expression"
    * "avoiding a /vendor lock-in/", "avoid the walled garden problem"
- Kontext wissenschaftlicher Publikationen
  - "potential to engage more people sooner"
  - "Trust [...] assessed by repeated independent validation"

2.3 Solid-Anwendungen

- Laut `https://github.com/solid/solid`
  - Multi-User-Anwendungen
    * Austausch über verteiltes Dateisystem
    * Das Web ist dies Dateisystem
  - Linked Data Platform (LDP) 1.0 (Primer) definiert Regeln für Read-Write-Linked-Data-Architektur
    * **HTTP-Operationen** für Lesen/Erzeugen/Ändern/Löschen (GET/PUT/POST/PATCH/DELETE)
    * REST [Fie00]
      · Architekturstil, Programmierparadigma
      · Prinzipien: Client-Server, Zustandslosigkeit, Caching, einheitliche Schnittstelle (z. B. URIs, MIME, HTTP), Schichtenarchitektur
    * Neue Anwendungen ohne Server-Änderungen
    * **RDF** als Datenmodell
      · Verschiedene Serialisierungen, z. B. N3, Turtle (`*.ttl`)

2.3.1 Linked Data

- (Ausführlicher in kommenden Terminen)
- URIs identifizieren „Dinge“
  - (Web-Seiten, Likes, Personen, Konzepte, . . .)
  - `https://ruben.verborgh.org/profile/#me`
    - Web-Browser ruft Dokument ohne **Fragment** `#me` ab
    - Fragment (typischerweise) als ID innerhalb des Dokuments
- Standardisierte **Vokabulare** (Ontologien)
  - RDF für Darstellung von Bezügen in Tripeln
    - Subjekt, Prädikat, Objekt
      - `:me foaf:name "Ruben Verborgh"@en`
      - `:me foaf:img <https://ruben.verborgh.org/images/ruben.jpg>`
    - **Präfixe** definieren Vokabulare
      - Z. B. `foaf` für `http://xmlns.com/foaf/0.1/`
      - Achtung, Vokabular-URIs in erster Linie als Identifikatoren, nicht notwendig URLs

2.4 Solid-Tutorial

- Inspiration
  - Kennung anlegen `https://solidcommunity.net/`
  - Gemeinsame Schritte

3 Grundlegende Begriffe

3.1 Vertrauen

- Vertrauen im Offshoring-Kontext aufbauend auf Giddens in [KN08]:
  - Trust is emotional commitment
    - [Gid90]: “confidence in the reliability of a person or system, regarding a given set of outcomes or events, when that confidence expresses a faith in the probity or love of another, or in the correctness of abstract principles”
    - trust in ability, benevolence, integrity
    - process-based (prior exchanges, reputation), characteristic-based (social similarities), institutional-based (certificates, insurance, law)

3.1.1 Vertrauen und Trusted Computing

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

3.2 Privatsphäre

- Privatsphäre aufbauend auf [Int97]
  - Categories
    - (a) No access to person or personal realm: Right to be left alone
    - (b) Control over personal information
    - (c) Freedom from judgment or scrutiny by others
  - Aspects
    - Relational and relative concept, community, interaction
    - Personal domain
    - Control access
    - Control distribution
    - Immunity against judgments
  - Privacy as clearing from which autonomy, trust, and accountability can emerge

3.3 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.“

3.4 Autonomie und Privatsphäre

- Selbstbestimmung auf voriger Folie
- Eben Moglen [Mog13] (auf Deutsch): Privatsphäre besitzt ökologische Dimension
  - Psychologische, kulturelle, soziale und politische Autonomie des Einzelnen in Relation zum Netz
- 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

3.5 Privatsphäre und Kommunikation

- Gibt es noch Vier-Augen-Gespräche?
  - Über welche (Sicherheits-) Eigenschaften verfügen sie? (Jahrtausende alter Standard)
- Online
  - Off-The-Record-Kommunikation [BGB04]
    - Vertraulichkeit, Authentizität, Abstreitbarkeit
    - (Perfect) Forward Secrecy
  - Signal-Protokoll (siehe [Coh+17]) und OMEMO als Weiterentwicklung auch für Gruppen-Chat

3.6 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“

3.7 Freie Software

- Erinnerung
  - „Frei“ wie in Freiheit, nicht Freibier; siehe [Sta86; Cro+08]
  - Vier Freiheiten
    1. Software ausführen (auch geänderte Versionen)
    2. Software untersuchen
    3. Kopien weitergeben
    4. Veränderte Versionen weitergeben

4 Dezentralisierte IT-Systeme

4.1 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?

4.2 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
    * Solid

- Peer-To-Peer-Netze sind dezentral
  - Peer to peer (P2P) [AS04] in Reinform
    * Jede/r kann mit gleichen Rechten teilnehmen
    * Zuerst File Sharing, heute bis zur Blockchain [Wal19]

4.3 User Data Manifesto 2.0

- Manifest für Grundrechte zu eigenen Daten im Internetzeitalter

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

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
- Solid kombiniert obige Aspekte

Literatur

[AS04] Stephanos Androutsellis-Theotokis und Diomidis Spinellis. “A Survey of Peer-to-peer Content Distribution Technologies”. In: *ACM Comput. Surv.* 36.4 (2004), S. 335–371. DOI: 10.1145/1041680.1041681. URL: http://doi.acm.org/10.1145/1041680.1041681.

[BGB04] Nikita Borisov, Ian Goldberg und Eric Brewer. "Off-the-record Communication, or, Why Not to Use PGP". In: *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society*. WPES '04. 2004, S. 77–84. DOI: 10.1145/1029179.1029200. URL: http://doi.acm.org/10.1145/1029179.1029200.

[Cap+17] Sarven Capadisli u. a. "Decentralised authoring, annotations and notifications for a read-write web with dokieli". In: *International Conference on Web Engineering*. 2017, S. 469–481. URL: https://doi.org/10.1007/978-3-319-60131-1_33.

[Coh+17] Katriel Cohn-Gordon u. a. "A Formal Security Analysis of the Signal Messaging Protocol". In: *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2017, S. 451–466. DOI: 10.1109/EuroSP.2017.27. URL: https://www.douglas.stebila.ca/files/research/papers/EuroSP-CCDGS17-full.pdf.

[Cro+08] Kevin Crowston u. a. "Free/Libre Open-source Software Development: What We Know and What We Do Not Know". In: *ACM Comput. Surv.* 44.2 (2008), 7:1–7:35. DOI: 10.1145/2089125.2089127. URL: http://doi.acm.org/10.1145/2089125.2089127.

[Fie00] Roy Thomas Fielding. "Architectural Styles and the Design of Network-based Software Architectures". Diss. University of California, Irvine, 2000. URL: https://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm.

[Gid90] Anthony Giddens. *The Consequences of Modernity*. Stanford University Press, 1990.

[Int97] Lucas D. Introna. "Privacy and the computer: why we need privacy in the information society". In: *Metaphilosophy* 28.3 (1997), S. 259–275.

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

[KN08] Séamas Kelly und Camilla Noonan. "Anxiety and psychological security in offshoring relationships: the role and development of trust as emotional commitment". In: *Journal of Information Technology* 23.4 (2008), S. 232–248.

[Mog13] Eben Moglen. "The Tangled Web We Have Woven". In: *Commun. ACM* 56.2 (2013), S. 20–22. DOI: 10.1145/2408776.2408784. URL: http://doi.acm.org/10.1145/2408776.2408784.

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

[Sta86] Richard M. Stallman. “What is the Free Software Foundation?” In: *GNU’s Bulletin* 1.1 (1986). URL: https://www.gnu.org/bulletins/bull1.txt.

[Wal19] Jim Waldo. “A Hitchhiker’s Guide to the Blockchain Universe”. In: *Commun. ACM* 62.3 (2019), S. 38–42. DOI: 10.1145/3303868. URL: http://doi.acm.org/10.1145/3303868.

Lizenzangaben