Social Networks versus Security and Privacy

Christian Grothoff

27.4.2017

Was ist ein “Soziales Netzwerk”?

Funktionen eines Sozialen Netzwerks

Muss:

- Benutzer erzeugen Profile und Nachrichten ("user-generated content")
- Benutzer verbinden sich bzw. subskribieren Kanäle
- Kommunikation wird über diese Verbindungen gesteuert

Funktionen eines Sozialen Netzwerks

Muss:

- Benutzer erzeugen Profile und Nachrichten ("user-generated content")
- Benutzer verbinden sich bzw. subskribieren Kanäle
- Kommunikation wird über diese Verbindungen gesteuert

Optional:

- Erzeugung von Gruppen
- Suche nach Profilen / Themen

Was ist der Wertbeitrag für Benutzer?

Was ist der Wertbeitrag für Benutzer?

Vergemeinschaftlichung der Filterfunktion zur Bewältigung der Informationsflut

Anwendungsgebiete

Geschäftlich

XING

Nachrichten

diaspora*

Bitmessage

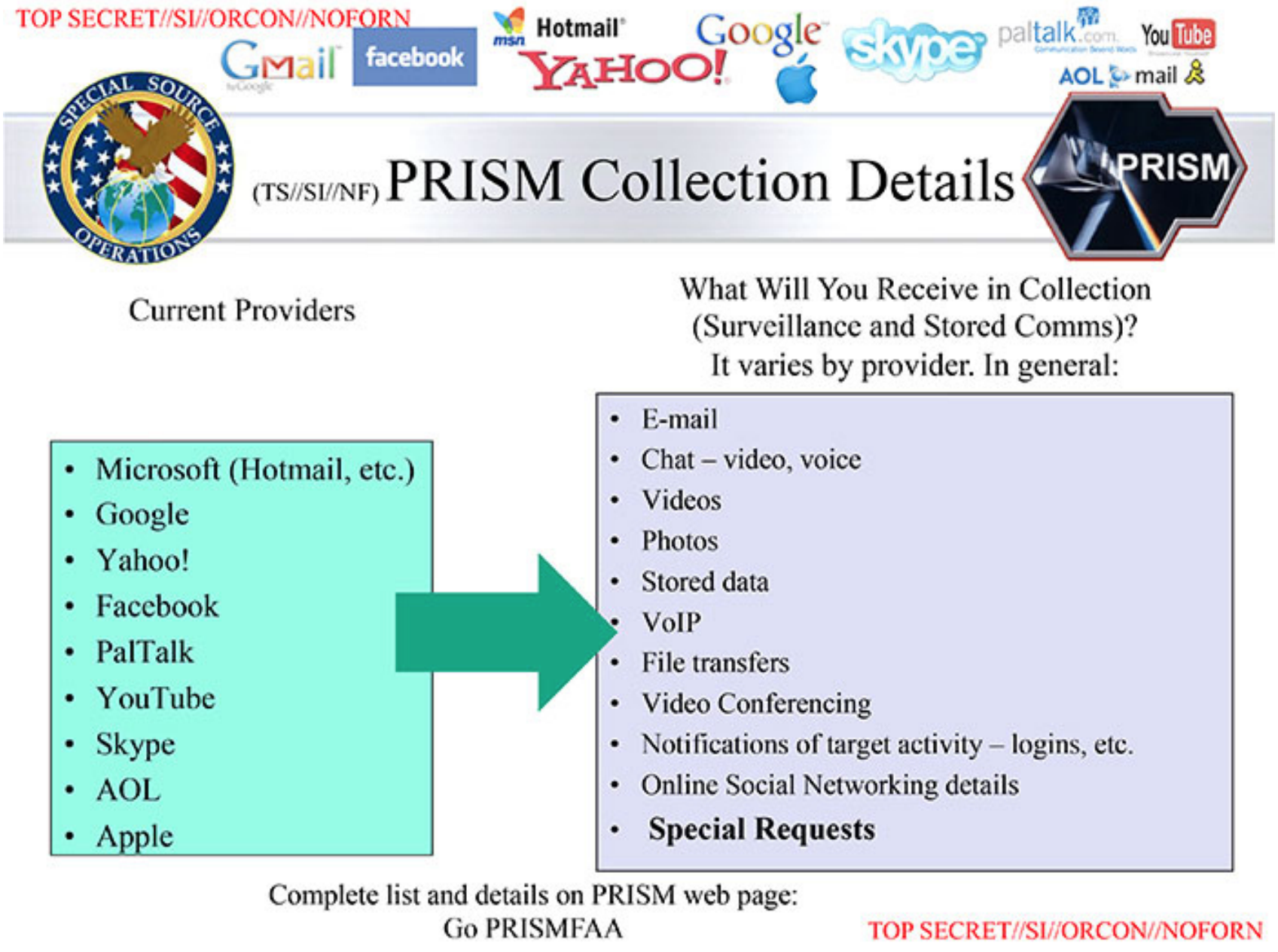
Freundschaften

tinder

gnusocial

Was sind die gesellschaftlichen Risiken?

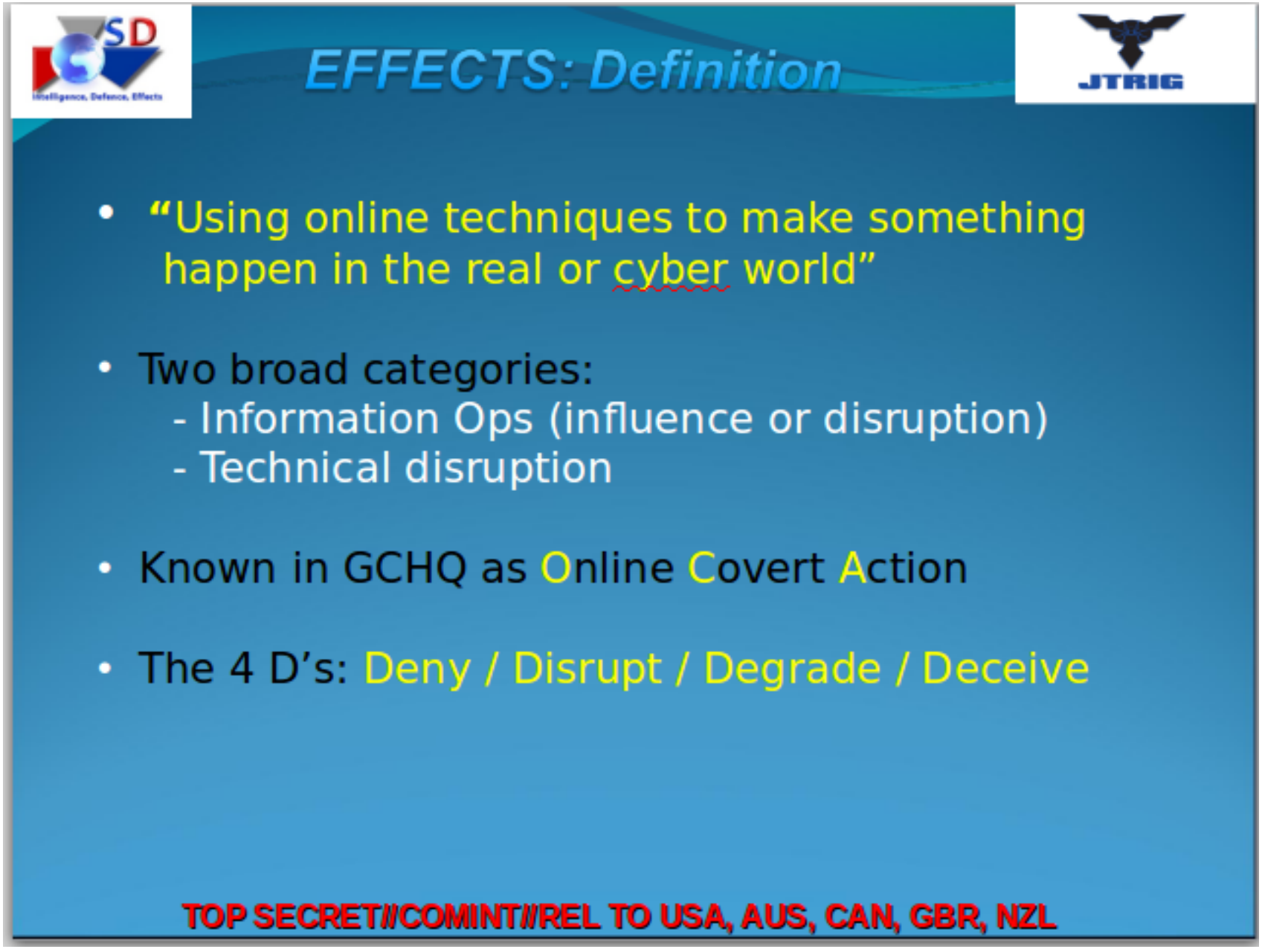
Risiken und Nebenwirkungen: Überwachung



Risiken und Nebenwirkungen: Zersetzung

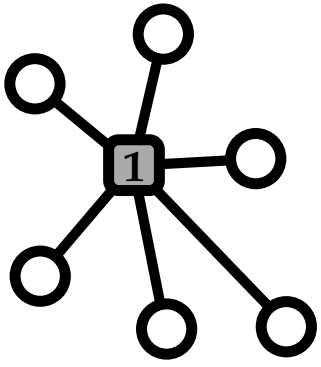
Risiken und Nebenwirkungen: Zersetzung

Risiken und Nebenwirkungen: Zersetzung



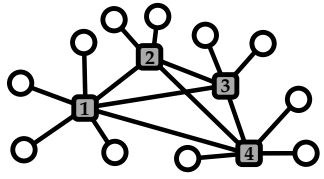
Organisationsstrukturen / Architektur

Zentralisiert



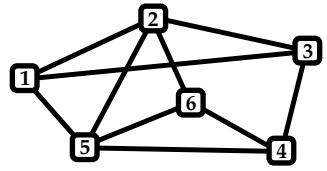
(@potus)

Föderiert (*)



(user@provider)

Dezentralisiert (*)



(DSTJBRRKZ8TBW
3FGK6BOM5QXWT
9WYNZ45H5MCV4
HY7ST64Q8T9FO)

(*) Der irreführende Betriff “verteilt” wird in diesem Zusammenhang auch manchmal gebraucht.

Beispiele

Zentralisiert

Föderiert

diaspora*

[matrix]

Dezentralisiert

Bitmessage

Vorteile von Zentralisierung

Vorteile von Zentralisierung

- Professionelle Administration
- Skalierbarkeit
- Effektive Datenauswertung

Nachteile von Zentralisierung

Nachteile von Zentralisierung

- Abhängigkeit vom Anbieter

Vorteile von Föderation

Vorteile von Föderation

- Externalisierung der Administration
- Datenauswertung erschwert
- Wettbewerb zwischen Anbietern

Nachteile von Föderierung

Nachteile von Föderierung

- Komplexität
- Degeneration zu Zentralisierung

Vorteile von Dezentralisierung

Vorteile von Dezentralisierung

- Unabhängigkeit
- Datenschutz

Nachteile von Dezentralisierung

Nachteile von Dezentralisierung

- persönliche Verantwortung für den Betrieb
- praktische Probleme wg. Internetarchitektur (NAT, Firewalls)
- Suchfunktion fehlt oder schwierig

Geschäftsmodelle bei Zentralisierung

Geschäftsmodelle bei Zentralisierung

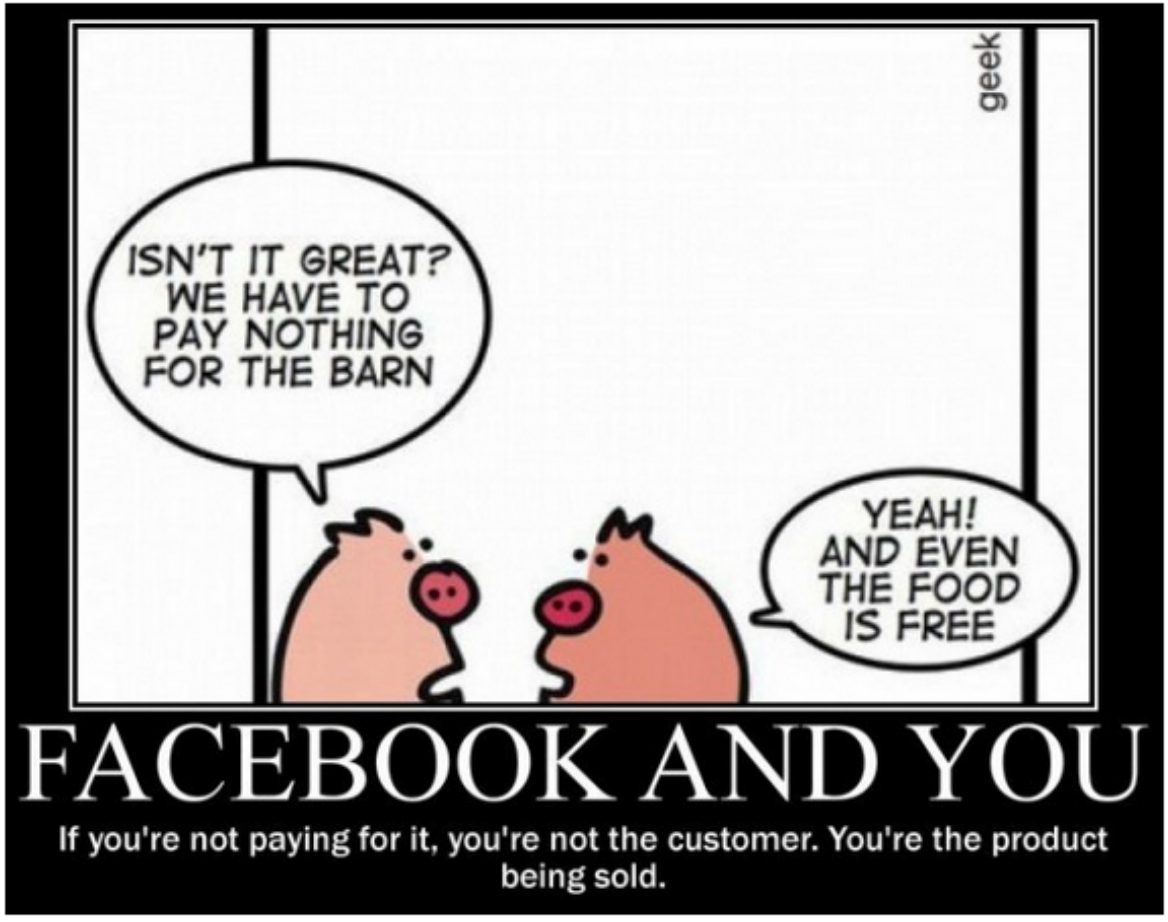
- Werbung

Geschäftsmodelle bei Zentralisierung

- Werbung
- Bezahldienst

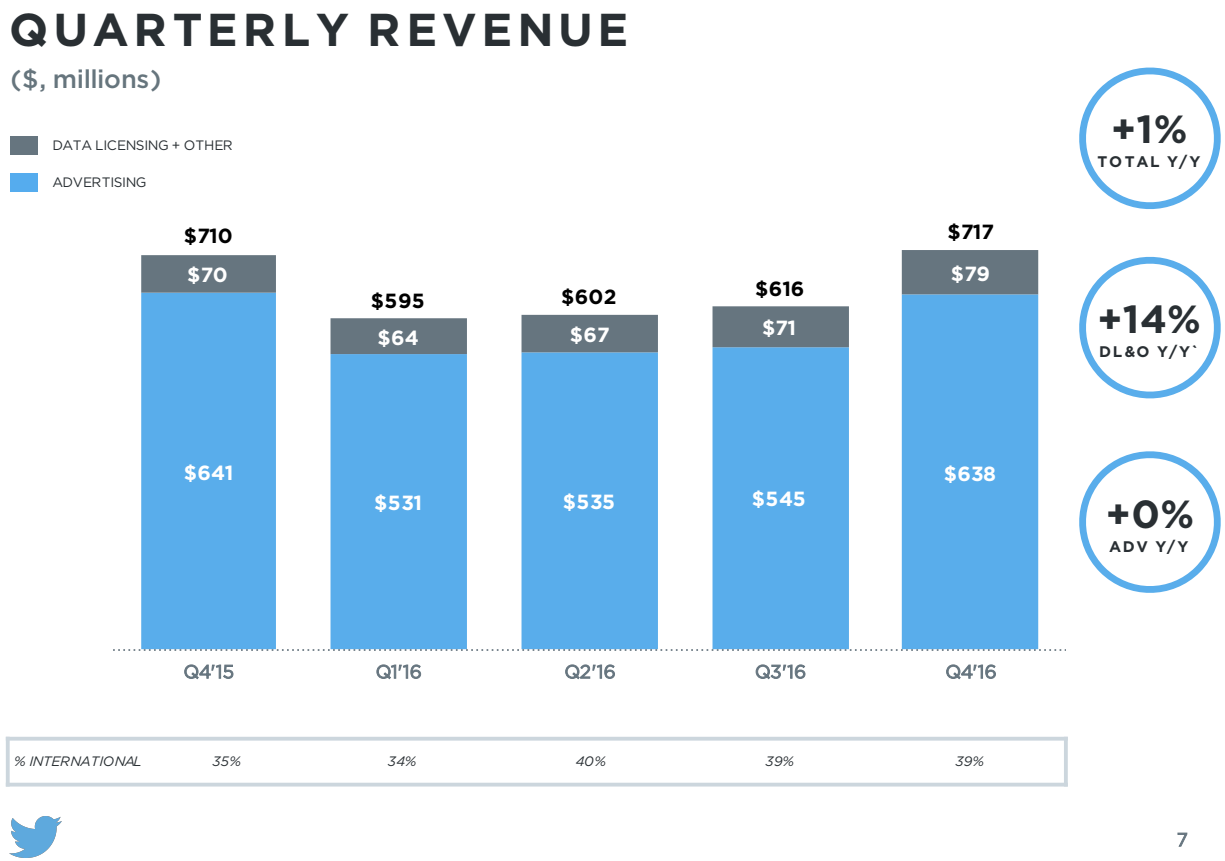
Geschäftsmodelle bei Zentralisierung

- Werbung
- Bezahldienst
- Datenlizensierung



Beispiel: Twitter

- Twitter Firehose was turned into a commercial "full take" API
- `https://gnip.com/`: Twitter subsidiary for Data Licensing[1]



[1] `http://mashable.com/2014/04/15/twitter-buys-gnip/`

Wer zahlt?

- Gnip partners with NetBase (and many others)[2]
- NetBase is funded by In-Q-Tel[3]
- In-Q-Tel was chartered by the CIA in 1999, presumably receiving hundreds of millions in funding over the years[4]

---

[2] http://www.destinationcrm.com/Articles/PrintArticle.aspx?ArticleID=86570

[3] https://en.wikipedia.org/wiki/In-Q-Tel

[4] http://www.washingtonpost.com/wp-dyn/content/article/2005/08/14/AR2005081401108.html

Beispiel: Pathar

From: `http://interc.pt/1XxSU1R`

Geschäftsmodelle bei Föderation

- Werbung

Geschäftsmodelle bei Föderation

- Werbung
- Bezahldienst

Geschäftsmodelle bei Föderation

- Werbung
- Bezahldienst
- Spenden

Geschäftsmodelle bei Dezentralisierung

- Spenden

Geschäftsmodelle bei Dezentralisierung

- Spenden
- Hardwareverkauf (`http://freedomboxfoundation.org/`)

Technologien für Zentralisierung

- HTTP, HTTPS
- Load balancing
- verteilte Datenbanken

Technologien für Föderation

- SMTP, XMPP
- PubSubHubbub

https://www.youtube.com/watch?v=B5kHx0rGkec (1'2010)

Technologien für Dezentralisierung und Datenschutz

- Verteilte Hash Tabellen (DHTs)
- GNU Name System
- **Secure Multiparty Computation (SMC)**

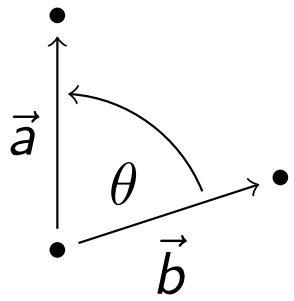
Technologien für Dezentralisierung und Datenschutz

- Verteilte Hash Tabellen (DHTs)
- GNU Name System
- **Secure Multiparty Computation (SMC)**
  - Alice und Bob haben private Daten a_i and b_i.
  - Alice und Bob führen ein Protokoll aus und berechnen gemeinsam $f(a_i, b_i)$.
  - Nur einer von beiden lernt das Ergebnis (i.d.R.)
  - Angreifermodel (i.d.R.): ehrlich, aber neugierig!

Beispiel: Skalarproduct

Motivation

- Scalarproduct $\Rightarrow$ Kosinus-Ähnlichkeit:



$$\vec{a} \cdot \vec{b} = ||\vec{a}|| \cdot ||\vec{b}|| \cos\theta \qquad (1)$$

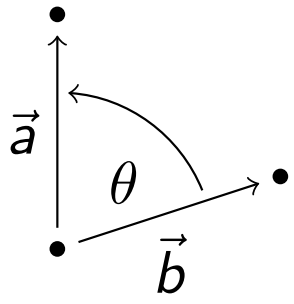
$$\Leftrightarrow \cos\theta = \frac{\vec{a} \cdot \vec{b}}{||\vec{a}|| \cdot ||\vec{b}||} \qquad (2)$$

- Nützlich für collaborative filtering!

Beispiel: Skalarproduct

Motivation

- Scalarproduct $\Rightarrow$ Kosinus-Ähnlichkeit:



$$\vec{a} \cdot \vec{b} = ||\vec{a}|| \cdot ||\vec{b}|| \cos\theta \qquad (1)$$

$$\Leftrightarrow \cos\theta = \frac{\vec{a} \cdot \vec{b}}{||\vec{a}|| \cdot ||\vec{b}||} \qquad (2)$$

- Nützlich für collaborative filtering!

Eigenschaften

- Private Eingangsdaten bleiben geschützt (aber Anzahl der Interaktionen muss begrenzt werden)
- Ausreichend effizient in Bandbreite und Rechenzeit

Das Protokoll[5]

Alice's public key ist $A = g^a$, ihr private key ist a. Alices schickt an Bob $(g_i, h_i) = (g^{r_i}, g^{r_i a + a_i})$ mit zufälligen Werten r_i für $i \in M$.
Bob antwortet mit

$$\left(\prod_{i\in M} g_i^{b_i}, \prod_{i\in M} h_i^{b_i}\right) = \left(\prod_{i\in M} g_i^{b_i}, (\prod_{i\in M} g_i^{b_i})^a g^{\sum_{i\in M} a_i b_i}\right)$$

Alice kann dann berechnen

$$\left(\prod_{i\in M} g_i^{b_i}\right)^{-a} \cdot \left(\prod_{i\in M} g_i^{b_i}\right)^{a} \cdot g^{\sum_{i\in M} a_i b_i} = g^{\sum_{i\in M} a_i b_i}.$$

Falls $\sum_{i\in M} a_i b_i$ ausreichend klein ist, kann Alice dann das Skalarprodukt durch Lösung des DLP bestimmen.

[5] Joint work with Tanja Lange

Vorläufige Auswertung

Länge	ECC-2^{20}	ECC-2^{28}
25	2 s	29 s
50	2 s	29 s
100	2 s	29 s
200	3 s	30 s

Die (Vor)berechnung für ECC-2^{28} ist $\times 16$ mal teurer als die für ECC-2^{20} da die Tabelle eine Grösse von $\sqrt{n}$ hat.

Zusammenfassung

- Kollaboratives Filtern ist zentrale Funktion sozialer Netzwerke
- Staaten nutzen soziale Netzwerke für mehr als “nur” Überwachung
- Kernfunktionen sozialer Netzwerke könnten datenschutzfreundlich bereitgestellt werden
- Betrieb und Entwicklung datenschutzfreundlicher Netzwerke erfordert technische und betriebswirtschaftliche Kreativität

Offene Fragen?

Literatur:

- Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System*. **13th International Conference on Cryptology and Network Security**, 2014.
- Geert Lovink and Miriam Rasch. *Unlike Us Reader: Social Media Monopolies and their Alternatives*. Institute of Network Cultures, 2013.
- John Naughton. *Death by drone strike, dished out by algorithm*, **The Guardian**, 21.2.2016.
- Lee Fang. *The CIA is investing in firms that mine your Tweets and Instagram photos*. **The Intercept**, 14.4.2016.

"Totalitarianism is man's escape from the fearful realities of life into the virtual womb of the leader. (...) The mystic center is in control of everything; man need no longer assume responsibility for his own life. The order and logic of the prenatal world reign. There is peace and silence, the peace of utter submission."
–Joost A. Merloo, Rape of the Mind (1956)