TECHNISCHE UNIVERSITÄT DRESDEN

PRIVACY AND SECURITY

Thorsten Strufe
Professur Privacy and IT Security

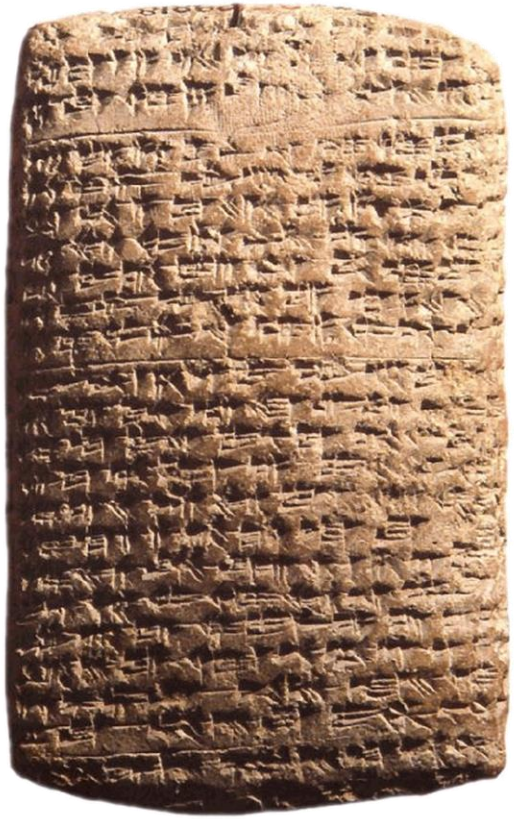
Forschungslinie 2019

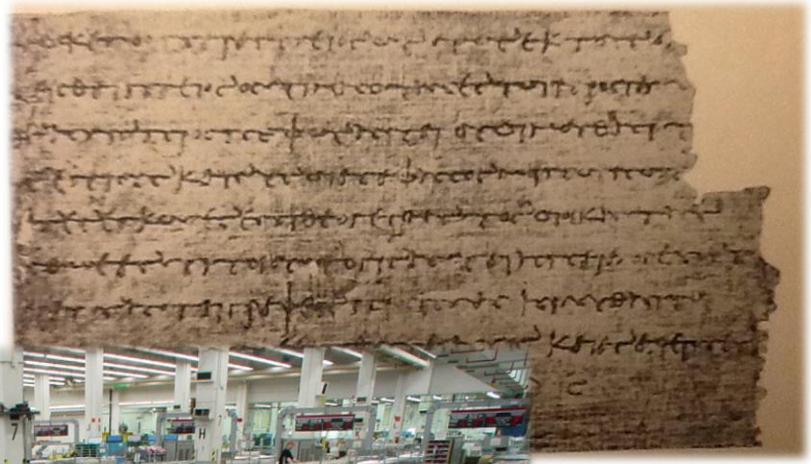
https://tud.de/inf/ps

Dresden, 06.05.2019

DRESDEN concept

Mail and Telecommunications

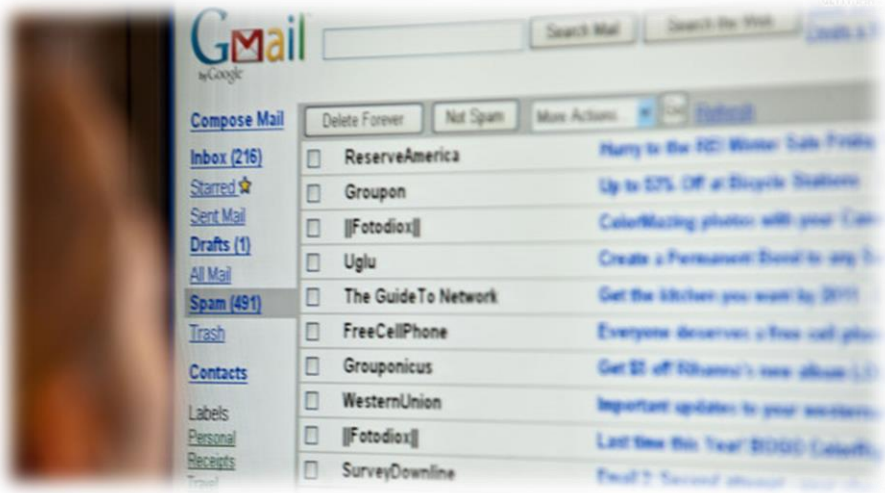




Information Acquisition

Access: Type and Scope

Welcome to the new Millenium!



Access: Type and Scope Today

1: Central service providers

2: Global access over the Internet

Konvergenz und Segmentierung

PRIVACY AND SECURITY

Web-Anfragen konvergieren auf die Seiten von 6 Firmen
- Erfolg basierend auf starker Personalisierung

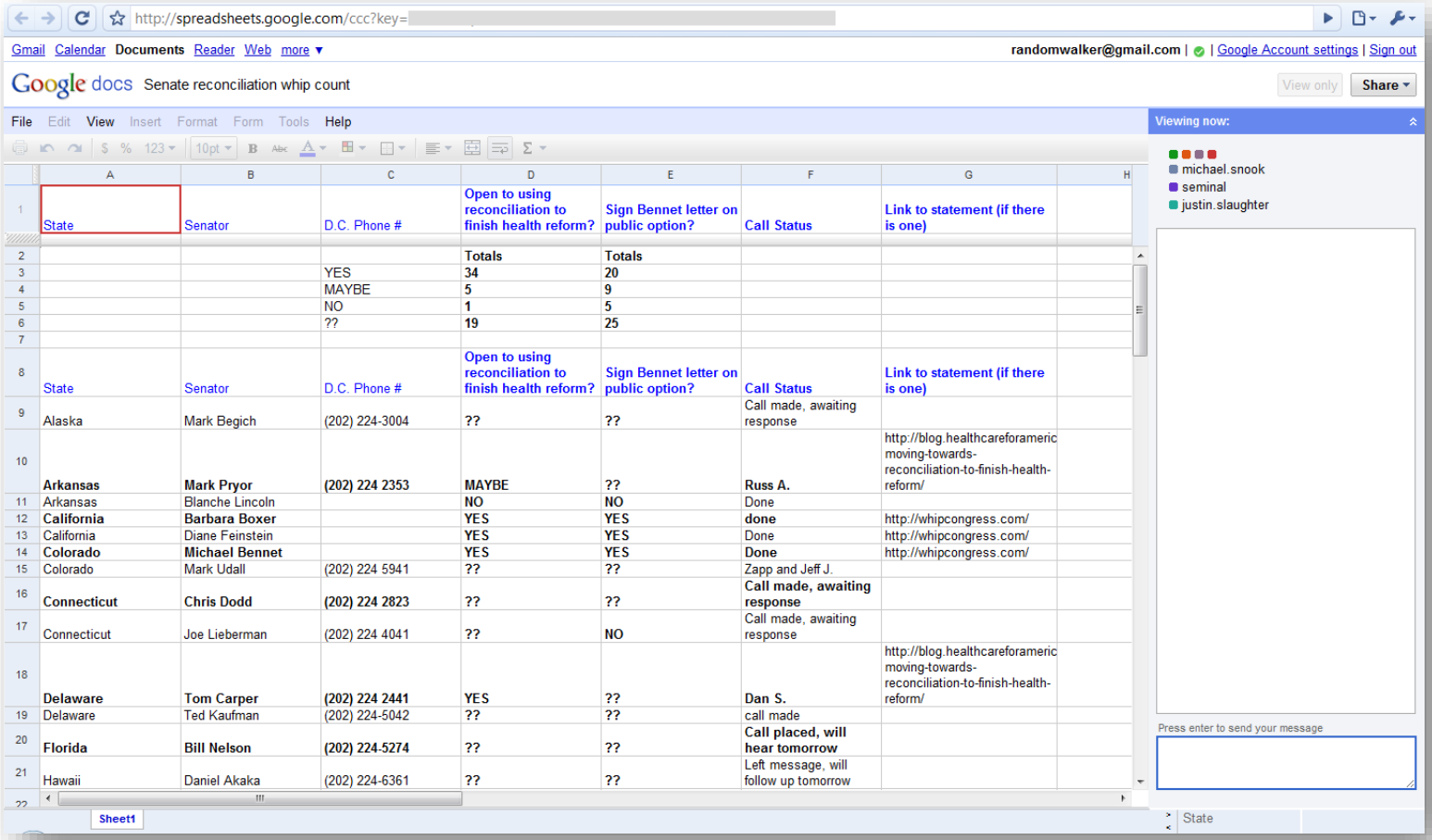
Meinungsbildung konvergiert auf große Anbieter
- Facebook: 1.94 Mrd Nutzer
- Twitter, Google+, reddit

Transparente Einbindung Dritter
- Hosting, Clouds
- Content Delivery Networks
- Analytics

Plattform-Gedanke
- Facebook Plattform
- Mobile Betriebssysteme

[Nielsen]
[Datanyze]

Beobacht- und Ableitbare Informationen



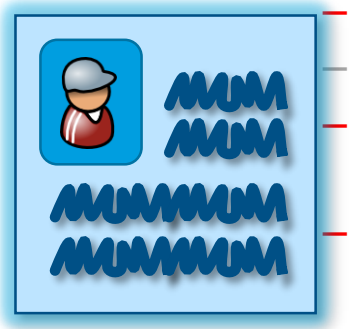
	A	B	C	D	E	F	G
1	State	Senator	D.C. Phone #	Open to using reconciliation to finish health reform?	Sign Bennet letter on public option?	Call Status	Link to statement (if there is one)
2				Totals	Totals		
3			YES	34	20		
4			MAYBE	5	9		
5			NO	1	5		
6			??	19	25		
7							
8	State	Senator	D.C. Phone #	Open to using reconciliation to finish health reform?	Sign Bennet letter on public option?	Call Status	Link to statement (if there is one)
9	Alaska	Mark Begich	(202) 224-3004	??	??	Call made, awaiting response	
10	**Arkansas**	**Mark Pryor**	**(202) 224 2353**	**MAYBE**	**??**	**Russ A.**	http://blog.healthcareforameric moving-towards-reconciliation-to-finish-health-reform/
11	Arkansas	Blanche Lincoln		NO	NO	Done	
12	**California**	**Barbara Boxer**		**YES**	**YES**	**done**	http://whipcongress.com/
13	California	Diane Feinstein		YES	YES	Done	http://whipcongress.com/
14	**Colorado**	**Michael Bennet**		**YES**	**YES**	**Done**	http://whipcongress.com/
15	Colorado	Mark Udall	(202) 224 5941	??	??	Zapp and Jeff J.	
16	**Connecticut**	**Chris Dodd**	**(202) 224 2823**	**??**	**??**	**Call made, awaiting response**	
17	Connecticut	Joe Lieberman	(202) 224 4041	??	NO	Call made, awaiting response	
18	**Delaware**	**Tom Carper**	**(202) 224 2441**	**YES**	**??**	**Dan S.**	http://blog.healthcareforameric moving-towards-reconciliation-to-finish-health-reform/
19	Delaware	Ted Kaufman	(202) 224-5042	??	??	call made	
20	**Florida**	**Bill Nelson**	**(202) 224-5274**	**??**	**??**	**Call placed, will hear tomorrow**	
21	Hawaii	Daniel Akaka	(202) 224-6361	??	??	Left message, will follow up tomorrow	

Beobachtbare und Ableitbare Informationen

PRIVACY AND SECURITY

Angegeben, explizit

- Erstellte Inhalte
- Kommentare
- Strukturelle Interaktion (Kontakte, +1)



Extrahiert

- Präferenz- und
- Gesichtserkennungsmodelle
- Private Details

Metadaten

- *Sitzungsartefakte*
- *Interessen* (besuchte Profile; Gruppen, Diskussionen)
- *Einfluss*
- Clickstreams, Werbe-Präferenz
- *Kommunikation* (Endpunkte, Art, Intensität, Frequenz, Ausmaß)
- *Ort* (IP; geteilt; GPS-Koordinaten)

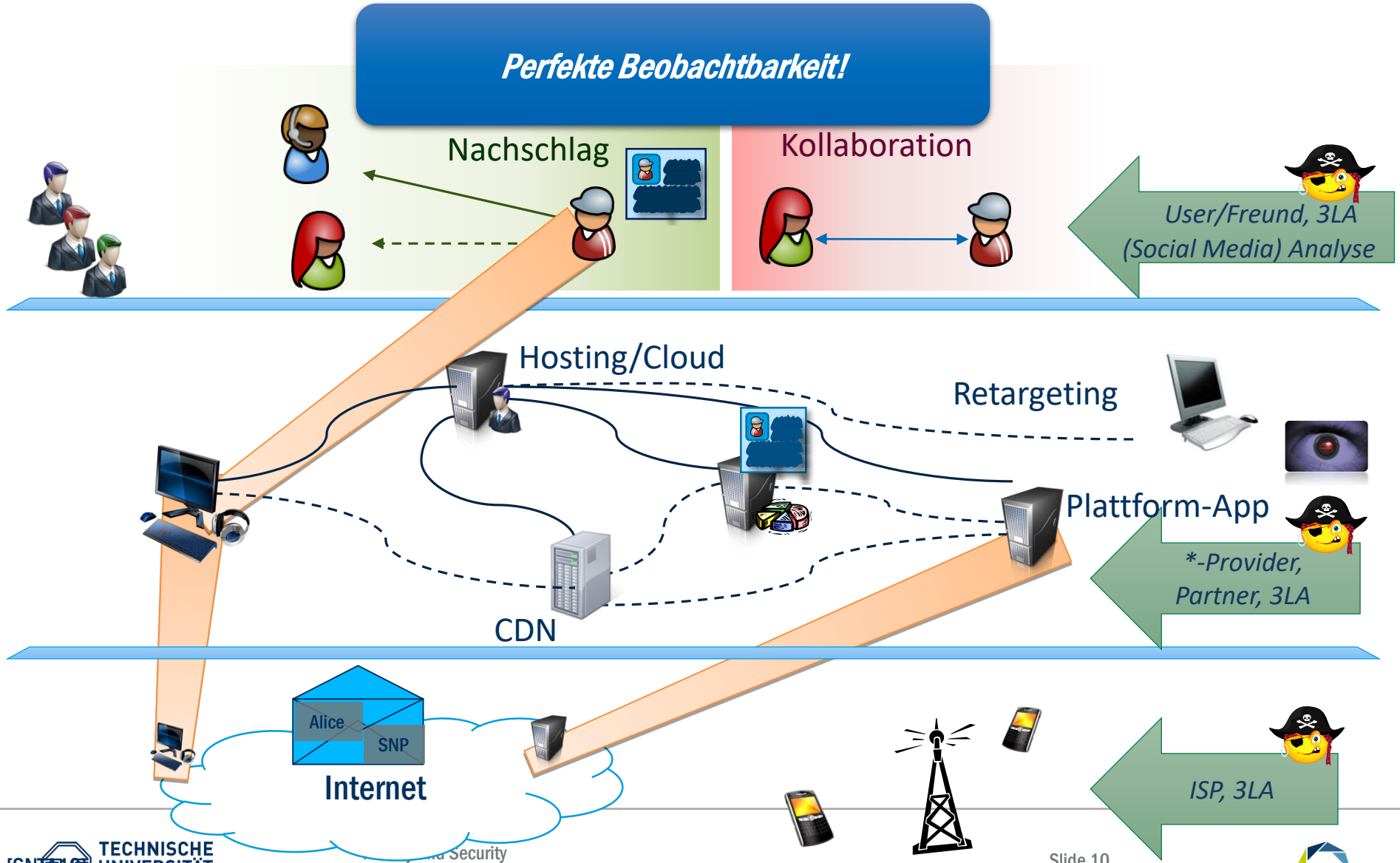
Extern

- Tracking in Werbe-Netzwerken

Soziodemographische Daten aus dem RUM umfassen Geschlecht, Alter, Einkommensgruppe, …,Wohnungsart, …, Bildungsgrad, …, Berufsart, Personenstand, Haushaltsgröße, …, [politische|Freizeit-] Interessen, …, persönlicher Besitz, …, Versicherungen, Investments,… [AGOF]

Einsortierung der Akteure und Datenabflüsse

PRIVACY AND SECURITY



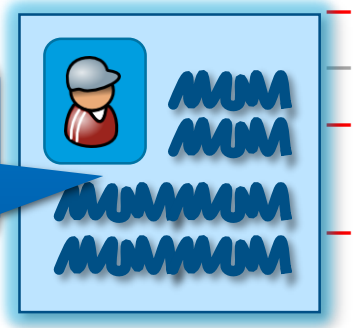
Beobachtbare und Ableitbare Informationen

PRIVACY AND SECURITY

Angegeben, explizit

- Erstellte Inhalte
- Kommentare
- Strukturelle Interaktion (Kontakte, +1)

Ich hab doch nichts zu verstecken!?



Extrahiert

- Präferenz- und
- Gesichtserkennungsmodelle
- Private Details

Metadaten

- ***Sitzungsartefakte***
- ***Interessen*** (besuchte Profile; Gruppen, Diskussionen)
- ***Einfluss***
- Clickstreams, Werbe-Präferenz
- ***Kommunikation*** (Endpunkte, Art, Intensität, Frequenz, Ausmaß)
- ***Ort*** (IP; geteilt; GPS-Koordinaten)

Extern

- Tracking in Werbe-Netzwerken

Soziodemographische Daten aus dem RUM umfassen Geschlecht, Alter, Einkommensgruppe, …,Wohnungsart, …, Bildungsgrad, …, Berufsart, Personenstand, Haushaltsgröße, …, [politische|Freizeit-] Interessen, …, persönlicher Besitz, …, Versicherungen, Investments,… [AGOF]

Beobacht- und Ableitbare Informationen

PRIVACY AND SECURITY

Angegeben, explizit

- Erstellte Inhalte
- Kommentare
- Strukturelle Interaktion (Kontakte, +1)

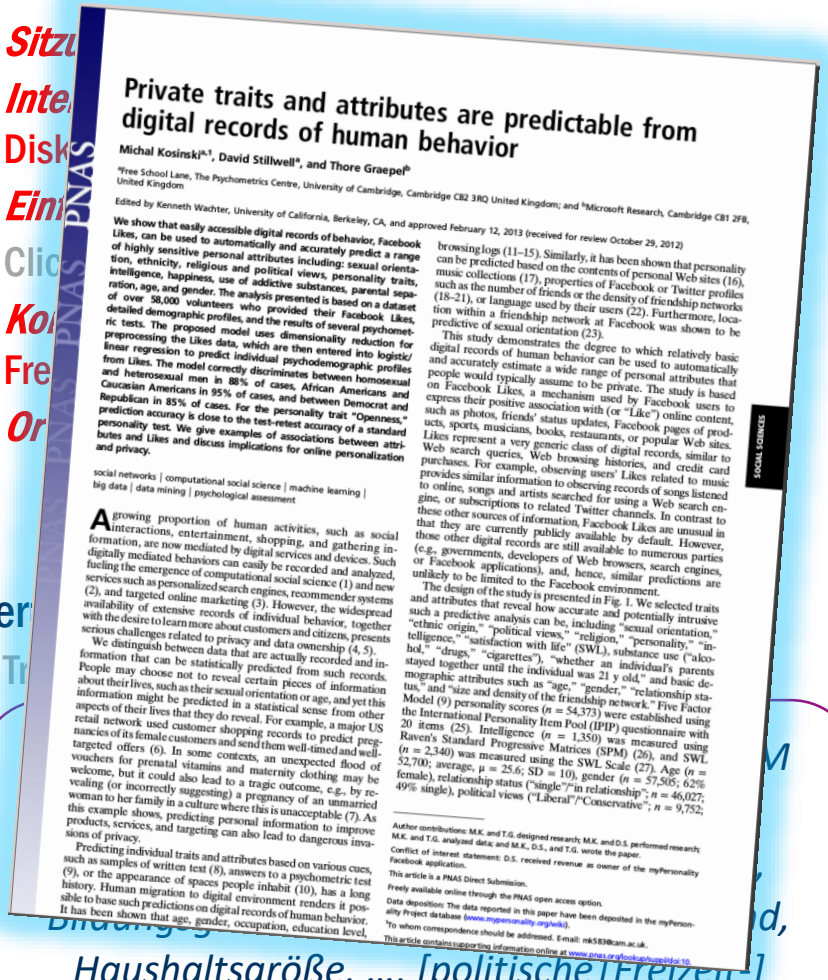
Ich hab doch nichts zu verstecken!?

Extrahiert

- Präferenz- und
- Gesichtserkennungsmodelle
- Private Details

Metadaten

- *Sitzu*
- *Inte*
- Disk
- *Eini*
- Clic
- *Koi*
- Fre
- *Or*



PNAS

SOCIAL SCIENCES

Private traits and attributes are predictable from digital records of human behavior

Michal Kosinski[a,1], David Stillwell[a], and Thore Graepel[b]

[a]Free School Lane, The Psychometrics Centre, University of Cambridge, Cambridge CB2 3RQ United Kingdom; and [b]Microsoft Research, Cambridge CB1 2FB, United Kingdom

Edited by Kenneth Wachter, University of California, Berkeley, CA, and approved February 12, 2013 (received for review October 29, 2012)

We show that easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. The analysis presented is based on a dataset of over 58,000 volunteers who provided their Facebook Likes, detailed demographic profiles, and the results of several psychometric tests. The proposed model uses dimensionality reduction for preprocessing the Likes data, which are then entered into logistic/linear regression to predict individual psychodemographic profiles from Likes. The model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases. For the personality trait "Openness," prediction accuracy is close to the test-retest accuracy of a standard personality test. We give examples of associations between attributes and Likes and discuss implications for online personalization and privacy.

social networks | computational social science | machine learning | big data | data mining | psychological assessment

A growing proportion of human activities, such as social interactions, entertainment, shopping, and gathering information, are now mediated by digital services and devices. Such digitally mediated behaviors can easily be recorded and analyzed, fueling the emergence of computational social science (1) and new services such as personalized search engines, recommender systems (2), and targeted online marketing (3). However, the widespread availability of extensive records of individual behavior, together with the desire to learn more about customers and citizens, presents serious challenges related to privacy and data ownership (4, 5).

We distinguish between data that are actually recorded and information that can be statistically predicted from such records. People may choose not to reveal certain pieces of information about their lives, such as their sexual orientation or age, and yet this information might be predicted in a statistical sense from other aspects of their lives that they do reveal. For example, a major US retail network used customer shopping records to predict pregnancies of its female customers and send them well-timed and well-targeted offers (6). In some contexts, an unexpected flood of vouchers for prenatal vitamins and maternity clothing may be welcome, but it could also lead to a tragic outcome, e.g., by revealing (or incorrectly suggesting) a pregnancy of an unmarried woman to her family in a culture where this is unacceptable (7). As this example shows, predicting personal information to improve products, services, and targeting can also lead to dangerous invasions of privacy.

Predicting individual traits and attributes based on various cues, such as samples of written text (8), answers to a psychometric test (9), or the appearance of spaces people inhabit (10), has a long history. Human migration to digital environment renders it possible to base such predictions on digital records of human behavior. It has been shown that age, gender, occupation, education level, browsing logs (11–15). Similarly, it has been shown that personality can be predicted based on the contents of personal Web sites (16), music collections (17), properties of Facebook or Twitter profiles such as the number of friends or the density of friendship networks (18–21), or language used by their users (22). Furthermore, location within a friendship network at Facebook was shown to be predictive of sexual orientation (23).

This study demonstrates the degree to which relatively basic digital records of human behavior can be used to automatically and accurately estimate a wide range of personal attributes that people would typically assume to be private. The study is based on Facebook Likes, a mechanism used by Facebook users to express their positive association with (or "Like") online content, such as photos, friends' status updates, Facebook pages of products, sports, musicians, books, restaurants, or popular Web sites. Likes represent a very generic class of digital records, similar to Web search queries, Web browsing histories, and credit card purchases. For example, observing users' Likes related to music provides similar information to observing records of songs listened to online, songs and artists searched for using a Web search engine, or subscriptions to related Twitter channels. In contrast to these other sources of information, Facebook Likes are unusual in that they are currently publicly available by default. However, those other digital records are still available to numerous parties (e.g., governments, developers of Web browsers, search engines, or Facebook applications), and, hence, similar predictions are unlikely to be limited to the Facebook environment.

The design of the study is presented in Fig. 1. We selected traits and attributes that reveal how accurate and potentially intrusive such a predictive analysis can be, including "sexual orientation," "ethnic origin," "political views," "religion," "personality," "intelligence," "satisfaction with life" (SWL), substance use ("alcohol," "drugs," "cigarettes"), "whether an individual's parents stayed together until the individual was 21 y old," and basic demographic attributes such as "age," "gender," "relationship status," and "size and density of the friendship network." Five Factor Model (9) personality scores (n = 54,373) were established using the International Personality Item Pool (IPIP) questionnaire with 20 items (25). Intelligence (n = 1,350) was measured using Raven's Standard Progressive Matrices (SPM) (26), and SWL (n = 2,340) was measured using the SWL Scale (27). Age (n = 52,700; average, μ = 25.6; SD = 10), gender (n = 57,505; 62% female), relationship status ("single"/"in relationship"; n = 46,027; 49% single), political views ("Liberal"/"Conservative"; n = 9,752;

Author contributions: M.K. and T.G. designed research; M.K. and D.S. performed research; M.K. and T.G. analyzed data; and M.K., D.S., and T.G. wrote the paper.

Conflict of interest statement: D.S. received revenue as owner of the myPersonality Facebook application.

This article is a PNAS Direct Submission.

Freely available online through the PNAS open access option.

Data deposition: The data reported in this paper have been deposited in the myPersonality Project database (www.mypersonality.org/wiki).

[1]To whom correspondence should be addressed. E-mail: mk583@cam.ac.uk.

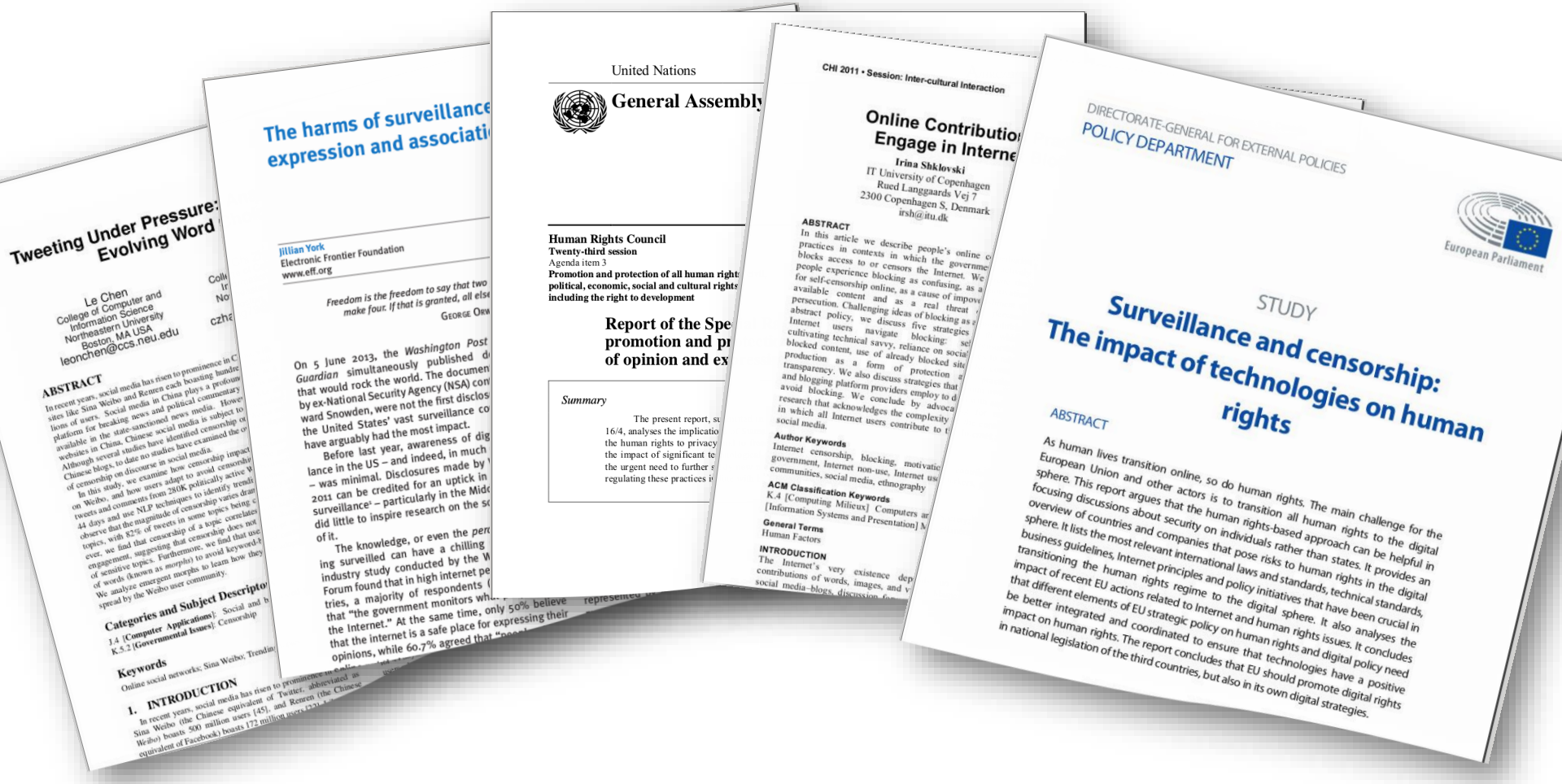
This article contains supporting information online at www.pnas.org/lookup/suppl/doi:10.

Bildungsg… d,

Haushaltsgröße, …, [politische|Freizeit-] Interessen, …, persönlicher Besitz, …, Versicherungen, Investments,… [AGOF]

Der Einfluss von Überwachung und Zensur

PRIVACY AND SECURITY



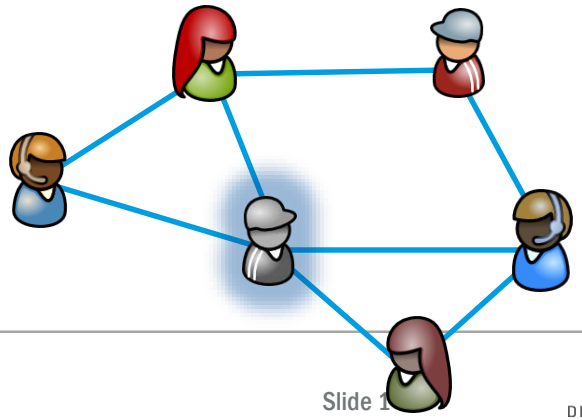
„Es sind ja nur Meta-Daten“

„Facebook Mining“ Angriffe

Vorlesung 5/7 Semester (Studenten ohne ML-Erfahrung)

Eingabedaten:
- Teilprofile
- Nachbarschaft

Mit hoher Genauigkeit inferiert:
- Geschlecht
- Alter
- Bildungsstand
- Arbeitgeber-Treue
- Sexuelle Präferenzen
- Politische Einstellungen



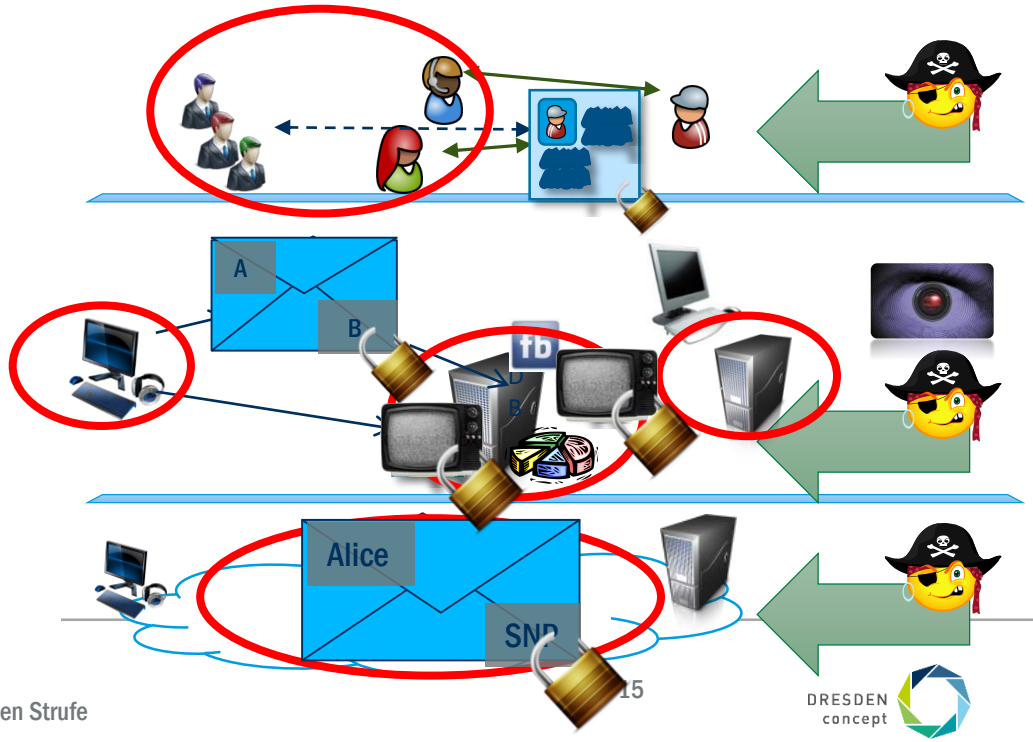
Lösungsklassen und Beiträge des Lehrstuhls

ROSI

DNA

DYNAMIC NETWORK ANALYZER

- zur Verständ
  ions-Erken



IT-Sicherheit

PRIVACY AND SECURITY

Die Aufgabe der IT-Sicherheit:

Reduktion operationeller Risiken von IT-Systemen

- Modellierung von System und Umwelt
- Erhebung und Spezifikation von Sicherheitsanforderungen
- Bedrohungsanalysen
- Risiko-Einschätzungen
- Design, Konstruktion und Umsetzung von Schutzmechanismen

Interlude: Safety und Security

PRIVACY AND SECURITY

(Funktions-)Sicherheit (*safety*)

Ziel: Schutz vor Schäden durch Fehlfunktionen

- technisches Versagen; Alterung, Stromausfall, Schmutz
- menschliches Versagen; Dummheit, mangelnde Ausbildung, Fahrlässigkeit
- höhere Gewalt; Feuer, Blitzschlag, Erdbeben

→ Fehlerminimierung: Zuverlässigkeit, Testen

(IT-)Sicherheit (*security*)

Ziel: Schutz vor Schäden durch ***zielgerichtete Angriffe*** auf IT-Systeme

- Social-Engineering, Erpressung, Wirtschaftsspionage, Überwachung…
- Terrorismus, Vandalismus

→ Schutz <u>eines</u> IT-Systems, seiner Daten und Benutzer

Was ist eine Bedrohung?

PRIVACY AND SECURITY

Abstrakte Definition:

- Bedrohungen sind mögliche *Ereignisse*, oder Reihungen von Ereignissen und Aktionen, die zu einer *Verletzung eines oder mehrerer Sicherheitsziele* führt
- Eine Instanziierung einer Bedrohung ist ein ***Angriff***

Beispiel:

- Ein Hacker bricht in einen Firmencomputer ein
- Mutwillige Manipulation von Bankdaten
- Sabotage und temporäre Abschalten einer Webseite
- Nutzung von Diensten im Namen einer anderen Partei
- Die Deutsche Post “findet heraus” (und verkauft) dass in Ihrem Haus nur AfD-Wähler mit einem Einkommen <25k p.a. leben

Also was sind Sicherheitsziele?

Etwas formaler: Ziele der IT Sicherheit

PRIVACY AND SECURITY

Vertraulichkeit (Confidentiality)
- Übertragene und gespeicherte Daten dürfen nur legitimierten Empfängern zugänglich sein
- Vertraulichkeit der Identität wird als Anonymität bezeichnet

Integrität (Integrity)
- Veränderungen an Daten müssen detektiert werden
- (Bedarf der Identifikation des Absenders!)

Verfügbarkeit (Availability)
- Informationen und Dienste sollen berechtigten Nutzern in angemessener Frist zugänglich sein

Zurechenbarkeit (Accountability)
- Die verantwortliche Partei für eine Operation soll identifizierbar sein

Kontrollierter Zugriff (Controlled Access)
- Nur authorisierte Parteien sollen in der Lage sein, auf Dienste oder Informationen zuzugreifen

Und was war das mit Datenschutz?

PRIVACY AND SECURITY

Sicherheit schützt Daten (und Services/Systeme)

Privacy ist der Schutz von Individuen ***vor*** Daten

- Kontrolle über Benutzung der Daten durch andere (Institutionen)
- Geben und entziehen von Einwilligung zur Nutzung
- Setzt voraus:
  - Transparenz von Datensammlung und -verarbeitung
  - … mögliche Auswirkungen (***informierte*** Einwilligung)
  - Datenminimierung *(hilft auch für die Sicherheit!)*

In related news: 25. 5. 2018 -> EU-DSGVO!

Bedrohungspotenziale – Angreifermodell

PRIVACY AND SECURITY

Kein Schutz vor einem allmächtigen Angreifer!

Ein allmächtiger Angreifer …

- kann alle ihn interessierenden Daten erfassen
- kann Daten unbemerkt ändern
- kann die Verfügbarkeit des Systems durch physische Zerstörung beeinträchtigen

→ Angreifermodell

- Intention und Rolle des Angreifers
- Verhalten des Angreifers
- Verbreitung des Angreifers
- Fähigkeiten und Kapazität des Angreifers

Research Clusters

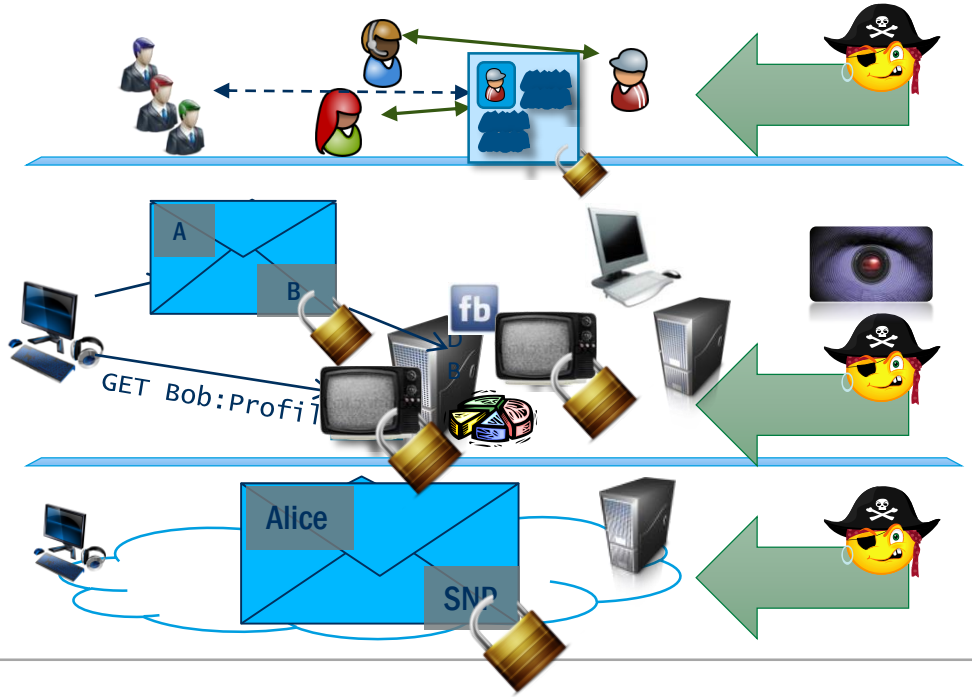
PRIVACY AND SECURITY

- ***Network Security***
  - Protected transmission
  - SDN/(N)FV Security
  - Reactive Security

- ***Privacy Enhancing Tech***
  - Anonymous services (F2F)
  - Network anonymisation

- ***Service Protection***
  - Private Measurement & Analytics
  - Private anomaly detection
  - Trusted Execution

- ***User Understanding***
  - Intention recognition
  - Bot/campaign detection
  - User support



Cluster PETs

PRIVACY AND SECURITY

Goals

- Freedom of speech
- Censorship resistance
- Privacy despite 3-letter agencies

Approaches

- Decentralized service provision
  - Distributed Social Networking
  - Darknets
- Network layer anonymization

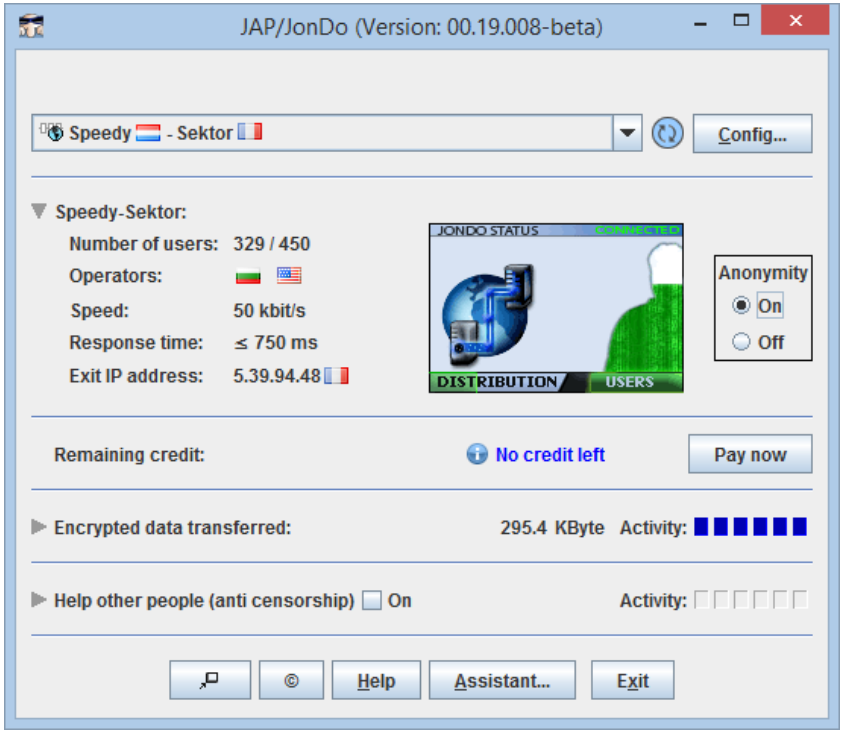
[Hotsocial12]

The AN.ON Project – ANonymity.ONline since 2000

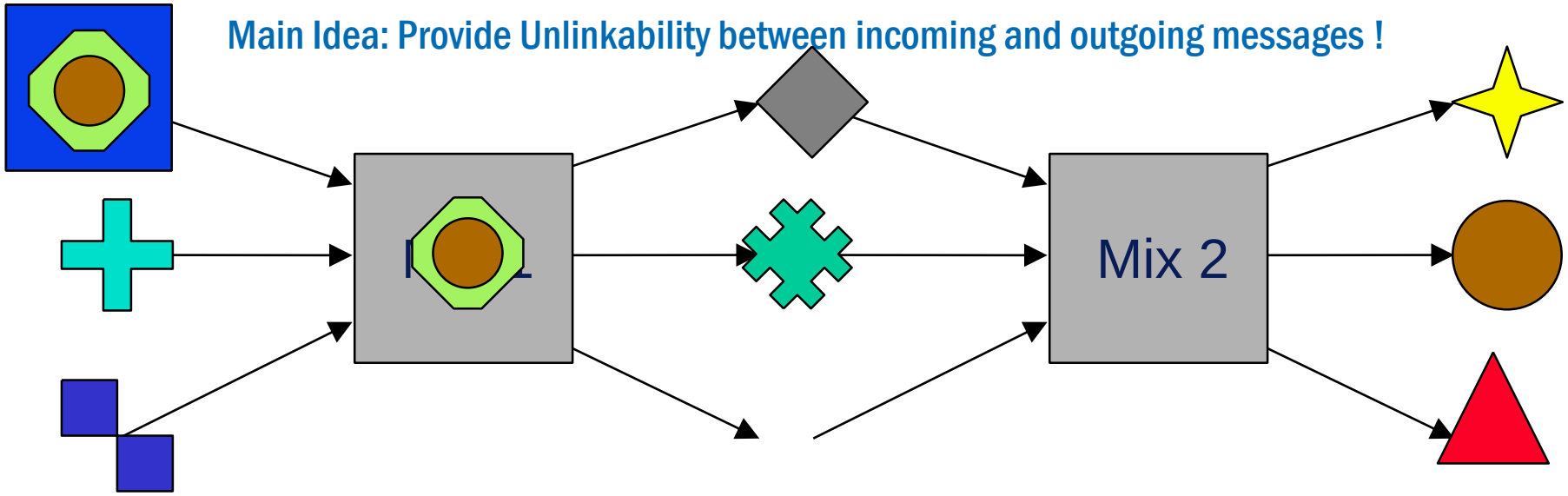
PRIVACY AND SECURITY

Network Layer Anonymization:

- long track record in the area of "anonymous and unobservable communication"
- holistic view: consideration of complex requirements (law enforcement, censorship resistance, etc.)
- since 2001 practical realisation within the project "AN.ON"
- implementation and operation of a anonymisation service based on Mixes



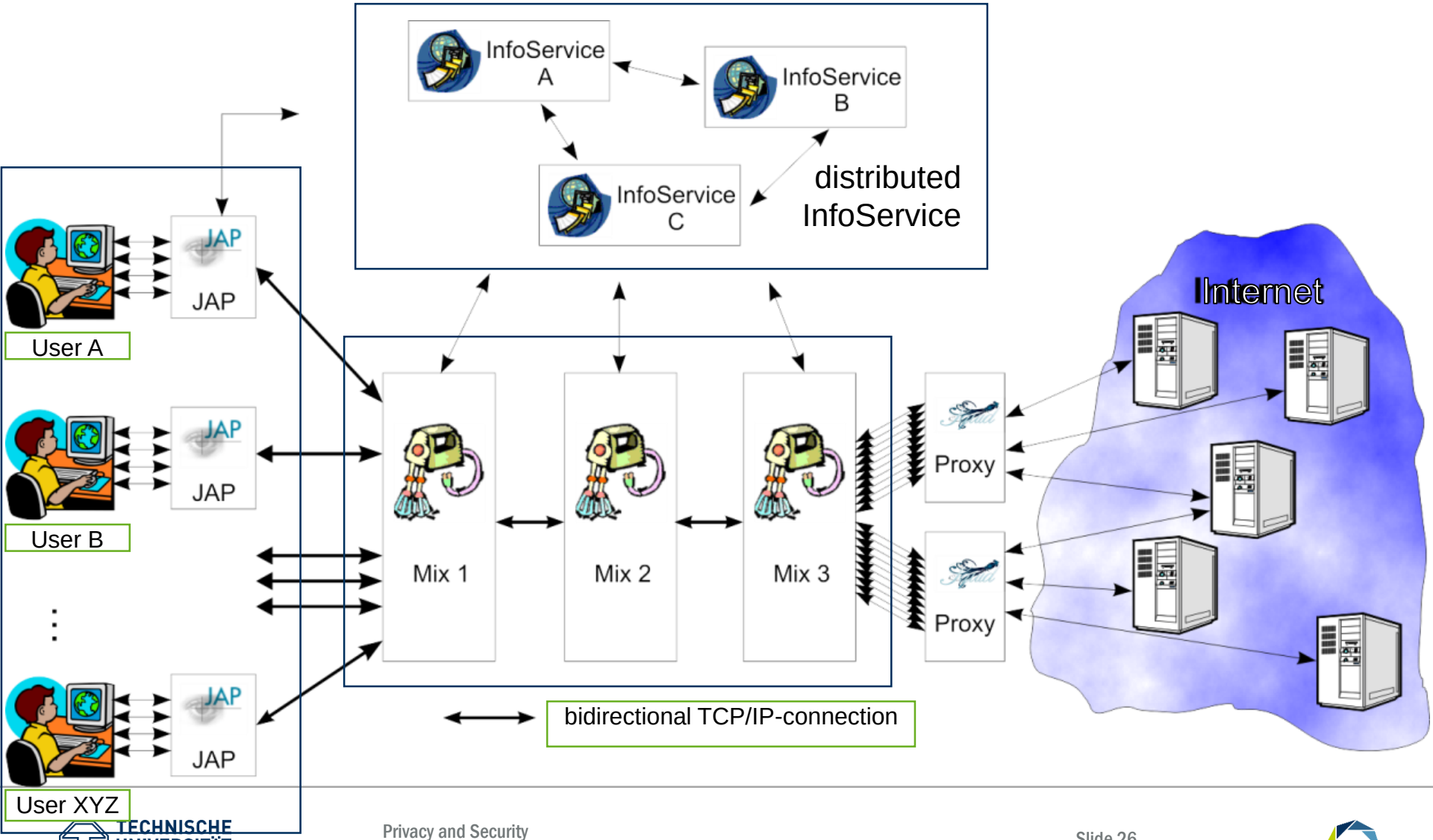
The Mix-technique



A Mix samples messages in a batch, changes their coding and forwards them in a different order.

Only if all Mixes work together they can deanonymise a communication relation

Overview of the AN.ON system



Research Clusters

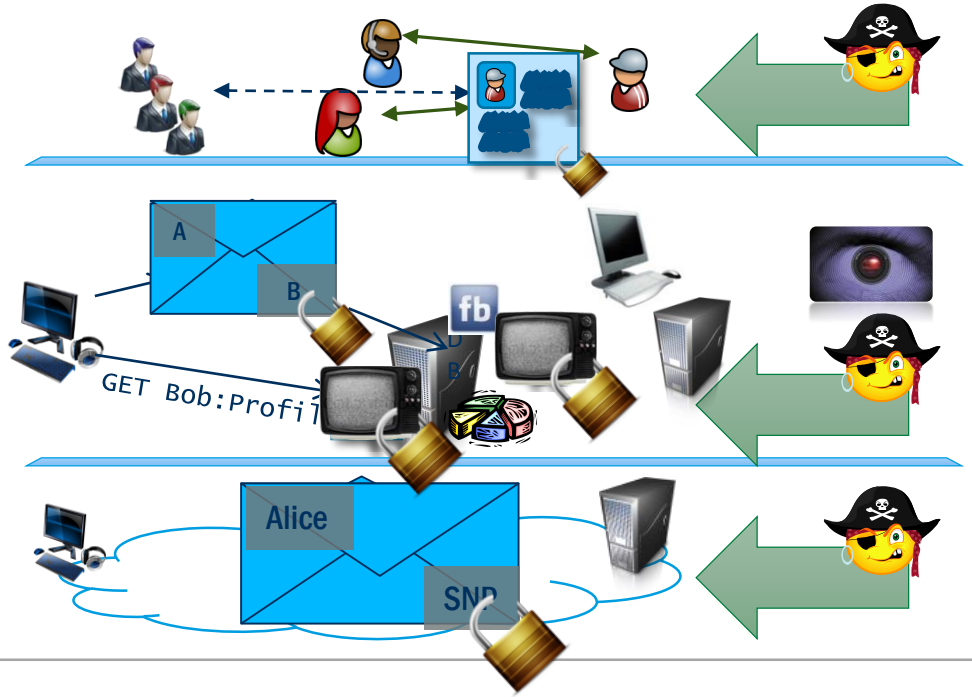
PRIVACY AND SECURITY

- ***Network Security***
  - Protected transmission
  - SDN/(N)FV Security
  - Reactive Security

- ***Privacy Enhancing Tech***
  - Anonymous services (F2F)
  - Network anonymisation

- ***Service Protection***
  - Private Measurement & Analytics
  - Private anomaly detection
  - Trusted Execution

- ***User Understanding***
  - Intention recognition
  - Bot/campaign detection
  - User support



PETs: Verteilung von Daten und Kontrolle

Dezentralisierung der Dienste

Federated SNS

diaspora*

DOSN

Frankfurter Allgemeine
ZEITUNG FÜR DEUTSCHLAND

Deutscher Bundestag

Social overlays/F2F

TED
IDEASWORTHSPREADING

[ICC14]
[Comm.Mag]
[INFOCOM13]

[INFOCOM15]
[INFOCOM16]
[INFOCOM17]

Resilient Social Overlays

Prevent identification, censorship and retribution.

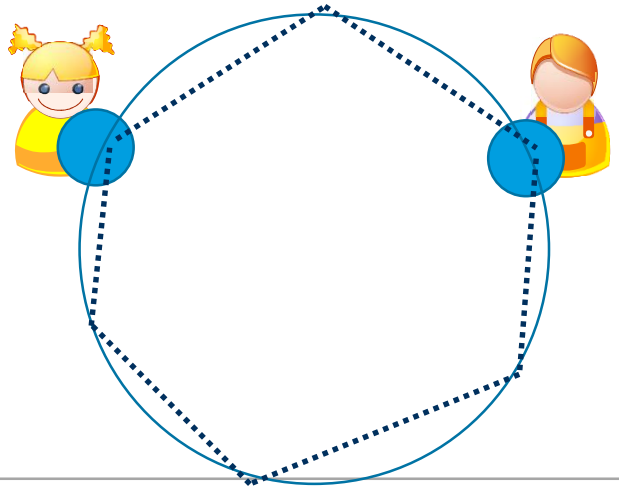
From DOSN to darknets: Tightening requirements

- Concealed participation
- Unobserveability
- Metadata privacy (sender-, receiver-, relationship anonymity)

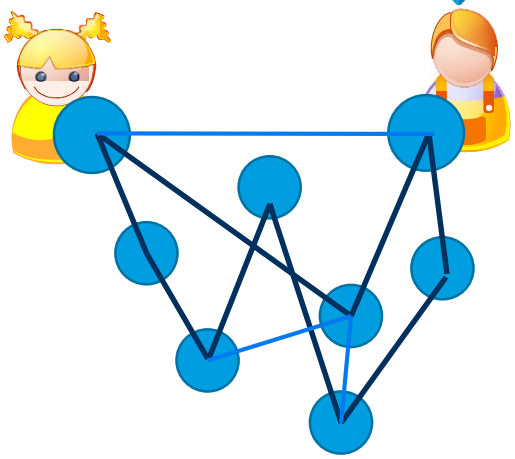
So where‘s the problem?

Classic overlays:

- Disclosure of IP address
- Eclipse, X-hole attacks



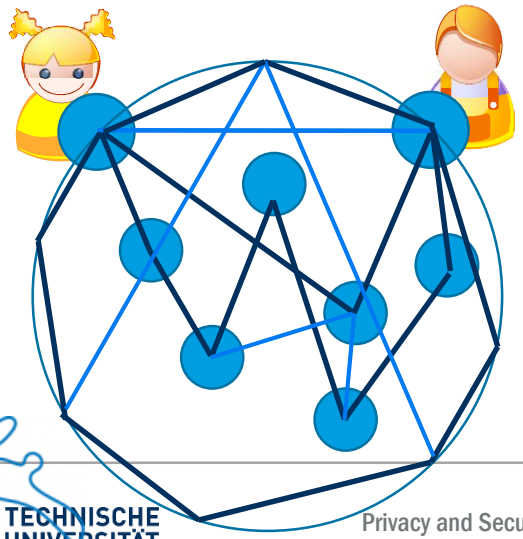
Social Overlays: Embedding/Virtual Overlays



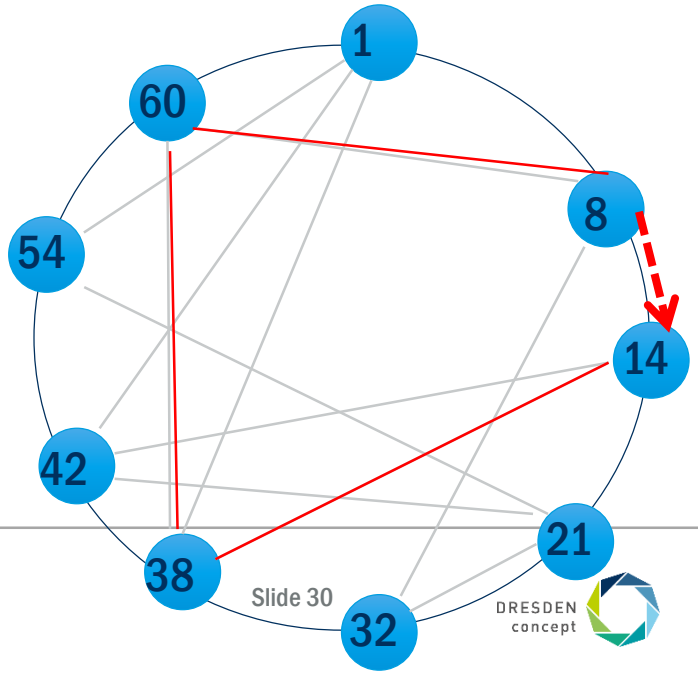
Concepts of social overlays:

- Constrain connectivity to social links
- Contain information
- Attempt to route messages

Embeddings



Virtual overlays



Trust graph
Virtual Link
Tunnel 8-14

Virtual Overlays – Tunnel Maintenance

PRIVACY AND SECURITY

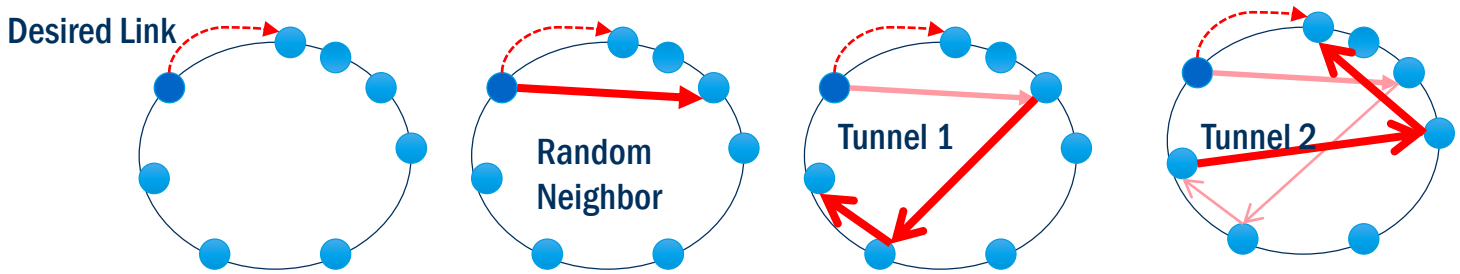
Establishment & Maintenance of tunnels („trails“)

– Flooding

- Finds shortest paths, is *excessively* expensive

– Routing

- Leverage overlay routing to trail endpoint
- Concatenate existing tunnels



[1] Roos and Strufe: INFOCOM 2015

Can Virtual Overlays be Cost-Efficient (Polylog)?

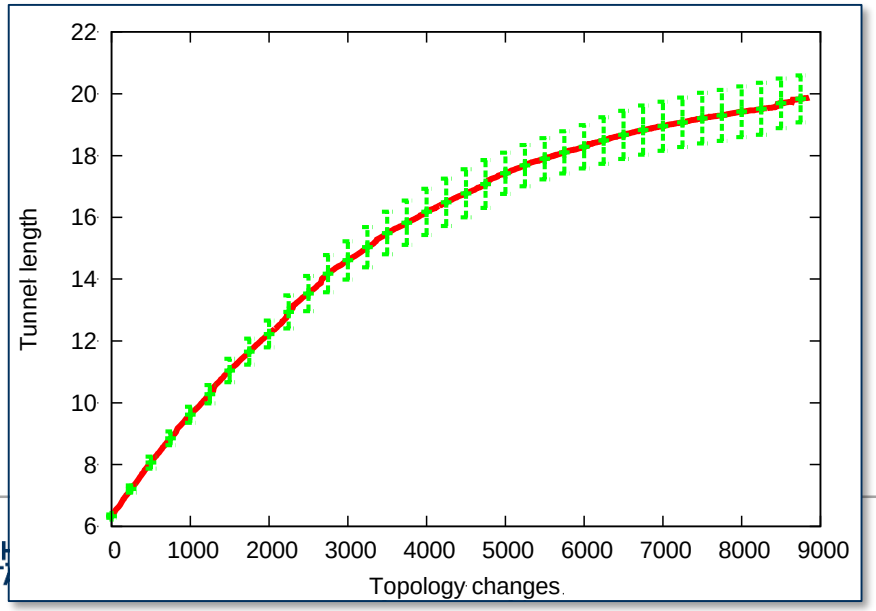
PRIVACY AND SECURITY

Flooding: no-brainer

Concatenation of trails: Proof by contradiction

1. Model dynamic virtual overlays as a stochastic process
2. Assume polylog stabilization
3. Show tunnel length increases beyond polylog

→ *New trail is longer than removed trail with high probability*



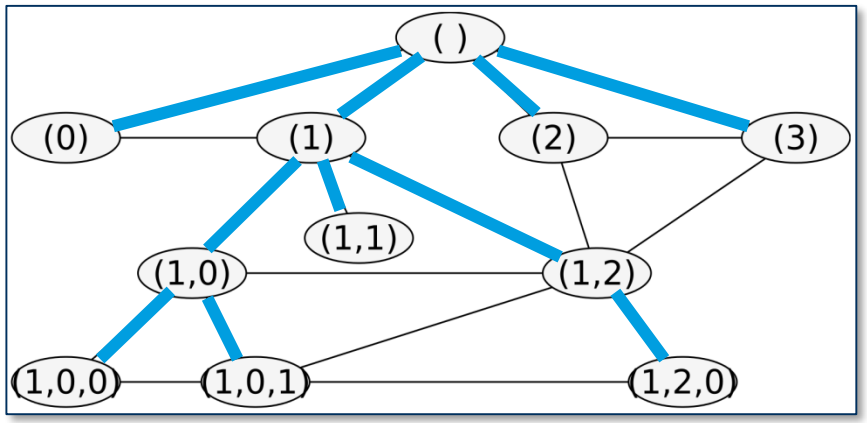
[1] Roos and Strufe: INFOCOM 2015
[2] Roos et al.: PETS 2014

Enhancing Freenet's Embedding

Distortion extends paths

Aim: *greedy embedding*

Trees can be embedded



PIE tree embedding

1. Find spanning tree
2. Enumerate children

Challenges:

- Tree addresses
  - Leak neighborhood
  - Addresses leak receiver
- Attacks on tree construction

Distance metric:

$$d(s,t) := |s| + |t| - 2cpl(s,t)$$

[KiVS13]

Recovering Sender and Receiver Anonymity

PRIVACY AND SECURITY

Receiver anonymity

- (Return) address needed
- Distance: longest prefix match

- Blinded addresses:
  1. Randomize:
     $[1,2,0] \rightarrow [r_1,r_2,r_3]$
  2. Padding
     $[r_1,r_2,r_3] \rightarrow [r_1,r_2,r_3, r_{k+1}, \ldots ,r_L]$
  3. Blinding
     $k, [r_1,..,r_L] \rightarrow (k,[h(r_1 \oplus k),h(r_2 \oplus h(r_1 \oplus k)...])$

- Distance metrics:

$$d_1(s,t) := |s|+|t|-2cpl(s,t)$$
$$d_2(s,t) := L - cpl(s,t) - \delta$$

Theoretical analysis

Performance Bounds

- Tree routing O(log n)
- Tree maintenance O(log n)
  per join/leave

Security Analysis

- Plausible deniability: Receiver cannot uniquely be identified
- Minimal information loss to allow for routing

[1] Roos, Beck, and Strufe: INFOCOM 2016

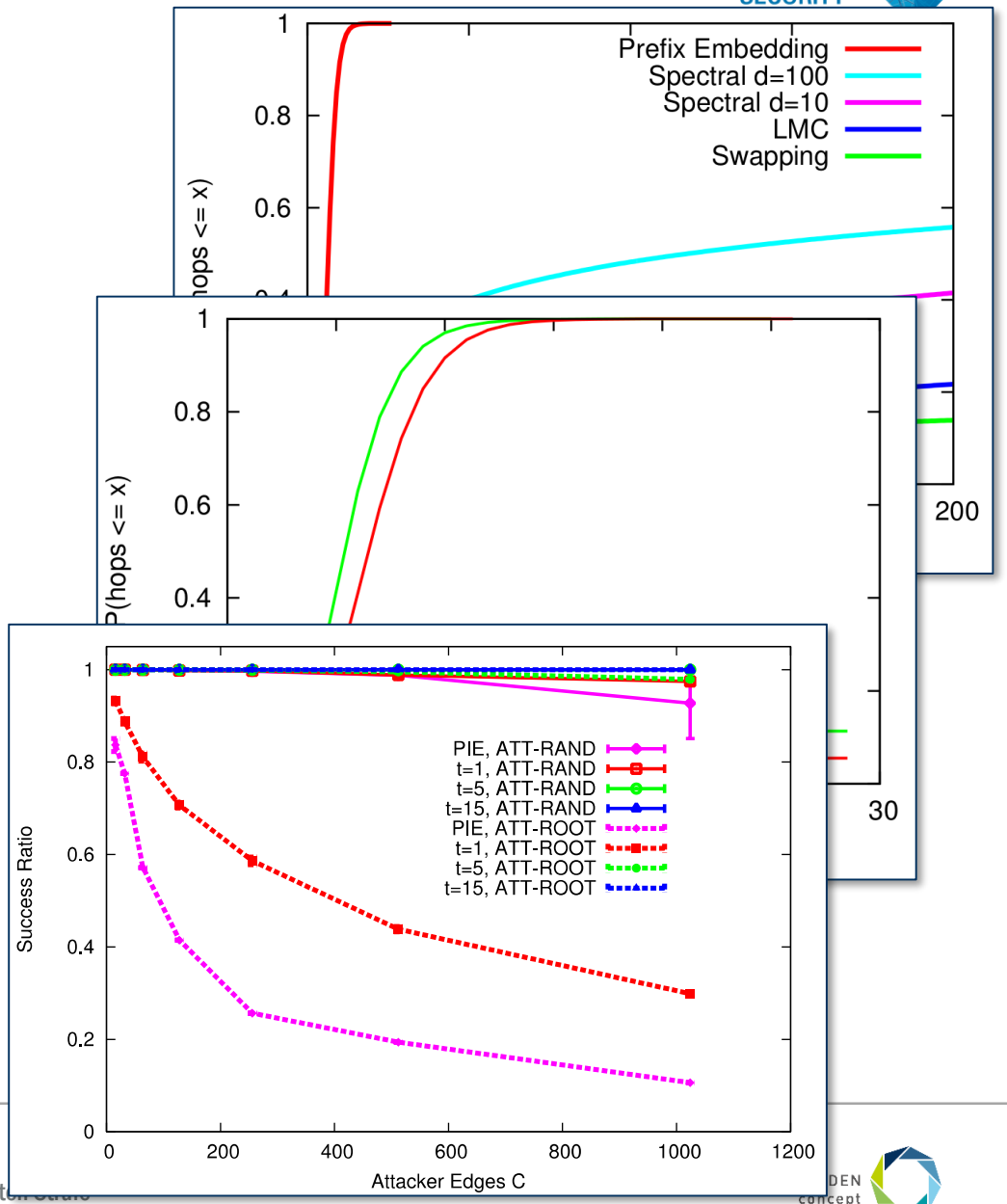
Performance Evaluation

TE is a greedy embedding

Simulation Experiment
- Topology: PGP Web of Trust
- Embeddings: Freenet/RW
- Routing: DDFS/Greedy

Is it robust?

Summary:
- *It's robust and fast!*



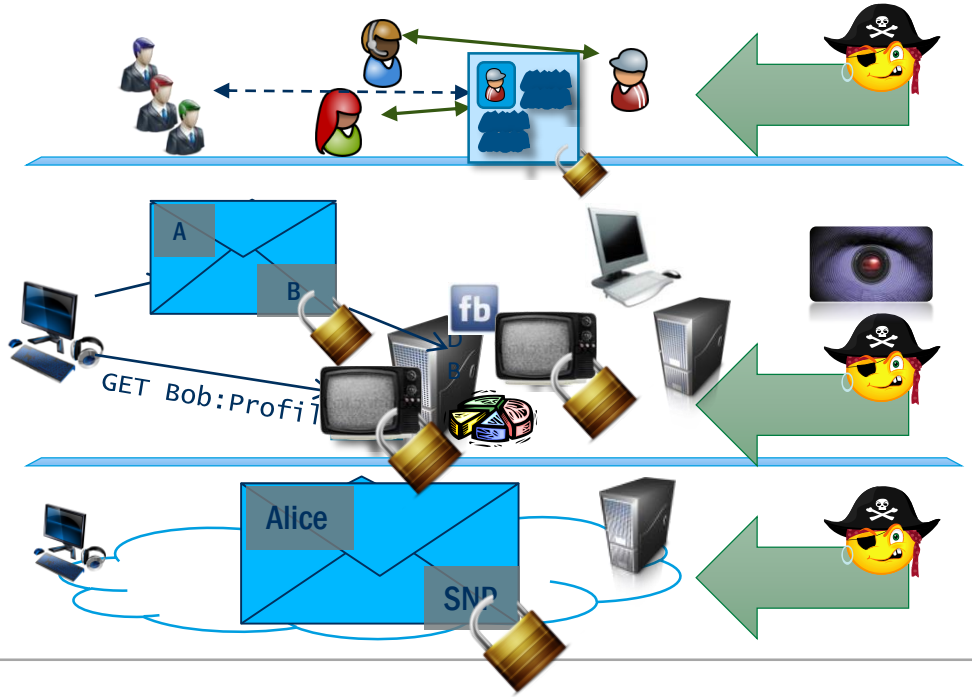
Research Clusters

- ***Network Security***
  - Protected transmission
  - SDN/(N)FV Security
  - Reactive Security

- ***Privacy Enhancing Tech***
  - Anonymous services (F2F)
  - Network anonymisation

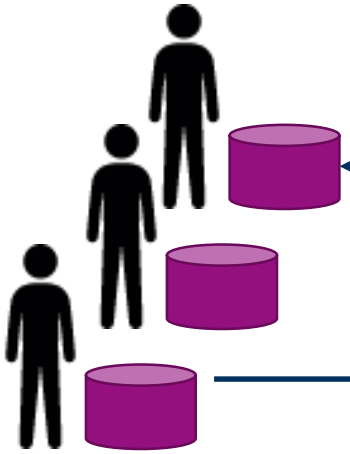
- ***Service Protection***
  - Private Measurement & Analytics
  - Private anomaly detection
  - Trusted Execution

- ***User Understanding***
  - Intention recognition
  - Bot/campaign detection
  - User support



PrivApprox: Stream-Analytics mit Privacy

Wie passen Utility und Privacy zusammen?



Empfehlungen, Werbung

Private Daten

Online Dienste

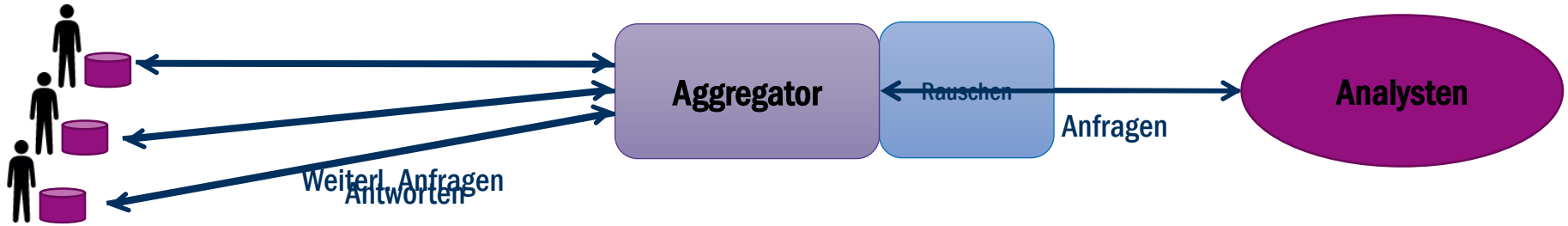
Privatsphäre

Analytics mit hohem Nutzen

[ATC17]
[Middleware17]

PrivApprox: Stream-Analytics mit Privacy

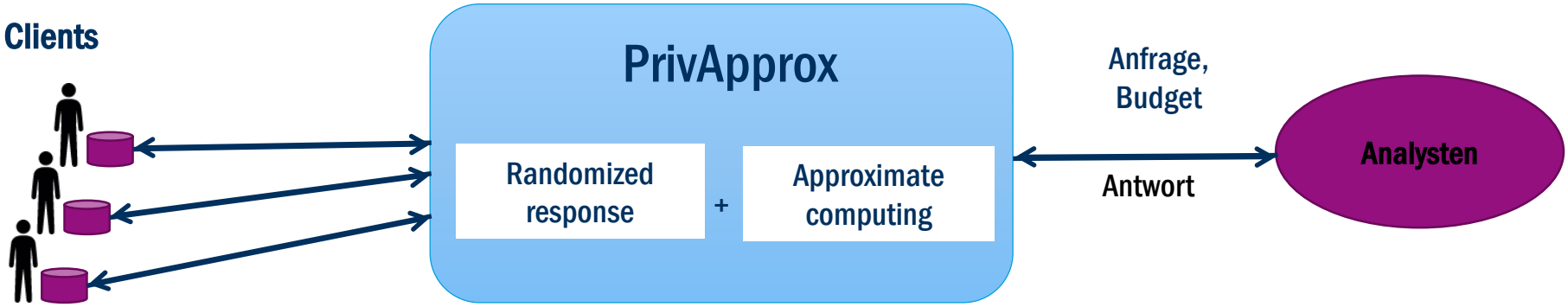
Wie passen Utility und Privacy zusammen?



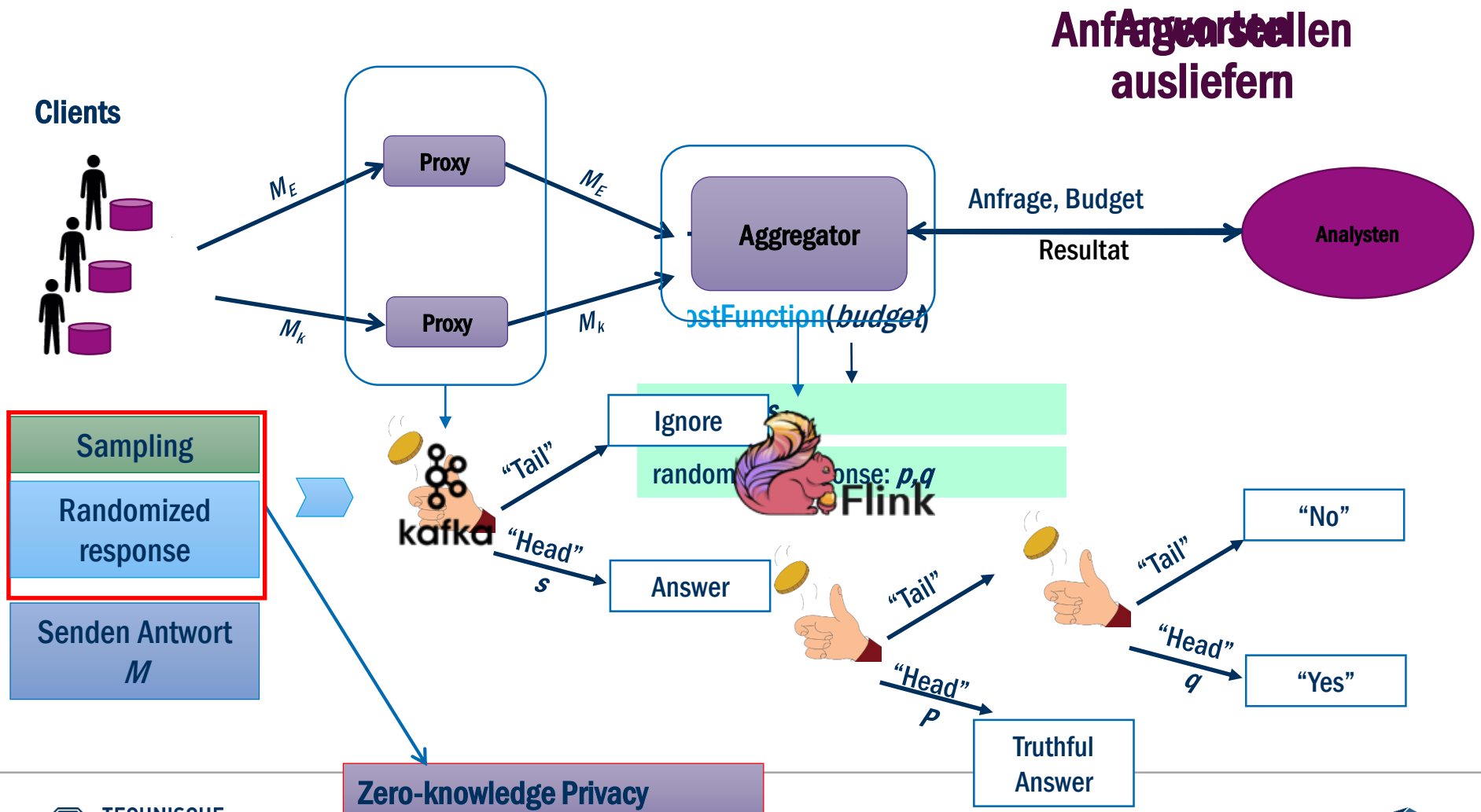
PrivApprox: Idee

Sampling senkt Komplexität (Latenz) und Detail

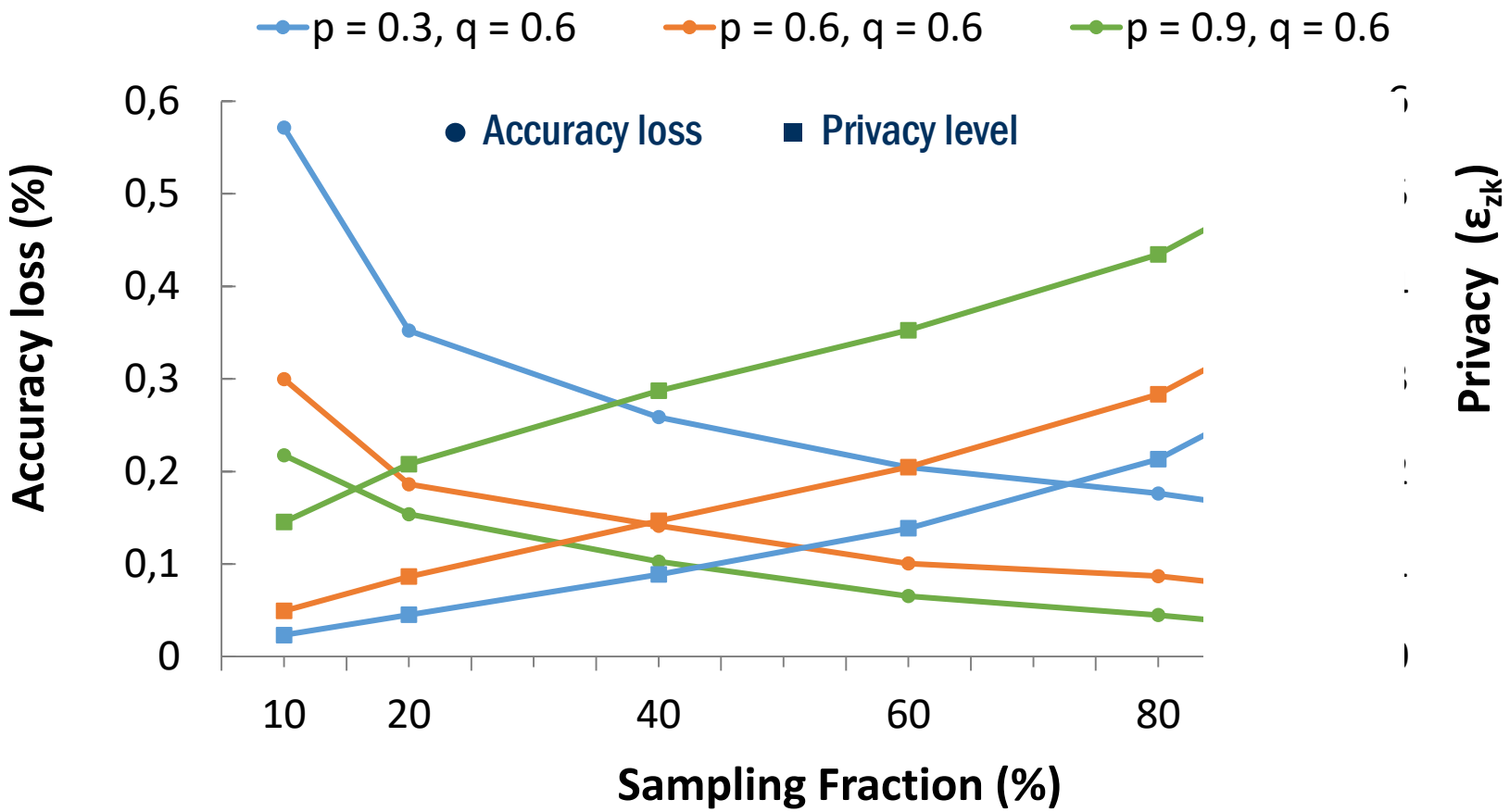
Randomized Response erhöht Datenschutz



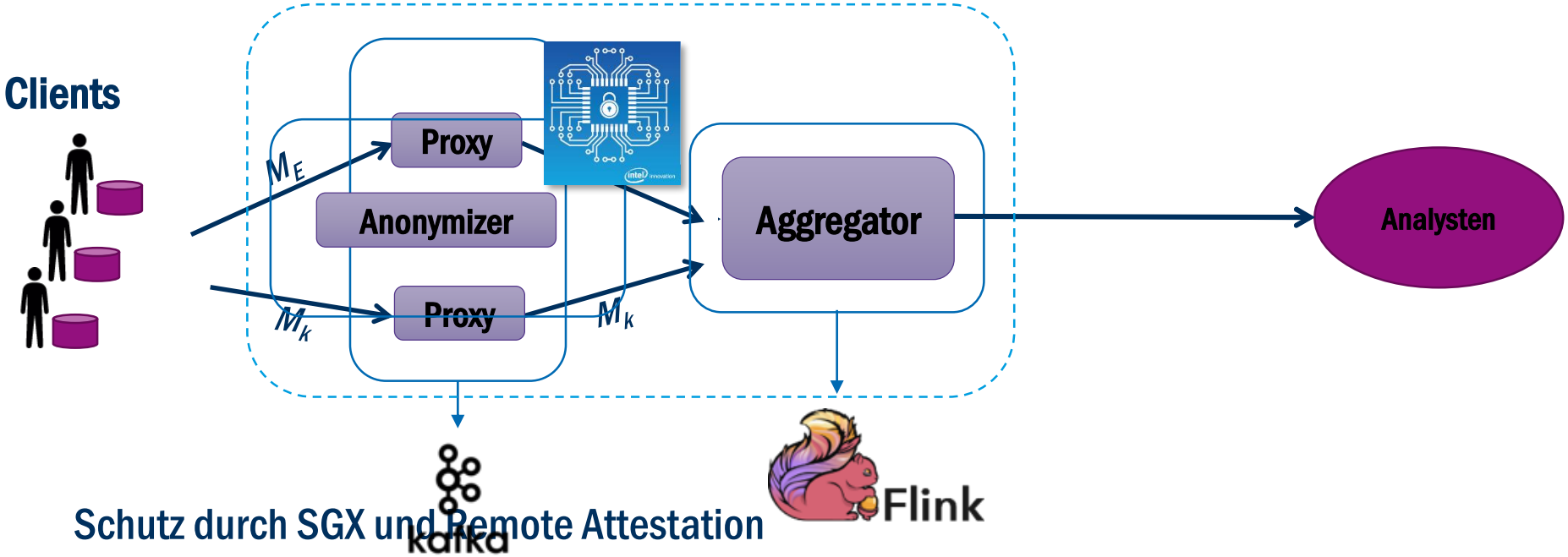
PrivApprox: Workflow



PrivApprox: Genauigkeit vs Datenschutz



PrivApprox: Erweiterungen



Schutz durch SGX und Remote Attestation

Tradeoff Privacy - Einsetzbarkeit

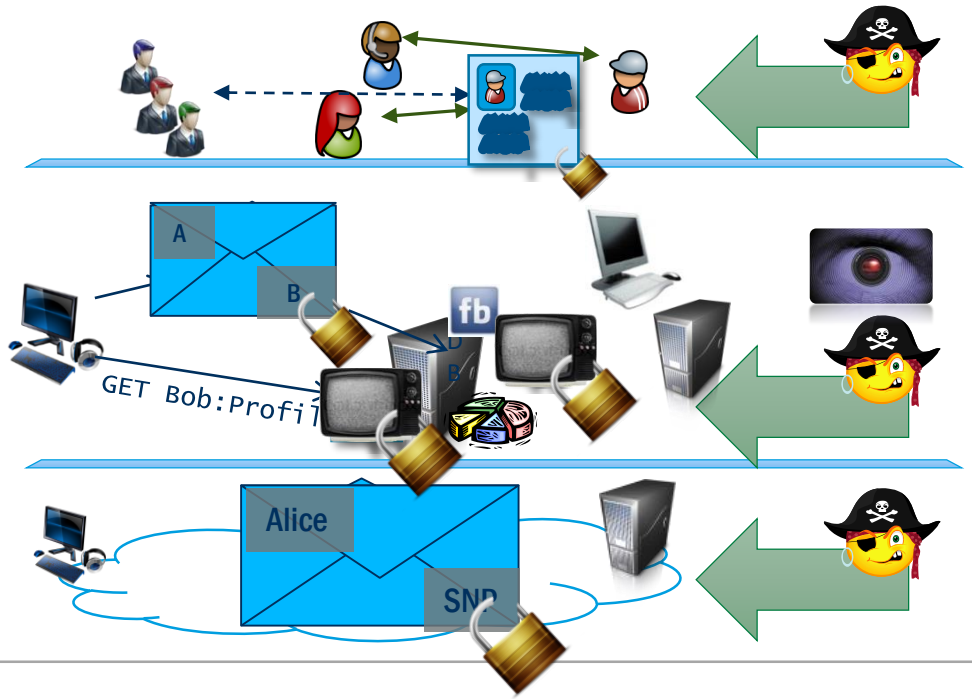
Research Clusters

- ***Network Security***
  - Protected transmission
  - SDN/(N)FV Security
  - Reactive Security

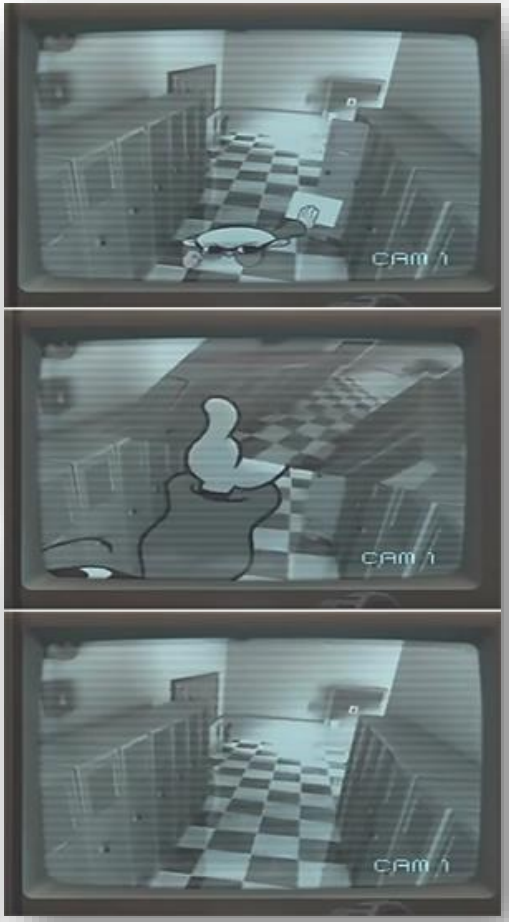
- ***Privacy Enhancing Tech***
  - Anonymous services (F2F)
  - Network anonymisation

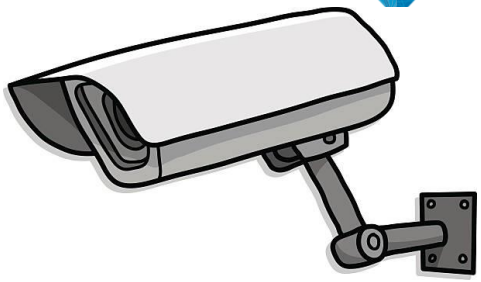
- ***Service Protection***
  - Private Measurement & Analytics
  - Private anomaly detection
  - Trusted Execution

- ***User Understanding***
  - Intention recognition
  - Bot/campaign detection
  - User support



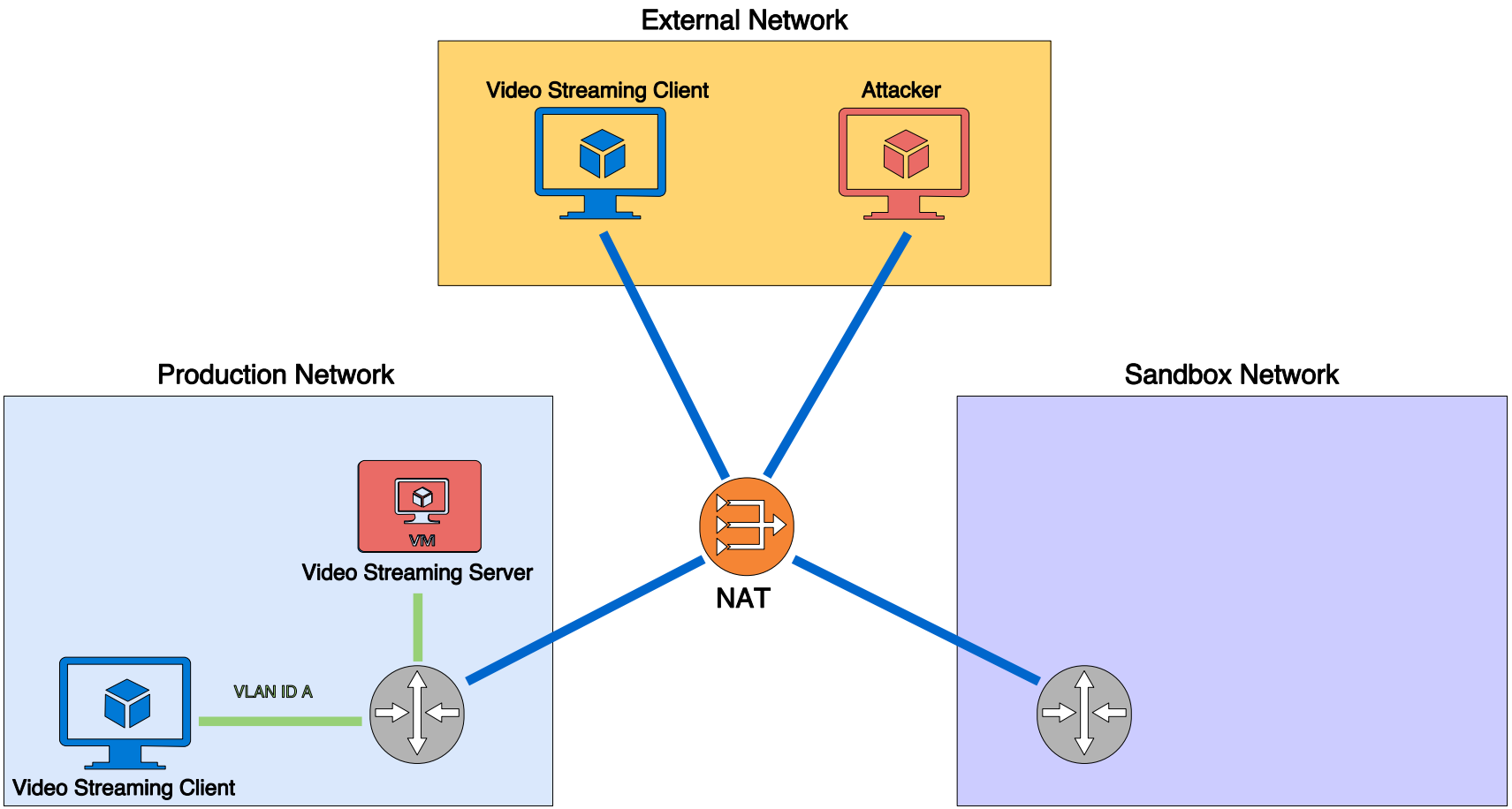
Quarantining Attack „While-it-Happens“



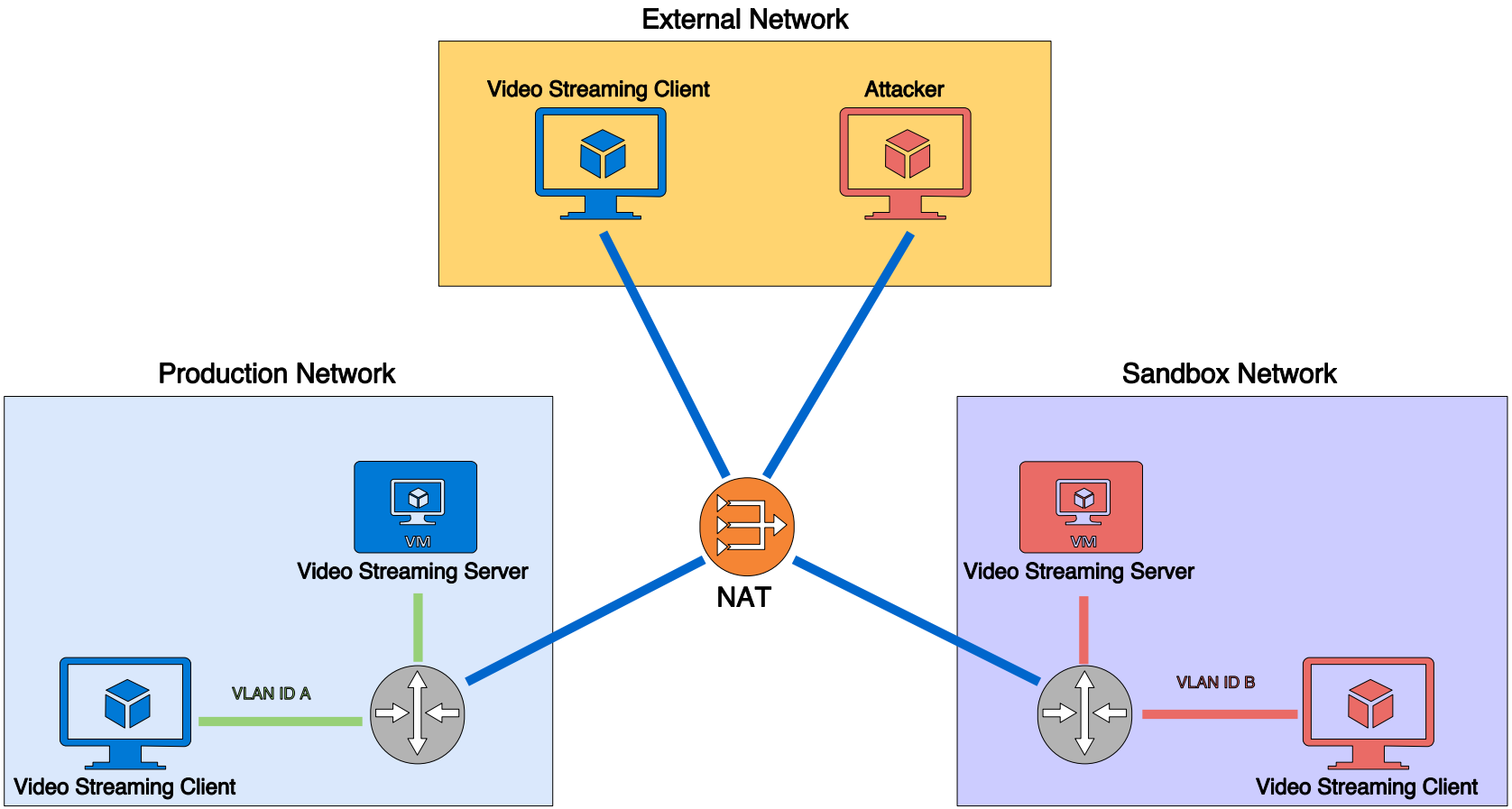


[RAID16]
[EuroSPEC19]

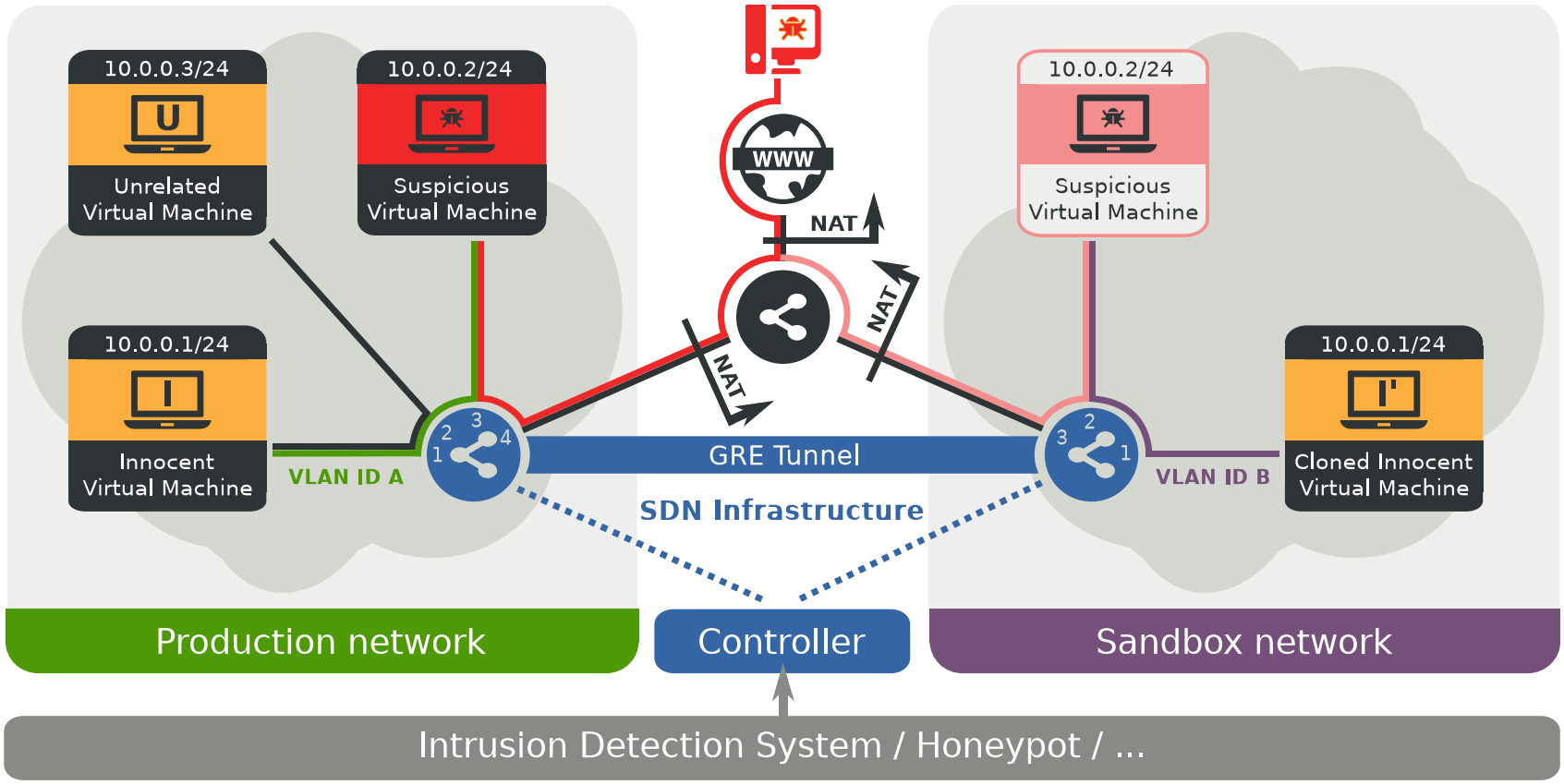
Streaming the Surveillance Footage



Confining the Attacker



System architecture



P&S im Lehrkanon

PRIVACY AND SECURITY

FS	Wintersemester	FS	Sommersemester
1		2	Informations- und Kodierungstheorie
3	Betriebssysteme & Sicherheit	4	*Forschungslinie*
5	**BAS-4** *SaC-1*	6	**BAS-4** *SaC-2/Crypto*
7		8	**Vert-4,** ANW/AFT, Beleg *SaC-2/Crypto/Resilient Networking*
9	**Vert-4**, ANW/AFT *FB-Mining*	10	Diplom/Masterarbeit

BAS-4:

- Security & Crypto 1
- S&C 2 (PETs)
- Crypto

Vert-4:

- S&C 1
- A&C 2 (PETs)
- Crypto
- Resilient Networking

FS	Wintersemester	FS	Sommersemester
B1		B2	Informations- und Kodierungstheorie
B3		B4	
B5	**B-510** Betriebssysteme & Sicherheit	B6	**B-520** Bachelor-Thesis
M1	**BAS-4**	M2	**BAS-4, VERT-4, ANW**
M3	**Vert-4, FPA**	M4	Master-Thesis

B-510/B-520:

- Security & Crypto 1
- S&C 2 (PETs)
- Seminare/Praktika

Vielen Dank

Wir freuen uns auf Sie!

References

[TED16] https://www.youtube.com/watch?v=0wsJSYmVk-U

[Nielsen] https://nielsen.com

[Datanyze] https://datanyze.com/market-share/

[FC11] "Cryptographic treatment of private user profiles". F Günther, M Manulis, T Strufe. International Conference on Financial Cryptography and Data Security, 40-54, 2011

[SNTA10] „Security and privacy in online social networks".L-A Cutillo, M Manulis, T Strufe. Handbook of Social Network Technologies and Applications, 497-522

[PNAS13] "Private traits and attributes are predictable from digital records of human behavior". Michal Kosinski, David Stillwell, and Thore Graepel. PNAS April 9, 2013. 110 (15) 5802-5805;

[Hotsocial12] Paul, Thomas, Benjamin Greschbach, Sonja Buchegger, and Thorsten Strufe. "Exploring decentralization dimensions of social networking services: adversaries and availability." In Proceedings of ACM Workshop on Hot Topics on Interdisciplinary Social Networks Research, pp. 49-56. 2012.

[ENC11] "Anonymous Web Browsing and Publishing". Köpsell, Stefan. Encyclopedia of Cryptography and Security. Springer US, 2011. 40-42.

[ICC14] „An additional protection layer for confidential OSNs posts". F Armknecht, M Hauptmann, S Roos, T Strufe. Communications (ICC), 2014 IEEE International Conference on, 3746-3752

[CommMag] "Safebook: A privacy-preserving online social network leveraging on real-life trust". LA Cutillo, R Molva, T Strufe. IEEE Communications Magazine 47 (12)

[INFOCOM13] Stefanie Roos and Thorsten Strufe. "A Contribution to Analyzing and Enhancing Darknet Routing". In INFOCOM, 2013.

[INFOCOM15] Stefanie Roos and Thorsten Strufe. "On the impossibility of efficient self-stabilization in virtual overlays with churn". In IEEE INFOCOM, 2015.

[INFOCOM16] Stefanie Roos, Martin Beck, and Thorsten Strufe. "Anonymous Addresses for Efficient and Resilient Routing in F2F Overlays". In IEEE INFOCOM, 2016.

[INFOCOM17] Stefanie Roos, and Martin Byrenheid, and Clemens Deusser, and Thorsten Strufe. „BD-CAT: Balanced Dynamic Content Addressing in Trees". In IEEE INFOCOM 2017

[KiVS13] Andreas Hoefer, Stefanie Roos, and Thorsten Strufe. „Greedy Embedding, Routing and Content Addressing for Darknets". In KiVS/NetSys, 2013.

[PETS14] Stefanie Roos, Benjamin Schiller, Stefan Hacker, and Thorsten Strufe. „Measuring freenet in the wild: Censorship-resilience under observation". In PETS, 2014.

[MHN11] Frederik Armknecht and Thorsten Strufe. „An Efficient Distributed Privacy-preserving Recommendation System". In IEEE Med-Hoc-Net, 2011.

[WWW18] "Buzz in Social Media: Detection of Short-lived Viral Phenomena". C Deusser, N Jansen, J Reubold, B Schiller, O Hinz, T Strufe. Companion of the The Web Conference 2018 on The Web Conference 2018, 1443-1449, 2018

[ATC17] Do Le Quoc, Martin Beck, Pramod Bhatotia, Ruichuan Chen, Christof Fetzer, and Thorsten Strufe. "Privacy-Preserving Stream Analytics", In USENIX ATC, 2017

[Middleware17] „StreamApprox: approximate computing for stream analytics". DL Quoc, R Chen, P Bhatotia, C Fetzer, V Hilt, T Strufe. Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference, 185-197

[CNS17] „Privacy-preserving audience measurement in practice—Opportunities and challenges". S Passmann, A Lauber-Roensberg, T Strufe. Communications and Network Security (CNS), 2017 IEEE Conference on, 444-449

[EuroSPEC19] Amr Osman, Simon Hanisch, and Thorsten Strufe: „SeCoNetBench: A modular framework for Secure Container Networking Benchmarks", 2019

[RAID16] Pascal Brueckner, Martin Beck, and Thorsten Strufe. "Poster: Increasing the exposure of honeypots". In Research in Attack, Intrusions, and Defenses, 2016.