Thorsten Strufe
Chair for Privacy and Security

Alles vernetzt – aber nichts davon sicher?

Seniorenakademie Dresden

(mit Dank an Dr. Stefan Köpsell)

Dresden, 22.02.2019

Kurzer persönlicher Hintergrund

1998 – Gründer der „Multiple Choice GmbH“ (Hamburg)

2001 – Diplom Informatik, TU Ilmenau

2007 – Promotion zu Zensurresistenz, TU Ilmenau

2008 – Team „Safebook“ (EURECOM, Frankreich)

2009 – Professor für P2P-Systeme (TU Darmstadt)
Team „Facebook Privacy Watcher/Ampel“
PI DFG FOR „QuaP2P“, PI DFG SFB „MAKI“

2014 – Professor für Privacy and Security (TU Dresden)
Team HoneySens, AN.ON, Sprecher EXC CeTI
PI DFG GK RoSI, PI DFG SFB „HAEC“, PI 5G-Lab

Kurzer Überblick

PRIVACY AND SECURITY

Wer wir sind

Einige Grundlagen der IT-Sicherheit

- Public-Key Crypto
- Bitcoin und Blockchains

Vernetzung und deren Caveats

Einige Gedanken zur „Connected World“

TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

190 Years of Success

1828	Founded as engineering school
1890	„Royal Saxon Technical College“
1945	Largely destroyed
1946	Reopened as „TH Dresden“
1961	Technical University
1990	Full, comprehensive university
2012	University of Excellence

Facts and Figures

- Germany‘s only comprehensive TU
- Students: 33.506
  - International: 4.739 from 125 nations
  - Fresh-men: 7.808
- 122 Study programmes in 18 faculties
- > 8.200 employees
- Overall budget: 528.5 mio €
  - 257.7 mio € in third-party funding
- 3 (+2) Excellence clusters

TU Dresden: University of Excellence

Exzellenz 2018

PRIVACY AND SECURITY

PHYSICS OF LIFE

- Health sciences, bio medicine/eng., CS
- *“to investigate the **fundamental issues in cell and developmental biology”***
- understand the underlying biological processes of life as complex physical phenomena

Stephan Grill

CeTI
Centre for Tactile Internet with Human-in-the-Loop

- Networking, CS, psychology & med.
- *„to **democratize skills and promote equitiy through technology“***
- expediting the efficient cooperation between human and machine

Frank Fitzek, Shu-Chen Li, Thorsten Strufe

ct.qmat

- Smart materials and structures
- *„to **pioneer materials with tailor-made functions in all areas of modern technology”***
- placing emphasis on quantum mechanisms on the atomic scale

Matthias Vojta, with Uni Würzburg

TECHNISCHE UNIVERSITÄT DRESDEN

PRIVACY AND SECURITY

Cluster of Excellence

CeTI

Centre for Tactile Internet with Human-in-the-Loop

Technische Universität Dresden

Excellence Strategy

Funding Period 2019–2025

DRESDEN concept

Research motivation

Where do we stand?

Aim of *current Internet:*
Democratise access to **information** for everybody independently of location or time.

Research motivation

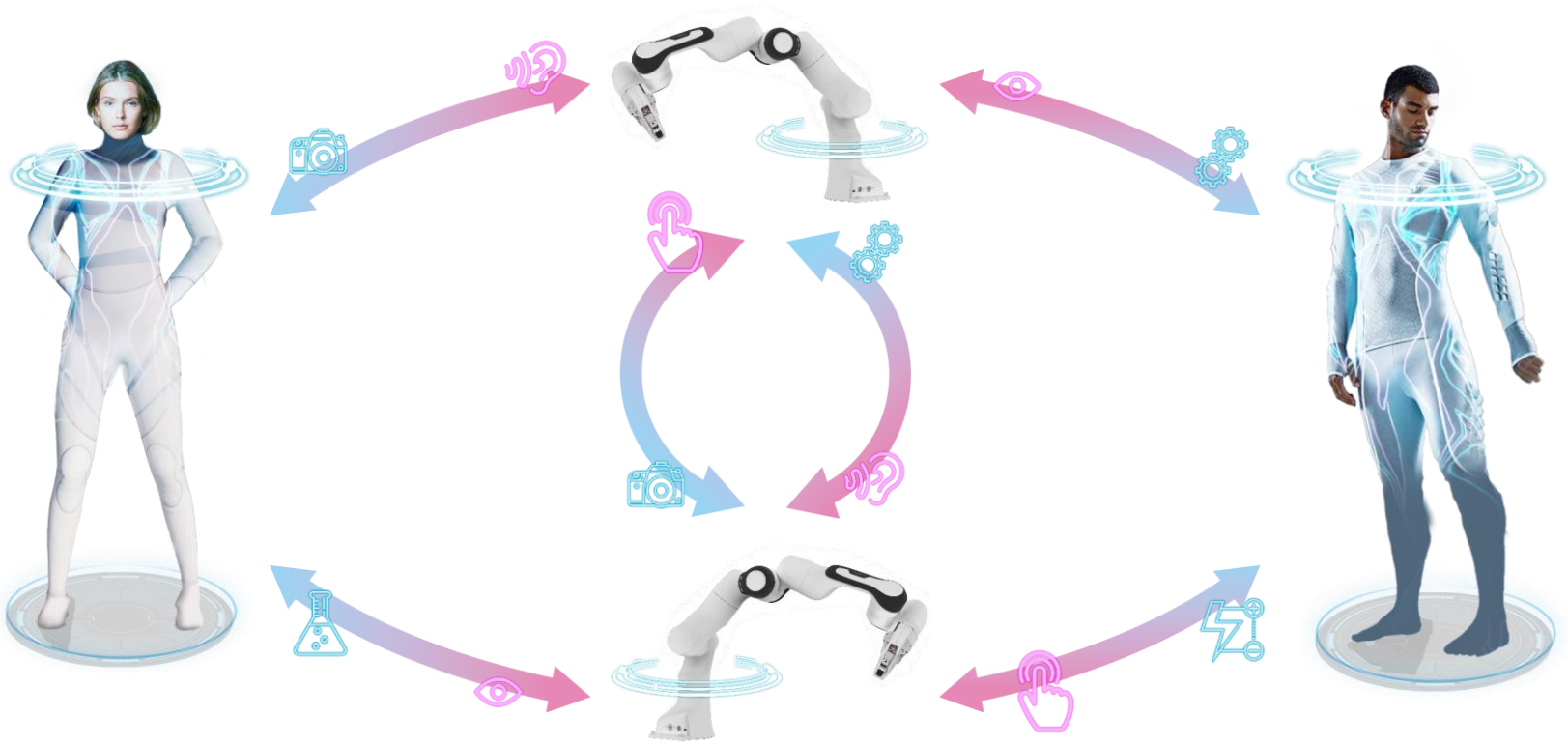
Where do we want to go?

PRIVACY AND SECURITY

Aim of *Tactile Internet with Human-in-the-Loop:*
Democratise access to **skills and expertise** to promote equity for people of different genders, ages, cultural backgrounds, or physical limitations.

Research motivation

CeTI vision / Beyond state of the art / Human–machine augmentation



The CeTI Use Cases

Use case (U) layers

Precision – Distance – Target group – Resilience

Research methodology

How are we doing it?

PRIVACY AND SECURITY

CeTI multifaceted impact

Research

- Information theory, networking and computing, sensors and actuators, understanding of human and machine learning
- Interdisciplinary research

Economy

- Time to market enabling Industry 4.0
- Favour local production
- Existing collaboration with relevant industry partners

Society

- Teach kids
- Human–machine co-working
- Support elderly (demographic change)
- Democratise skills

Facts and Figures

- Institute of Automatic Computing 1956
- Founding of the Faculty in 1969

- 26 (+3) Professors, 6 Institutes
- 1.764 students (+ ~350 PhD students)
- ~300 graduates annually

- Over 200 ongoing research projects
- > 10mio€ third-party research funds

- 29 spin-offs since 2000

Key Research Areas

Software technology for CPS & mobile systems

Cloud Computing and Internet security

Big Data and knowledge extraction

Human-computer interaction & visual comp.

Formal analysis of artificial systems

Modeling & simulating natural systems

Systemarchitektur („Systems“)

PRIVACY AND SECURITY

Herausforderungen und Methodik

- Wir bauen (und untersuchen) die IT-Infrastruktur
- Ziel: Verstehen von (verteilten) Algorithmen, Protokollen, Architekturen
- Dazu Entwicklung, Implementierung, Vermessung von (Angriff auf) Systeme(n) mit Verständnis fundamentaler (theoretischer) Eigenschaften

Professuren

- Professur für Betriebssysteme
- Professur für Datenbanken
- Professur für Rechnernetze
- Professur für Systems Engineering
- Professur für Datenschutz und Datensicherheit

Lehre

- Grundlagenvorlesungen Betriebssysteme, Sicherheit, Rechnernetze, Datenbanken, Programmierung

Kurzer Überblick

PRIVACY AND SECURITY

Wer wir sind

Einige Grundlagen der IT-Sicherheit

- Public-Key Crypto
- Bitcoin und Blockchains

Vernetzung und deren Caveats

Einige Gedanken zur „Connected World“

„Sicherheit“: Safety vs. 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 eines IT-Systems, seiner Daten und Benutzer

Was ist eine Bedrohung?

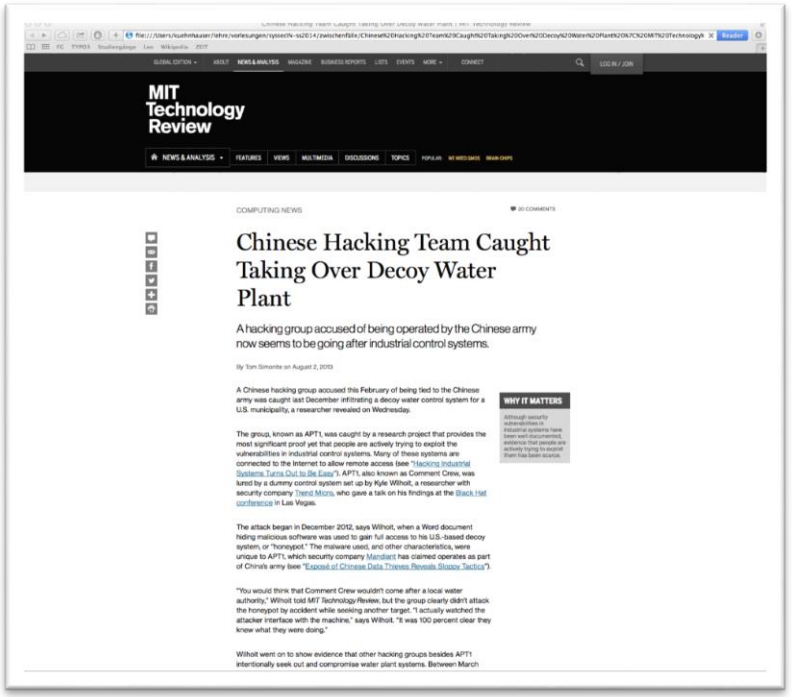
Abstrakte Definition:

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

Beispiele für Bedrohungen:

- Unerlaubter Zugriff auf Firmendaten durch Hacker
- Mutwillig manipulierte von Bank- oder Zeugnisdaten
- Ausfall einer Webseite wegen Sabotage/temporäres Abschalten
- Nutzung von Diensten im Namen einer anderen Partei

Angriffsziele und Angreifer



Die Hitlisten:

Angriffsziele

- wirtschaftliche und politische Macht
- finanzieller Gewinn
- Schaden anrichten
- Herausforderungen meistern

Angreifer

- professionelle Organisationen (bezahlt von Konkurrenzunternehmen, fremden Staaten)
- aktive und ehemalige Mitarbeiter
- Terroristen
- Hacker

Bedrohungspotenziale – Angreifermodell

PRIVACY AND SECURITY

Generell: 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

Angabe der maximal berücksichtigten Stärke eines Angreifers, d.h., Stärke des Angreifers, gegen die ein bestimmter Schutzmechanismus gerade noch sicher ist

Bedrohungspotenziale – Angreifermodell

Inhalt des Angreifermodells

- Intention des Angreifers

  (Zerstören, Stören, Zugriff auf etwas)

- Verhalten des Angreifers
  (passiv/aktiv, beobachtend/verändernd)

- Vermögen (Capabilities)
  - Rechenkapazität
    (komplexitätstheoretisch (un)beschränkt)
  - Verfügbare Mittel
    (Zeit, Geld)

- Kontrolle des Angreifers (Area of control)
  - Rollen des Angreifers
    (Nutzer, Außenstehender, …)
  - Verbreitung des Angreifers
    (kontrollierte Subsysteme, Leitungen, …)

Sicherheitsziele in Anwendungsdomänen

Internet/Telefonie-Anbieter:

- Schutz der Privatsphäre der Kunden
- Einschränkung des Zugriffs zu administrativen Funktionen
- Sicherung gegen Unterbrechungen

Firmen und Forschungseinrichtungen

- Schutz der Privatsphähre der Mitarbeiter
- Vertraulichkeit von Forschungsergebnissen (NDA!)
- Authentizität von Nachrichten und Dokumenten (Verträge, Zeugnisse)
- Sicherstellung des Betriebs

Alle Teilnehmer:

- Verhinderung des Eindringens durch außenstehende Hacker

Sicherheitsziele werden auch als ***security objectives*** bezeichnet

Etwas formaler: Ziele der IT Sicherheit

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 und Privacy?

Sicherheit schützt Daten (und Services/Systeme)

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

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

Terminologie: Datenschutz & Datensicherheit

PRIVACY AND SECURITY

Datenschutz

—alle Vorkehrungen zur Verhinderung unerwünschter (Folgen der) Datenverarbeitung für die Betroffenen *(Persönlichkeitsrecht)*, rechtliche und technische Aspekte

—Beschränkung auf juristische Vorkehrungen →

- Technisch-organisatorischer Datenschutz: technische und organisatorische Ziele und Maßnahmen, die zur Durchsetzung der juristischen Ziele notwendig sind

Datensicherung

—Maßnahmen, Vorkehrungen und Einrichtungen zum Schutz von „Daten“

Datensicherheit (IT-Sicherheit)

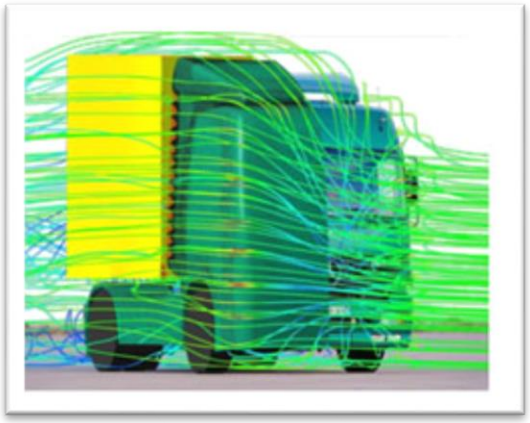
—***Ziel:*** Sicherung der Funktion und Eigenschaften eines IT-Systems trotz unerwünschter Ereignisse (verbleibende Risiken tragbar)

Aber welche Daten denn?

PRIVACY AND SECURITY

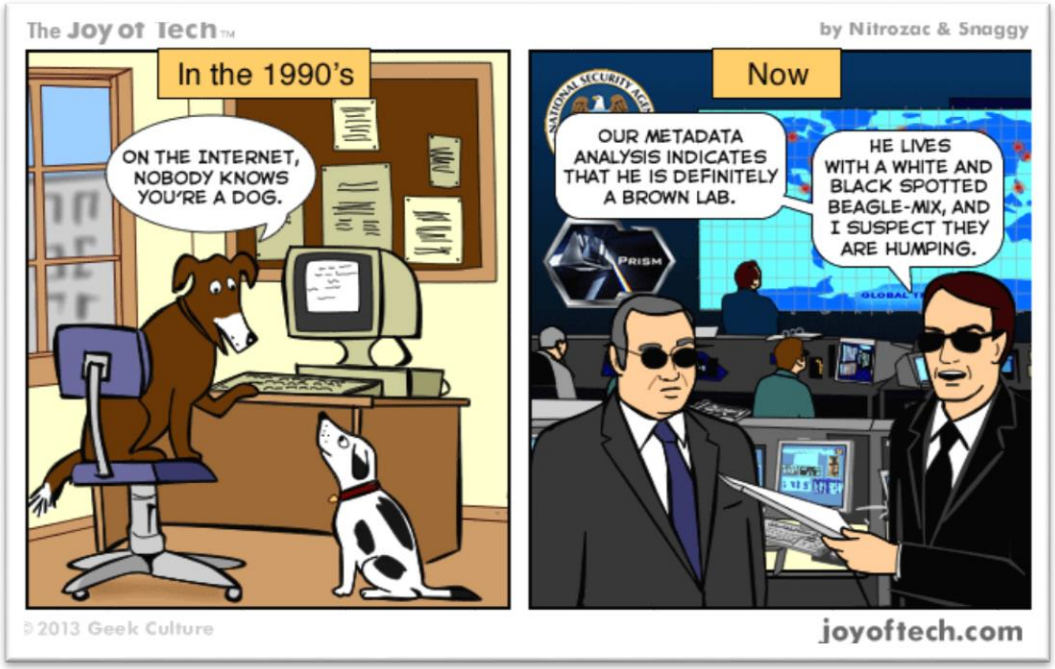
Daten ohne ***Personenbezug***

- Simulationsdaten
- Messungen in Experimenten



Daten ***mit Personenbezug***

- Arten
  - Inhalte
  - Verkehrsdaten
- Veröffentlichung
  - Bewusst
  - Unbewusst



Beobacht- und Ableitbare Information

Explizit
- —Created content
- —Comments
- —Structural interaction (contacts, likes)

„Metadaten“
- —***Session artifacts*** (time of actions)
- —***interest*** (retrieved profiles; membership in groups/participation in discussions)
- —***influence***
- —Clickstreams, ad preferences
- —***communication*** (end points, type, intensity, frequency, extent)
- —***location*** (IP; shared; gps coordinates)

Abgeleitet
- —Preference– and
- —Image recognition models

Extern verkettet
- —Observation in ad networks

Einschub: „Es geht nur um Verkehrsdaten“

PRIVACY AND SECURITY

Verkehrsdaten-Brisanz

Teilnehmer kontrollierter Studie

- *Riefen Familie,…*
- *… Gentlemen Establishments,*
- *… Waffenladen,*
- *… Headshop und Baumarkt,*
- *…Medizinische Spezialisten,*
- *…Familienplanung, Eltern, Frauenarzt*

[1] https://cyberlaw.stanford.edu/blog/2013/11/what%27s-in-your-metadata

Inferenz-“Angriffe“

15 Studenten, 4. Studienjahr

„Angriff“ auf Nutzerdaten
Informationen über „Freunde“

Erfolgreich prädiziert:

- Geschlecht
- Alter
- Wohnort
- Bildungsniveau
- Sexuelle Präferenzen
- Politische Meinung

Einschub: „Es geht nur um Verkehrsdaten“

Verkehrsdaten-Brisanz

Teilnehmer kontrollierter Studie

- *Riefen Familie,…*
- *… Gentlemen Establishments,*
- *… Waffenladen,*
- *… Headshop und Baumarkt,*
- *…Medizinische Spezialisten,*
- *…Familienplanung, Eltern, Frauenarzt*

Infere

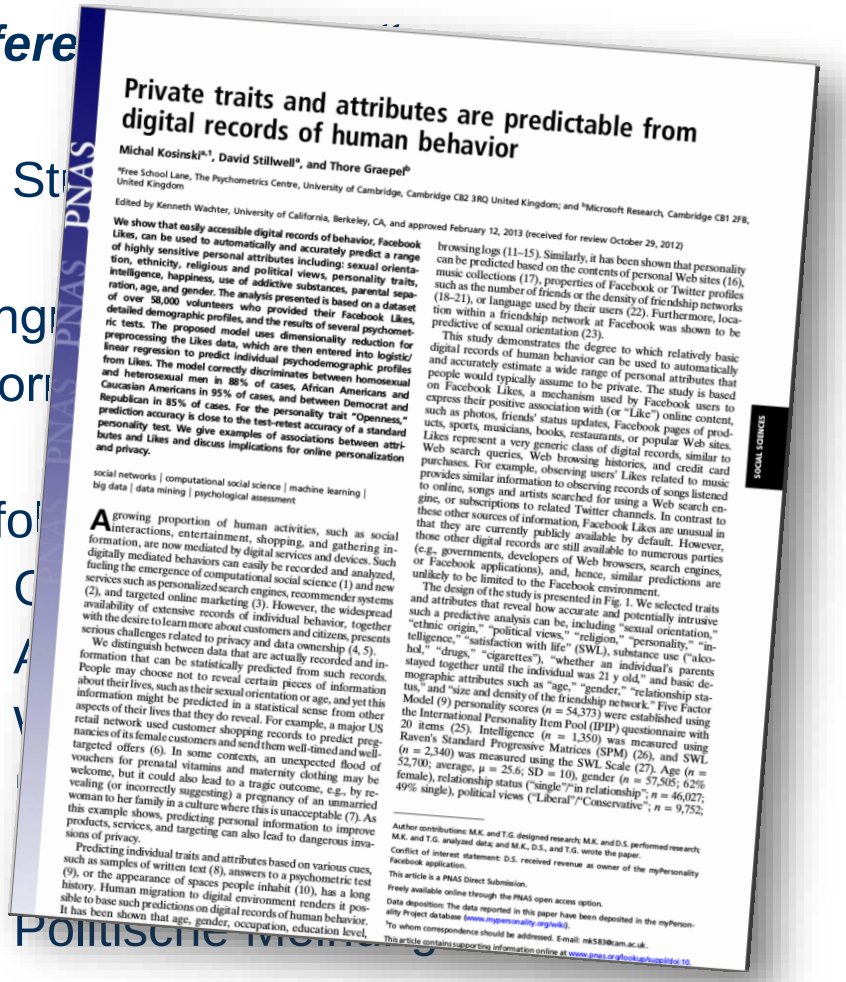
15 St

„Angr

Infor

Erfol

- C
- A
- V
- P
- P
- Politische Meinung



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 (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).

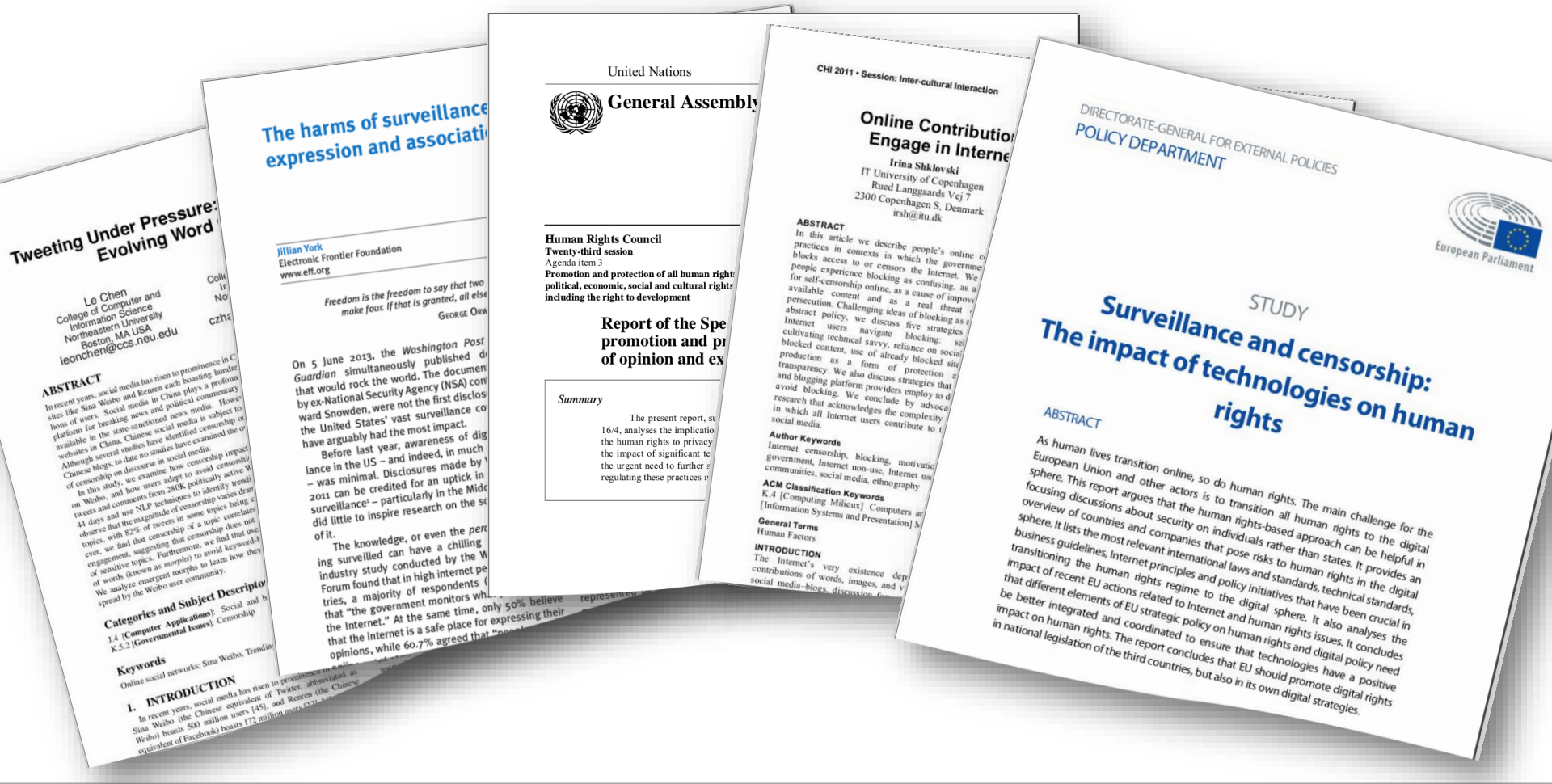
[1]To whom correspondence should be addressed. E-mail: mk583@cam.ac.uk.

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

SOCIAL SCIENCES

[1] https://cyberlaw.stanford.edu/blog/2013/11/what%27s-in-your-metadata

„Ich hab nichts zu verbergen“



Kurzer Überblick

Wer wir sind

Einige Grundlagen der IT-Sicherheit

- Public-Key Crypto
- Bitcoin und Blockchains

Vernetzung und deren Caveats

Einige Gedanken zur „Connected World“

Tafelarbeit

Binäre Zahlen

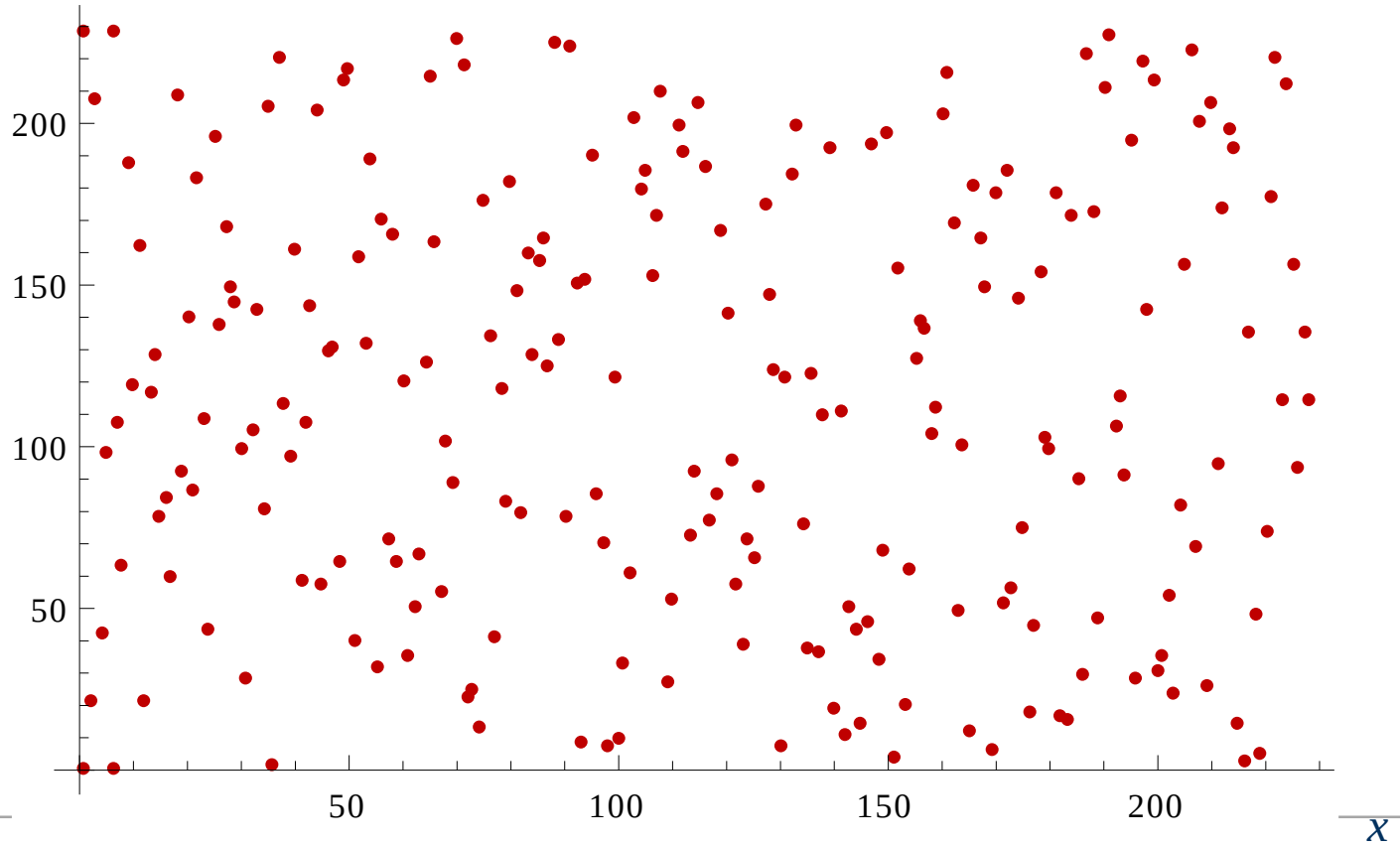
Rechnen mit Restklassen
(„Sie fliegen um 22 Uhr von „Dresden International“ nach Bangkok, wo Sie 10 Stunden später ankommen“)

Einwegfunktionen
(„5^{17} errechnen Sie einfach, die 17. Wurzel aus 762.939.453.125 nur mit leichtem Murren“, „23^5 vs $\log_{23}(6.436.343)$“

Für Computer z.B. das Potenzieren in Restklassen vs. dem diskreten Logarithmus

Diskreter Logarithmus für p = 229, g = 6

$y = \log_6 x \bmod 229$



Schlüsselvereinbarung: Diffie-Hellman(-Merkle)

Wie können wir das nutzen?

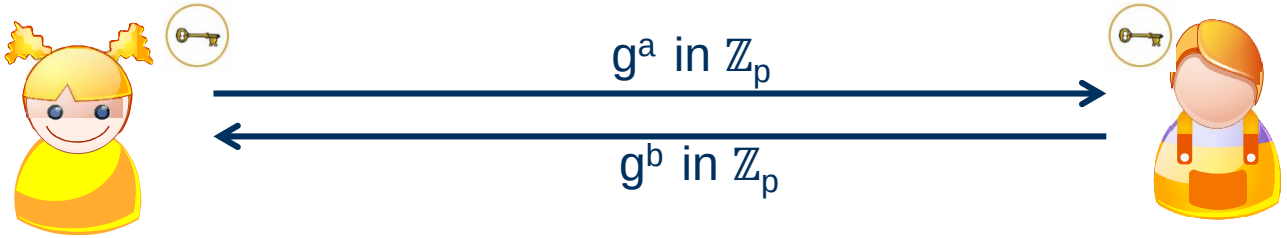
Beobachtungen:

1. Diskreter Logarithmus (einige Umkehrfunktionen) schwer zu lösen
2. Potenzgesetze: $(g^x)^y = g^{xy} = g^{yx} = (g^y)^x$

Idee:

Wahl zyklischer Gruppe $\mathbb{Z}_p^*$, generiert durch g

Alice wählt $a \xleftarrow{R} \{1,\ldots,(p-1)\}$, Bob wählt $b \xleftarrow{R} \{1,\ldots,(p-1)\}$



Alice berechnet: $(g^b)^a$ in $\mathbb{Z}_p$ (mod p) $= g^{ab}$ in $\mathbb{Z}_p$ = Bob berechnet $(g^a)^b$ in $\mathbb{Z}_p$

Bonus: Factoring (prime decomposition)

Theorem: all integers > 1 are either prime or a product of primes.

Factoring:

Consider set of integers $\mathbb{Z}_{(2)}(n) = \{ N=pq$, where p,q are n-bit primes$\}$

Task: Find the prime factors (p *and* q) of a random N in $\mathbb{Z}_{(2)}(n)$

Best known algorithm (NFS): $\exp(\tilde{O}(\sqrt[3]{n}))$ for n-bit integers

Current world record: RSA-768 (232 digits) (200 machine years)

Consumed enough energy to heat to boiling point 2 olympic pools…
(Breaking RSA-2380 equivalent to evaporating all water on earth)

Lenstra, Kleinjung, Thomé

Was bedeutet “groß”? (Etwas Kontext)

PRIVACY AND SECURITY

Reference Numbers Comparing Relative Magnitudes			
Reference	***Magnitude***		
Seconds in a year	≈ 3	$* 10^{7}$	
Seconds since creation of solar system	≈ 2	$* 10^{17}$	$\approx 4.6 * 10^{9}$ y
Clock cycles per year (50 MHz computer)	≈ 1.6	$* 10^{15}$	
Instructions per year (i7 @ 3.0 GHz)	$\approx 2^{63} \approx 7.15$	$* 10^{18}$	
Binary strings of length 64	2^{64} ≈ 1.8	$* 10^{19}$	
Binary strings of length 128	2^{128} ≈ 3.4	$* 10^{38}$	
Binary strings of length 256	2^{256} ≈ 1.2	$* 10^{77}$	
Number of 75-digit prime numbers	≈ 5.2	$* 10^{72}$	
Number of 80-digit prime numbers	≈ 5.4	$* 10^{77}$	
Electrons in the universe	≈ 8.37	$* 10^{77}$	

Brute Force Angriffe

PRIVACY AND SECURITY

Brute force attack, try all keys until intelligible plaintext found:

—Crypto can be attacked by brute force

—On average, half of all possible keys will have to be tried

Average Time Required for Exhaustive Key Search

Key Size [bit]	***Number of keys***	***Time required at 1 encryption / μs***	***Time required at 10^6 encryption / μs***
32	$2^{32} = 4.3 * 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 * 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 * 10^{38}$	2^{127} μs = $5.4 * 10^{24}$ y	$5.4 * 10^{18}$ years

i7 could get to around 10^4 encryptions/μs
GPU can perform around $7x10^5$ hashes

Time since human/chimpanzee lines diverged: $5×10^6$ years,
Homo sapiens: $5×10^4$ years

Vielen Dank für Ihr Interesse und die Mitarbeit! ☺

Auf besonderen Wunsch: Bonus-Folien Bitcoin

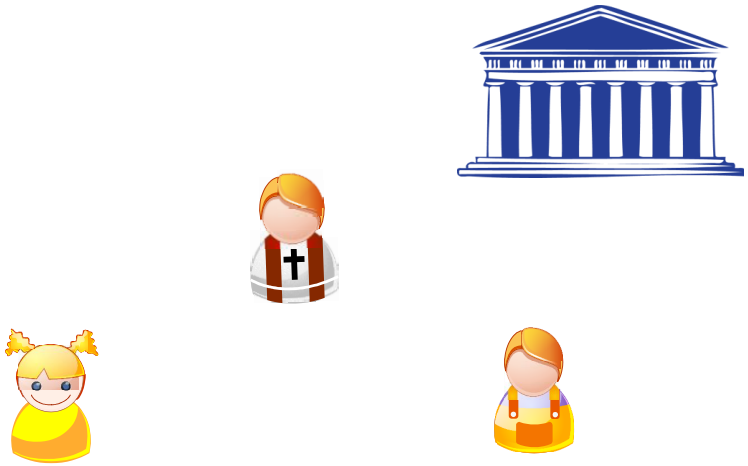
Über die Sinnhaftigkeit von

- Blockchain
- Bitcoin
- Smart Contracts

Protocols and Cryptography (*B‘coin*)

Consensus in the physical world

- Alice and Bob make an agreement…
- *Ownership*: A villager trades his hut for some whiskey, the other villagers register and (the ledger) remember(s)…



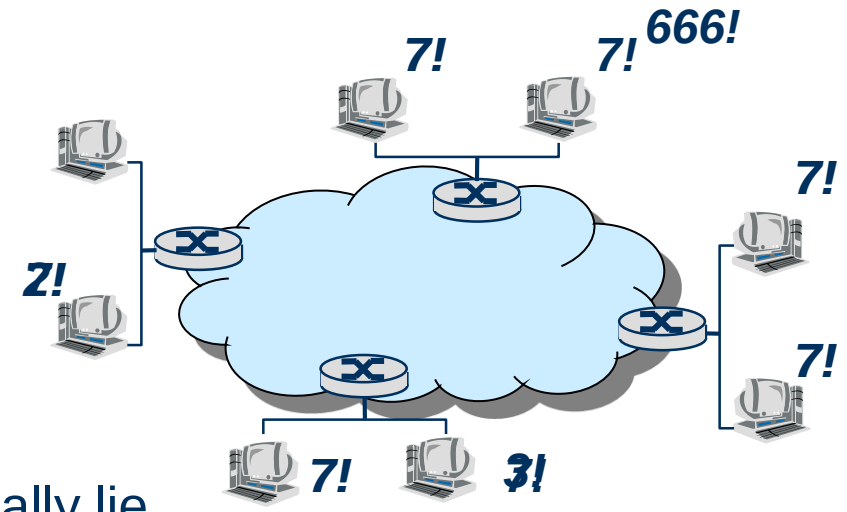
Protocols and Cryptography (*B'coin*)

PRIVACY AND SECURITY

Consensus in IT – the goal that is hard to achieve

- Simple, at absence of malice, perfect memory

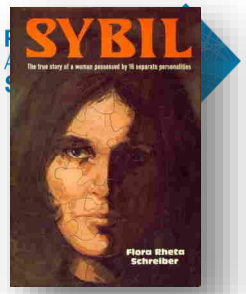
- Simple, if less than half of the participants make mistakes
  → Majority vote



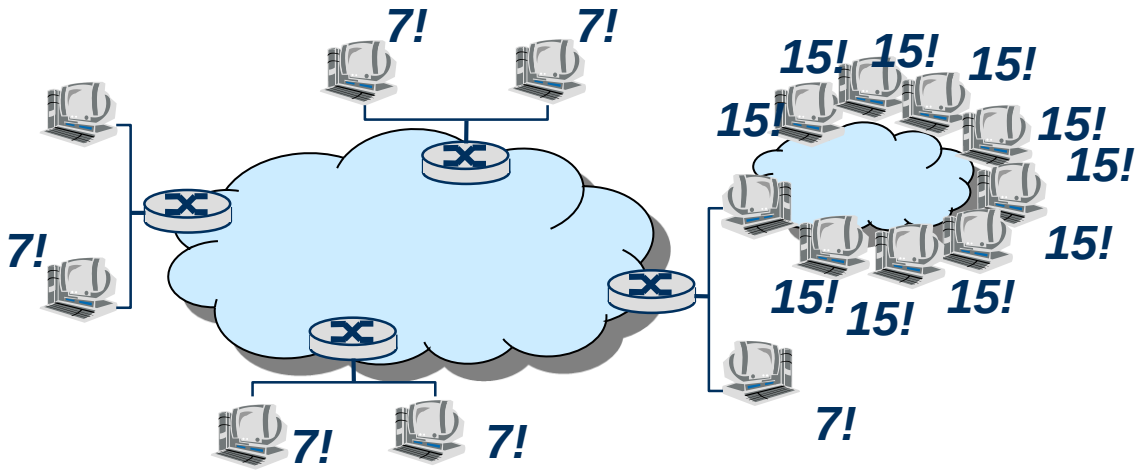
- Slightly complicated but possible if less than 1/3 of participants strategically lie
  → Byzantine fault tolerance, consensus protocols

- How do we know how many ***individuals participate***?

The Sybil Attack (Douceur 2001)



Meet Sybil Dorsett and her dissociative identity disorder

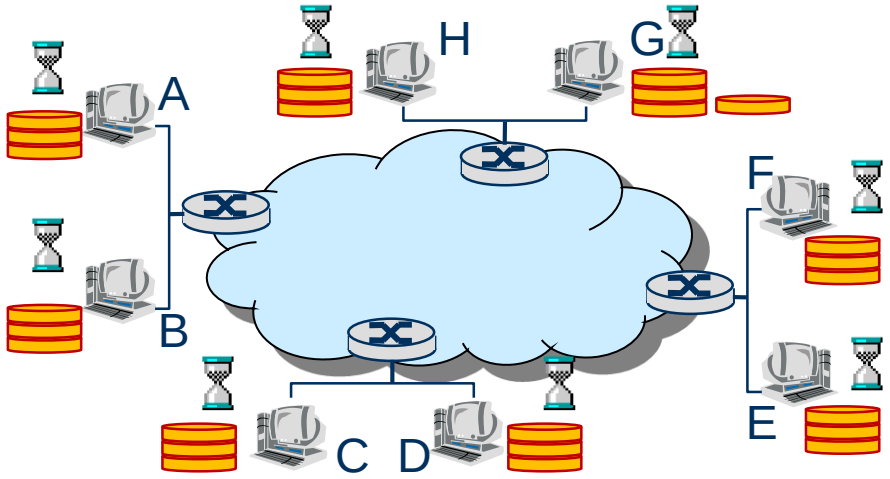


How do we agree on a consensus now, who are the honest parties?

- Delegated to third parties: Proof by certificate
- Direct identity validation:
  - Solve a puzzle each participant can only solve once during a given period: *Proof of work*

Consensus on Possession – A Registry / Ledger

PRIVACY AND SECURITY



1: Everybody gets 3 coins

2: Transactions A->H, B->D, E->A

How do we achieve consensus?

3: At epoch end solve puzzle[1] (state, transactions, *„me+1“*)

4: First shouts solution! (G: „Solution is X!“)

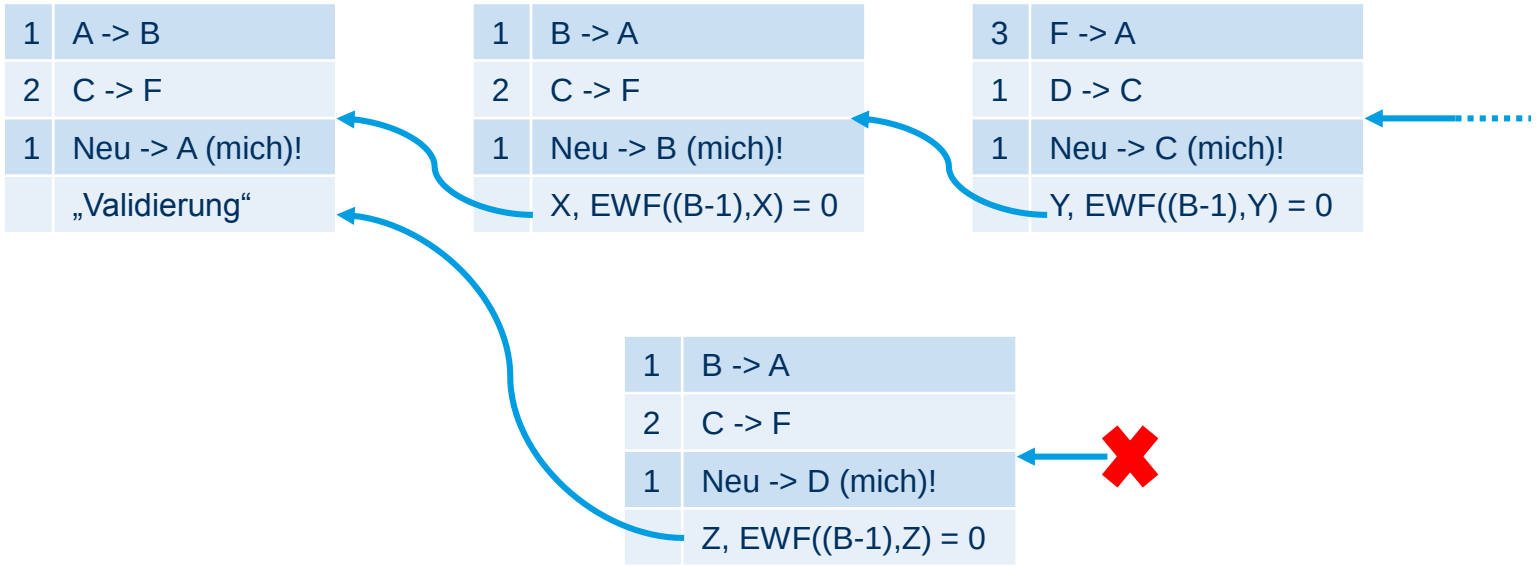
Everybody: Agree on new state, go to step 2

3	A,B,C,D,E,F,G ,H
4	D,H,G
3	A,C,F
2	B,E

Are we sure? Let‘s agree on the longest block chain. After six or seven rounds, nobody will have enough electricity (power to generate different puzzle solutions) to change my and all subsequent *accepted* blocks…

[1] Puzzle: Guess input for required ouput of a one-way function

Die „Blockchain“…



Zusammenfassung:

- Ineffiziente Konsensfindung über tatsächlichen Besitz
- Ineffiziente Speicherung des Katasters

„Smart“ Contracts

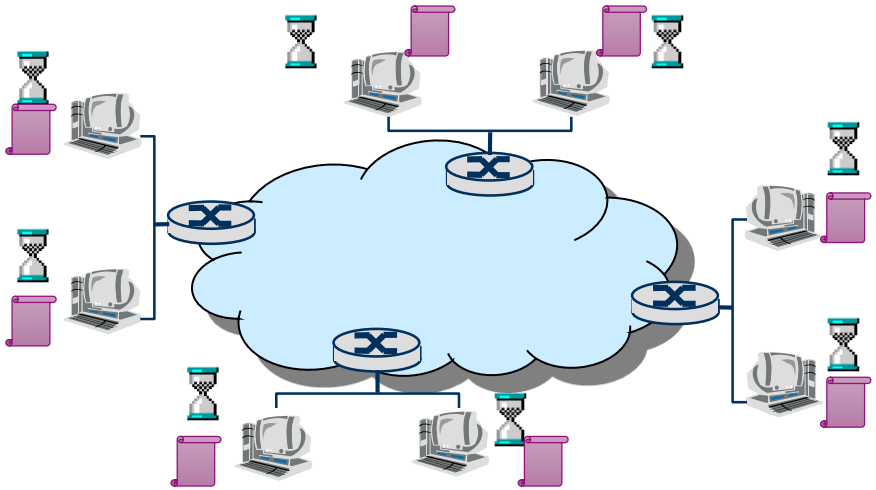
Replace transactions to participants with simple programs, e.g.:

„Here‘s a coin.

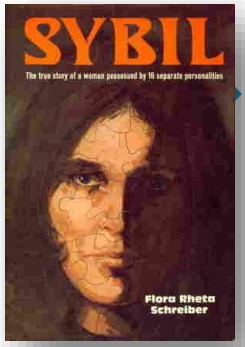
If I there‘s a transaction from A to somebody

then give this coin to A“

(Once this happened, the coin is gone!).



A few Observations on Blockchain-Technology



- The ledger is public (so are all transactions)
- The ledger grows constantly (~210GB/~1TB)

- Blockchains are limited in speed (approx. 6 to 20 Tx/s vs 2k Tx/s for Visa)

- Trust is based on
  - burning electricity (and the assumption that „bad guys“ can‘t burn more electricity than „good guys“)
  - the majority agrees to accept the longest chain *(oh, unless...)*[1]

- „Smart“ contracts rely on ***trusted input*** and their effect (other than system-internal blockchain transactions) has to be ***enforced by external means***.
- Coins spent by „smart“ contracts are spent – either the contract holds a coin, or you have to trust that the committing participant has more coins
- „Smart“ contracts are code. Programmers make mistakes. *(Trust me.)*

- It’s solely necessary to defeat the Sybil attack *(uncertified nodes) – which does not apply for any business model of a serious company.*

[1] http://bit.ly/2EuZ68B