Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Ringvorlesung Digitale Gesellschaft – eine Gestaltungsaufgabe, Universität Kassel, 21. Dezember 2016

Cybersicherheit und Cyberdatenschutz

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Cybersicherheit und Cyberdatenschutz

- Wir bezahlen mit unseren Daten
  - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
  - Innere Sicherheit und Überwachung
- Die Internetwirtschaft kann es
  - aber wo bleibt die Innovation?
- Ethische Dimensionen
  - Information Governace Technologies
- Drohnenkrieg
  - Militärischer Einsatz von Informationstechnologie

Mit Werbung wird Geld verdient! — Auch im Handel

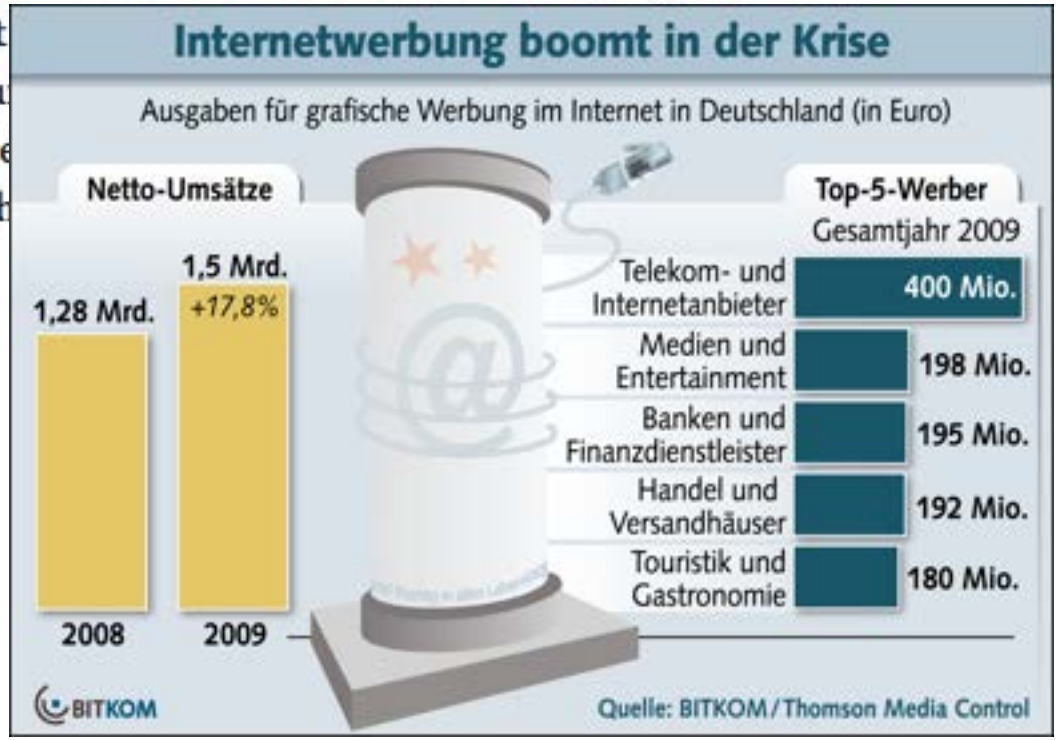
Marketing: Sieben Dollar Umsat...

www.zeit.de/wirtschaft/2011-01/werbung-internet/seite-2

Wie Werbung wirkt

Seite 2/2 Sieben Dollar Umsatz für einen Dollar Werbung

Der Einzelhändler stellte ihnen sämtliche Informationen zur Verfügung, die
er über seine Kunden gesammelt
auf die Nutzerdaten von Yahoo u
Millionen Personen konnten sie
einen Account bei Yahoo als auch

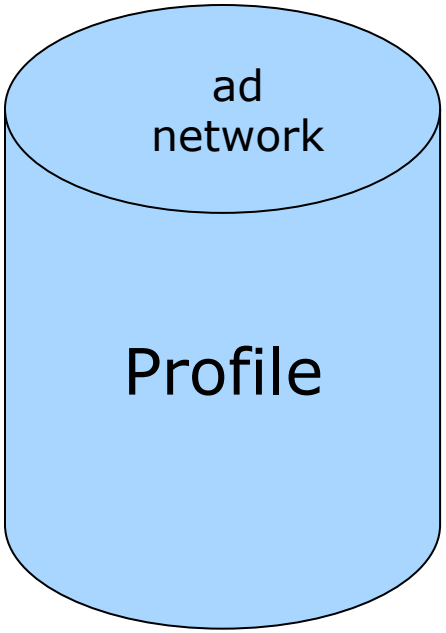


Third-Party Cookies

GET http://adnet.example.net/banner1.gif
Cookie: guid=8867563
Referer: http://www.bookshop.example

GET http://adnet.example.net/banner2.gif
Cookie: guid=8867563
Referer: http://www.healthinfo.example

GET http://adnet.example.net/banner3.gif
Cookie: guid=8867563
Referer: http://www.lifeinsurance.example



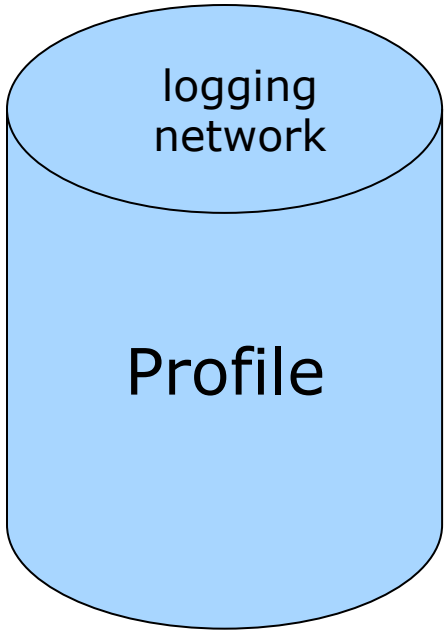
Schutz: Cookies beim Schließen des Browsers löschen

Mobile logging networks

App 1: SN-Device, start, stop, …
82031M6UV2F, 2012-12-19T16:39:57,
2012-12-19T16:45:33

App 2: SN-Device, start, stop, address book, …
82031M6UV2F, 2012-12-20T12:19:11,
2012-12-20T12:25:01, data

App 3: SN-Device, start, stop, location info, …
82031M6UV2F, 2012-12-20T12:21:23,
2012-12-20T12:21:55, data



Schutzmöglichkeiten?

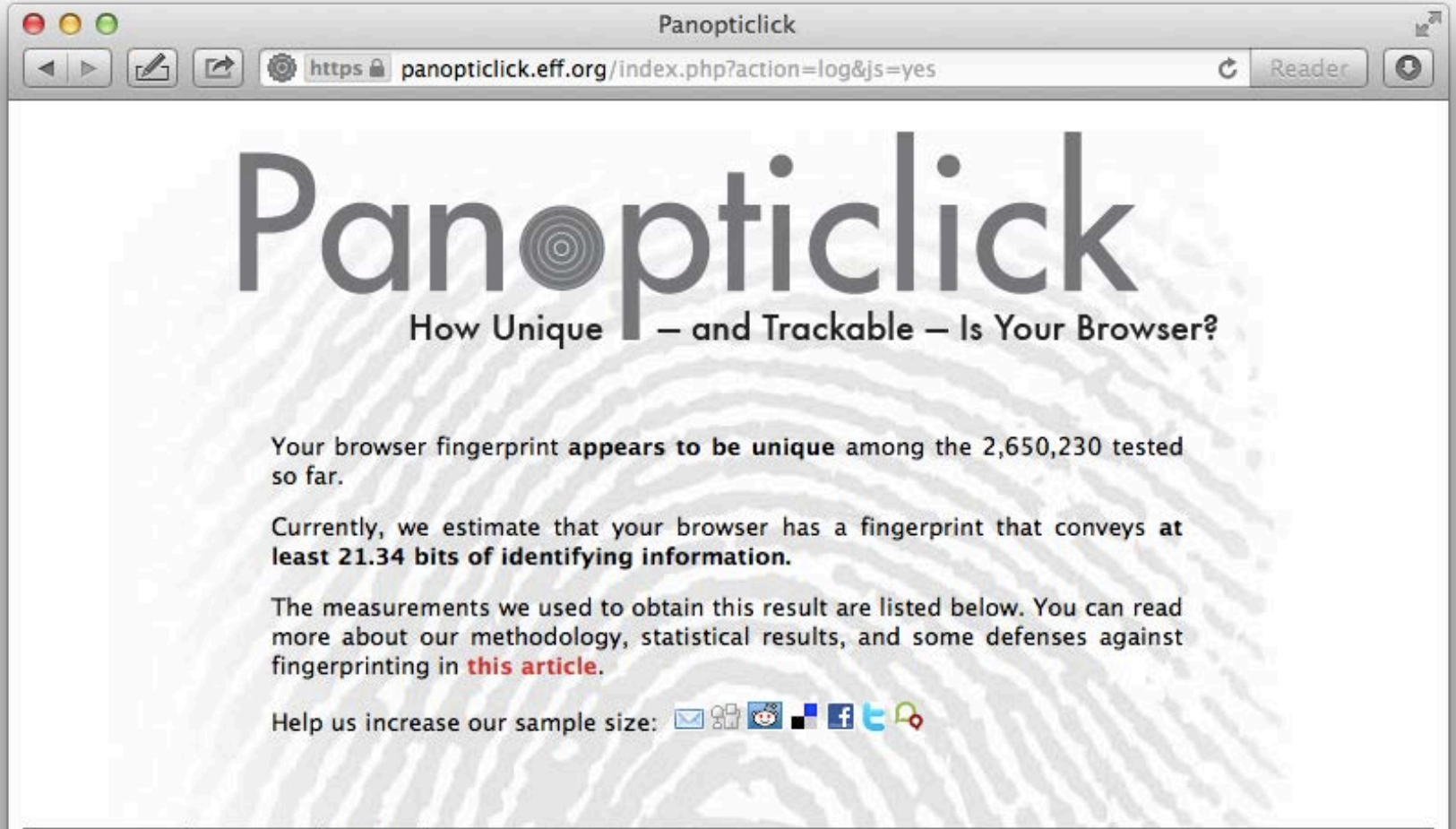
- Verkettung anhand des «Browser Fingerprints» (ohne Cookies)

- Verwendete Verkettungsmerkmale und deren Entropie:
  - User Agent: ca. 10 Bit
  - HTTP_ACCEPT Headers: ca. 7 Bit
  - Browser Plugin Details: ca. 20 Bit
  - Time Zone: ca. 2,5 Bit
  - Screen Size and Color Depth: ca. 5 Bit
  - System Fonts: >=21 Bit
  - Are Cookies Enabled? ca. 0,4 Bit
  - Limited supercookie test? ca. 1 Bit

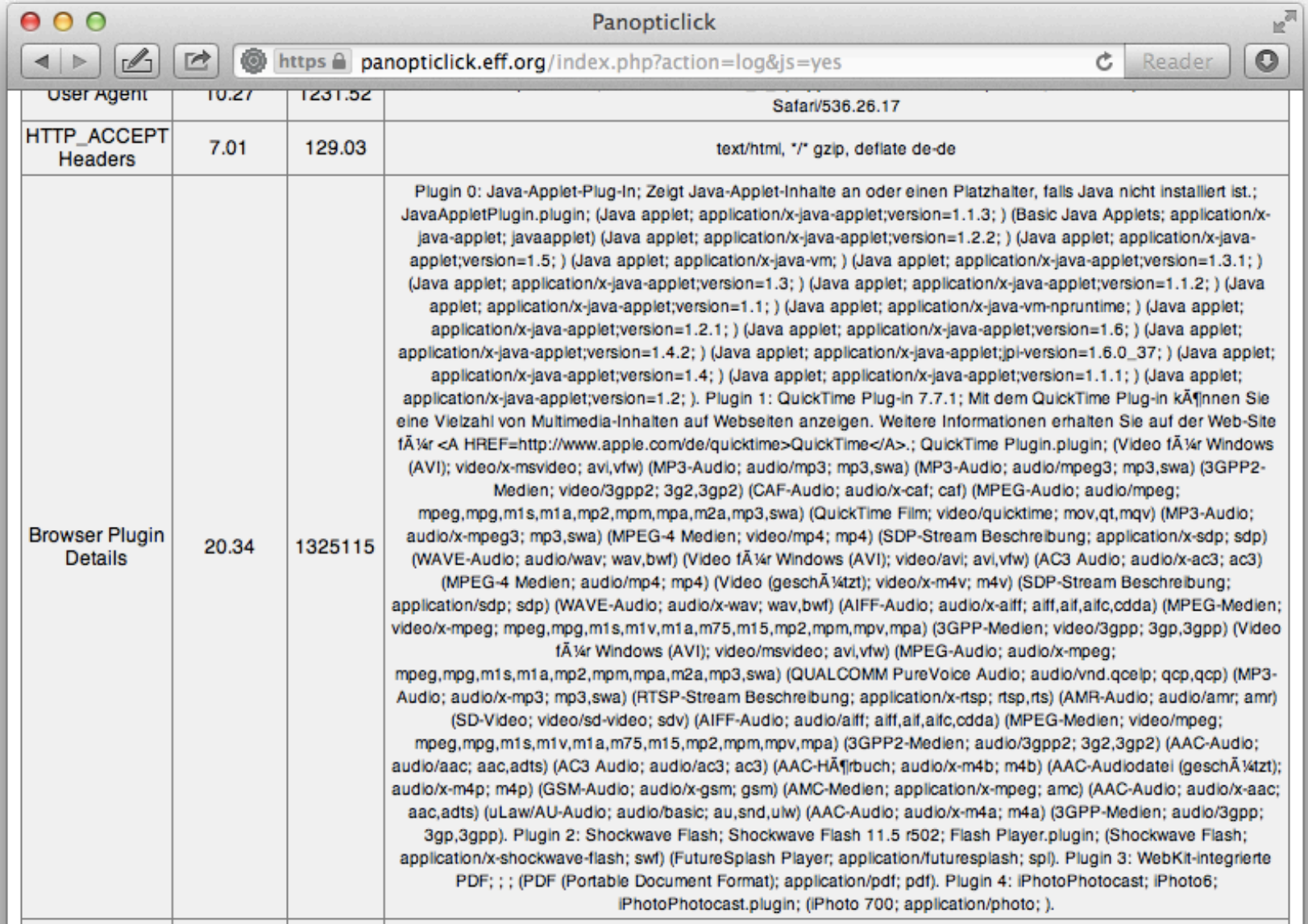
- https://panopticlick.eff.org

Panopticlick

Eckersley 2010



Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	10.27	1231.52	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/536.26.17 (KHTML, like Gecko) Version/6.0.2 Safari/536.26.17
HTTP_ACCEPT	7.01	129.02	



User Agent	10.27	1231.52	Safari/536.26.17
HTTP_ACCEPT Headers	7.01	129.03	text/html, */* gzip, deflate de-de
Browser Plugin Details	20.34	1325115	Plugin 0: Java-Applet-Plug-In; Zeigt Java-Applet-Inhalte an oder einen Platzhalter, falls Java nicht installiert ist.; JavaAppletPlugin.plugin; (Java applet; application/x-java-applet;version=1.1.3;) (Basic Java Applets; application/x-java-applet; javaapplet) (Java applet; application/x-java-applet;version=1.2.2;) (Java applet; application/x-java-applet;version=1.5;) (Java applet; application/x-java-vm;) (Java applet; application/x-java-applet;version=1.3.1;) (Java applet; application/x-java-applet;version=1.3;) (Java applet; application/x-java-applet;version=1.1.2;) (Java applet; application/x-java-applet;version=1.1;) (Java applet; application/x-java-vm-npruntime;) (Java applet; application/x-java-applet;version=1.2.1;) (Java applet; application/x-java-applet;version=1.6;) (Java applet; application/x-java-applet;version=1.4.2;) (Java applet; application/x-java-applet;jpi-version=1.6.0_37;) (Java applet; application/x-java-applet;version=1.4;) (Java applet; application/x-java-applet;version=1.1.1;) (Java applet; application/x-java-applet;version=1.2;). Plugin 1: QuickTime Plug-in 7.7.1; Mit dem QuickTime Plug-in kÃ¶nnen Sie eine Vielzahl von Multimedia-Inhalten auf Webseiten anzeigen. Weitere Informationen erhalten Sie auf der Web-Site fÃ¼r <A HREF=http://www.apple.com/de/quicktime>QuickTime</A>.; QuickTime Plugin.plugin; (Video fÃ¼r Windows (AVI); video/x-msvideo; avi,vfw) (MP3-Audio; audio/mp3; mp3,swa) (MP3-Audio; audio/mpeg3; mp3,swa) (3GPP2-Medien; video/3gpp2; 3g2,3gp2) (CAF-Audio; audio/x-caf; caf) (MPEG-Audio; audio/mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QuickTime Film; video/quicktime; mov,qt,mqv) (MP3-Audio; audio/x-mpeg3; mp3,swa) (MPEG-4 Medien; video/mp4; mp4) (SDP-Stream Beschreibung; application/x-sdp; sdp) (WAVE-Audio; audio/wav; wav,bwf) (Video fÃ¼r Windows (AVI); video/avi; avi,vfw) (AC3 Audio; audio/x-ac3; ac3) (MPEG-4 Medien; audio/mp4; mp4) (Video (geschÃ¼tzt); video/x-m4v; m4v) (SDP-Stream Beschreibung; application/sdp; sdp) (WAVE-Audio; audio/x-wav; wav,bwf) (AIFF-Audio; audio/x-aiff; aiff,aif,aifc,cdda) (MPEG-Medien; video/x-mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP-Medien; video/3gpp; 3gp,3gpp) (Video fÃ¼r Windows (AVI); video/msvideo; avi,vfw) (MPEG-Audio; audio/x-mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QUALCOMM PureVoice Audio; audio/vnd.qcelp; qcp,qcp) (MP3-Audio; audio/x-mp3; mp3,swa) (RTSP-Stream Beschreibung; application/x-rtsp; rtsp,rts) (AMR-Audio; audio/amr; amr) (SD-Video; video/sd-video; sdv) (AIFF-Audio; audio/aiff; aiff,aif,aifc,cdda) (MPEG-Medien; video/mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP2-Medien; audio/3gpp2; 3g2,3gp2) (AAC-Audio; audio/aac; aac,adts) (AC3 Audio; audio/ac3; ac3) (AAC-HÃ¶rbuch; audio/x-m4b; m4b) (AAC-Audiodatei (geschÃ¼tzt); audio/x-m4p; m4p) (GSM-Audio; audio/x-gsm; gsm) (AMC-Medien; application/x-mpeg; amc) (AAC-Audio; audio/x-aac; aac,adts) (uLaw/AU-Audio; audio/basic; au,snd,ulw) (AAC-Audio; audio/x-m4a; m4a) (3GPP-Medien; audio/3gpp; 3gp,3gpp). Plugin 2: Shockwave Flash; Shockwave Flash 11.5 r502; Flash Player.plugin; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 3: WebKit-integrierte PDF; ; ; (PDF (Portable Document Format); application/pdf; pdf). Plugin 4: iPhotoPhotocast; iPhoto6; iPhotoPhotocast.plugin; (iPhoto 700; application/photo;).

Beispiel für Anwendung von Browser Fingerprint

- Laterpay: Bezahldienstanbieter für Micropayments

- Zitat aus den AGBs für Nutzer von Laterpay:

> «Was macht LaterPay um, Ihr Internet-fähiges Endgerät zu identifizieren?
>
> LaterPay verwendet unterschiedliche Verfahren um sicherzustellen, dass der Bezahlinhalteanbieter dem richtigen Endgerät ermöglicht, von dem Vertrauensvorschuss zu profitieren und Inhalte zu konsumieren, bevor eine Registrierung erfolgt.
>
> Hierfür werden wahlweise Browser Fingerprint und die IP-Adresse, Daten des Bezahlinhalteanbieters, Protokolleigenschaften sowie Cookies verwendet.»

https://www.laterpay.net/terms/

Device Fingerprinting

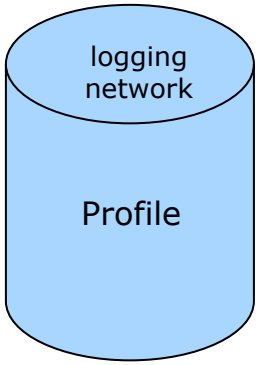
- Unique? App
  - Auskunft über mögliche Identifier
- Entwickelt an der Uni Erlangen
  - zeigt Möglichkeiten des Device Fingerprinting

http://www.iphone-ticker.de/oh-mein-gott-so-eindeutig-laesst-jedes-iphone-zuordnen-66244/

App 1: SN-Device, start, stop, …
82031M6UV2F, 2012-12-19T16:39:57,
2012-12-19T16:45:33

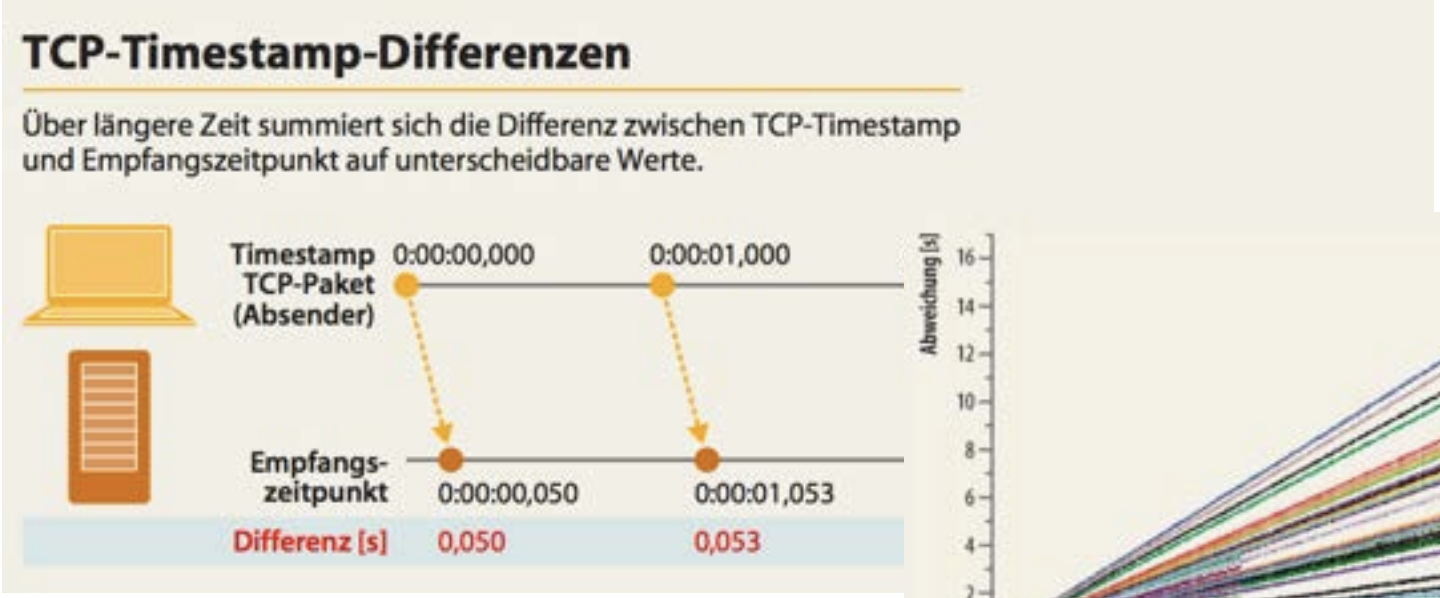
App 2: SN-Device, start, stop, address book, …
82031M6UV2F, 2012-12-20T12:19:11,
2012-12-20T12:25:01, data

App 3: SN-Device, start, stop, location info, …
82031M6UV2F, 2012-12-20T12:21:23,
2012-12-20T12:21:55, data



Messung von Timings zur Identifikation von (mobilen) Geräten

- Langzeitbeobachtung von deterministischen, gerätespezifischen Ungenauigkeiten der internen Uhr eines Geräts

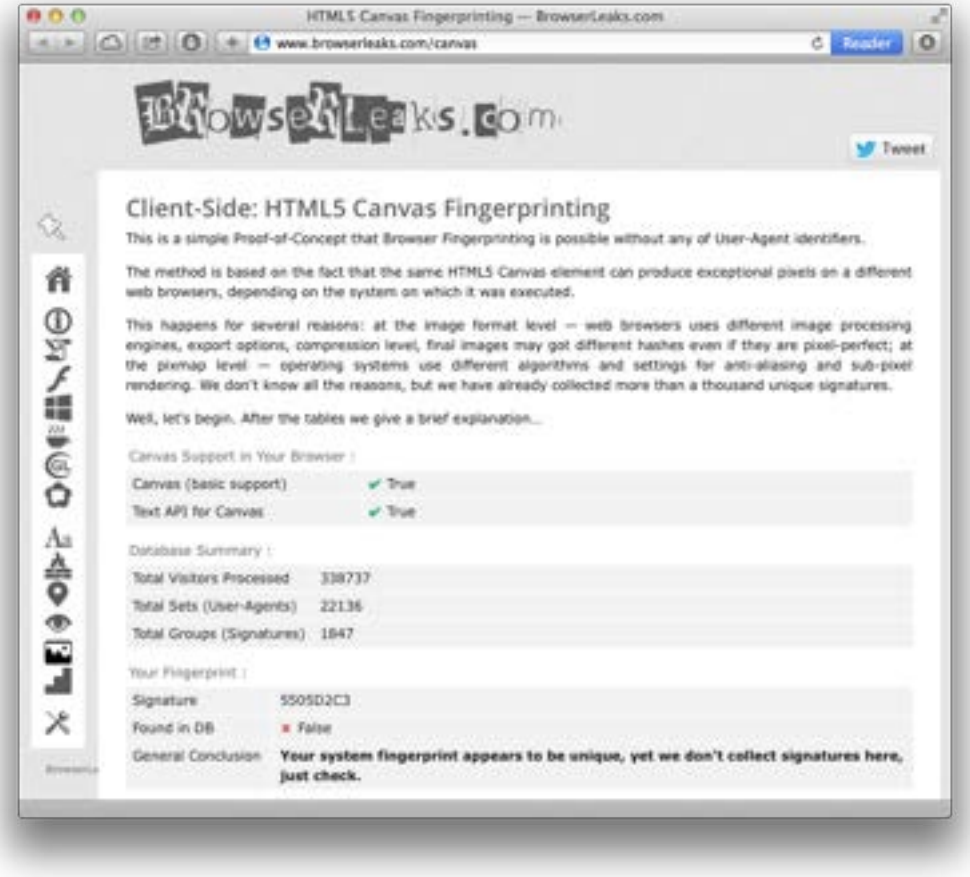


- Schutz:
  - Modifikation des TCP-Standards
  - Hinzufügen eines künstlichen Time-Jitter

Tadayoshi Kohno, Remote physical device fingerprinting, 2005 und c't 11 (2014) 160-161

Canvas Fingerprinting

- winzige Darstellungsunterschiede innerhalb des Browsers ermöglichen individuelle Verkettung

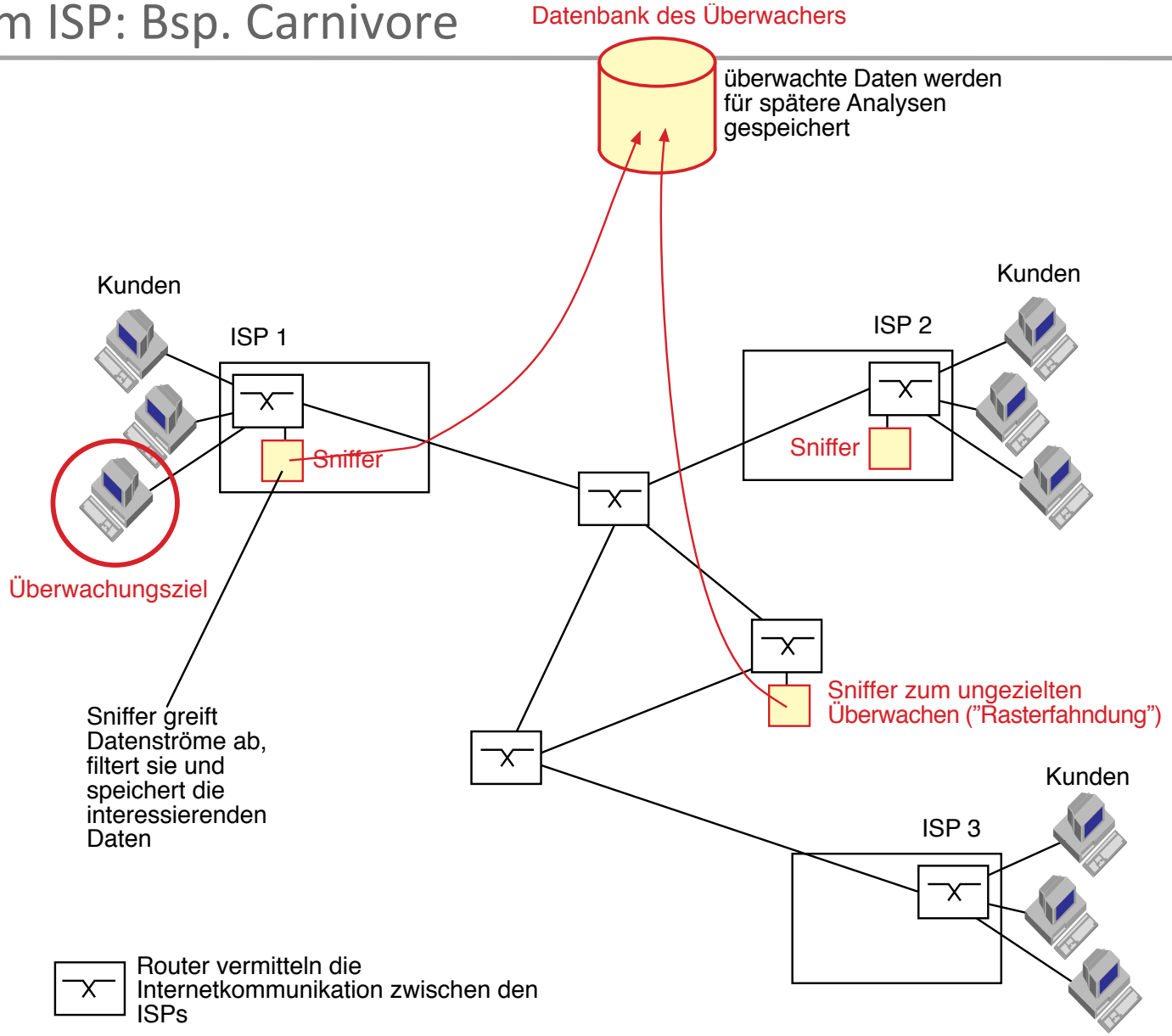


Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, Claudia Diaz. The Web never forgets: Persistent tracking mechanisms in the wild. CCS 2014

Cybersicherheit und Cyberdatenschutz

- Wir bezahlen mit unseren Daten
  - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
  - Innere Sicherheit und Überwachung
- Die Internetwirtschaft kann es
  - aber wo bleibt die Innovation?
- Ethische Dimensionen
  - Information Governace Technologies
- Drohnenkrieg
  - Militärischer Einsatz von Informationstechnologie

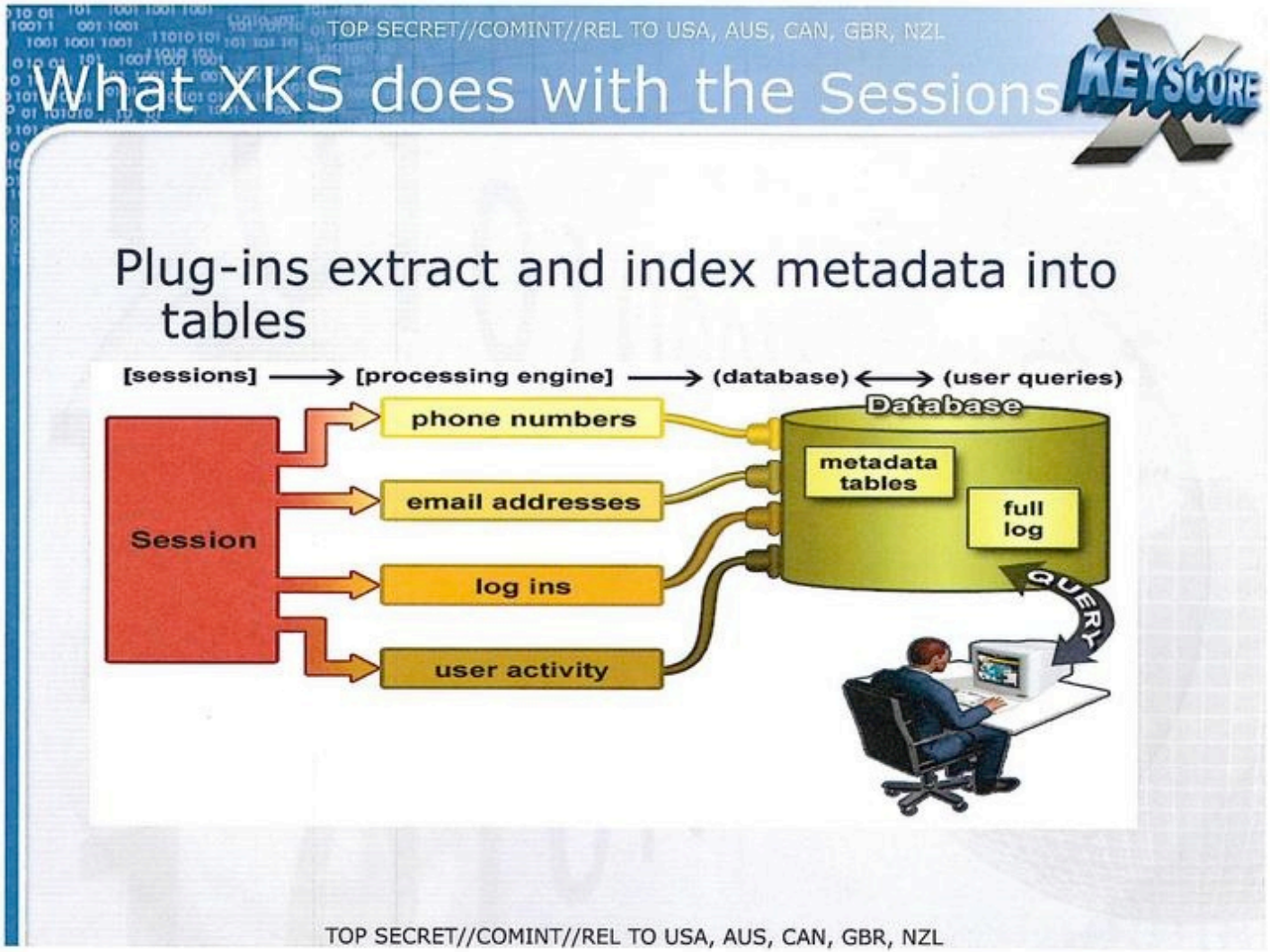
Sniffing beim ISP: Bsp. Carnivore



Sniffing beim ISP: Bsp. Carnivore

Datenbank des Überwachers

Quelle: Wikimedia



Bundestrojaner, Stuxnet

- Darf sich der Staat auch solcher Angriffsmethoden bedienen,
  - die zwar dem Schutz des Staates und seiner Bürger dienen, jedoch die Integrität und Vertrauenswürdigkeit von IT-Systemen untergraben und schlimmstenfalls auch gegen ihn selbst verwendet werden können?

- IT-Sicherheitsstrategien

	klassisch	«modern» → Cyberspionage, Cyberhacking, Cyberwar
Prävention	Encryption, Access Control	
Detektion	Intrusion Detection	
Reaktion	Dynamische Firewalls	

Bundestrojaner, Stuxnet

- Darf sich der Staat auch solcher Angriffsmethoden bedienen,
  - die zwar dem Schutz des Staates und seiner Bürger dienen, jedoch die Integrität und Vertrauenswürdigkeit von IT-Systemen untergraben und schlimmstenfalls auch gegen ihn selbst verwendet werden können?

- Antwort: «Neues Computergrundrecht»
  - Bundesverfassungsgericht im Februar 2008:
    - Grundrecht auf «Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme»
    - Erlaubte Einschränkungen:
      - Gefährdung von Leib, Leben und Freiheit einer Person
      - Gefährdung der Grundlagen des Staates
      - Gefährdung der Grundlagen der Existenz der Menschen

Darf sich der Staat auch solcher Angriffsmethoden bedienen?

- Implementierungen
  - politisch motivierte staatliche Angriffe mit oder auf IT-Systeme anderer Staaten (Cyberwarfare)
    - Stuxnet
  - Gesetzlich erlaubte Telekommunikationsüberwachung und Beweissicherung (Online Durchsuchung) direkt auf dem PC eines Verdächtigen
    - Staatstrojaner / Bundestrojaner

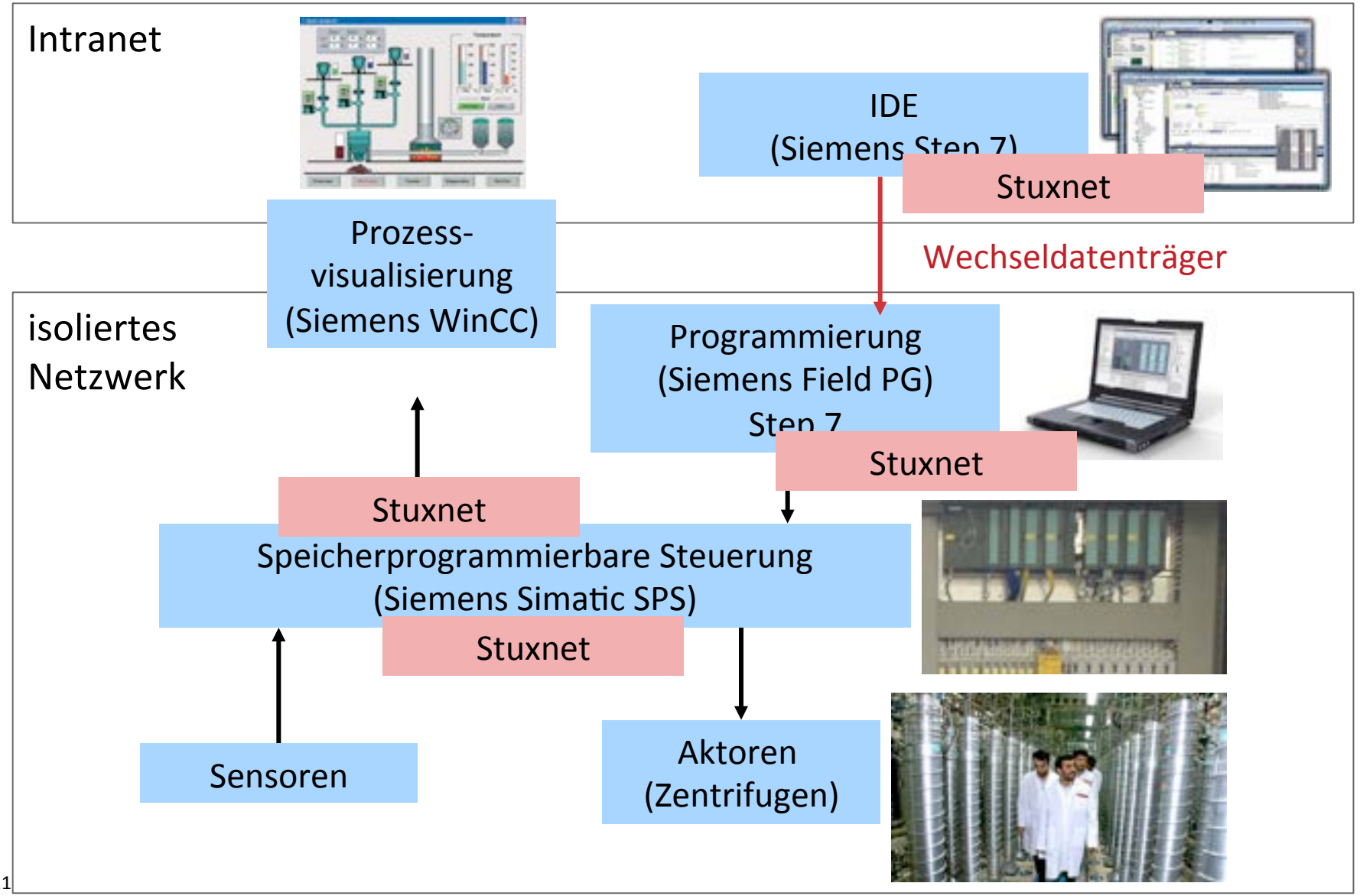
Stuxnet

- Internetwurm, der mit dem Ziel entwickelt wurde, die innerbetrieblichen Abläufe eines speziellen Typs von Industrieanlagen empfindlich zu stören.

  - Entdeckung im Juli 2010
  - Ziel: Unbemerkte Änderung von Programmteilen in speicherprogrammierbaren Steuerungen (SPS)
  - Verwendet vier Zeroday-Exploits zur Verbreitung und Rechteausweitung
  - Insiderwissen für Entwicklung erforderlich
  - Selbstzerstörung (nur Windows-Komponente) nach 35 Tagen


Bild von Natanz (Majid Saeedi/Getty Images)

Stuxnet - Szenario (Industrieanlage)



Stuxnet

- Urheber: USA und Israel
  - Anordnung von 2006 von US-Präsident Gerorge W. Bush
  - in 2010 bestätigt durch Präsident Obama

Quelle: New York Times: Obama Order Sped Up Wave Of Cyberattacks Against Iran. June 1, 2012, page A1

- Besonderheiten
  - Kombination mehrerer unbekannter Zero-Day-Exploits
  - befällt nur bestimmte Systeme (laut Symantec ca. 70% im Iran)
  - Infektionsweg über mehrere Systemgrenzen hinweg
  - P2P-Kommunikation infizierter Systeme
  - Update-Mechanismus
  - Verwendung gestohlener Zertifikate

Staatstrojaner

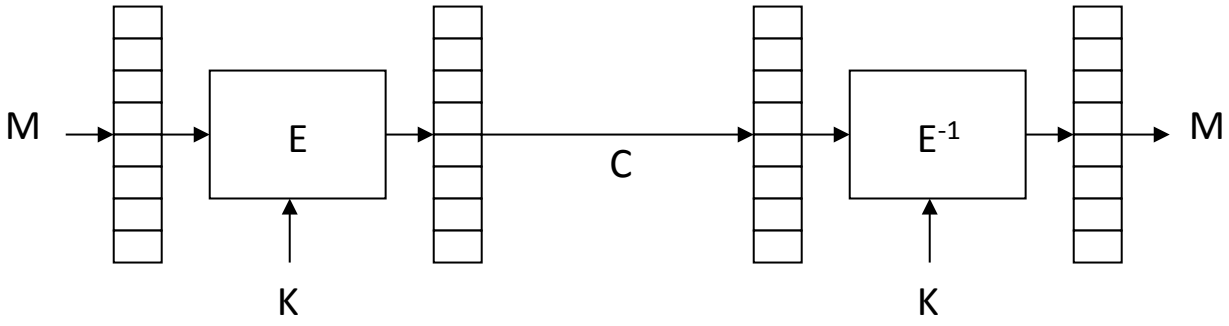
- Haupteinsatzgebiet ist die sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)
  - Oktober 2011 entdeckt
  - Mehrfach unabhängig durch Reverse Engineering analysiert und publiziert
    - Chaos Computer Club
    - Universität Mannheim

- Auftragsarbeit:
  - Auftraggeber: deutsche Sicherheitsbehörden
  - entwickelt von Digitask GmbH
  - geht vermutlich zurück auf eine Skype-Capture-Unit vom September 2007

Staatstrojaner

- Funktionen
  - Ausleiten des Skype-Datenverkehrs
  - Screenshots, Mikrofon einschalten, Keylogger
  - Nachladefunktion

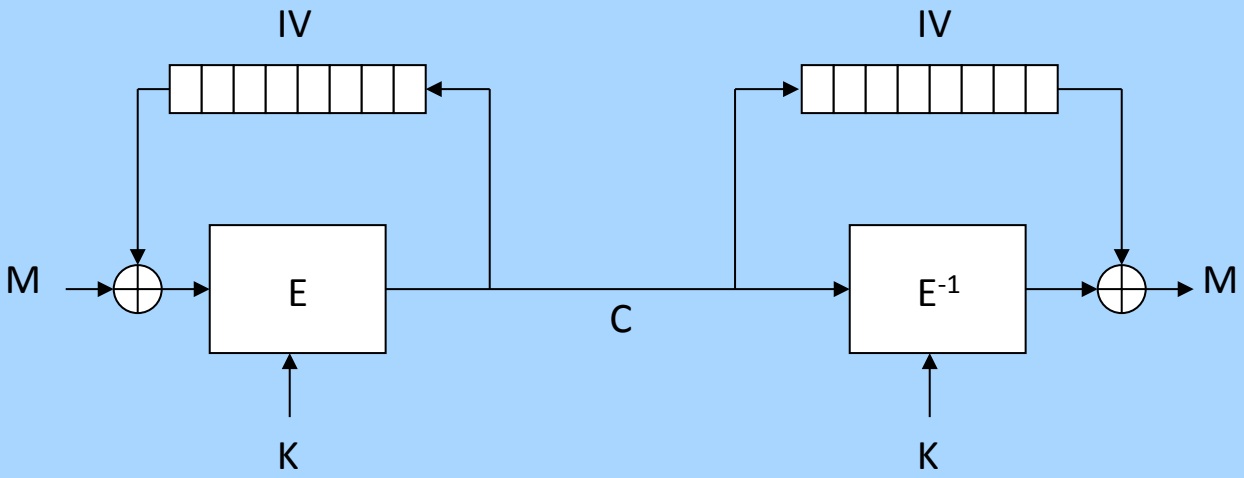
  - Schwach verschlüsselte Kommunikation mit einem Command-and-Control-Server im Ausland (USA)
    - AES im ECB-Mode mit fest kodiertem Schlüssel



Staatstrojaner

- Schwach verschlüsselte Kommunikation mit einem Command-and-Control-Server im Ausland (USA)
  - AES im ECB-Mode mit fest kodiertem Schlüssel

- Richtig wäre: Cipher Block Chaining (CBC) verwenden.



$C_0 = IV$
$C_i = E(K, M_i \oplus C_{i-1})$

$C_0 = IV$
$M_i = E^{-1}(K, C_i) \oplus C_{i-1}$

Spannungsfeld von Freiheit und Sicherheit

- Ziel der Informationssicherheit: möglichst wenig Vertrauen in andere setzen müssen
  - Wo keine Sicherheit erreichbar ist, bleibt nur Vertrauen [müssen]

- Freiheit: insbesondere Grundrechte
  - Recht auf informationelle Selbstbestimmung
  - Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme (Computer-Grundrecht)

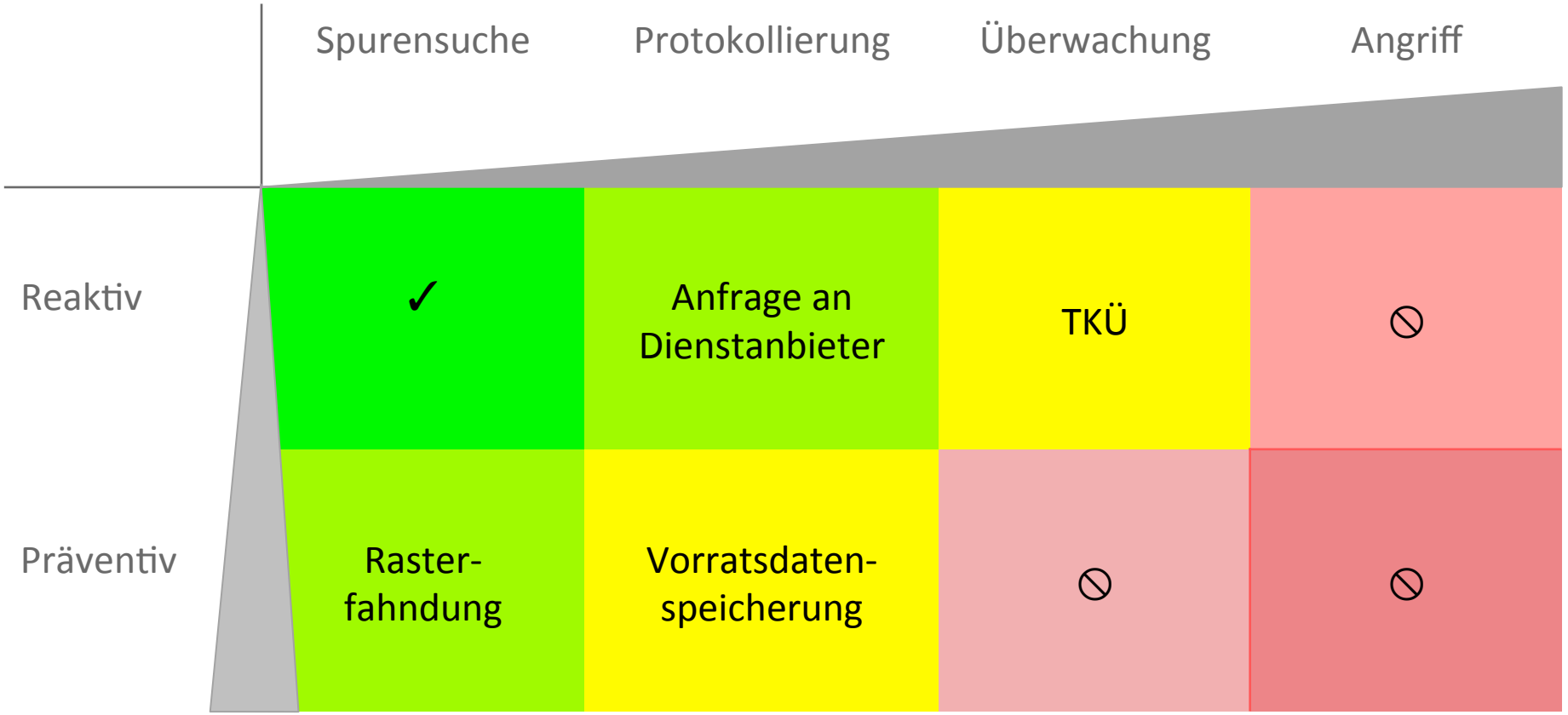
- Sicherheit
  - Vorratsdatenspeicherung
  - Bundestrojaner

«Nur in schweren Fällen …»

… aber die Bürger erleiden Vertrauensverlust gegenüber dem Staat

Eingriffstiefe in die Freiheit

- Darf sich der Staat solcher Angriffsmethoden bedienen?

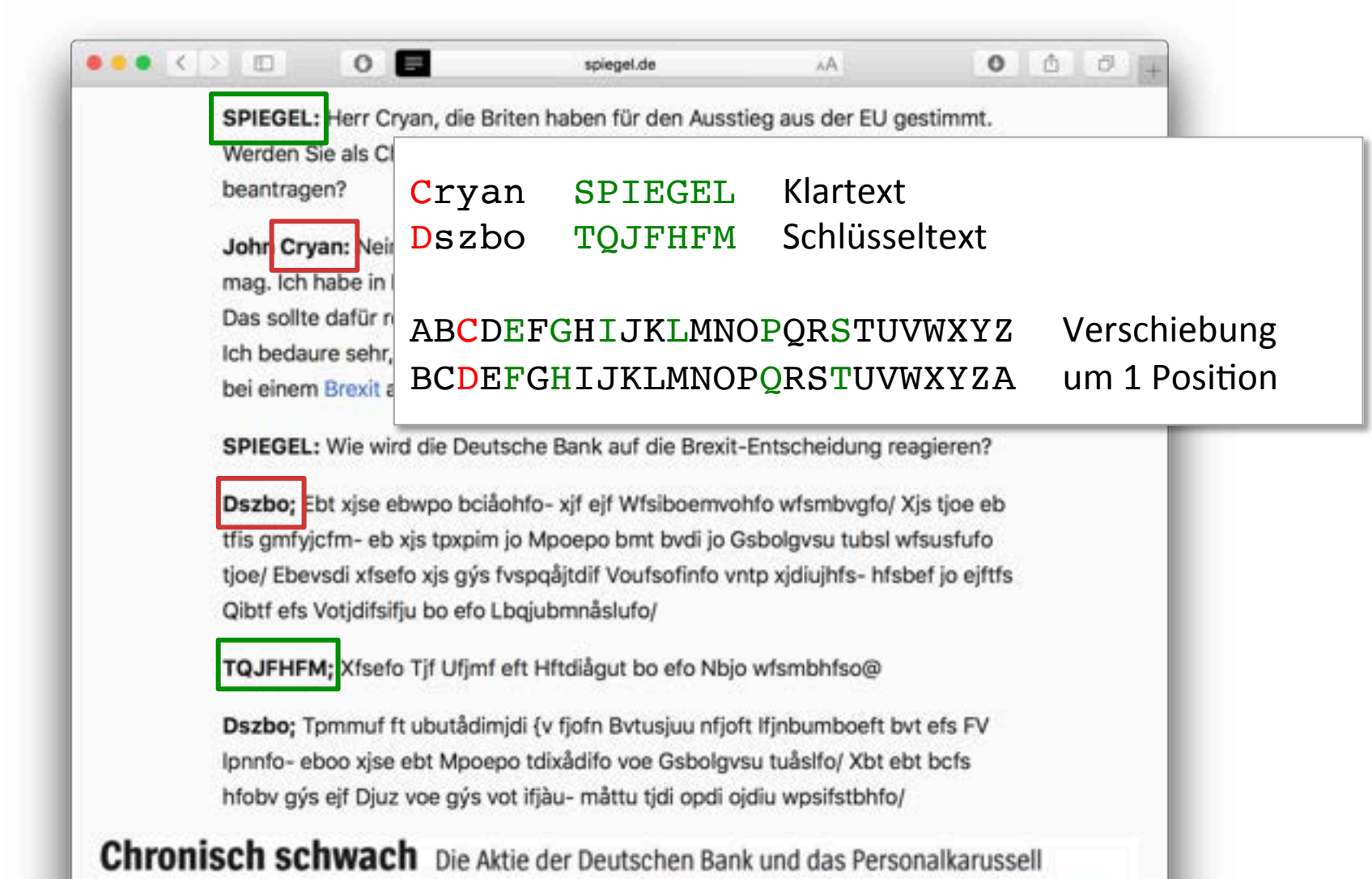


Cybersicherheit und Cyberdatenschutz

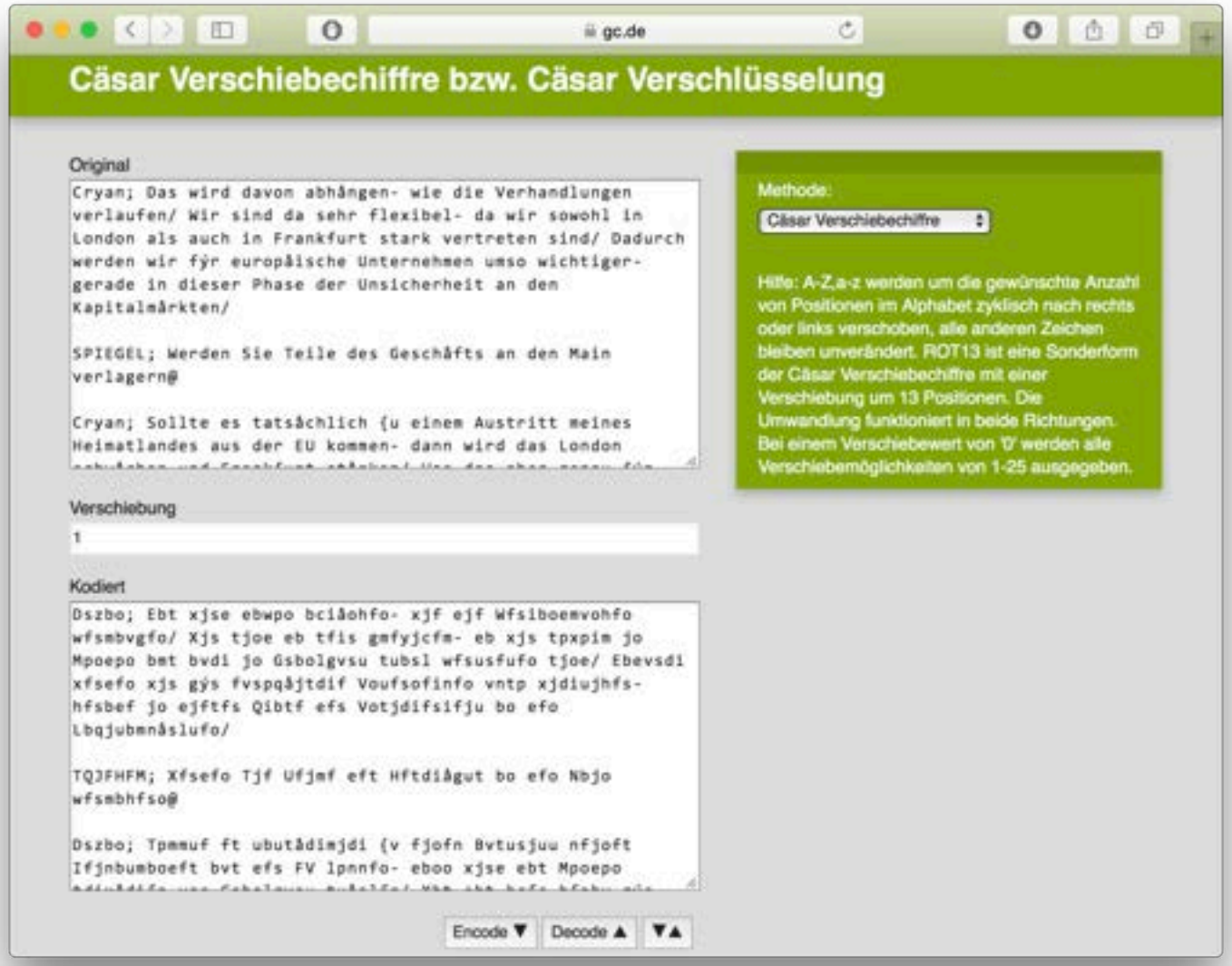
- Wir bezahlen mit unseren Daten
  - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
  - Innere Sicherheit und Überwachung
- Die Internetwirtschaft kann es
  - aber wo bleibt die Innovation?
- Ethische Dimensionen
  - Information Governace Technologies
- Drohnenkrieg
  - Militärischer Einsatz von Informationstechnologie

Beispiel für Verschiebechiffre – Spiegel Plus

Quelle: http://andreas-zeller.blogspot.de/2016/06/spiegel-online-nutzt-unsichere-casar.html



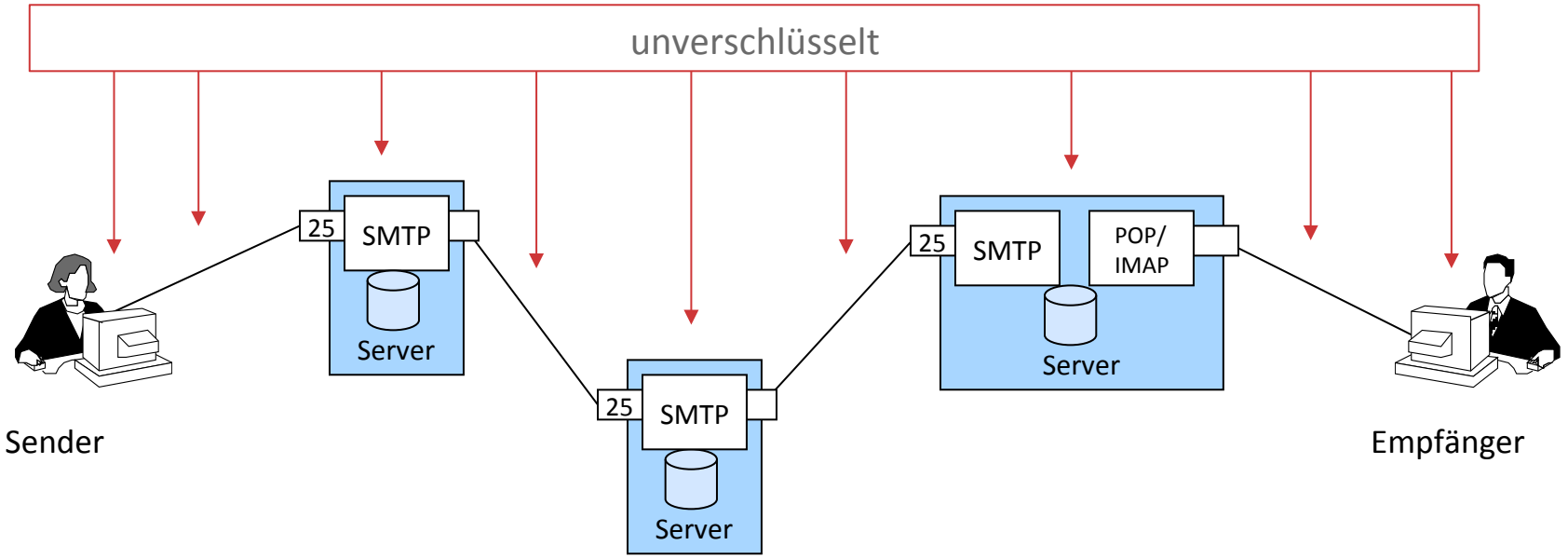
Beispiel für Verschiebechiffre



https://gc.de/gc/caesar/

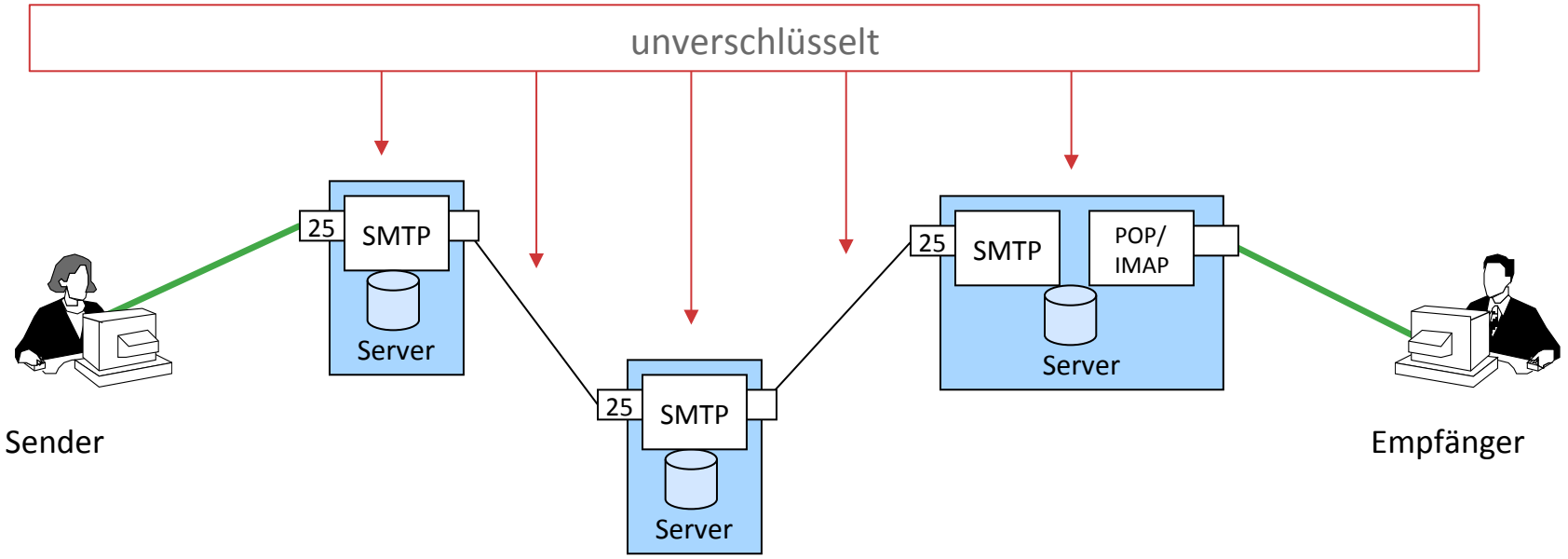
Grundlagen der E-Mail-Kommunikation

- Store & Forward-Prinzip:
  - E-Mail wird nicht direkt an Empfänger, sondern über MTA (Mail Transfer Agents) geschickt
- Senden via SMTP: Textbasiertes Protokoll auf TCP-Port 25
- Empfangen: POP, IMAP



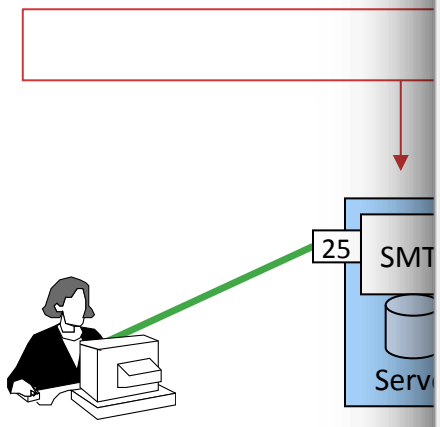
Verbindungsverschlüsselung

- SMTP/POP/IMAP over SSL
  - Verschlüsselte Teilstrecke zwischen
    - Sender und MTA
    - MTA und Empfänger
  - alle MTAs können mitlesen

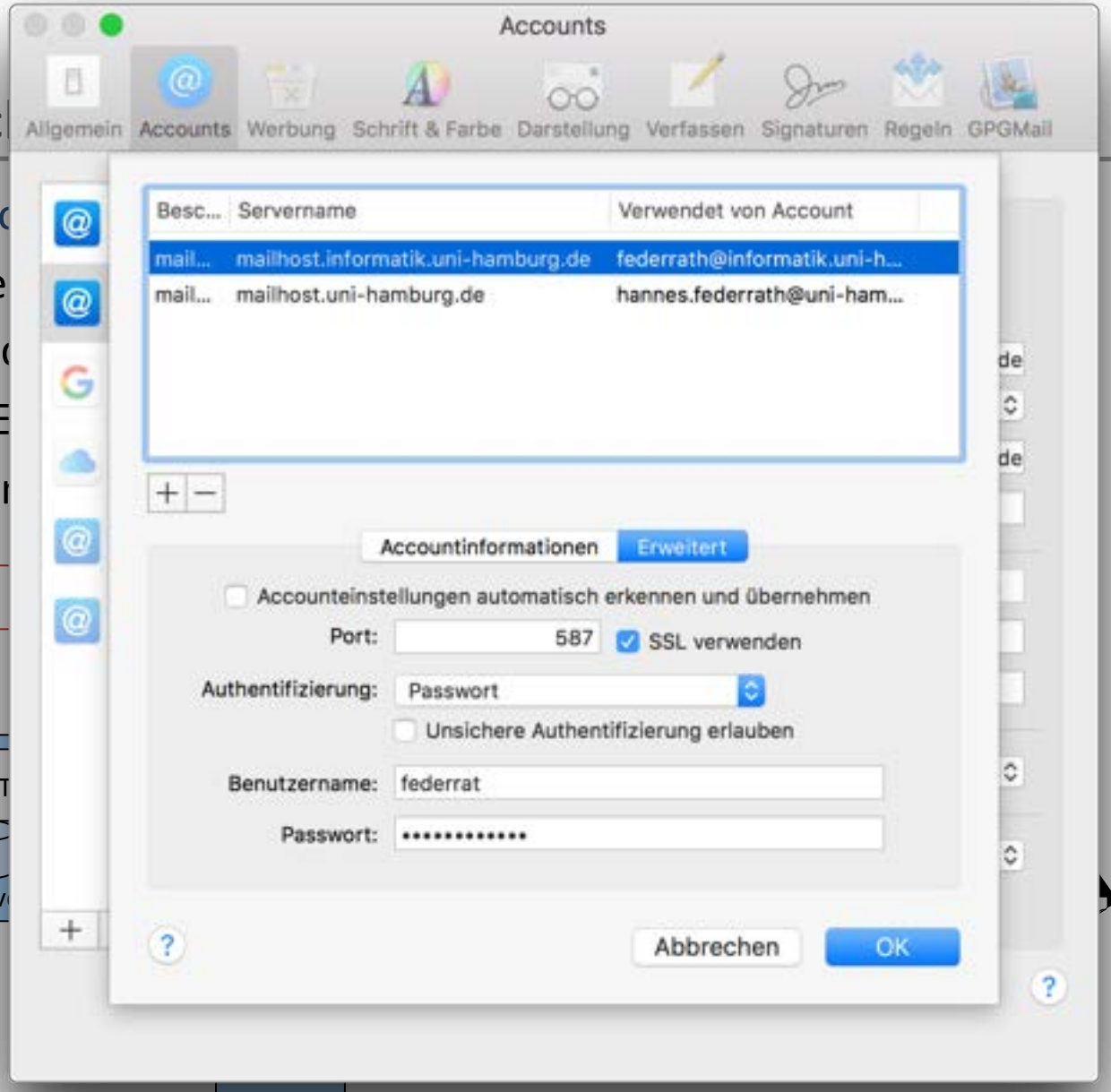


Verbindungsversch

- SMTP/POP/IMAP
  - Verschlüsselte
    - Sender und
    - MTA und E
  - alle MTAs könn

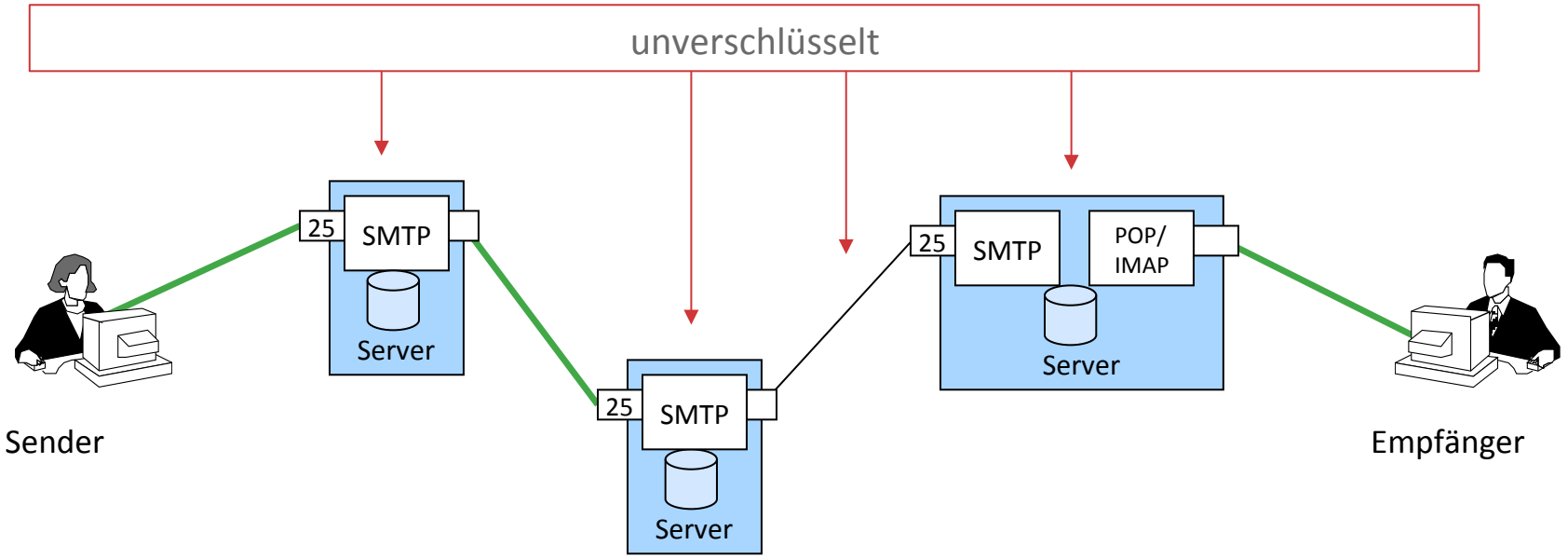


Sender



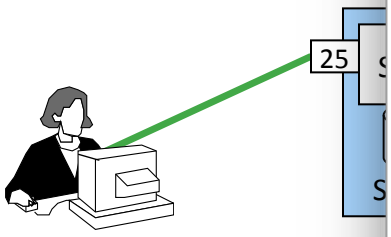
Verbindungsverschlüsselung

- SMTP/POP/IMAP over SSL
- Verschlüsselung zwischen MTAs
  - Verschlüsselte Teilstrecke zwischen MTAs
  - nicht alle Teilstrecken müssen verschlüsselt sein
  - alle MTAs können mitlesen



Verbindungsvers

- SMTP/POP/IMA
- Verschlüsselung
  - Verschlüssel
  - nicht alle Tei
  - alle MTAs kö



Sender

www.heise.de/newsticker/meldung/

heise online

"E-Mail Made in Germany": SSL-Verschlüsselung für (fast) alle

UPDATE

09.08.2013 12:40 Uhr – Detlef Borchers

Die Deutsche Telekom und United Internet haben das Projekt **"E-Mail made in Germany"** [1] in Berlin vorgestellt. Dabei handelt es sich um eine SSL/TSL-Verschlüsselung zwischen den Mail-Servern und Rechenzentren der beteiligten Firmen, die ab sofort genutzt werden kann. Ab 2014 sollen nur noch SSL-verschlüsselte Mails transportiert werden. Rund 20 Millionen Kunden der Telekom und 30 Millionen von GMX und Web.de sollen die "deutsche E-Mail" nutzen können. Sie ist bereits in den Webmailern der beteiligten Firmen freigeschaltet und kommt automatisch zum Einsatz: Bei Eingabe von Empfängeradressen aus dem Mail-Verbund wird eine Information angezeigt, dass die Mails verschlüsselt übertragen werden. Bislang gibt es allerdings noch keine entsprechende Anzeige bei empfangenen Mails.

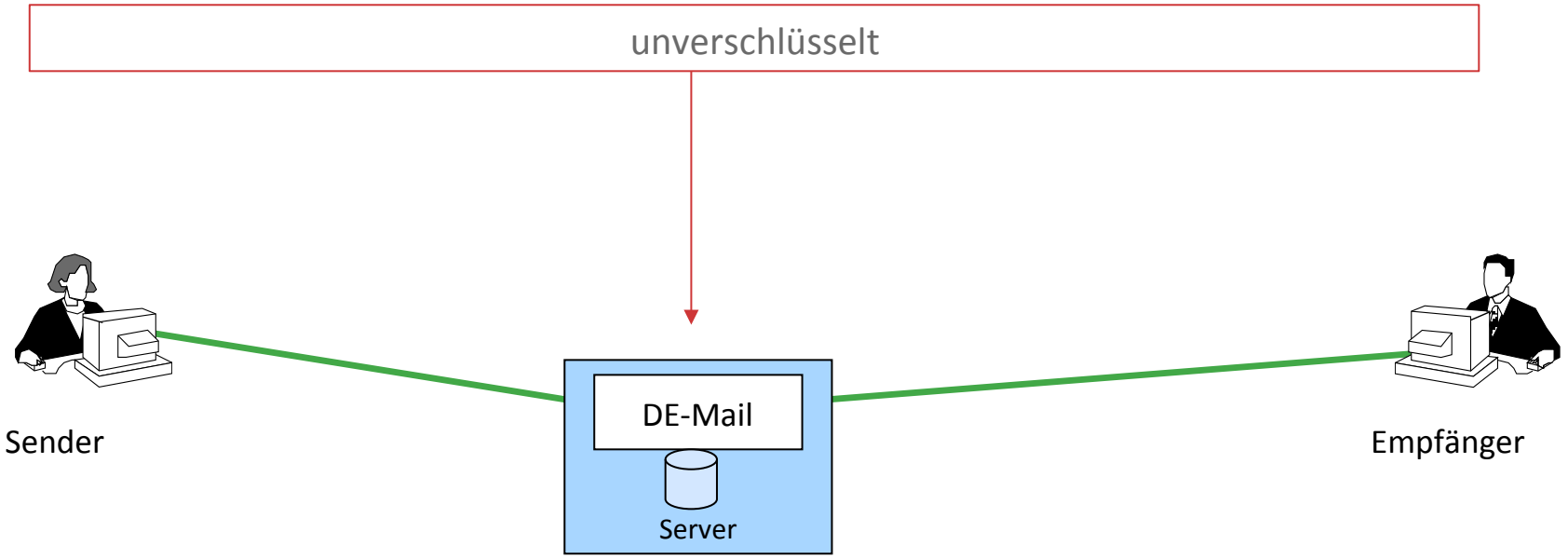
Die Web-Mailer der Telekom, von GMX und web.de zeigen ab sofort an, wenn ein E-Mail-Empfänger aus dem Verschlüsselungs-Verbund "E-Mail made in Germany" kommt.

Wie Telekom-Chef René Obermann erklärte, hofft man, dass sich andere Wettbewerber wie Freenet oder Arcor der deutschen Initiative anschließen werden. Geprüft werde derzeit, wie die Tochterfirmen Strato (Telekom) und 1&1 (United Internet) in das System eingebunden werden können, damit auch Kleingewerbetreibende mit Domains wie z.B. Obermann.de die sichere deutsche "Mail made in Germany" nutzen können. Zudem hofft Obermann darauf, dass aus der deutschen Initiative eine europäische wird. Ralph Dommermuth von United Internet erklärte, dass 90 Prozent der Mail innerhalb von Deutschland ausgetauscht werde und somit die "E-Mail made in Germany" zum Standard werde.

Meldung: https://heise.de/-1932962

Verbindungsverschlüsselung

- Sicherheit von DE-Mail etc.
  - gleiche Sicherheit wie «E-Mail Made in Germany»
  - keine Ende-zu-Ende-Verschlüsselung
  - Server kann mitlesen



Verbindungsverschlüsselung

- Sicherheit von DE-Mail etc.
  - gleiche Sicherheit wie «E-Mail Made in Germany»
  - keine Ende-zu-Ende-Verschlüsselung
  - Server kann mitlesen

Systeme von Absender und Empfänger die Identität der jeweils anderen Seite sicherstellen können. Eine Möglichkeit hierfür ist der Einsatz digitaler Zertifikate.

- Eine abschnittsweise Verschlüsselung der Übertragungswege soll Sicherheit gegen den Zugriff durch Unbefugte bieten.

Quelle: Wikipedia

Bei besonders hohen Anforderungen an die Vertraulichkeit der Nachrichten haben De-Mail-Nutzer wie bei herkömmlichen E-Mails die Möglichkeit, die mit De-Mail übermittelten Inhalte noch zusätzlich selbst zu verschlüsseln („Ende-zu-Ende-Verschlüsselung"). In diesem Fall erfolgt die Verschlüsselung auf dem Rechner des Absenders und die Entschlüsselung der Inhalte erst auf dem Rechner des Empfängers. Hierfür ist jedoch die Installation zusätzlicher Software erforderlich, die die Ver- und Entschlüsselung durchführt. Der Verzeichnisdienst, der bei De-Mail obligatorisch durch den Diensteanbieter angeboten werden muss, unterstützt den Anwender, indem dieser seinen öffentlichen Schlüssel anderen Anwendern zur Verfügung stellen kann. Es soll also ermöglicht werden, an einer zentralen Stelle nach öffentlichen Schlüsseln von Personen suchen zu können, um mit diesen vertraulich zu kommunizieren. Dies ist bisher nur schwer möglich und stellt den wesentlichen „Hemmschuh" für die Verbreitung von Verfahren zur Ende-zu-Ende-Verschlüsselung („Wo finde ich den gültigen Verschlüsselungsschlüssel meines Kommunikationspartners?"). Mit De-Mail soll auf diese Weise der Einsatz der Ende-zu-Ende-Verschlüsselung unterstützt und gefördert werden.

S/MIME oder OpenPGP können zusätzlich durch den Nutzer für die Abbildung der Ende-zu-Ende-Sicherheit eingesetzt werden. Die Liste der hauptsächlichen Sicherheitsfunktionen wurden in einem Dokument des BMI zusammengefasst.

Technische Konzeption [Bearbeiten | Quelltext bearbeiten]

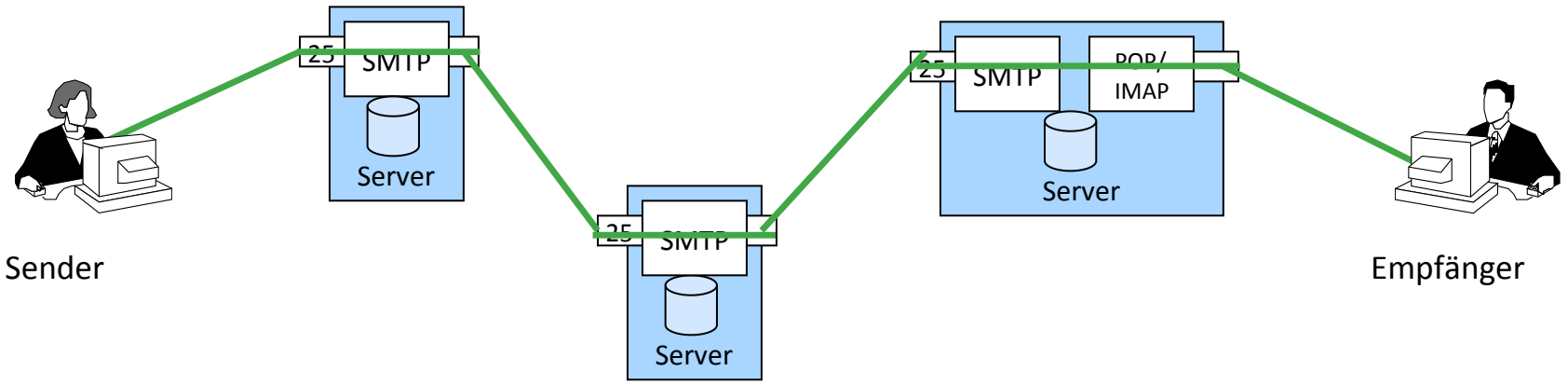
Das technische Konzept ist innerhalb von technischen Richtlinien beschrieben, die auf der Web-Seite des BSI[19] veröffentlicht sind.

Standardmäßige Transportsicherheit [Bearbeiten | Quelltext bearbeiten]

Sowohl die Kommunikation der De-Mail-Nutzer mit ihren De-Mail-Provider als auch die Kommunikation von De-Mail-Anbietern untereinander verläuft grundsätzlich über TLS-gesicherte Kommunikationskanäle.[5] Reicht einem Nutzer das dadurch realisierte Sicherheitsniveau nicht

Ende-zu-Ende-Verschlüsselung schützt die Vertraulichkeit

- Ende-zu-Ende-Verschlüsselung
  - Inhalte sind durchgehend verschlüsselt
  - MTAs (Server) können nicht mitlesen
  - Adressierungsinformation kann nicht mit verschlüsselt werden
- Konkrete Ende-zu-Ende-Verschlüsselungslösungen
  - S/MIME
  - PGP



Ende-zu-Ende-Verschlüsselung schützt die Vertraulichkeit

- Verschlüsselte E-Mail (schematisch):

Von: alice@example.de

An: bob@mail.com

Betreff: Abendessen

-----BEGIN ENCRYPTED MESSAGE-----
AkRFMRcwFQYDVQQDEw5Sb2xmIFdlbmRvbHNreTEUMBI
GA1UECBMLRGV1dHNjaGxhbmxEzARBgNVBAcTClJlZ2V
uc2J1cmcxDzANBgNVBAoTBnBaXZhdDEkMCIGCSqGSIb
3DQEJARYVcm9sZi53ZW5kxza3lAZ214LmRlMIGfMA0G
CSqGSIb3DQEBAQUAA4GNABDCBiQKBgQDUVvgaQK9OQP
XvgZm2bU/QqDnsbemv83gDiSuCq07S/cSMiGFjEZas6
5MZ47W951LlNLvFTjwS2fUfsZ5oAxfU+RDWb3GgijZp
5cAxTfFKQ/amaWAtmCkt1FMntRXZ393gOkSSUlWQ7Cr
6GWAYF+deC5CuWptRPpSLYRqSwIDAQABMA0GCSqGSIb
3DQEBBAUAA4GBAIGVTNbu0eOTfGuuL0MWHLfVD
-----END ENCRYPTED MESSAGE-----

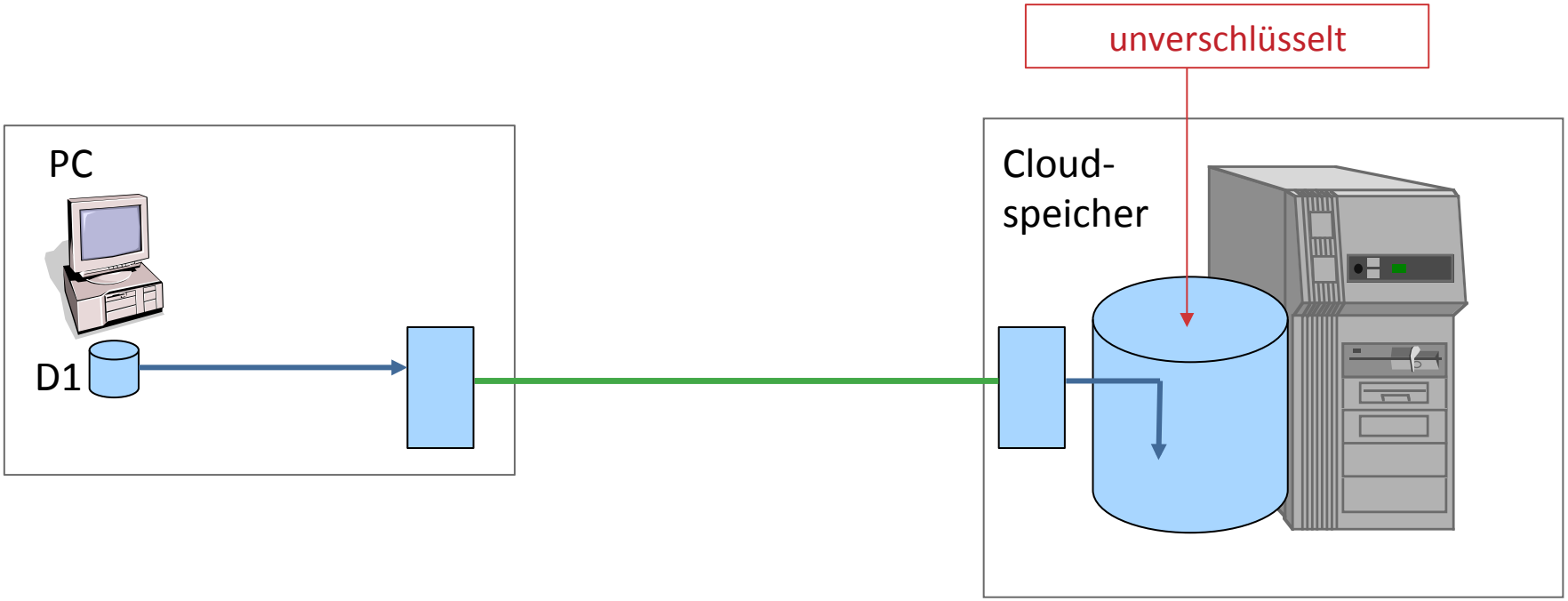
Konkrete Ende-zu-Ende-Verschlüsselungslösungen

- S/MIME (Secure Multipurpose Internet Mail Extensions)
  - ursprünglich von RSA Data Security Inc.
  - S/MIME v3 im Juli 1999 als IETF-Standard verabschiedet
  - in die meisten E-Mail-Clients integriert
  - One-pass processing: Die Mail ist in einem Schritt verarbeitbar, da alle benötigten Daten in die Mail selbst integriert sind

- PGP (Pretty Good Privacy)
  - 1991 von Philip Zimmermann entwickelt
  - heute: Open PGP, GnuPG (Gnu Privacy Guard)
  - Zahlreiche grafische Frontends erhältlich, z.B. GPA, WinPT
  - Plugins für verschiedene Mailclients, z.B. Outlook, Thunderbird, Pegasus, KMail

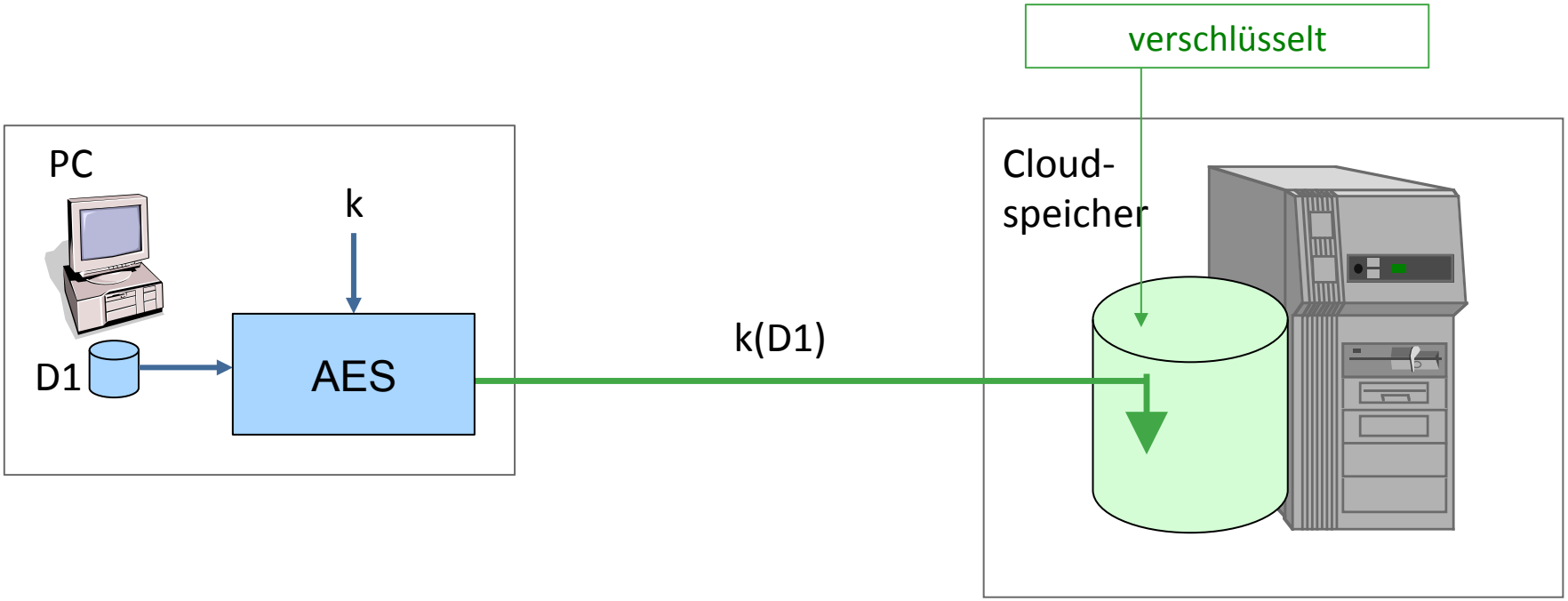
Verschlüsselte Cloud-Speicher

- Verbindungsverschlüsselung ist heute Standard

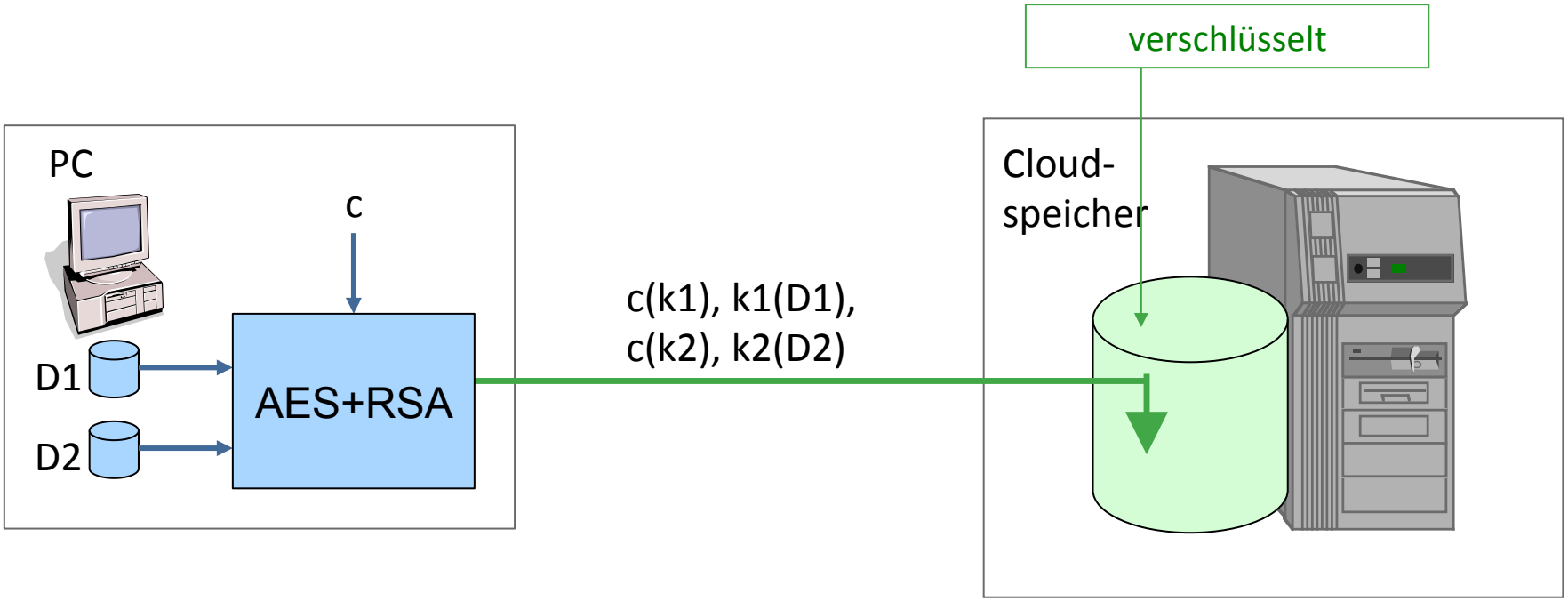


Verschlüsselte Cloud-Speicher

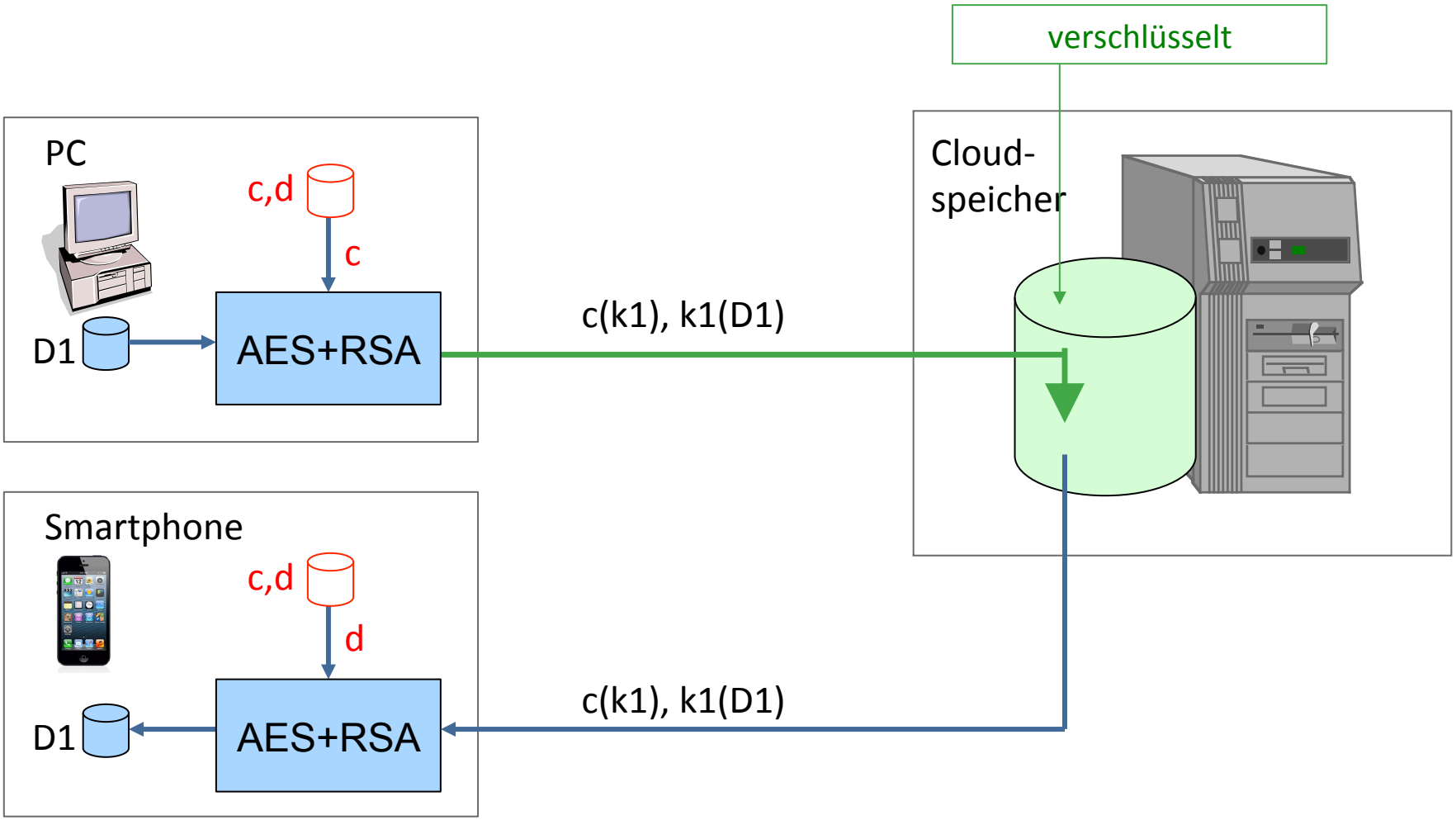
- Ende-zu-Ende-Verschlüsselung wäre kein Problem



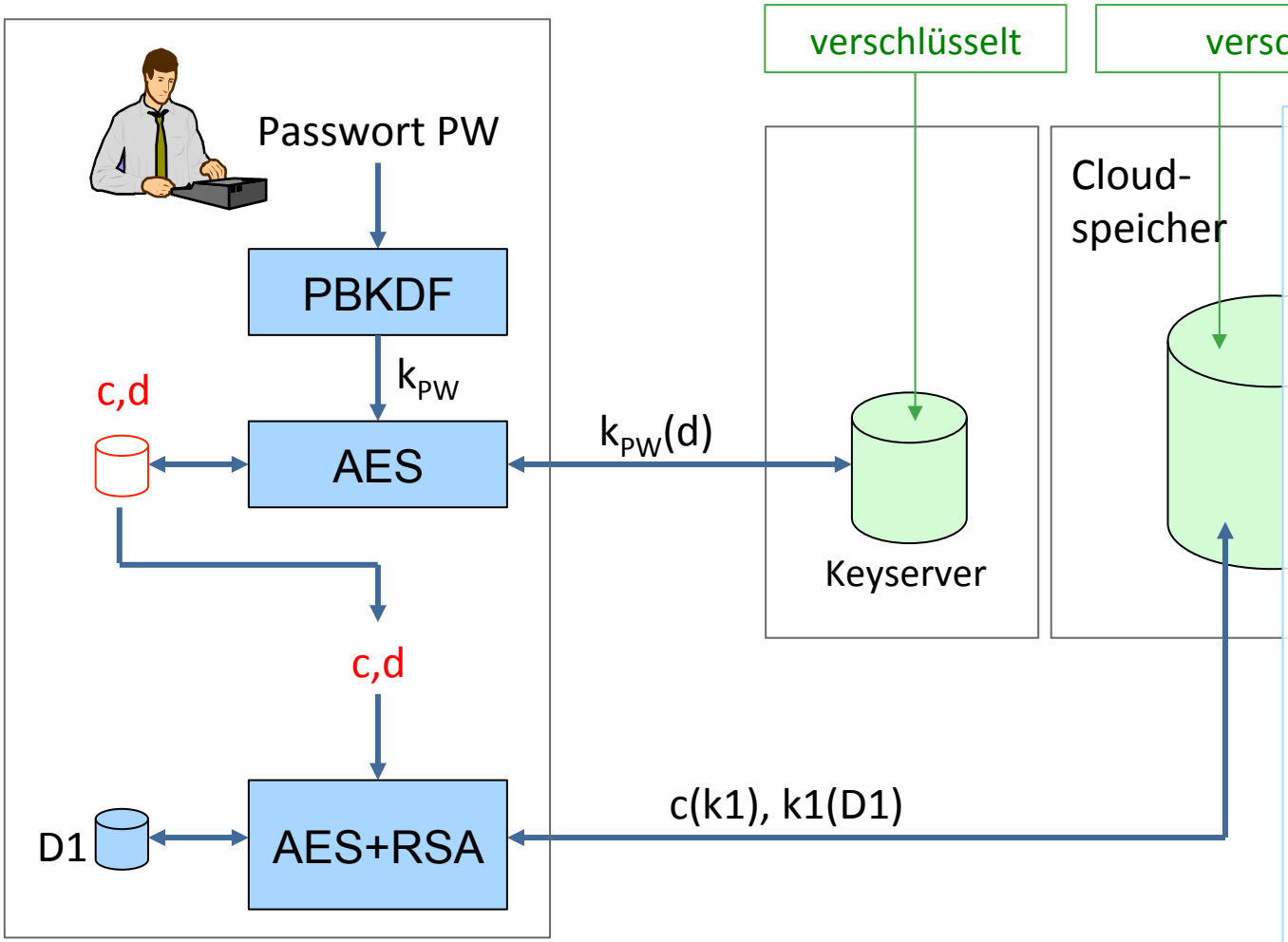
- Ende-zu-Ende-Verschlüsselung besser hybrid …



- Wie bekommt der Nutzer auf alle seine Geräte seine(n) Schlüssel?

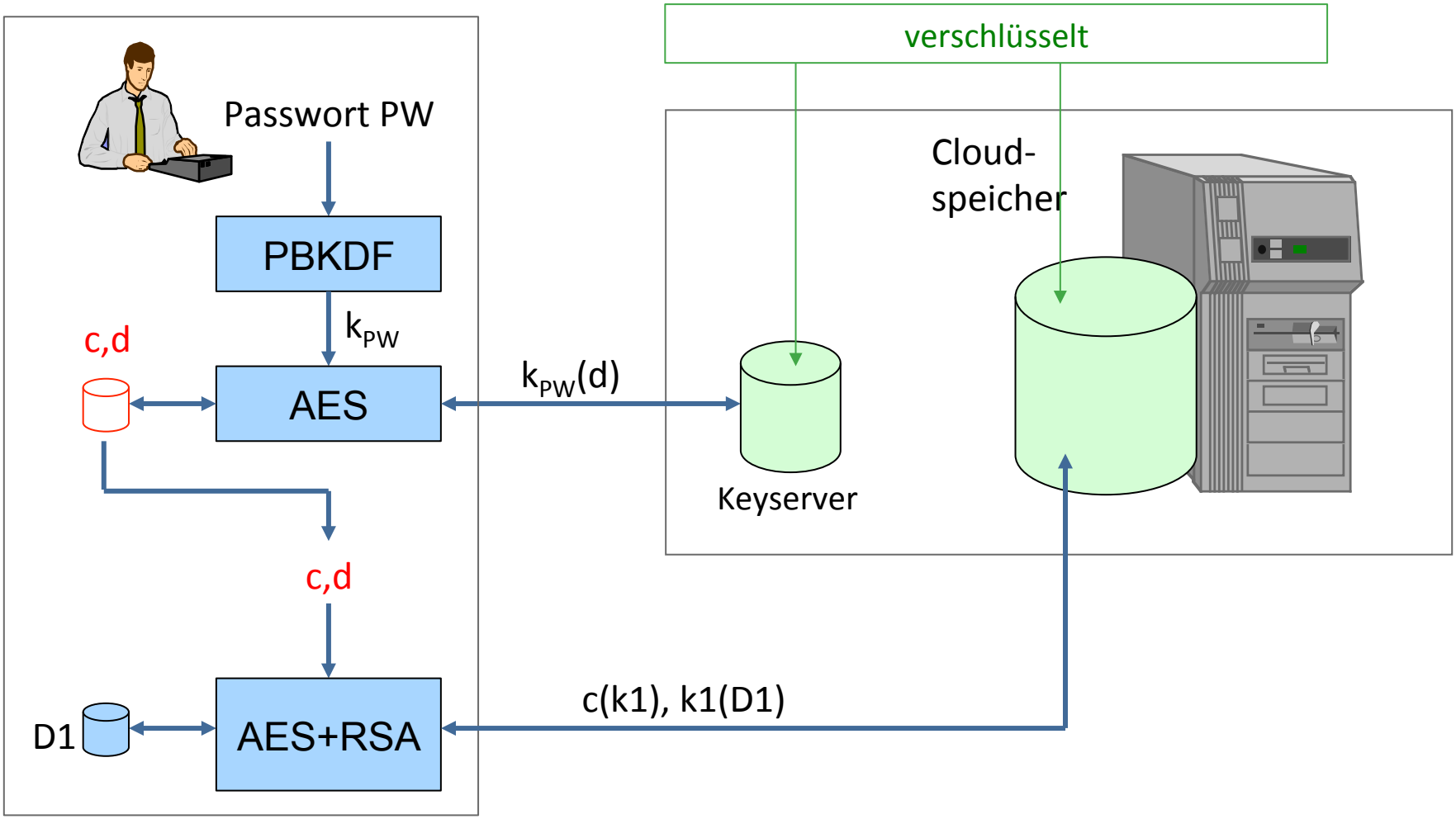


- Wie bekommt der Nutzer auf alle seine Geräte seine(n) Schlüssel?



- Das Schlüsselpaar c,d wird lokal beim Nutzer erzeugt.
- Aus dem Passwort PW wird ein symm. Schlüssel k_{PW} (Passwortschlüssel) abgeleitet.
- Mit dem Passwortschlüssel wird der private Schlüssel d verschlüsselt.
- Auf dem Keyserver werden abgelegt: Nutzername, c, $k_{PW}(d)$.
- Andere Geräte können sich den (verschlüsselten) privaten Schlüssel holen und nur bei Kenntnis von PW entschlüsseln. Der Betreiber des Keyservers erfährt nichts über d und alle damit verschlüsselten Schlüssel.

- Wie bekommt der Nutzer auf alle seine Geräte seine(n) Schlüssel?



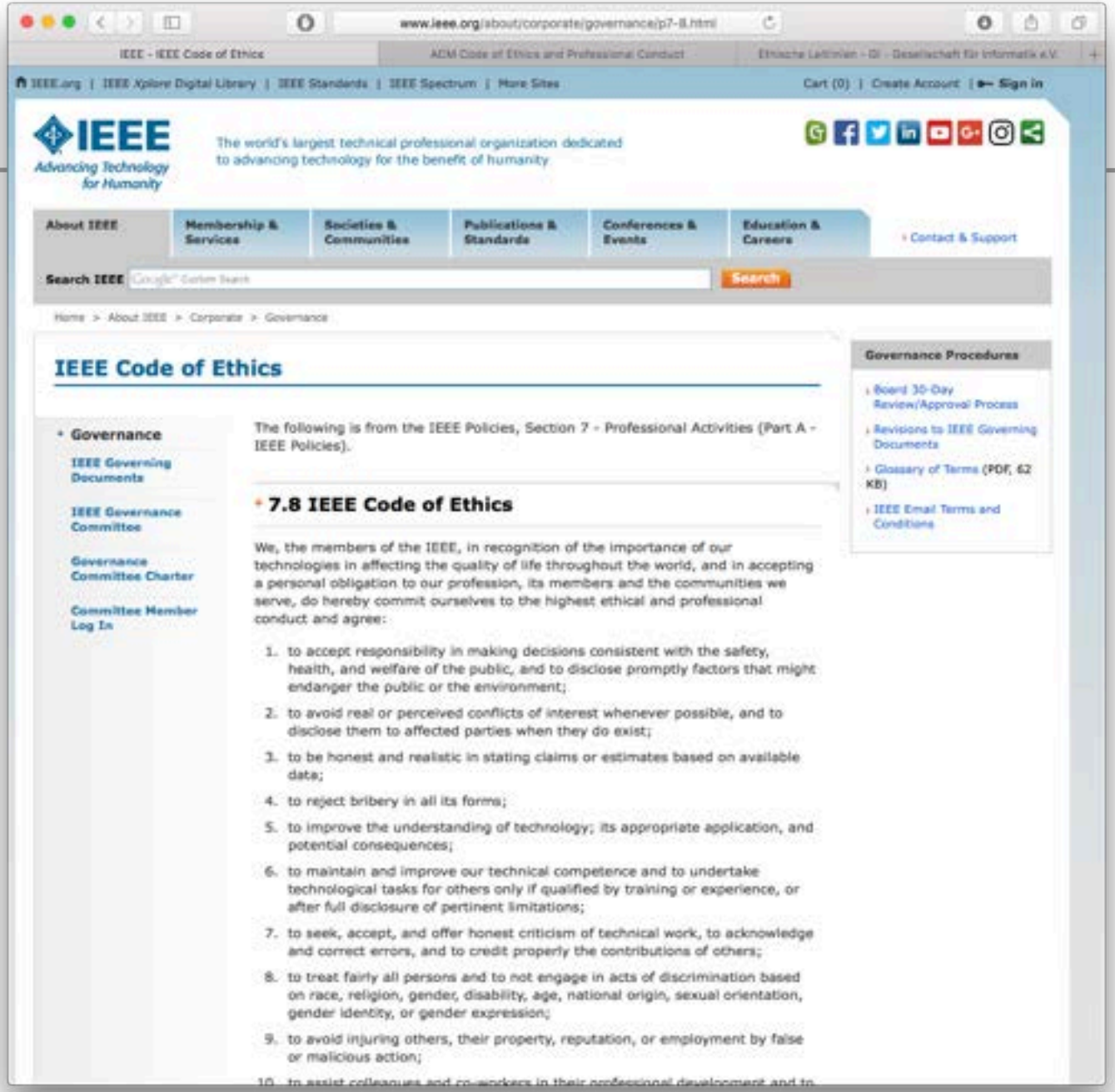
Ethische Dimensionen

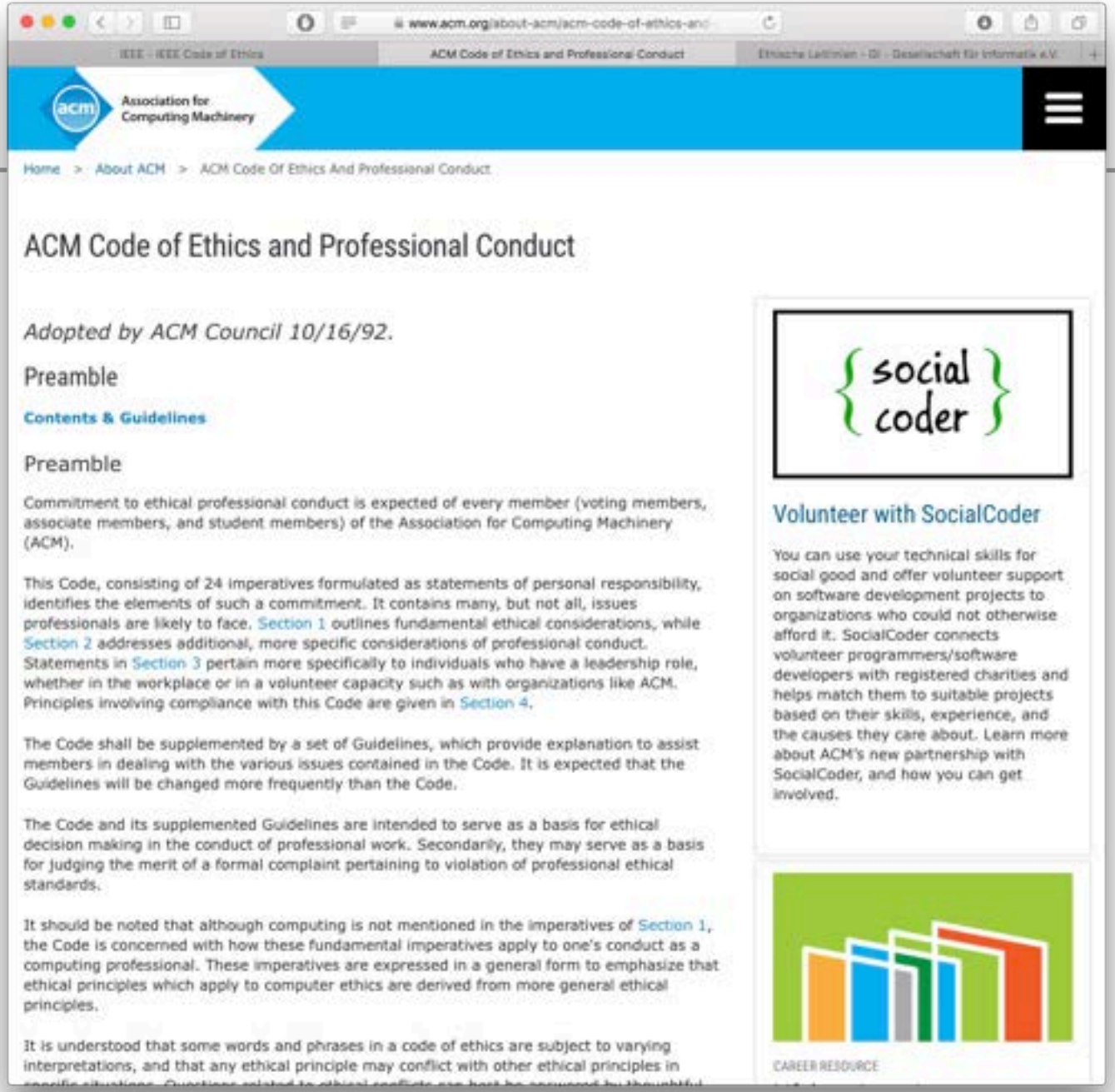
- Dreiteilung nach Simon, 2016:
  - Ethik des Berufs
  - Ethik des Designs
  - Ethik der Nutzung

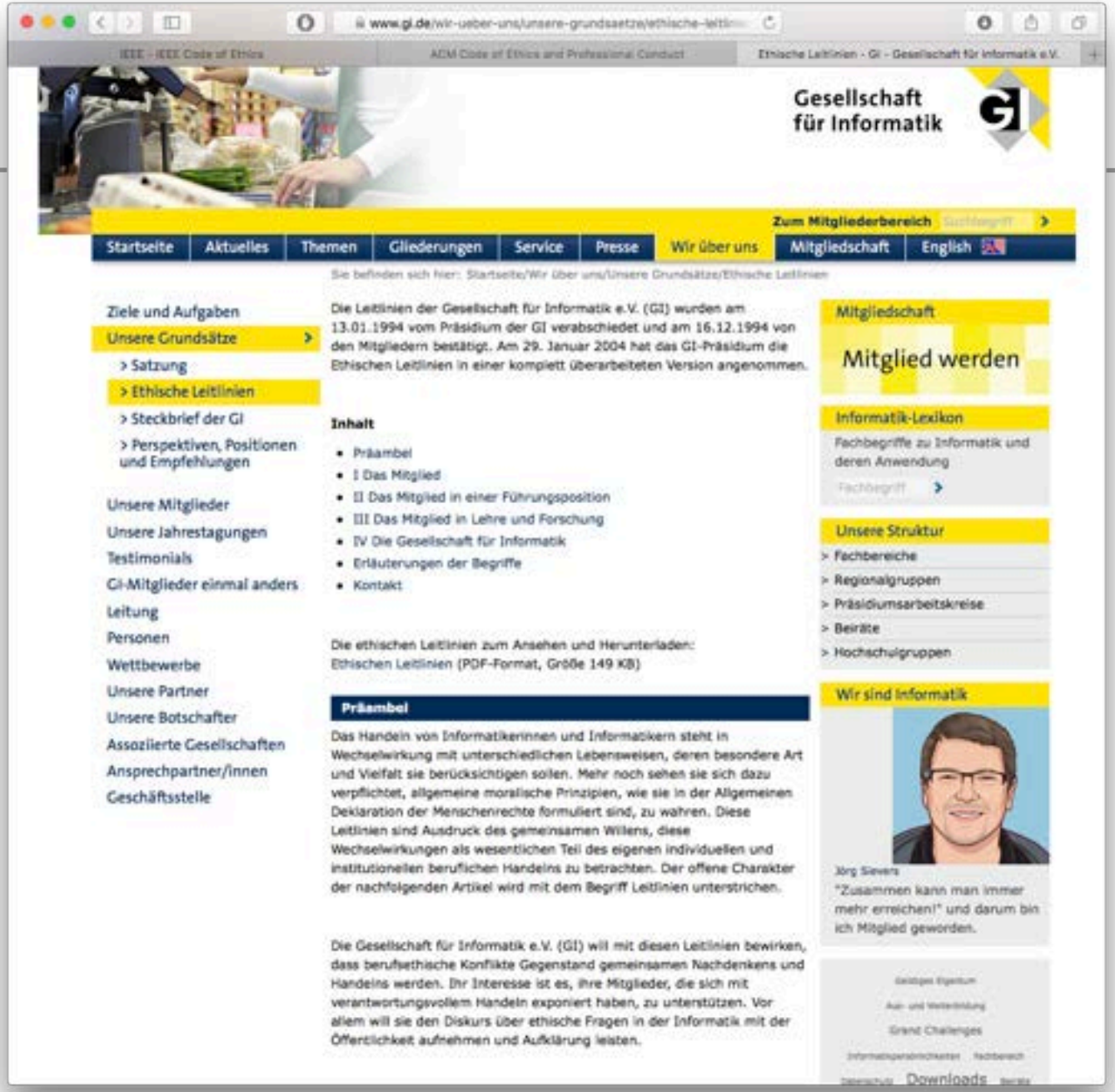
Ethische Leitlinien der Gesellschaft für Informatik

ACM Code of Ethics and Professional Conduct

IEEE Code of Ethics

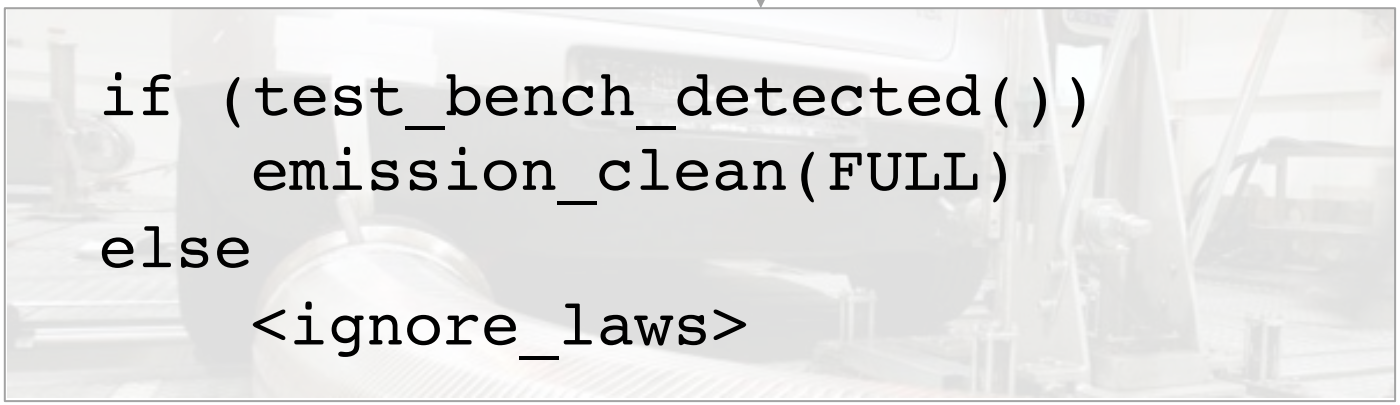

www.ieee.org/about/corporate/governance/p7-8.html
IEEE - IEEE Code of Ethics
ACM Code of Ethics and Professional Conduct
Ethische Leitlinien - GI - Gesellschaft für Informatik e.V.
IEEE.org | IEEE Xplore Digital Library | IEEE Standards | IEEE Spectrum | More Sites
Cart (0) | Create Account | Sign in
IEEE
Advancing Technology for Humanity
The world's largest technical professional organization dedicated to advancing technology for the benefit of humanity
About IEEE
Membership & Services
Societies & Communities
Publications & Standards
Conferences & Events
Education & Careers
Contact & Support
Search IEEE
Search
Home > About IEEE > Corporate > Governance
IEEE Code of Ethics
Governance
IEEE Governing Documents
IEEE Governance Committee
Governance Committee Charter
Committee Member Log In
The following is from the IEEE Policies, Section 7 - Professional Activities (Part A - IEEE Policies).
7.8 IEEE Code of Ethics
We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:
1. to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology; its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
Governance Procedures
Board 30-Day Review/Approval Process
Revisions to IEEE Governing Documents
Glossary of Terms (PDF, 62 KB)
IEEE Email Terms and Conditions


www.acm.org/about-acm/acm-code-of-ethics-and
IEEE - IEEE Code of Ethics
ACM Code of Ethics and Professional Conduct
Ethische Leitlinien - GI - Gesellschaft für Informatik e.V.
Association for Computing Machinery
Home > About ACM > ACM Code Of Ethics And Professional Conduct
ACM Code of Ethics and Professional Conduct
Adopted by ACM Council 10/16/92.
Preamble
Contents & Guidelines
Preamble
Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).
This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4.
The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.
The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.
It should be noted that although computing is not mentioned in the imperatives of Section 1, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.
It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in
social coder
Volunteer with SocialCoder
You can use your technical skills for social good and offer volunteer support on software development projects to organizations who could not otherwise afford it. SocialCoder connects volunteer programmers/software developers with registered charities and helps match them to suitable projects based on their skills, experience, and the causes they care about. Learn more about ACM's new partnership with SocialCoder, and how you can get involved.
CAREER RESOURCE

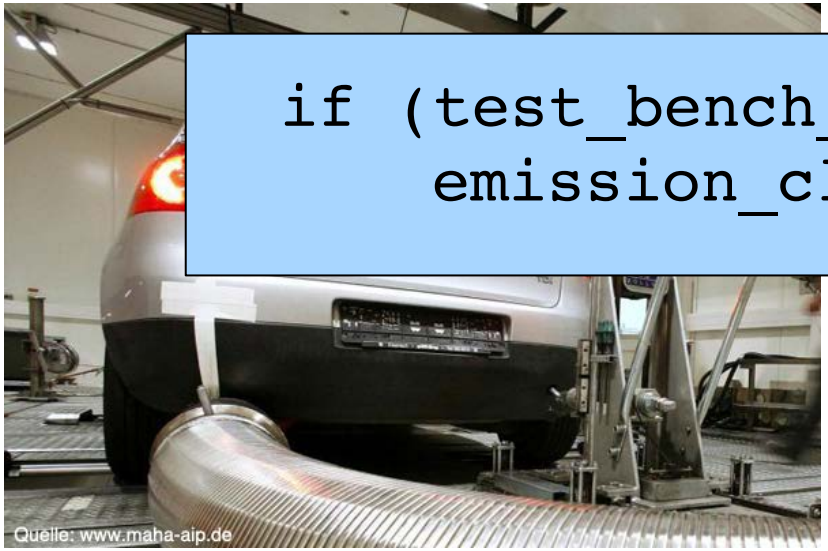

www.gi.de/wir-ueber-uns/unsere-grundsaetze/ethische-leitlinien
IEEE - IEEE Code of Ethics
ACM Code of Ethics and Professional Conduct
Ethische Leitlinien - GI - Gesellschaft für Informatik e.V.
Gesellschaft für Informatik
Zum Mitgliederbereich
Startseite
Aktuelles
Themen
Gliederungen
Service
Presse
Wir über uns
Mitgliedschaft
English
Sie befinden sich hier: Startseite/Wir über uns/Unsere Grundsätze/Ethische Leitlinien
Ziele und Aufgaben
Unsere Grundsätze
> Satzung
> Ethische Leitlinien
> Steckbrief der GI
> Perspektiven, Positionen und Empfehlungen
Unsere Mitglieder
Unsere Jahrestagungen
Testimonials
GI-Mitglieder einmal anders
Leitung
Personen
Wettbewerbe
Unsere Partner
Unsere Botschafter
Assoziierte Gesellschaften
Ansprechpartner/innen
Geschäftsstelle
Die Leitlinien der Gesellschaft für Informatik e.V. (GI) wurden am 13.01.1994 vom Präsidium der GI verabschiedet und am 16.12.1994 von den Mitgliedern bestätigt. Am 29. Januar 2004 hat das GI-Präsidium die Ethischen Leitlinien in einer komplett überarbeiteten Version angenommen.
Inhalt
Präambel
I Das Mitglied
II Das Mitglied in einer Führungsposition
III Das Mitglied in Lehre und Forschung
IV Die Gesellschaft für Informatik
Erläuterungen der Begriffe
Kontakt
Die ethischen Leitlinien zum Ansehen und Herunterladen:
Ethischen Leitlinien (PDF-Format, Größe 149 KB)
Präambel
Das Handeln von Informatikerinnen und Informatikern steht in Wechselwirkung mit unterschiedlichen Lebensweisen, deren besondere Art und Vielfalt sie berücksichtigen sollen. Mehr noch sehen sie sich dazu verpflichtet, allgemeine moralische Prinzipien, wie sie in der Allgemeinen Deklaration der Menschenrechte formuliert sind, zu wahren. Diese Leitlinien sind Ausdruck des gemeinsamen Willens, diese Wechselwirkungen als wesentlichen Teil des eigenen individuellen und institutionellen beruflichen Handelns zu betrachten. Der offene Charakter der nachfolgenden Artikel wird mit dem Begriff Leitlinien unterstrichen.
Die Gesellschaft für Informatik e.V. (GI) will mit diesen Leitlinien bewirken, dass berufsethische Konflikte Gegenstand gemeinsamen Nachdenkens und Handelns werden. Ihr Interesse ist es, ihre Mitglieder, die sich mit verantwortungsvollem Handeln exponiert haben, zu unterstützen. Vor allem will sie den Diskurs über ethische Fragen in der Informatik mit der Öffentlichkeit aufnehmen und Aufklärung leisten.
Mitgliedschaft
Mitglied werden
Informatik-Lexikon
Fachbegriffe zu Informatik und deren Anwendung
Unsere Struktur
> Fachbereiche
> Regionalgruppen
> Präsidiumsarbeitskreise
> Beiräte
> Hochschulgruppen
Wir sind Informatik
Jörg Sievers
"Zusammen kann man immer mehr erreichen!" und darum bin ich Mitglied geworden.
Downloads

Ethische Dimensionen

- Dreiteilung nach Simon, 2016:
  - Ethik des Berufs
  - Ethik des Designs
  - Ethik der Nutzung

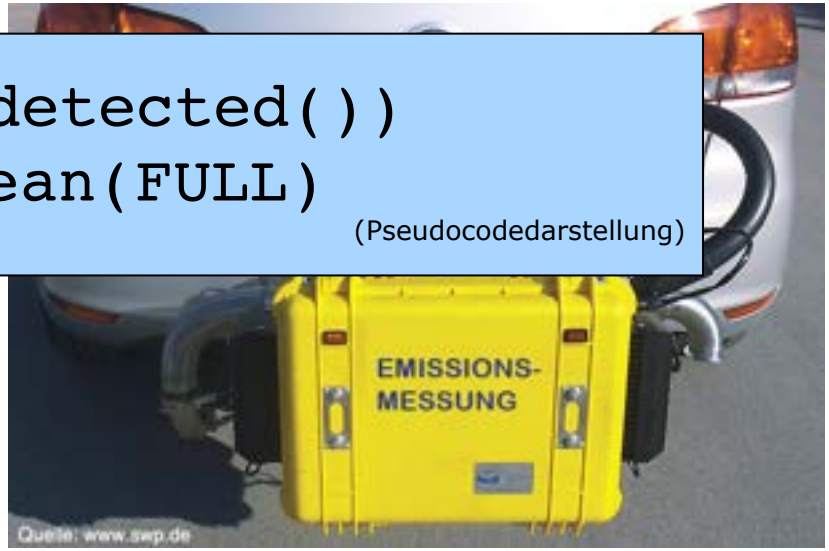


Abgasmessungen auf dem Prüfstand und mobil




```
if (test_bench_detected())
    emission_clean(FULL)
```

(Pseudocodedarstellung)



- Adaptive Motorsteuerung erkennt anhand von Lenkradbewegungen, Umgebungsluftdruck, Raddrehzahlen und Motorlaufzeit die Messbedingungen

	Abgasreinigung	Kraftstoffverbrauch
Prüfstand	verbessert	hoch
Straße	reduziert	verringert

Verkehrszeichenerkennung mittels maschineller Lernverfahren

ERKENNUNG

REALITÄT	Gefahr	»normal«
Gefahr	richtig positiv	falsch negativ
»normal«	falsch positiv	richtig negativ

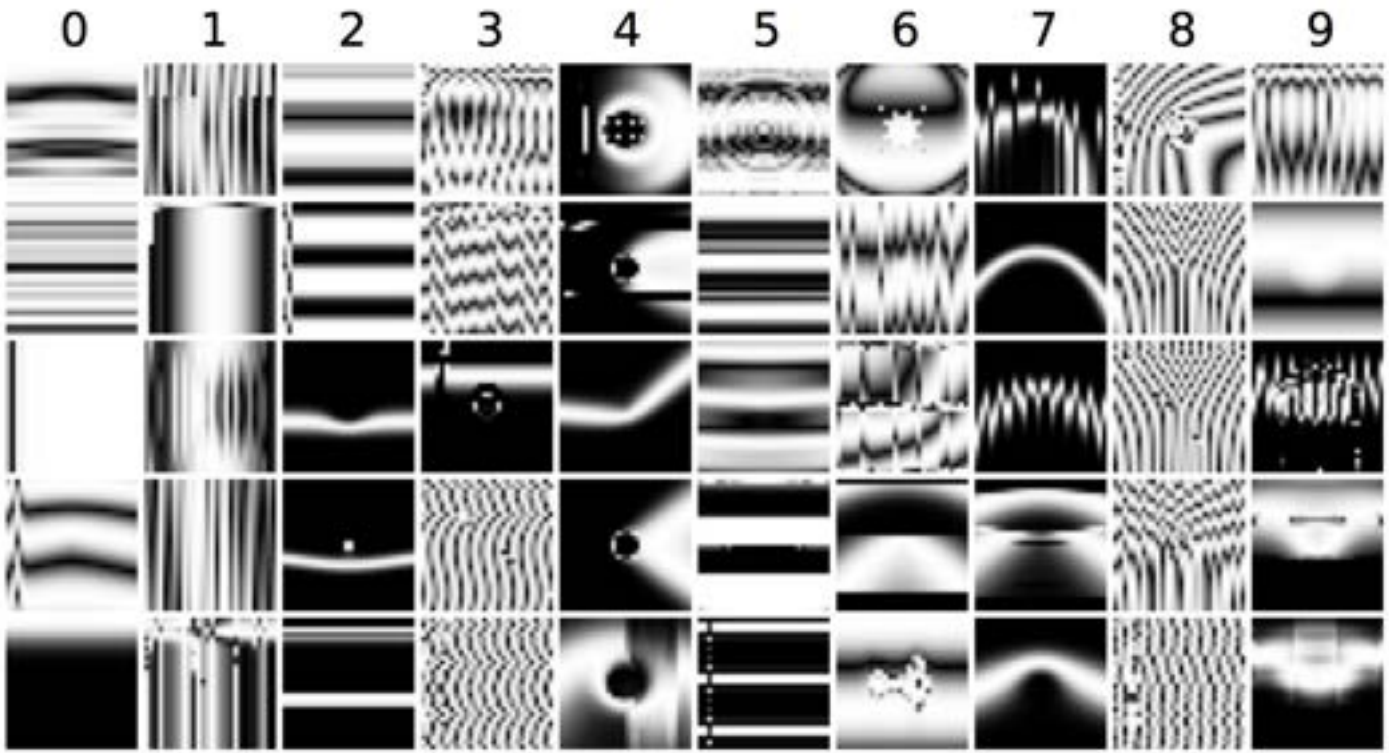
J. Stallkamp, M. Schlipsing, J. Salmen, C. Igel, Man vs. computer: Benchmarking machine learning algorithms for traffic sign recognition, Neural Networks, Volume 32, August 2012, Pages 323-332, ISSN 0893-6080

Verkehrszeichenerkennung mittels maschineller Lernverfahren

…klappt leider nicht immer

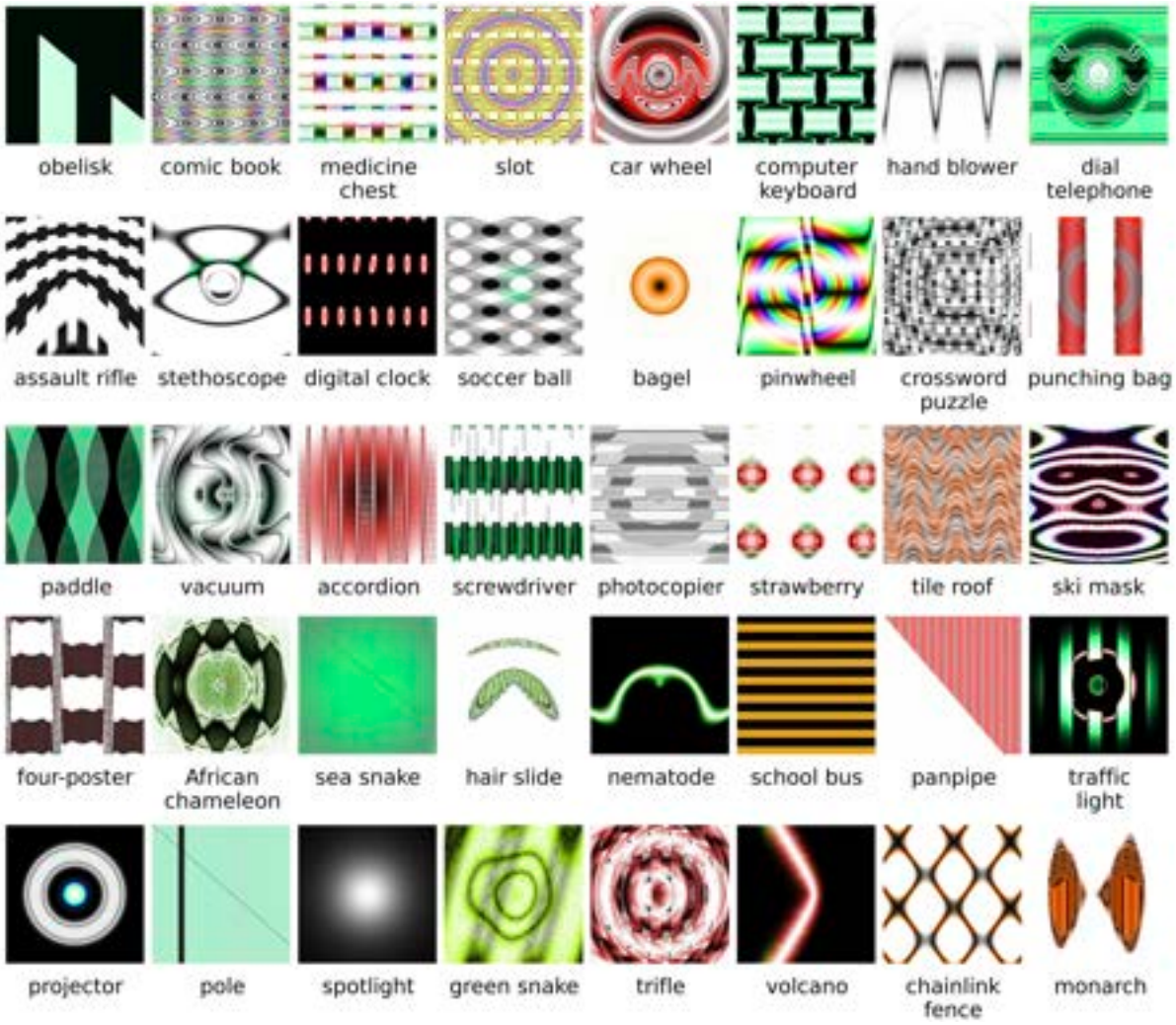
Erkannte Ziffer

Eingabedaten, die fälschlicherweise als Ziffer erkannt werden



Nguyen A, Yosinski J, Clune J. Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images. In CVPR ’15, IEEE, 2015.

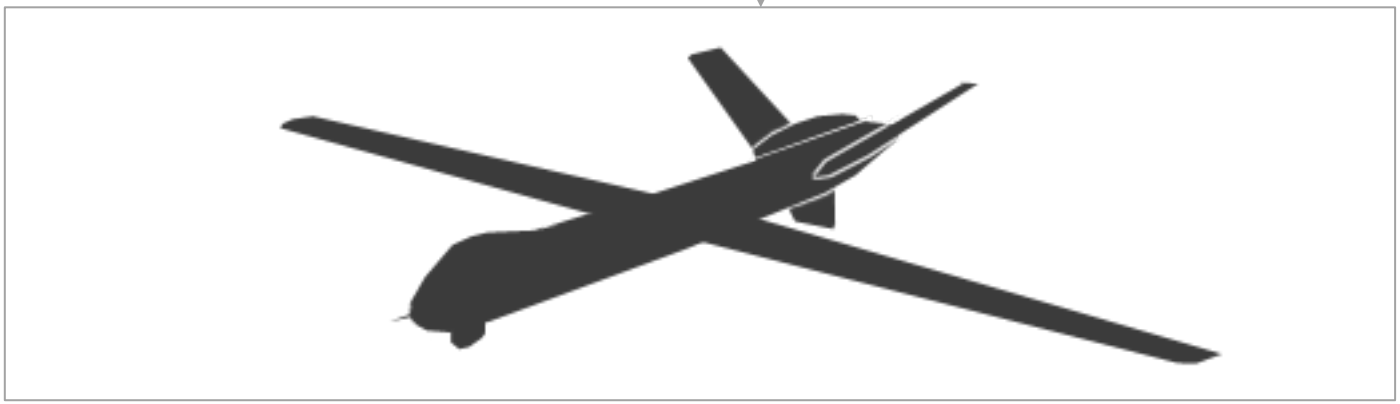
Gezielte Manipulationen eines autonomen Fahrzeugs möglich



Nguyen A, Yosinski J, Clune J. Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images. In CVPR ’15, IEEE, 2015.

Ethische Dimensionen

- Dreiteilung nach Simon, 2016:
  - Ethik des Berufs
  - Ethik des Designs
  - Ethik der Nutzung



Militärischer Einsatz von Informationstechnologie

Aufklärungsdrohne Heron 1 und deren Steuerung

Bilder: www.bundeswehr.de

- Spannungsfeld:
  - Fern-Aufklärung mittels Informationstechnik √
  - Fern-Tötung mittels Informationstechnik ?

Aus dem Beweisbeschluss SV-14 vom 7. Juli 2016 des 1. Untersuchungsausschusses der 18. Wahlperiode des Deutschen Bundestages:

«… Ist unter Berücksichtigung der festgestellten Bedingungen eine Telefonnummer – beziehungsweise eine IMEI- oder IMSI-Identifizierung – als einziges technisches Datum mittelbar oder unmittelbar ausreichend, um eine Fernlenkwaffe mit hinreichender Treffergenauigkeit für eine gezielte Tötung einsetzen zu können? …»

Geleakte Fassung unter https://tinyurl.com/gtv552j

Bild: https://upload.wikimedia.org/wikipedia/commons/3/33/MQ-9_Reaper_-_090609-F-0000M-777.JPG

IMSI-Catcher in Drohne simuliert Mobilfunkzelle

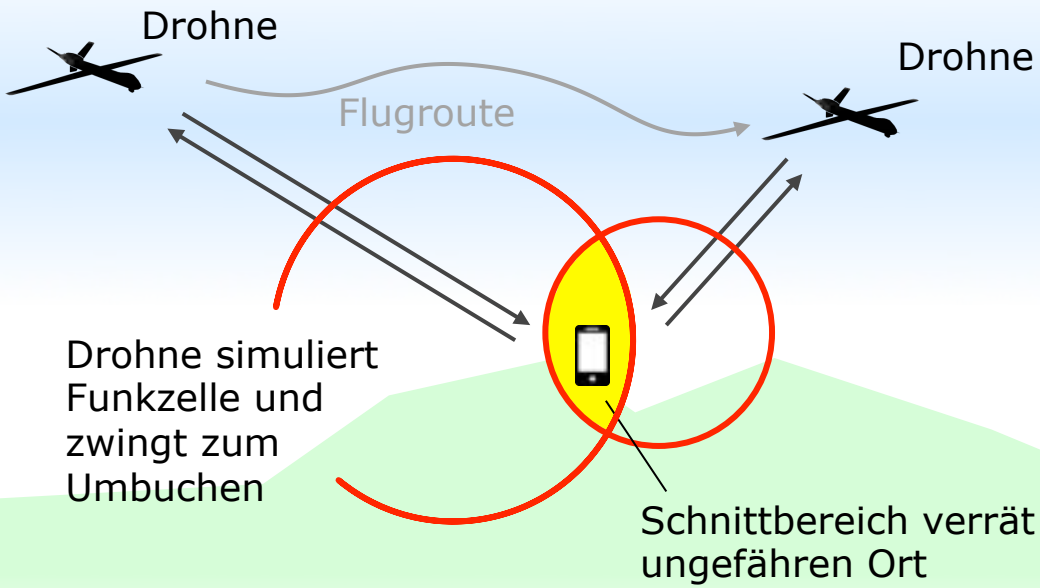
MFG wählt sich in die Funkzelle ein und es werden IMSI/TMSI und IMEI übertragen

Drohne bestimmt Empfangsrichtung der Funkwellen

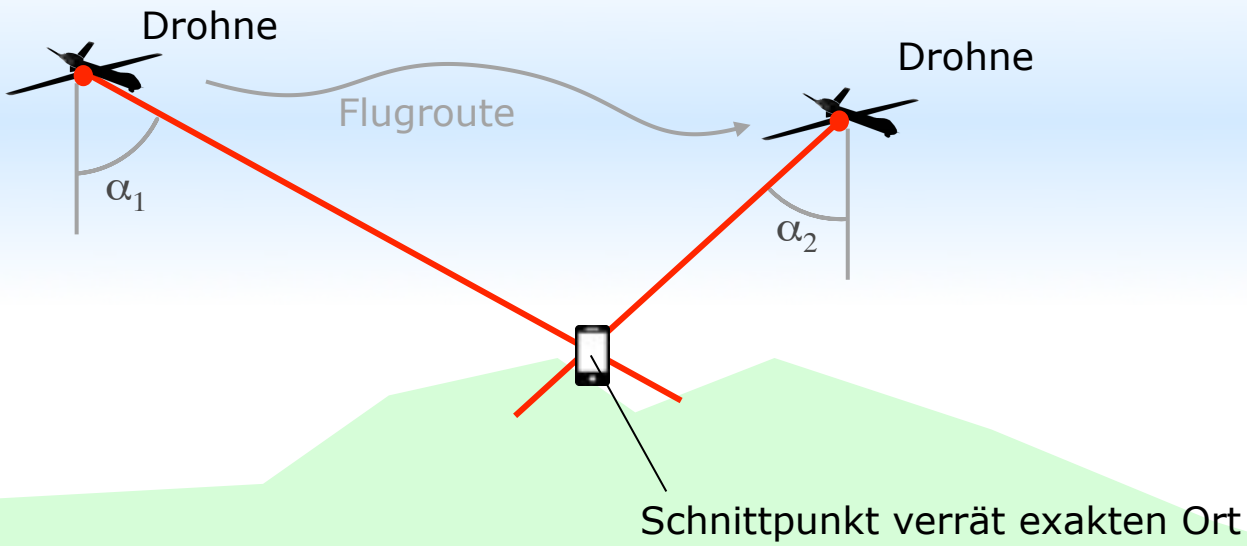
Positionsermittlung als Schnittpunkt der Erdoberfläche mit der Empfangsrichtung

Bild: https://upload.wikimedia.org/wikipedia/commons/3/33/MQ-9_Reaper_-_090609-F-0000M-777.JPG

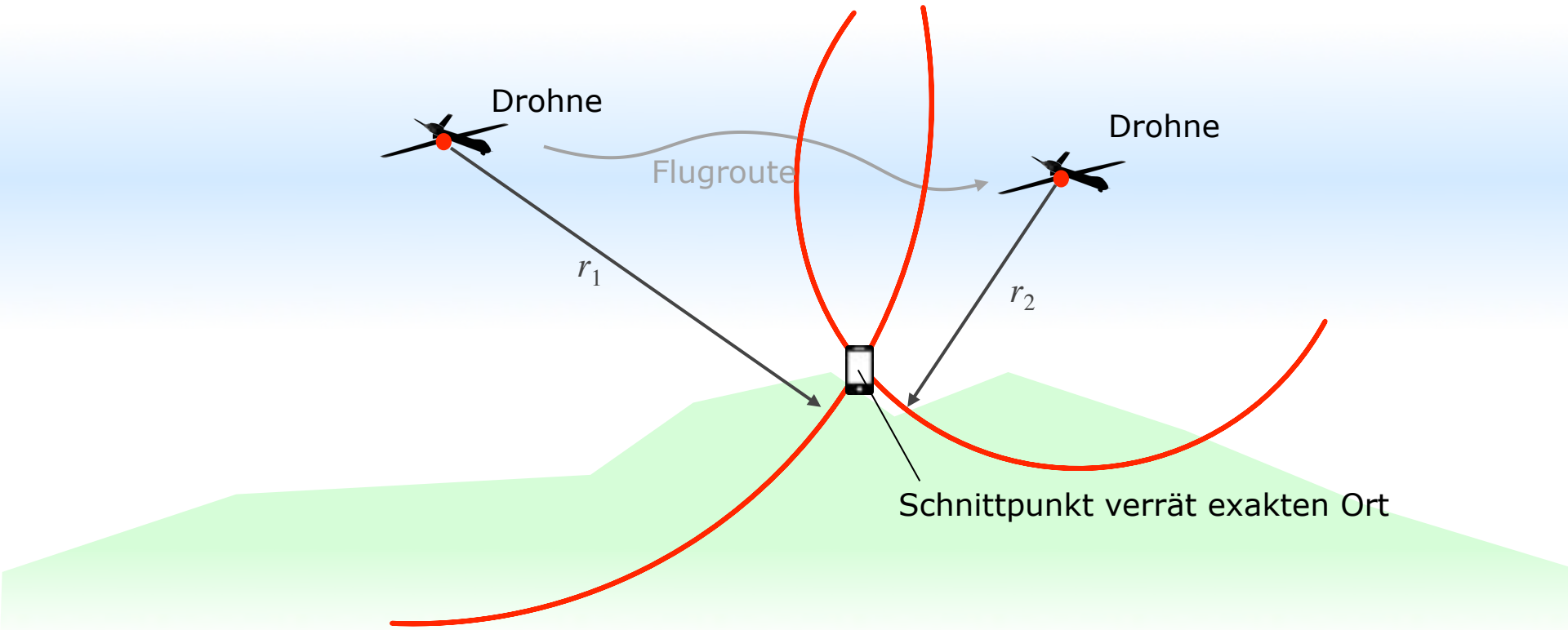
IMSI-Catcher in Drohne simuliert Mobilfunkzelle



Drohne bestimmt Empfangsrichtung der Funkwellen



Drohne bestimmt Empfangsrichtung der Funkwellen

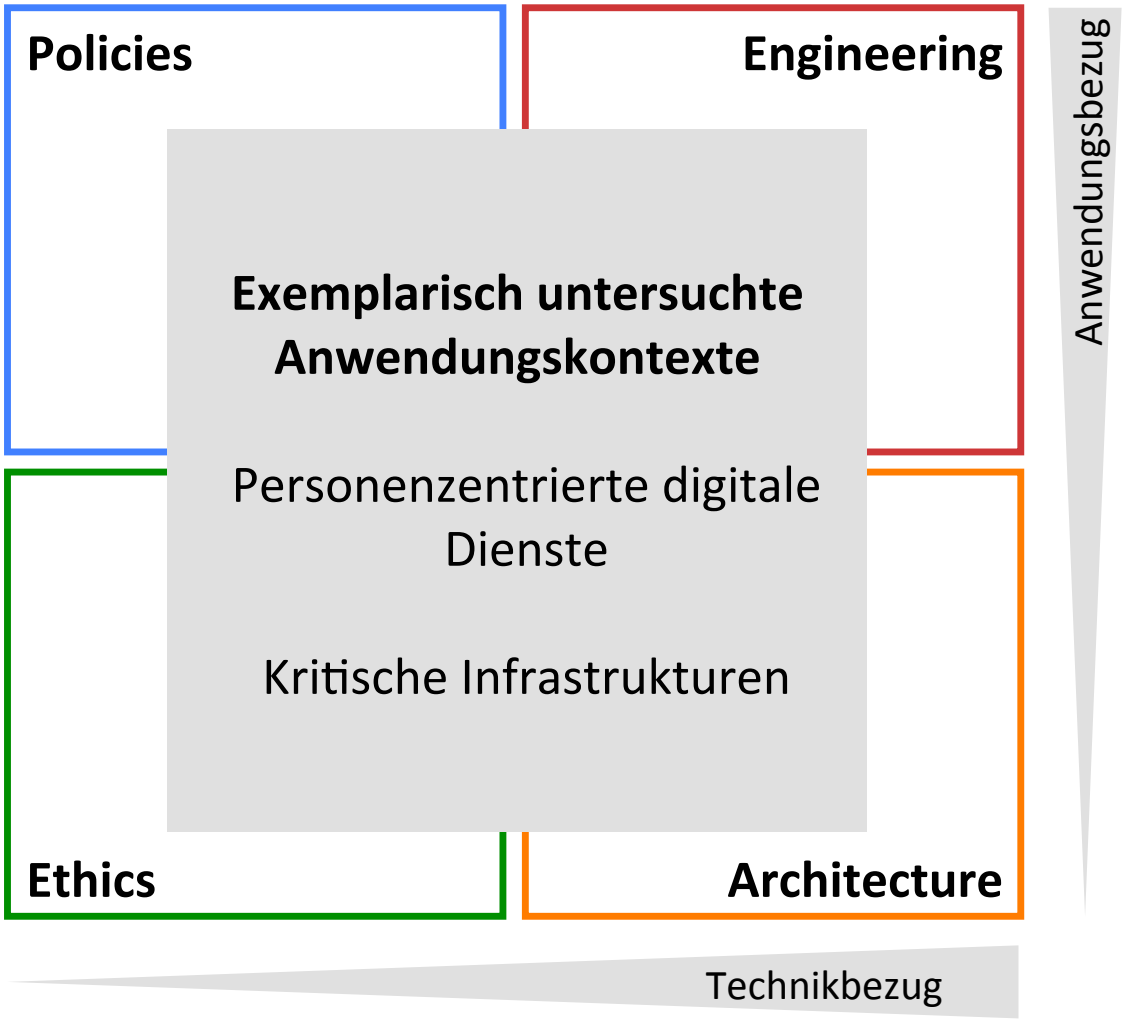


Information Governance Technologies

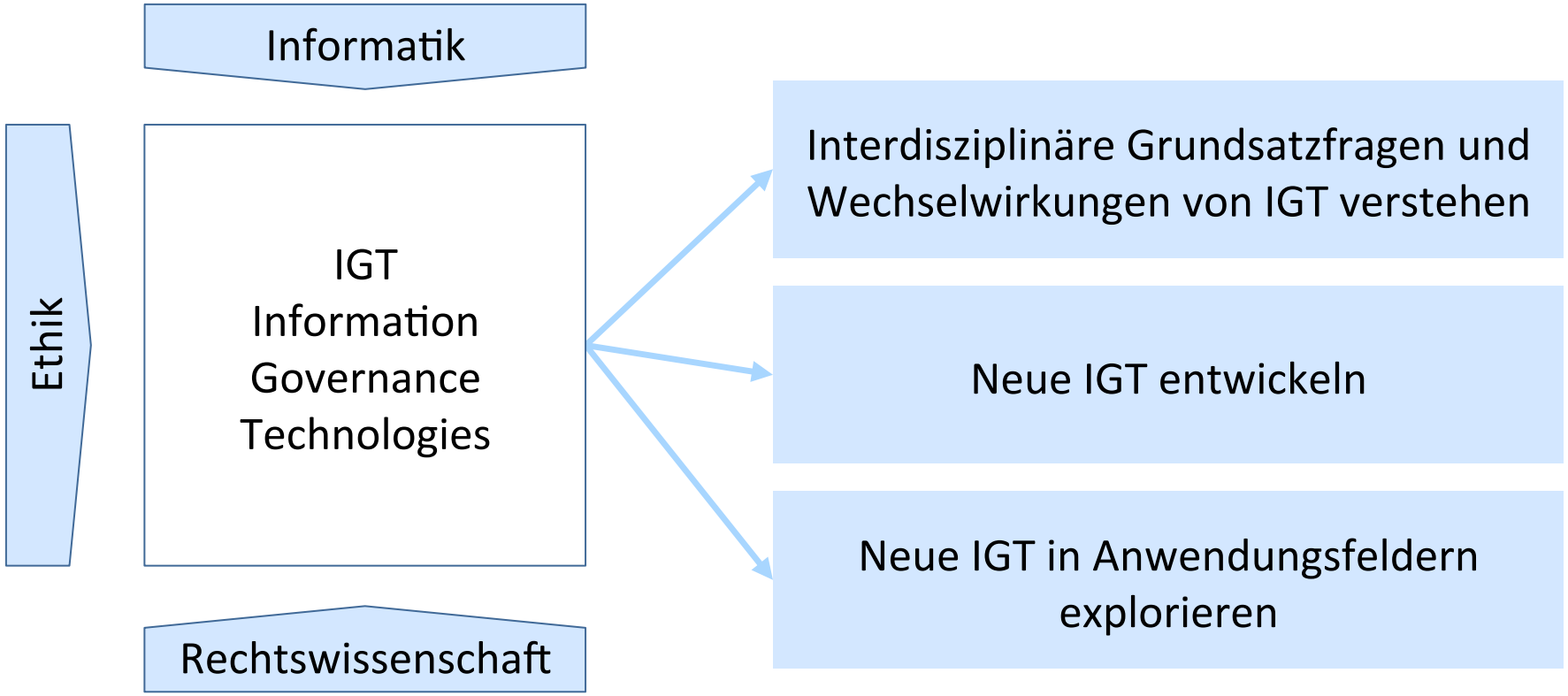
Verbundprojekt mit Uni Hamburg, TU Hamburg, Hans-Bredow-Institut

Projektbeginn vorauss. 1. Juni 2017, für 3 Jahre gefördert

Projektziel: Die menschenzentrierten technischen Möglichkeiten für den verantwortlichen Umgang mit Daten in der digitalen Gesellschaft erforschen



Information Governance Technologies



Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

https://svs.informatik.uni-hamburg.de