Biometrie: das Spannungsfeld von Komfort, Falscherkennung und Fälschungen

Prof. Dr. Claus Vielhauer
Technische Hochschule Brandenburg,
FB Informatik & Medien
Angewandte Informatik / Datensicherheit

Überblick

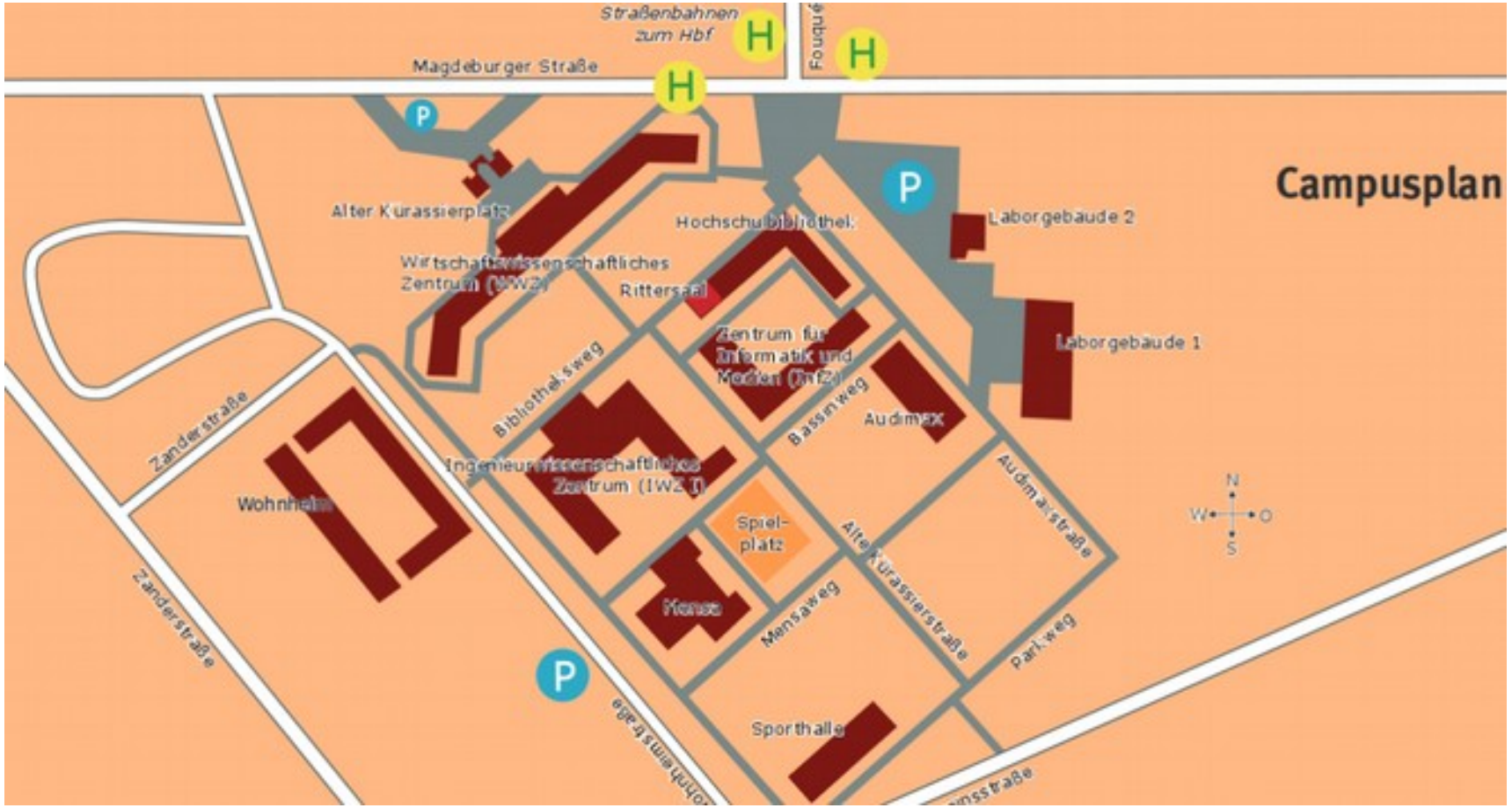
- Einführung
- Grundlagen Biometrie (ganz kurz, versprochen)
- Biometrische Fehler & Modalitäten
- Angriffe: Biometrische Fälschungen
- Privatsphäre: Biometrisches Schnüffeln
- Biometrie, DSGVO & UNO Menschenrechte
- Fazit: What to do? Selbsthilfe!

Einführung

Technische Hochschule
Brandenburg
University of
Applied Sciences

Von der Kürassierkaserne zur Hochschule

Einführung


Campusplan
Straßenbahnen zum Hbf
Magdeburger Straße
Alter Kürassierplatz
Hochschulbibliothek
Laborgebäude 2
Laborgebäude 1
Rittersaal
Bibliotheksweg
Bassinweg
Audimax
Wohnheim
Zanderstraße
Spiel-platz
Mensa
Mensaweg
Alte Kürassierstraße
Audimaxstraße
Parkweg
Sporthalle
N
W
O
S

Einführung

- IT Sicherheit an der THB insgesamt
  - Studiengänge und Vertiefungen
    - Informatik Master & Bachelor (z.B. Profil Security & Forensics)
    - Security-Management Master (berufsbegleitend)
    - Online-Studienformen
  - Forschungschwerpunkte:
    - „Interdisziplinäre Sicherheitsforschung„
    - „Digitale Transformation“ und
    - „Energie- und Ressourceneffizienz“
  - Labore: (Netzwerk-) Sicherheit, Forensik & Biometrie, Smarthome, digitale Spurenauswertung, ...
  - Projekte: Drittmittel Industrie/öffentlich...

Abbildung,
Siehe:

http://www.forschungslandkarte.de/
Profilbildende-forschung-an-fachhochschulen/
kartensuche.html

Bildquelle:
http://www.forschungslandkarte.de/profilbildende-forschung-an-fachhochschulen/kartensuche.html
, 12.06.2017

Einführung

- Ich selber…
  - Seit 2002 an der Otto-von-Guericke Universität Magdeburg
  - Seit 2007 Professur „Angewandte Informatik/Medieninformatik, insbesondere Datensicherheit“
  - Lehre zu Sicherheitsthemen in Bachelor/Master
  - Forschung zu IT Sicherheit, Biometrie, Forensik, auch zusammen mit Industrie
  - Doktorandenausbildung
  - Entwicklung von Online-Studieninhalten
  - Biometrie seit 1999, u.a. 2 Bücher zum Thema Biometrie:
    - „Biometric user authentication for IT security : from fundamentals to handwriting“, Springer, (2005)
    - „User-Centric Privacy and Security in Biometrics“, IET, 2017

Einführung
… etwas Geschichte …

- **Begriff Biometrie: griechisch “bios“** (Leben) und **“metros“** for Metrik/Maß.
- Frühe Biometrie:
  - Hand- und Fußabdrücke (1563, João de Barros, Portugiesischer Eroberer)
- Bertillonage: anthropometric System
  - Kriminologie
    1883-1914
  - 11 Körpermasse *p(False Match)* ≈ 1:191.304
- Daktyloskopie (forensische Fingerspurenuntersuchung)
  - Kriminologie seit dem 20. Jahrhundert
  - AFIS seit den 1990ern

Einführung Bertillonage

Abbildung,
Siehe:

http://www.lexicolatry.com/2013/05/bertillonage.html

http://www.lexicolatry.com/2013/05/bertillonage.html

Picture see in http://www.lexicolatry.com/2013/05/bertillonage.html, website request 7.10.2013

Einführung Bertillonage

Abbildung,
Siehe:

Claus Vielhauer: Biometric User Authentication for it Security - From Fundamentals to Handwriting. Advances in Information Security 18, Springer 2006, isbn 978-0-387-26194-2, pp. 1-284

Einführung
1903: Will West Case

Quelle: https://82141360.weebly.com/uploads/1/6/9/5/16958524/5036243_orig.jpg

https://82141360.weebly.com/uploads/1/6/9/5/16958524/4339212_orig.png

Einführung
Daktyloskopie (Fingerabdrücke)

- Fingerabdrücke bereits auf frühzeitlichen Gegenständen
- Wissenschaftliche Studien:
  - 1684, Nehemia Grew: erste Studien zu Papillarleisten, Wirbelstrukturen
  - 1823, Purkinje: ertse Klassifikation nach Grundmuster
  - ca. 1859, Sir William Herschel (Chief Magistrate of the Hooghly district in Jungipoor, India): Fingerabdrucke sind persistent und individuell, erste Anwendung zur Authentifizierung von Dokumenten etc.
  - 1880, H. Fauld, empirische Studien zu Individualität
  - 1888, F. Galton, Einführung der sog. Minutien Merkmale
  - 1899, E. Henry, neuartiges Fingerabdruck-Klassifikationssystem (“Henry system”)
  - Ab 1960, FBI, UK Home Office and Paris Police Department beginnen Entwicklungen für automatisches Fingerabdrucksystem – basiert auf Rillenmustern im Fingerabdruck

Einführung
Daktyloskopie (Fingerabdrücke)

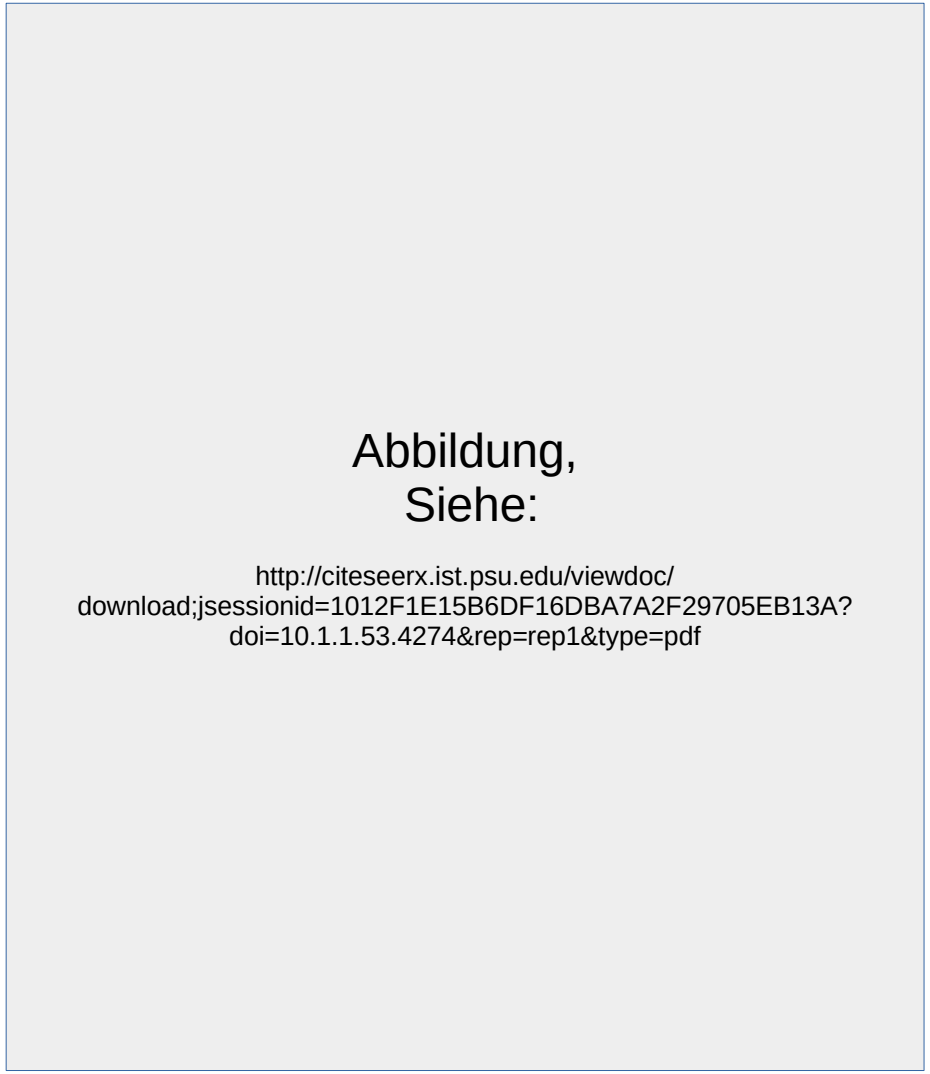
- Today, three levels of structures can be derived from fingerprint images:
  - Global Level Features (top),
  - Minutiae-based features (lower left) and
  - sweat pore feature examples (lower right) for fingerprint images

Abbildung,
Siehe:

From Claus Vielhauer: Biometric User Authentication for it Security - From Fundamentals to Handwriting.
Advances in Information Security 18,
Springer 2006, isbn 978-0-387-26194-2, pp. 1-284

From Claus Vielhauer: Biometric User Authentication for it Security - From Fundamentals to Handwriting. Advances in Information Security 18, Springer 2006, isbn 978-0-387-26194-2, pp. 1-284

Einführung
Fingerabdrücke – Minutien Merkmale



Lin *Hong*, Yifei *Wan*, and Anil *Jain*: *Fingerprint Image Enhancement*: Algorithm and. Performance Evaluation. See in http://www.math.tau.ac.il/~turkel/imagepapers/fingerprint.pdf or http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=1012F1E15B6DF16DBA7A2F29705EB13A?doi=10.1.1.53.4274&rep=rep1&type=pdf, website request 17.10.2013

Einführung
Fingerabdrücke – Will West Case (2)

https://82141360.weebly.com/uploads/1/6/9/5/16958524/9115685.jpg?418

Einführung
Fingerabdrücke – Causa Brandon Mayfield

Abbildung,
Siehe:

http://www.justice.gov/oig/special/s0601/exec.pdf

See: James L. Wayman, Ph.D., San Jose State University: „What is a Biometric Test? Examining the questions we ask”

See also in [DoJ06] U.S. Department of Justice: „A Review of the FBI’s Handling of the Brandon Mayfield Case.“ 2006. [Online], http://www.justice.gov/oig/special/s0601/exec.pdf , website request, 11.10.2013

Einführung
Fingerabdrücke – Causa Shirley McKie

Ian McKie and Michael Russel; „The Price of Innocence”, BIRLIN, ISBN-10 1841585750, 2007

Biometrische Fehler & Modalitäten

Abbildung,
Siehe:

http://ijarcsse.com/Before_August_2017/docs/papers/Volume_4/4_April2014/V4I4-0407.pdf

Quelle: Gursimarpreet Kaur, Dr.Chander Kant Verma: “Comparative Analysis of Biometric Modalities”, http://ijarcsse.com/Before_August_2017/docs/papers/Volume_4/4_April2014/V4I4-0407.pdf, 2017

Biometrische Fehler & Modalitäten

- Ergo: alles gut und unter Kontrolle?

Leider nein :-(

Bildquelle: Frank Schwichtenberg, unverändert, Diese Datei ist lizenziert unter der Creative-Commons-Lizenz „Namensnennung 4.0 international“, https://upload.wikimedia.org/wikipedia/commons/thumb/b/b7/Anonymous_%E2%80%93_CeBIT_2016_00.jpg/499px-Anonymous_%E2%80%93_CeBIT_2016_00.jpg

Angriffe: Biometrische Fälschungen

Bildquelle: Max Braun, https://upload.wikimedia.org/wikipedia/commons/b/b2/Sch%C3%A4uble_Fingerprint_stamp_%283561866525%29.jpg, unverändert, lizensiert unter der Creative-Commons-Lizenz „Namensnennung – Weitergabe unter gleichen Bedingungen 2.0 generisch“

Angriffe: Biometrische Fälschungen

Abbildung,
Siehe:

https://koeln.ftp.media.ccc.de/contributors/berlin/biometrie/h264-hd/
biometrie-12-deu-Die_Sendung_mit_dem_Chaos_-_Iris-Scanner_im_Samsung_Galaxy_S8_hd.mp4

Quelle: https://koeln.ftp.media.ccc.de/contributors/berlin/biometrie/h264-hd/biometrie-12-deu-Die_Sendung_mit_dem_Chaos_-_Iris-Scanner_im_Samsung_Galaxy_S8_hd.mp4, abgerufen 2.5.2019

Angriffe: Biometrische Fälschungen

Abbildung,
Siehe:

https://www.heise.de/mac-and-i/meldung/iPhone-X-Zwillingsmaske-soll-Apples-Face-ID-sofort-ueberlisten-3902705.html

Bildquelle: Leo Becker, https://www.heise.de/mac-and-i/meldung/iPhone-X-Zwillingsmaske-soll-Apples-Face-ID-sofort-ueberlisten-3902705.html, Version 2 der Maske soll Face ID schneller überlisten. (Bild: Bkav), abgerufen 02.05.2019

Angriffe: Biometrische Fälschungen

Abbildung,
Siehe:

https://arxiv.org/pdf/1901.08811

Bildquelle: Matteo Ferrara, Annalisa Franco and Davide Maltoni, “Face morphing detection in the presence of printing/scanning and heterogeneous image sources”, https://arxiv.org/pdf/1901.08811, abgerufen 02.05.2019

Angriffe: Biometrische Fälschungen

Abbildung,
Siehe:

https://arxiv.org/pdf/1901.08811

Bildquelle: Matteo Ferrara, Annalisa Franco and Davide Maltoni, “Face morphing detection in the presence of printing/scanning and heterogeneous image sources”, https://arxiv.org/pdf/1901.08811, abgerufen 02.05.2019

Angriffe: Biometrische Fälschungen

Bildquelle: http://spoofvoice.com/, abgerufen 02.05.2019

Angriffe: Biometrische Fälschungen

- **FAR/FRR/EER weitgehend als Präzisionsmaß akzeptiert, aber:**
  - **3 Fehler in 100 Tests bedeutet nicht, dass jeder Nutzer mit 3% Fehler rechnen kann - Doddington's zoo:**
  - „Sheep – easily accepted by the system"
  - „Goats – exceptionally unsuccessful at being accepted„
  - „Lambs –exceptionally vulnerable to impersonation"
  - „Wolves –exceptionally successful at impersonation"
- … weitere Fehlergrößen wie Failure To Acquire (FTA) Failure to Enrol Rate (FTE), False Identification Rate (FIR)...

Privatsphäre: Biometrisches Schnüffeln

Abbildung,
Siehe:

https://www.wienerzeitung.at/themen_channel/wz_digital/digital_news/996055_Alexa-hoert-den-Husten-ab.html

Quelle: https://www.wienerzeitung.at/themen_channel/wz_digital/digital_news/996055_Alexa-hoert-den-Husten-ab.html, 15.10.2018

Privatsphäre: Biometrisches Schnüffeln

- „(...) Die Handelskette Walmart hat ein interessantes Patent eingereicht: Einkaufswägen, die nicht nur ihre aktuelle Position sondern auch den aktuellen Puls, Blutdruck und die Temperatur der Kunden ermitteln und an einen Server schicken. Der überwacht die Daten kontinuierlich und kann Mitarbeiter informieren, dass ein Kunde persönliche Betreuung benötigt. (...)

Abbildung,
Siehe:

https://m.heise.de/security/meldung/
l-f-Walmart-patentiert-biometrische-Einkaufswagen-4184598.html

- Ein Schelm, wer hinter dem Antrag zu "System and method for a biometric feedback cart handle" anderes vermutet, als den Wunsch, im Notfall möglichst schnell Erste Hilfe leisten zu können. (...)

Quelle: Jürgen Schmidt, https://m.heise.de/security/meldung/l-f-Walmart-patentiert-biometrische-Einkaufswagen-4184598.html, 10.10.2018

Privatsphäre: Biometrisches Schnüffeln

- Telemetrie: „Windows 10 diagnostic data for the Full diagnostic data level (…)
  - Common Data (diagnostic header information)
  - Device, Connectivity, and Configuration data
  - Product and Service Usage data
  - Product and Service Performance data
  - Software Setup and Inventory data
  - Browsing History data
  - Inking, Typing, and Speech Utterance data (...)“

Quelle: Microsoft cooperation: https://docs.microsoft.com/en-us/windows/privacy/windows-diagnostic-data-1703, abgerufen 02.05.2019

Privatsphäre: Biometrisches Schnüffeln

- „(…) Inking, Typing, and Speech Utterance data (…)
  - Pen gestures (click, double click, pan, zoom, rotate)
  - Input latency, missed pen signals, number of frames, strokes, first frame commit time, sample rate
  - Palm Touch x,y coordinates
  - (…)
  - Text input from Windows Mobile on-screen keyboards except from password fields and private sessions
  - (...)
  - Whether user is known to be a child (…)“

Quelle: Microsoft cooperation: https://docs.microsoft.com/en-us/windows/privacy/windows-diagnostic-data-1703, abgerufen 02.05.2019

Biometrie, DSGVO & UNO Menschenrechte

- Art. 8 DSGVO Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft:
  - „(…) 1Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.(...)“

Quelle: Datenschutzgrundverordnung, Artikel 8

Biometrie, DSGVO & UNO Menschenrechte

Biometrische Datensammlungen:

Sensible Attribute nach:

- Allgemeine Erklärung der Menschenrechte (UNO 1948)
- DSGVO 2018

TABLE 1: Derived attributes. Abbreviations U and C refer to UDHR and CCPR respectively. Appended numbers refer to the Articles within the documents. Source ***[11][12][13]***

Attribute	Origin	Biometric Modalities
Race	U2, C2	Eye, **face**, **fingerprints**
Gender	U2, C2	Body, **face**, **fingerprints**, gait, gestures, hand, handwriting, speech
Language	U2, C2	Handwriting, speech
Freedom of Thought	U2, U18, U19, C2, C18, C19	Eye, **face**, gait, speech, wearable sensors
Nationality	U2, U15, C2, C24	**Face**, **fingerprints**, speech, handwriting
Age	U2, C2	Body, **face**, gait, gestures, handwriting, speech
Childhood	GDPR 8	Body, **face**, gait, gestures, handwriting, speech
Health	GDPR 9	Body, eye, **face**, **fingerprints**, gait, gestures, hand, handwriting, speech, wearable sensors
Sexual Orientation	GDPR 9	Eye, **face**

Quelle: Nicholas Whiskerd, Jana Dittmann & Claus Vielhauer: “A Requirement Analysis for Privacy Preserving Biometrics in view of Universal Human Rights and Data Protection Regulation”, First published in the Proceedings of the 26th European Signal Processing Conference (EUSIPCO-2018) in 2018, published by EURASIP

Persönliche Schutzmaßnahmen - Positive Anreize: „digitale Selbstverteidigung“

Erforschung von Methoden zur De-Attributierung von Biometrie-Daten

AMBER (Advanced Mobile BioMetRics) project, sponsored by the Marie Sklodowska-Curie EU Framework for Research and Innovation Horizon 2020, under Grant Agreement No. 675087.

https://www.amber-biometrics.eu

TABLE 3: Identified solutions in the literature of derived attribute protections by selective de-identification.

Biometric Modality	Attribute	Solutions (None-Partial-Complete)
Face	Race / Nationality	Partial
	Gender	Complete
	Freedom of Thought	None
	Age / Childhood	None
	Health	Partial
	Sexual Orientation	None
Fingerprint	Race / Nationality	None
	Gender	Complete

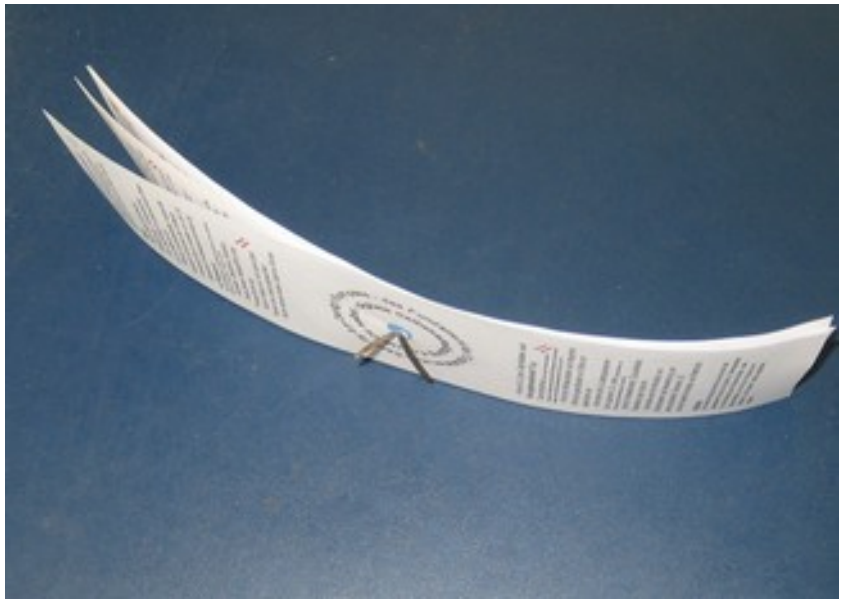
Quelle: Nicholas Whiskerd, Jana Dittmann & Claus Vielhauer: “A Requirement Analysis for Privacy Preserving Biometrics in view of Universal Human Rights and Data Protection Regulation”, First published in the Proceedings of the 26th European Signal Processing Conference (EUSIPCO-2018) in 2018, published by EURASIP

Fazit

- „Normale“ Biometrie
  - Einsatz für Multifaktor-Identifikation heute Off-the-Shelf möglich
  - Wahl der Modalität je nach Einsatzgebiet / Sicherheitsniveau / Kosten /…
  - Fehler durch Falscherkennungen sind zu berücksichtigen / kalkulierbar?
- Aber: gezielte Angriffe (Fälschungen, Spoofing) auf biometrische Identitäten nehmen zu
  - Typischer ITS-Zyklus: Angriff ↔ Verteidigung
  - Spoofing ↔ Anti-Spoofing
- Perspektive:
  - Biometrie ohne Wissen der Nutzer, zur Profilierung (Gesundheit, Emotion, Ethnizität etc)!
  - Noch mehr Datenpreisgabe!
  - Privatsphäre!

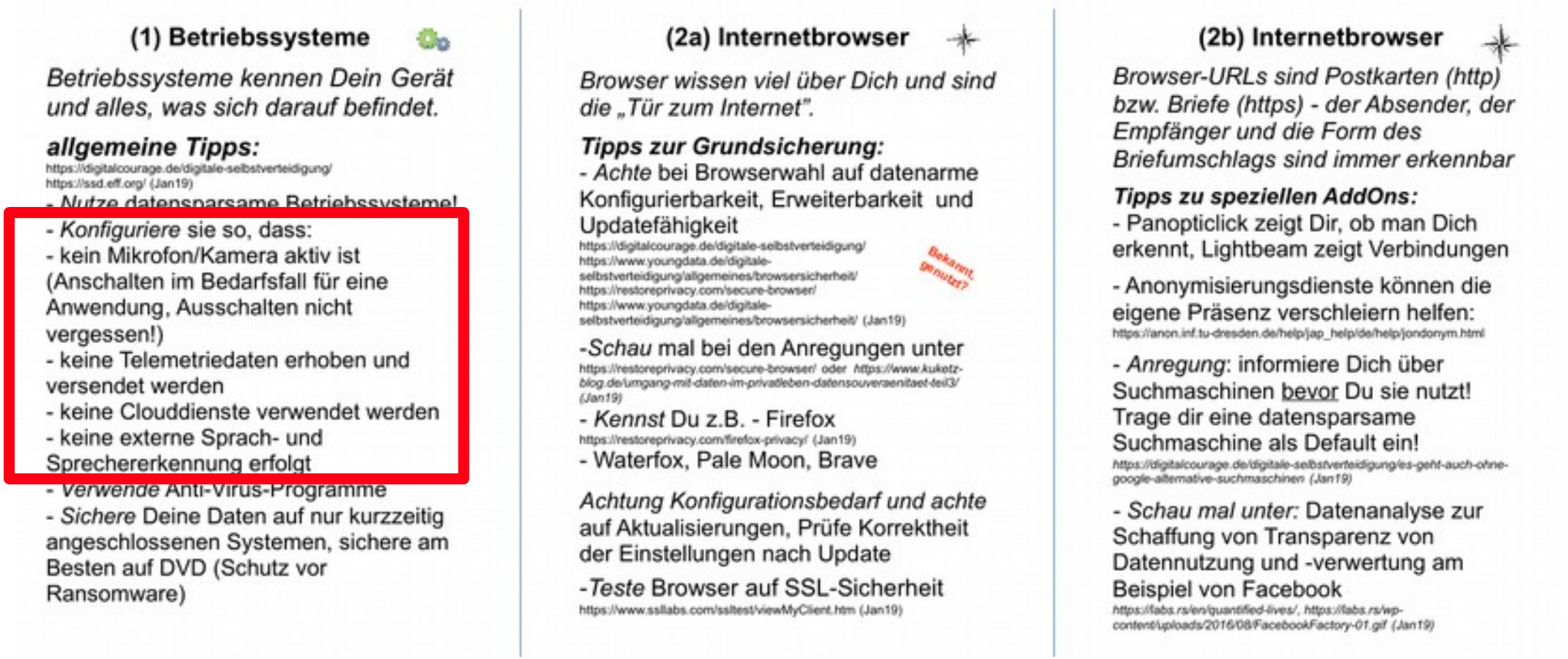
Fazit: What to do? Selbsthilfe!

- Digitale Selbstverteidigung:
  - Kompass für Digitale Selbstverteidigung: „Hilf Dir selbst - digitale Selbstverteidigung 4.0“
  - Projekt der Otto-von-Guericke-Universität Magdeburg (unter Creative Commons Lizenz)



Quelle: https://omen.cs.uni-magdeburg.de/itiamsl/deutsch/secbydesign/index.html, abgerufen 02.05.2019

Fazit: What to do? Selbsthilfe!



(1) Betriebssysteme

Betriebssysteme kennen Dein Gerät und alles, was sich darauf befindet.

allgemeine Tipps:

https://digitalcourage.de/digitale-selbstverteidigung/
https://ssd.eff.org/ (Jan19)

- *Nutze* datensparsame Betriebssysteme!
- *Konfiguriere* sie so, dass:
- kein Mikrofon/Kamera aktiv ist (Anschalten im Bedarfsfall für eine Anwendung, Ausschalten nicht vergessen!)
- keine Telemetriedaten erhoben und versendet werden
- keine Clouddienste verwendet werden
- keine externe Sprach- und Sprechererkennung erfolgt
- *Verwende* Anti-Virus-Programme
- *Sichere* Deine Daten auf nur kurzzeitig angeschlossenen Systemen, sichere am Besten auf DVD (Schutz vor Ransomware)

(2a) Internetbrowser

Browser wissen viel über Dich und sind die „Tür zum Internet".

Tipps zur Grundsicherung:

- *Achte* bei Browserwahl auf datenarme Konfigurierbarkeit, Erweiterbarkeit und Updatefähigkeit

https://digitalcourage.de/digitale-selbstverteidigung/
https://www.youngdata.de/digitale-selbstverteidigung/allgemeines/browsersicherheit/
https://restoreprivacy.com/secure-browser/
https://www.youngdata.de/digitale-selbstverteidigung/allgemeines/browsersicherheit/ (Jan19)

Bekannt, genutzt?

-*Schau* mal bei den Anregungen unter
https://restoreprivacy.com/secure-browser/ oder *https://www.kuketz-blog.de/umgang-mit-daten-im-privatleben-datensouveraenitaet-teil3/ (Jan19)*

- *Kennst* Du z.B. - Firefox
https://restoreprivacy.com/firefox-privacy/ (Jan19)
- Waterfox, Pale Moon, Brave

Achtung Konfigurationsbedarf und achte auf Aktualisierungen, Prüfe Korrektheit der Einstellungen nach Update

-*Teste* Browser auf SSL-Sicherheit
https://www.ssllabs.com/ssltest/viewMyClient.htm (Jan19)

(2b) Internetbrowser

Browser-URLs sind Postkarten (http) bzw. Briefe (https) - der Absender, der Empfänger und die Form des Briefumschlags sind immer erkennbar

Tipps zu speziellen AddOns:

- Panopticlick zeigt Dir, ob man Dich erkennt, Lightbeam zeigt Verbindungen

- Anonymisierungsdienste können die eigene Präsenz verschleiern helfen:
https://anon.inf.tu-dresden.de/help/jap_help/de/help/jondonym.html

- *Anregung*: informiere Dich über Suchmaschinen bevor Du sie nutzt! Trage dir eine datensparsame Suchmaschine als Default ein!
https://digitalcourage.de/digitale-selbstverteidigung/es-geht-auch-ohne-google-alternative-suchmaschinen (Jan19)

- *Schau mal unter:* Datenanalyse zur Schaffung von Transparenz von Datennutzung und -verwertung am Beispiel von Facebook
https://labs.rs/en/quantified-lives/, https://labs.rs/wp-content/uploads/2016/08/FacebookFactory-01.gif (Jan19)

- Und noch vieles mehr…..

Quelle: https://omen.cs.uni-magdeburg.de/itiamsl/deutsch/secbydesign/index.html, abgerufen 02.05.2019

Vielen Dank für Ihre Aufmerksamkeit!

„Manchmal ist **Biometrie drin**, obwohl es **nicht draufsteht**!“

Quelle: http://biometrics.mainguet.org/cartoons/cartoons.htm, abgerufen 07.05.2019