TÜVIT

Täuschungserkennung für Biometrie auf dem Prüfstand

Evaluation von Presentation Attack Detection

Boris Leidner | TÜVIT | Täuschungserkennung auf dem Prüfstand | 22.05.2023

Agenda

- Biometrie in sicherheitsrelevanten Anwendungen
- Biometrische Begriffe
- Instrumente für Präsentationsangriffe
- PAD-Technologien
- Herausforderungen
- Penetrationstests vs Funktionale Tests

Biometrie in sicherheitsrelevanten Anwendungen

Biometrie wird heute an vielen Stellen eingesetzt

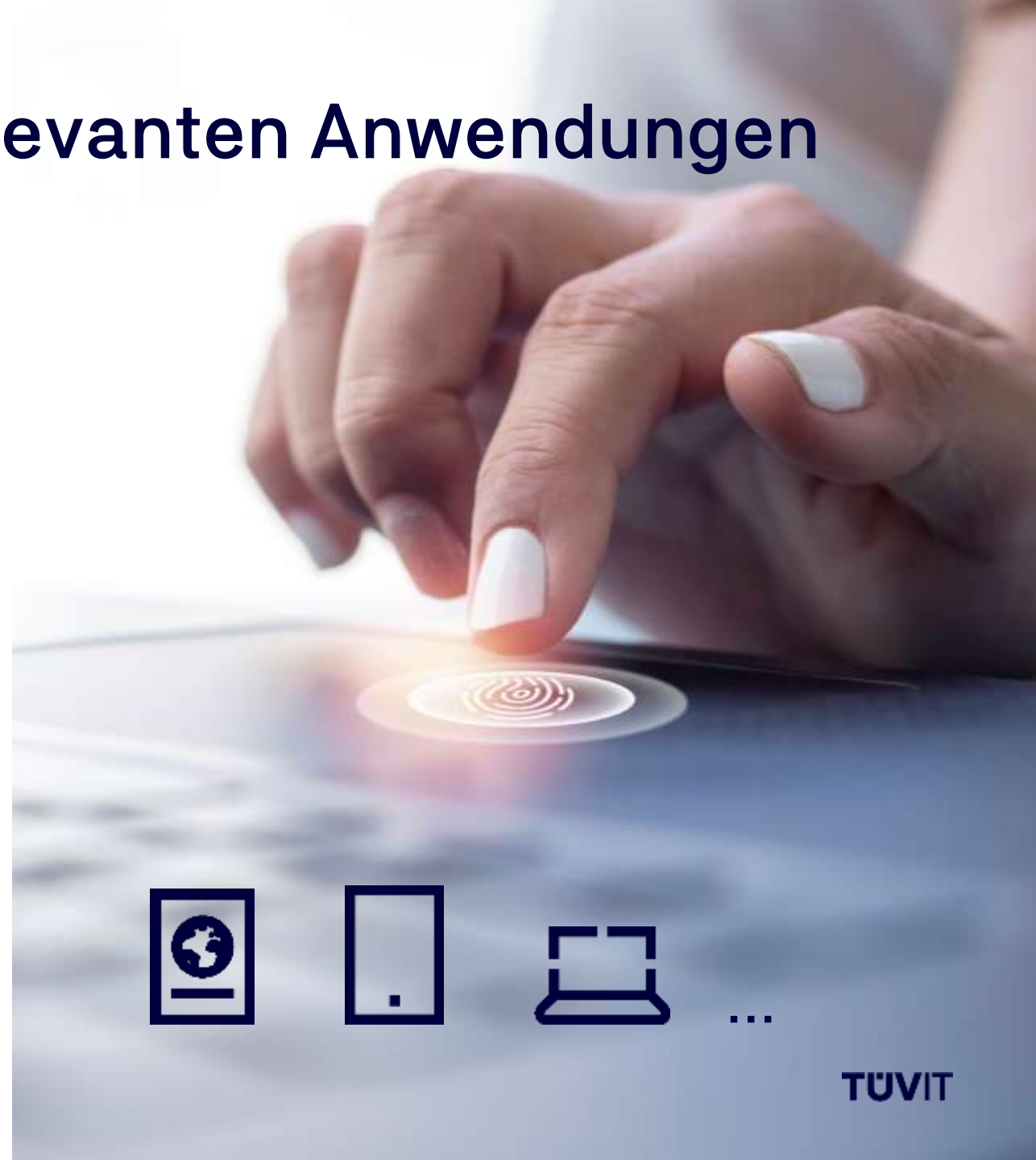
- Grenzkontrolle
- Identifizierungsdienste (z.B. für Banken)
- Zugangskontrollsysteme

Problem

- Biometrischen Daten können unbewusst abgegriffen und für Täuschungen reproduziert werden
- Leistungsfähigkeit von Täuschungserkennungen oftmals ungewiss

Lösung

- Bewertung und Prüfung der Täuschungserkennung



Biometrische Begriffe

Präsentation

- Interaktion des Benutzers mit dem biometrischen System zum Zweck der Aufnahme von biometrischen Daten.

Präsentationsangriff

- Präsentation gegenüber dem System, mit dem Ziel der Beeinflussung des biometrischen Systems.

Präsentationsangriffsinstrument (PAI)

- Biometrische Charakteristik oder Objekt, welche(s) bei einem Präsentationsangriff verwendet wird.

PAI-Spezies

- Klasse von PAI, die mit der selben Herstellungsmethode und auf Basis von unterschiedlichen biometrischen Charakteristiken hergestellt werden.

Presentation Attack Detection (PAD)

- Funktionalität für die Erkennung, ob es sich um eine normale Präsentation oder um einen Präsentations-angriff handelt.

TÜVIT

PAI für Fingerabdruckserkennung (Artefakte)

Materialien

Silikone

Latex

Gelatine

Leim/Kleber

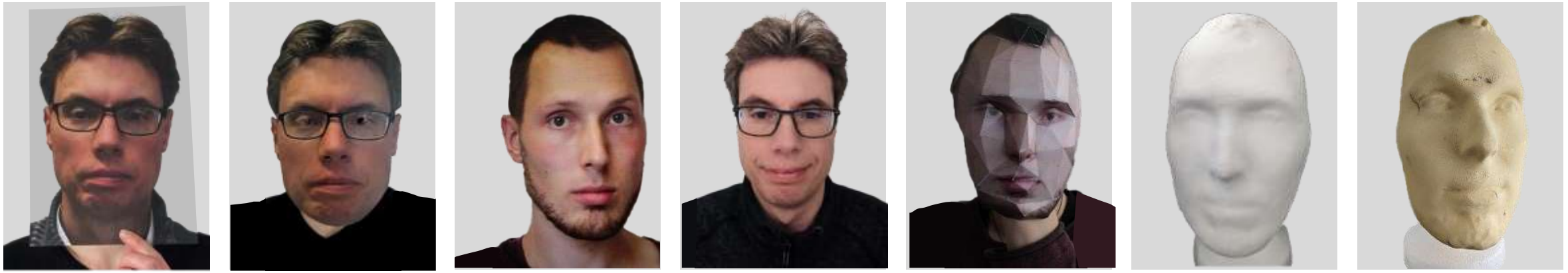
Fensterfarbe

Formfaktoren

- Fingerpads
- Vollständige Finger

TÜVIT

PAI für Gesichtserkennung (Artefakte)



+++ Fotos auf Papier ausgedruckt +++ Fotos auf elektronischem Gerät angezeigt +++
Videos auf elektronischem Gerät angezeigt +++ Fotos auf Textilien ausgedruckt +++
+++ 3D-Masken aus Papier, Silikon, 3D-Druck +++ u. a.

PAD-Technologien

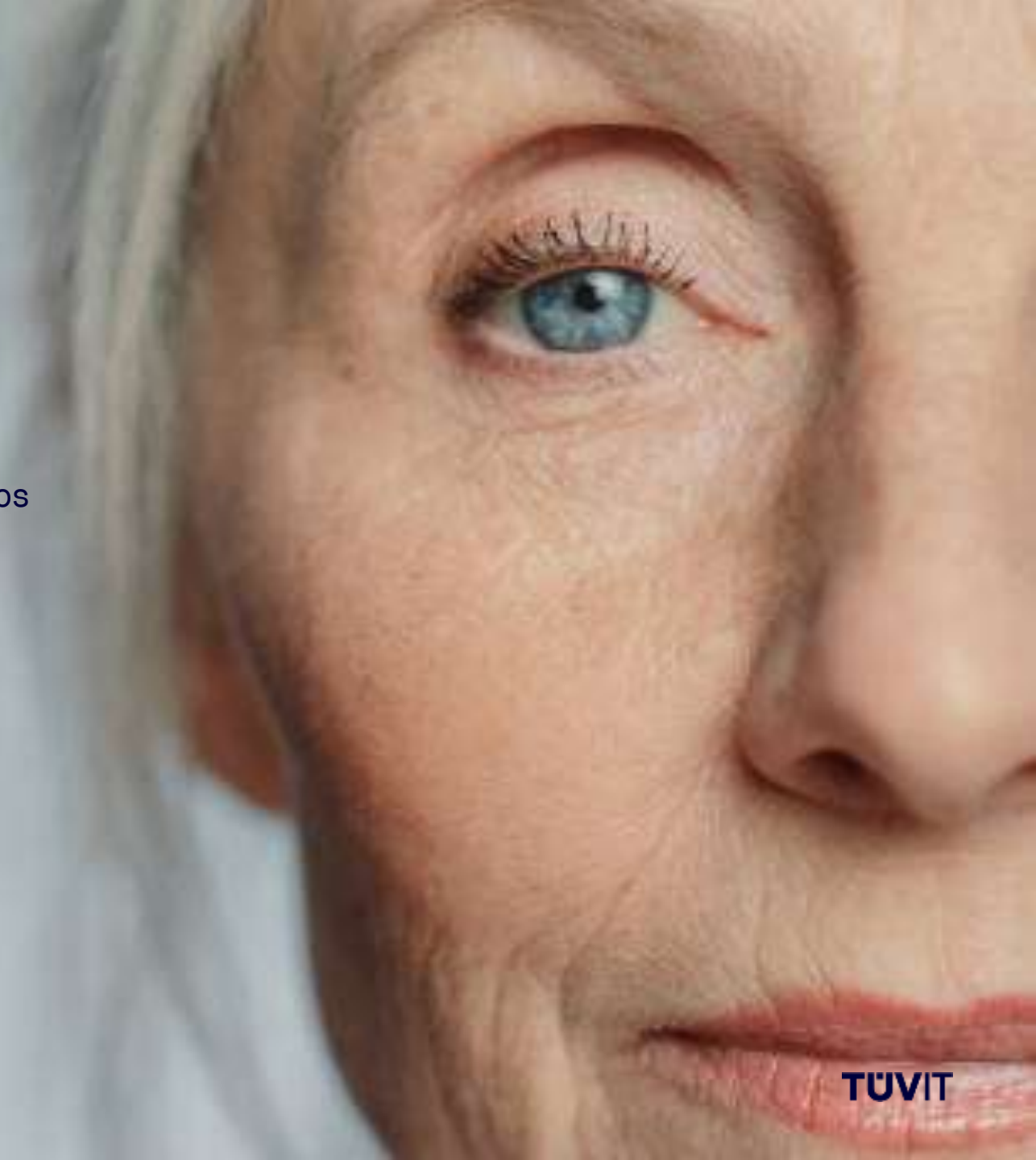
bei Fingerabdruck- und Gesichtserkennung

Rein software-basierte PAD-Ansätze

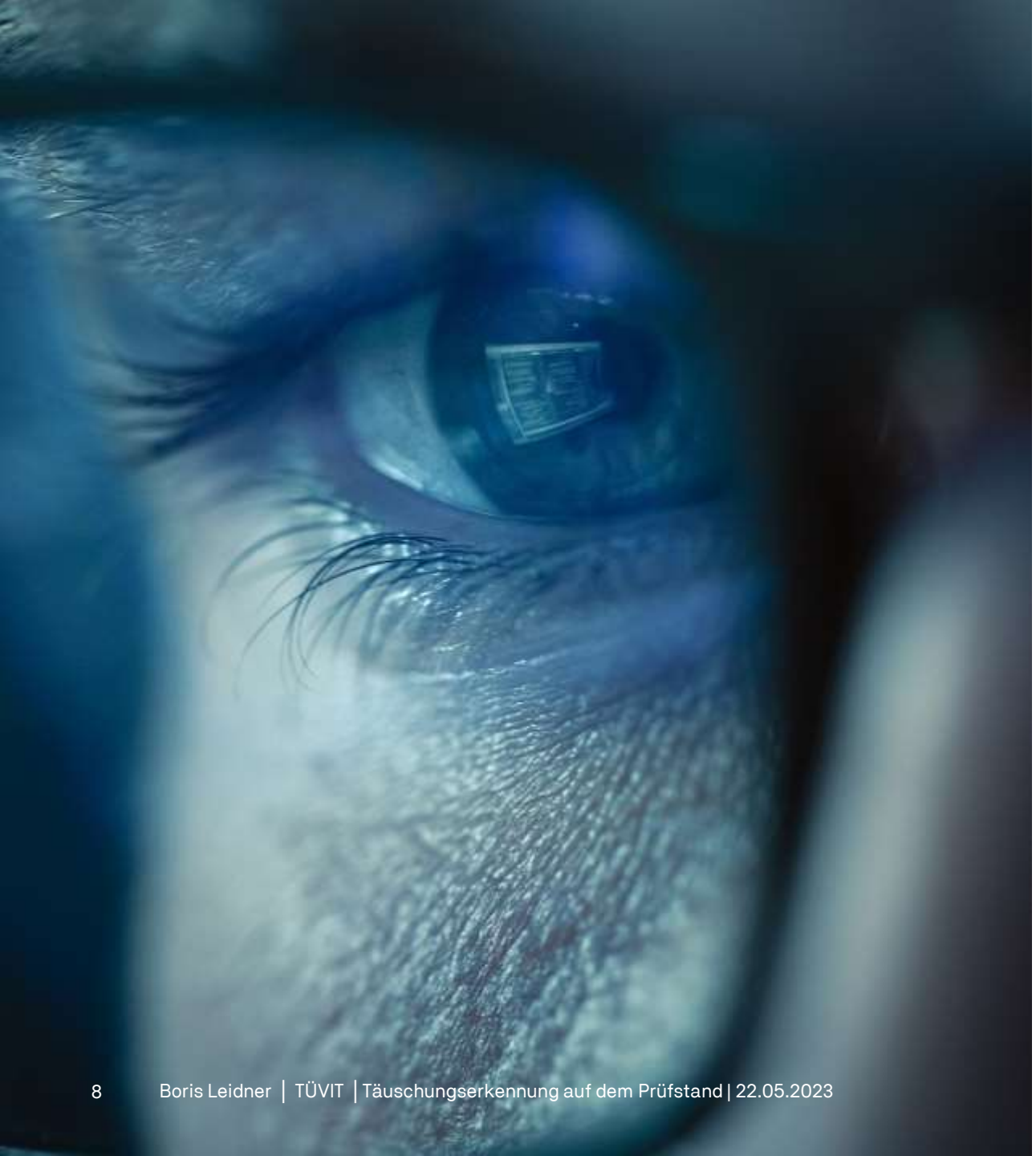
- Künstliche neuronale Netzwerke werden mit Bilddaten von Präsentationsangriffen trainiert
- Bewertung auf Basis eines oder mehrerer Bilder oder Videos
- Teilweise mit Challenges für den Nutzer (z.B. Kopfbewegungen, Augenzwinkern etc.)

PAD-Ansätze mit zusätzlicher Hardware

- Beispiele Fingerabdruckserkennung
  - Impedanzmessung (Hautwiderstand)
  - Pulsoxymetrie (Pulserkennung, Sauerstoffsättigung)
  - Optische Kohärenztomographie (OCT)
- Beispiele Gesichtserkennung
  - Wärmebildkamera (Infrarot)
  - Mehrere Kameras für 3D-Bild-Erzeugung



TÜVIT



PAD-Technologien

Herausforderungen bei der Prüfung

- PAD-Systeme sind nicht deterministisch und haben immer eine Fehlerquote.
- Theoretische Abschätzung der Sicherheit von PAD nicht möglich, daher empirische Untersuchungen (Stichproben) notwendig.
- Fehlerraten sind in Bezug auf IT-Sicherheit wenig aussagekräftig, da ein Angreifer sich auf die Schwächen eines jeden Systems konzentriert.
- PAI müssen regelmäßig erneuert werden, da Aussagekraft von Testergebnissen sinkt, wenn Stichprobe nicht verändert wird.
- PAI enthalten i.d.R. personenbezogene biometrische Informationen und sind daher aus Datenschutzsicht entsprechend zu behandeln.

TÜVIT

Aus der Praxis

Evaluation von PAD für Fingerabdruck

Common Criteria – Schutzprofile

- BSI-CC-PP-0118 – Biometric Mechanisms Protection Profile (BMPP)
- BSI-CC-PP-0062 – Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP)
- BSI-CC-PP-0063 – Fingerprint Spoof Detection Protection Profile (FSDPP)

- Funktionale Tests (Tests mit vorgegebenen PAI-Spezies)
- **Jedoch keine Schwachstellenanalyse und Penetrationstests!**

Was wird von der PAD erwartet?

- Präsentationsangriffe dürfen nicht *reproduzierbar erfolgreich* sein

Wie wird getestet?

- BSI gibt eine Liste von PAI vor, die bei der Prüfung betrachtet werden müssen (aktuell 29 PAI-Klassen)
- Je Klasse werden mehrere PAI erstellt (56 insgesamt)
- Jedes PAI wird 10 mal präsentiert

Wann hat die PAD bestanden?

- Von 10 Präsentationen, darf ein PAI maximal einmal nicht erkannt werden

Pentrationstests vs funktionale Tests

- Nehmen die Perspektive eines **intelligenten und motivierten Angreifers** ein
- Fokussieren auf die PAD-Technologie und ihre spezifischen **Eigenheiten und Schwächen**
- Präsentationsangriffe werden **iterativ verfeinert**
- Das benötigte **Angriffspotential** bestimmt, ob ein Präsentationsangriff relevant ist und nicht eine vorgegebene Liste von PAI

Relevante Aspekte für die Bestimmung des Angriffspotentials:

- Benötigte **Zeit** für Angriff inkl. Vorbereitung
- Benötigte **Expertise** des Angreifers
- Benötigte **Kenntnisse** über das System
- **Zugangsmöglichkeit** zum System
- Benötigtes **Equipment** für die Durchführung des Angriffs und der Identifikation der Schwachstelle
- **Zugang zu biometrischen Charakteristiken** notwendig?

Oft gering!

Das notwendige Angriffspotential für erfolgreiche Angriffe

Beispiel für Angriff (Gesichtsbild):
Video von dem Gesicht einer Person aufnehmen und einem Gesichtserkennungssystem präsentieren

- **Zeit**: < 1 Tag
- **Expertise**: gering
- **Kenntnisse**: gering
- **Zugangsmöglichkeit:** einfach
- **Equipment**: < 500 €
- **Zugang zu biometrischen Charakteristiken:** Fotos und Videos können leicht ohne Kenntnis der betroffenen Person aufgenommen werden

⇒ Angriffspotential: **Niedrig**

Beispiel für Angriff (Fingerabdruck):
Künstliche Fingerkuppe aus Holzleim herstellen und nicht überwachten Fingerabdrucksensor angreifen

- **Zeit**: < 1 Tag
- **Expertise**: gering
- **Kenntnisse**: gering
- **Zugangsmöglichkeit:** einfach
- **Equipment**: Baumarkt, < 100 €
- **Zugang zu biometrischen Charakteristiken:** einfach (Abdrücke können von glatten Oberflächen aufgenommen werden)

⇒ Angriffspotential: **Niedrig**

TÜVIT

TÜVIT

In Kontakt bleiben?

Boris Leidner

Produktmanager IT-Konformität

Tel.: +49 201 8999-531
Fax: +49 201 8999-666
E-Mail: b.leidner@tuvit.de