Angriffsvektoren auf Fernidentifikationssysteme: Demonstration und Einordung ihrer Kritikalität

Dominique Dresen, **Matthias Neu**, Markus Ullmann

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mögliche Angriffe

	Originales Dokument	Digital gefälschtes Dokument	Physisch gefälschtes Dokument
Originales Gesicht		z.B. VITO, CCC Angriff,…	s. Studie BKA
Face Swap	z.B. Authentifizieren mit gestohlenem Dokument	z.B. Kombination FaceSwap + VITO	z.B. Kombination FaceSwap + gefälschter Ausweis
Physische Maske	Masken, Schminke, …	z.B. Kombination Maske + VITO	z.B. Kombination Maske + gefälschter Ausweis

Video – Replay Attack, Digital Puppeteering, …

Demonstration Erstellung Ausweis & VITO

	Originales Dokument	Digital gefälschtes Dokument	Physisch gefälschtes Dokument
Originales Gesicht		z.B. VITO, CCC Angriff,…	
Face Swap			
Physische Maske			

Beispiel: VITO

Einschätzung des Angriffspotentials in Anlehnung an die Evaluationsmethodologie der CC: CEM

Common Criteria

Common Methodology for Information Technology Security Evaluation

Evaluation methodology

April 2017

Version 3.1
Revision 5

CCMB-2017-04-004

B.4.2.2 Factors to be considered

2019

The following factors should be considered during analysis of the attack potential required to exploit a vulnerability:

a) Time taken to identify and exploit (***Elapsed Time***);

b) Specialist technical expertise required (***Specialist Expertise***);

c) Knowledge of the TOE design and operation (***Knowledge of the TOE***);

d) ***Window of opportunity***;

e) ***IT hardware/software or other equipment*** required for exploitation.

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

Wird von TR 3147 („Vertrauensbewertung von Verfahren zur Identitätsprüfung natürlicher Personen“) verwendet.

CEMv3.R5, https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

Einschätzung des Angriffspotentials von VITO nach CEM-Kriterien

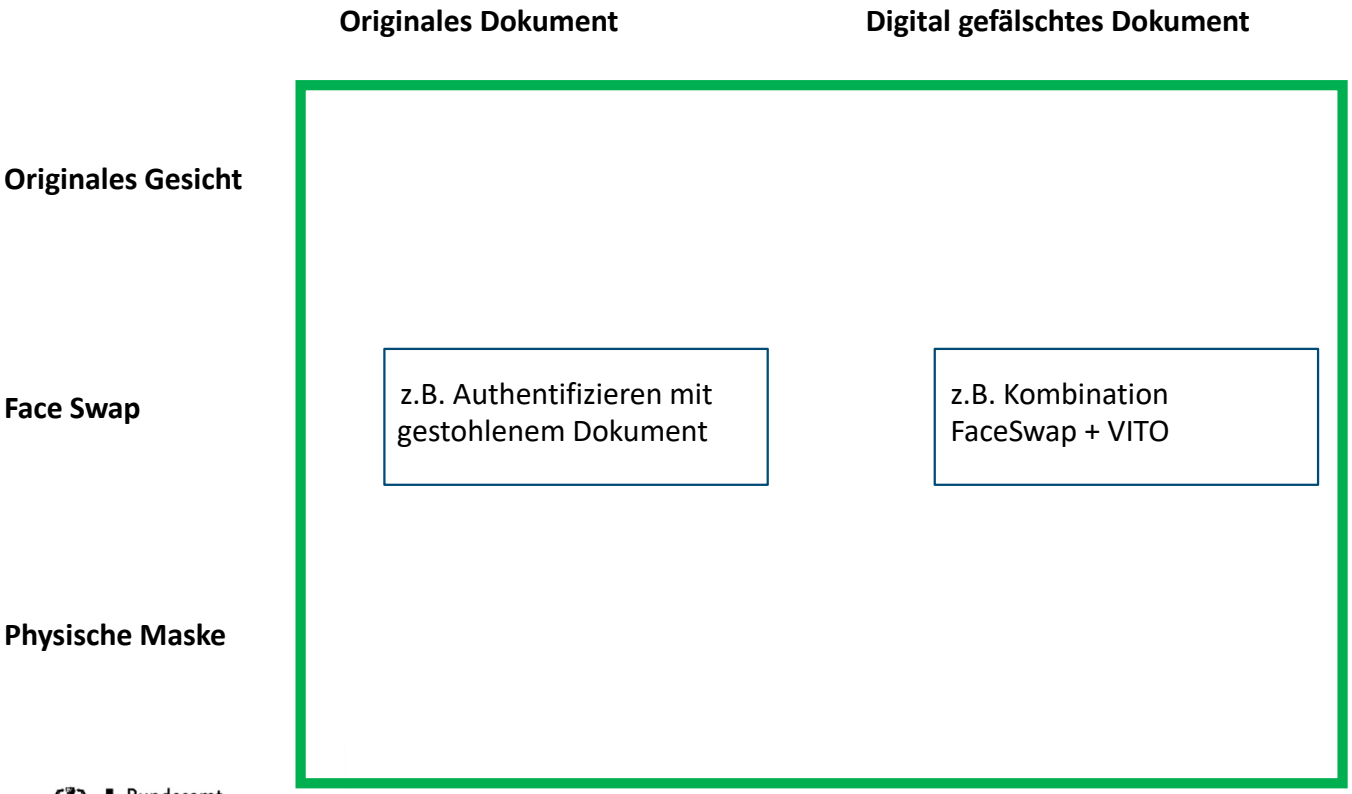
Attack / Criteria	Elapsed Time[1]	Expertise	Knowledge of TOE	Window of Opportunity	Equipment	Total ∑
Original Face + Digital mod. document	<= one day, 0	Proficient, 3	Public, 0	Unlimited access, 0	Standard, 0	3

- **Erste Einschätzung, keine finale Bewertung.**

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

1. Die Softwareentwicklung wird nicht als „Elapsed Time“ angesehen, da die Software stark reproduzierbar und verteilbar ist. Nur die benötigte Zeit für die Anwendung auf die Zielidentität wird berücksichtigt.

Demonstration Face Swap



Beispiel (Face-Swap)

Einschätzung des Angriffspotentials von Face Swap (+VITO) nach CEM-Kriterien

Attack / Criteria	Elapsed Time[1]	Expertise	Knowledge of TOE	Window of Opportunity	Equipment	Total ∑
Face Swap + stolen document	<= one week, 1	Proficient, 3	Public, 0	Unlimited access, 0	Standard, 0	4
Face Swap + Digital mod. document	<= one week, 1	Proficient, 3	Public, 0	Unlimited access, 0	Standard, 0	4

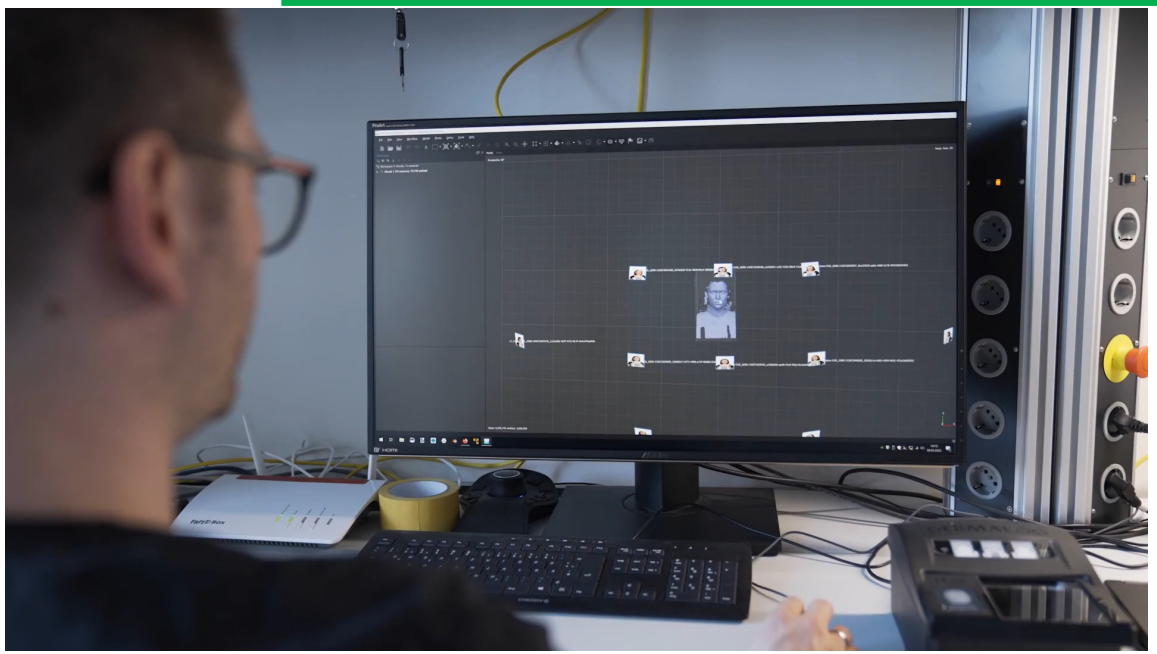
- **Erste Einschätzung, keine finale Bewertung.**

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

1. Die Softwareentwicklung wird nicht als „Elapsed Time“ angesehen, da die Software stark reproduzierbar und verteilbar ist. Nur die benötigte Zeit für die Anwendung auf die Zielidentität wird berücksichtigt.

Demonstration Maske

	Originales Dokument	Digital gefälschtes Dokument
Physische Maske	Masken, Schminke, …	z.B. Kombination Maske + VITO



Quelle: www.SPFXmasks.com

Einschätzung des Angriffspotentials von Maske (+VITO) nach CEM-Kriterien

Attack / Criteria	Elapsed Time[1]	Expertise	Knowledge of TOE	Window of Opportunity	Equipment	Total ∑
Physical Mask + (original document / Physically crafted document	<= two weeks, 2	Proficient, 3	Public, 0	Unlimited access, 0	Standard, 0	5

- **Erste Einschätzung, keine finale Bewertung.**

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

1. Die Softwareentwicklung wird nicht als „Elapsed Time“ angesehen, da die Software stark reproduzierbar und verteilbar ist. Nur die benötigte Zeit für die Anwendung auf die Zielidentität wird berücksichtigt.

Übersicht – Einordnung der Angriffe

Attack / Criteria	**Total ∑**
Original Face + **Digital** mod. document	3
Face Swap + stolen document	4
Face Swap + Digital mod. document	4
Physical Mask + (original document / Physically crafted document	5

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components::	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	Beyond High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

CEM	TR 3147
enhanced-basic	normal
moderate	substantial
high	high

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Kontakt

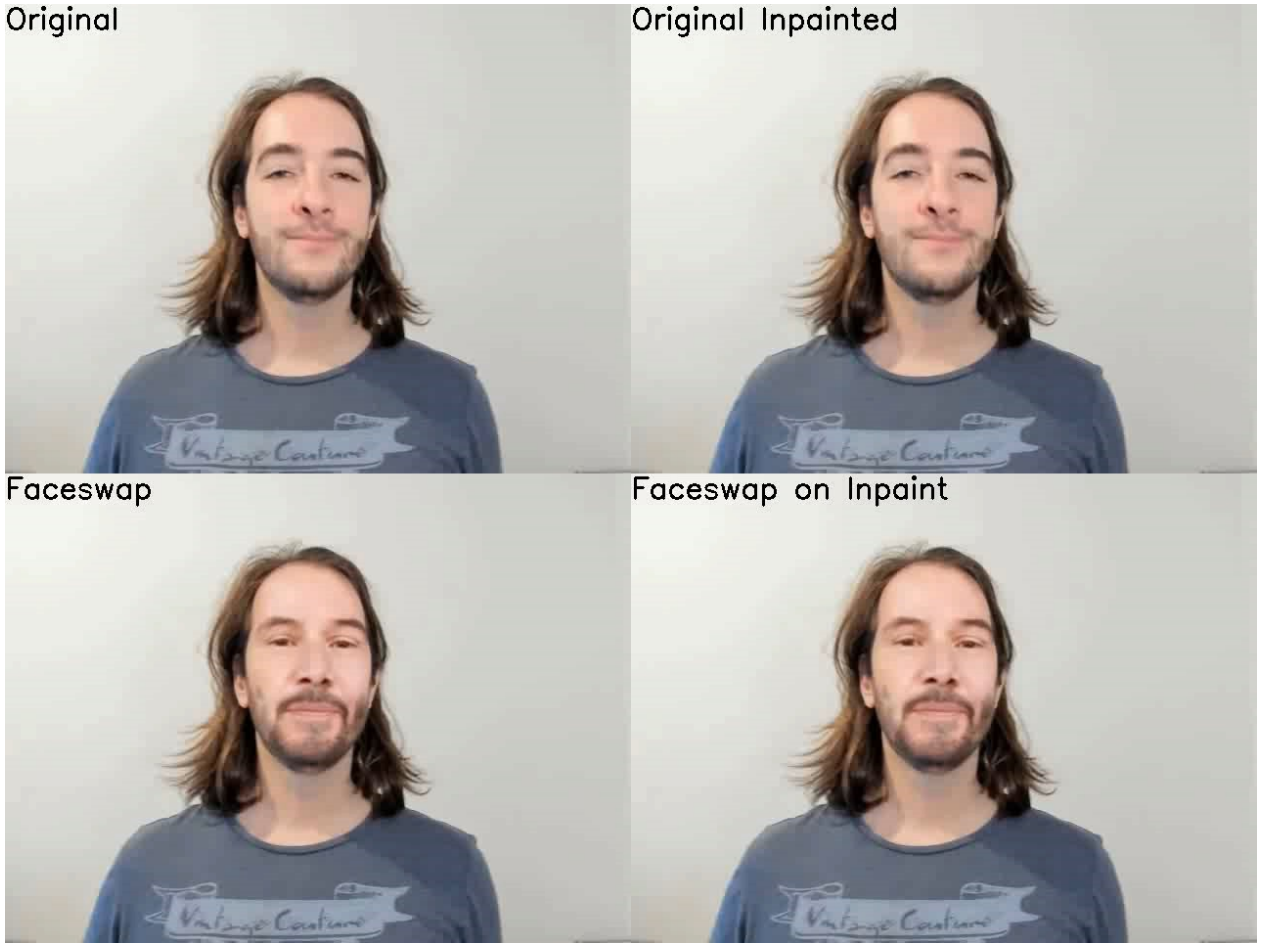
Matthias Neu
Referent

matthias.neu@bsi.bund.de
Tel. +49 (0) 228 9582 6604

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Backup: Überwindung von Gegenmaßnahmen
10€ Lösung gegen Gesichtsverdeckung



Backup: Überwindung von Gegenmaßnahmen
Alternative Lösung mittels Tiefenkamera