HANDBUCH BIOMETRIE HACKEN

KANNA LONI

gfk

HANDBUCH BIOMETRIE HACKEN

Kanna Loni

Berlin, März 2019
anna.kraher@servus.at

INTRO

INTRO

Alltäglich haben wir mit ihnen zu tun: biometrischen Systemen. Ob Gesichtserkennungssoftware im öffentlichen Raum oder Fingerabdrucksensoren auf unseren Smartphones. Biometrische Systeme sind Systeme zur Vermessung gewisser Merkmale von Lebewesen. Diese reichen von bekannteren Merkmalen wie Fingerabdruck, Iris, Gesicht und DNA bis über Handgeometrie, Venenstruktur, Klangfarbe der Stimme und Körpergeruch.

Sie können also sehr verschieden sein, sollten allerdings folgende 3 Anforderungen erfüllen:

1. Universalität
   Jede Person hat dieses Merkmal.
2. Einmaligkeit
   Keine 2 Personen haben das gleiche Merkmal.
3. Erfassbarkeit
   Das Merkmal muss auf eine Weise messbar sein.

In der Praxis erfüllen biometrische Eigenschaften nicht unbedingt alle diese Anforderungen. So sind beispielsweise die Fingerabdrücke von ca. 4% der Weltbevölkerung nicht eindeutig genug.

Biometrie wird sowohl zur Identifizierung, als auch zur Authentifizierung genutzt. Bei der Identifizierung handelt es sich um die Frage: Wer ist die Person? Hier wird das vorgelegte biometrische Merkmal mit allen in diesem System gespeicherten Referenzdaten verglichen. Dies wird beispielsweise in Überwachungssystemen verwendet, wie bei dem Pilotprojekt Gesichtserkennung am Bahnhof Südkreuz in Berlin.

Bei der Authentifizierung handelt es sich um die Frage: Ist die Person diejenige, die sie vorgibt zu sein? Hierbei prüft das System diese Frage durch eine Übereinstimmung – zwischen dem vorgelegten biometrischen Merkmal und dem im System zur vorgegebenen Person passenden Referenzmerkmal. Dies passiert zum Beispiel jedes mal, wenn Sie Ihr Smartphone mit Ihrem Fingerabdruck entsperren.

TRICKS & HACKS

Obwohl biometrische Systeme gerne verwendet werden, gibt es zahlreiche Schwachstellen. In diesem Handbuch soll es um verschiedene Arten und Weisen gehen, biometrische Systeme auszutricksen. Hierbei kann es sich um Unkenntlichmachung der eigenen biometrischen Merkmale handeln oder auch um Angriffe auf biometrische Systeme. Die Angriffsmöglichkeiten teilen sich in 3 verschiedene Gruppen:

1. Angriff unter Verwendung des Sensors
   Bei dieser Art von Angriffen wird dem Sensor vorgetäuscht, dass er das Merkmal der berechtigten Person erkannt hat. Hierunter zählen alle möglichen Arten von Attrappen.

2. Angriff auf die Datenkommunikation
   Hier zielt der Angriff auf die Verbindung des Sensors zum Computer. Wenn Daten beispielsweise unverschlüsselt übertragen werden, können diese abgefangen und ausgewertet werden.

3. Angriff auf die Templatedaten
   Templatedaten sind diejenigen Daten, die im System als Referenzdaten gespeichert sind. Zum Beispiel der Fingerabdruck, welcher bei der Registrierung gespeichert wird. Diese Art von Angriff zielt also direkt auf die im System gespeicherten Daten ab, indem diese gelöscht oder ausgetauscht werden.

Die Tricks & Hacks in diesem Handbuch beziehen sich auf Methoden zur Unkenntlichmachung oder sind Angriffe unter Verwendung des Sensors (Punkt 1). Diese sind oft ohne großes technisches Know-How durchführbar und benötigen meistens nicht sehr aufwendige finanzielle und zeitliche Ressourcen. In den Preisangaben der Anleitungen sind benötigte Gegenstände wie Computer, Drucker, Fotobearbeitungssoftware und Digitalkamera nicht inkludiert.

So let's get started!

FINGER ABDRUCK SENSOR

UNKENNTLICH MACHEN

Diese Anleitung kann benutzt werden, um Fingerabdrücke unkenntlich zu machen. Beispielsweise für die Beantragung eines neuen Reisepasses mit gespeicherten Fingerabdrücken (ePass).

Sekundenkleber
Wattestäbchen

zum Entfernen (optional):
Vaseline/Babyöl
Backpulver
Aceton
Seifenlauge
Gallseife
Spülmittel
Nagellackentferner
Stahlwolle/Topfkratzer
Nagelfeile


leicht


20min


3-10€

1. Zuerst eine kleine Menge Sekundenkleber auf die Mitte der Fingerkuppe auftragen.

2. Mit dem Plastikröhrchen eines Wattestäbchen den Kleber auf der Fingerkuppe verstreichen. Wichtig: den Sekundenkleber dünn auftragen, da er, wenn er zu dick aufgetragen wird brechen kann, was später an den Fingern zu sehen ist. Des Weiteren sollte die Schicht in einem Durchgang aufgetragen werden, da bei mehreren Schichten an den überlappenden Stellen weiße Ränder zu sehen sind.

3. Den überschüssigen Kleber mit dem Wattebausch des Stäbchens schnell abnehmen, sodass die Watte nicht an dem Kleber haften bleibt.

4. Der Sekundenkleber sollte nun die Papillarlinien (Rillen des Fingerabdrucks) ausgefüllt und somit den Fingerabdruck unkenntlich gemacht haben. Der Sekundenkleber wird sowohl beim Waschen der Hände als auch beim Benutzen von Handcreme haften bleiben.

5. Falls Sie diese Anleitung für die Beantragung eines Reisepasses mit eingescannten Fingerabdrücken verwenden, stellen Sie sicher, dass Sie eine Erklärung für Ihre unkenntlichen Fingerabdrücke haben. (Bspw. Hautkrankheiten oder erklären Sie, dass Sie in Ihrem Job mit Chemikalien wie Säuren oder Laugen arbeiten oder auch mit Schleifpapier. Beispielberufe/-hobbies dafür: Modellbau, Chemiker_in, Laborant_in, Mediziner_in, Fotografie/Filmentwicklung, Maler_in, Putzkraft, Autolackierer_in, Eisenbahnmodellbauer_in, Friseur_in, Künstler_in etc.)

6. Die eingeschmierten Stellen blättern schnell ab, deswegen ist es wichtig die Fingerkuppen erst kurz vor dem Fingerabdruckabgabetermin zu benetzen.

7. Normalerweise löst sich der Sekundenkleber nach einigen Tagen von selbst ab. Wenn man den Vorgang beschleunigen will, helfen Vaseline, Babyöl, Backpulver, Aceton, Seifenlauge, Gallseife, Spülmittel, Nagellackentferner, Stahlwolle/Topfkratzer oder eine Nagelfeile.

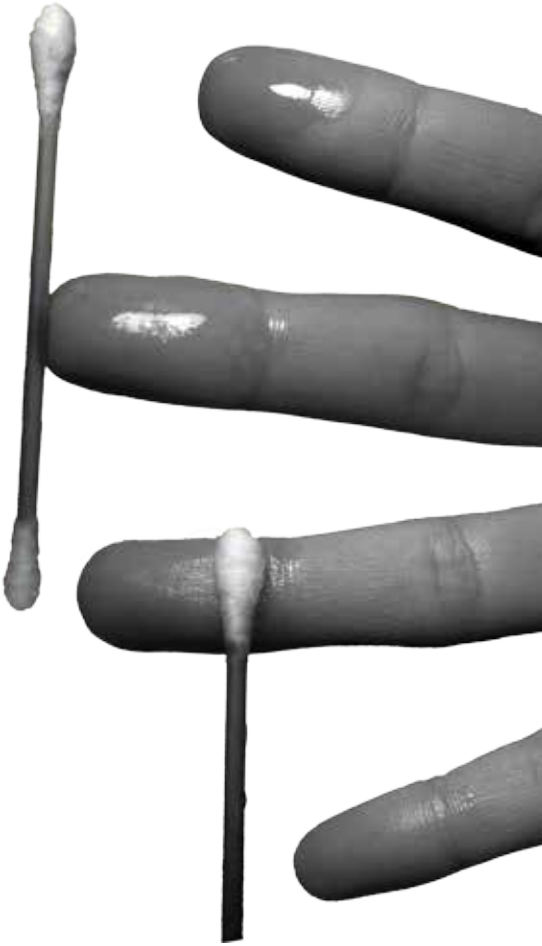

Abb. 1

ABDRUCK-VOM-GLAS-VERSION

Der Chaos Computer Club (CCC) hat auf ähnliche Art und Weise 2008 den Fingerabdruck des damaligen Bundesinnenministers Wolfgang Schäuble nachgemacht und veröffentlicht. Mit dieser Aktion protestierte der CCC gegen die zunehmende Erfassung und Verwertung biometrischer Daten.

Graphit Stäbchen (evtl. auch Kreide)
Schleifpapier
weicher Pinsel
transparentes Klebeband
weißes (bzw. schwarzes) Papier
Digitalkamera
Computer mit Fotobearbeitungssoftware
Drucker
durchsichtige Folie
Holzleim
Schere
hautfreundlicher Kleber


mittel


3h


30€

1. Zuerst wird der zu fälschende Fingerabdruck benötigt (z.B. zu finden an einem Glas).

2. Als nächstes das Graphitstäbchen (bzw. die Kreide) mithilfe des Schleifpapiers zu Pulver verreiben (alternativ kann auch gleich Graphitpulver verwendet werden). (siehe Abbildung auf Seite 17).

3. Nun eine großzügige Menge Graphitpulver auf die Stelle des Fingerabdrucks auftragen. Anschließend dieses mit dem Pinsel mit kleinen kreisenden Bewegungen vorsichtig auf dem Abdruck verteilen. Das überschüssige Pulver mit dem Pinsel abtragen und eventuell vorsichtig wegpusten. (siehe Abbildung auf Seite 17).

4. Ein Stück Klebefilm abreißen und dieses auf die Stelle des Abdrucks kleben. Das Klebeband wieder abnehmen und auf ein weißes Blatt Papier kleben. Wenn weiße Kreide verwendet wurde, dann ein schwarzes Blatt Papier benutzen. (siehe Abbildungen auf Seite 17/18).

5. Ein möglichst scharfes Foto von dem Fingerabdruck machen. Die Papillarlinien in einem Fotobearbeitungsprogramm klar erkennbar machen und das Foto an die tatsächliche Größe des Fingers anpassen (siehe Abbildung auf Seite 19).

6. Das Foto auf einer durchsichtigen Folie mit einem Tintenstrahldrucker ausdrucken. Die Druckerschwärze bildet somit eine 3-dimensionale Struktur.

7. Nun ca. 1 cm Holzleim auf dem ausgedruckten Fingerabdruck verstreichen. Den Leim trocknen lassen und den Fingerabdruck ausschneiden. Den getrockneten Holzleim von der Folie lösen und mit dem hautfreundlichen Kleber am Finger ankleben.

Abb.2

Schritt 2 (1)

Schritt 3

Schritt 2 (2)

Schritt 4

(zum Schutz wurde dieses Bild entschärft)

Abb.3

Abb. 4

FOTO-VERSION

2014 wurde auf diese Art und Weise vom CCC der Fingerabdruck von Ursula von-der-Leyen veröffentlicht (siehe Abbildung rechts).

hochauflösendes Foto des Fingers
Computer
Fotobearbeitungssoftware
Drucker
durchsichtige Folie
Holzleim
Schere
hautfreundlicher Kleber


mittel


2h


20€

1. Am Computer mit der speziellen Fotobearbeitungssoftware den Fingerabdruck extrahieren und so bearbeiten, dass die Linien deutlich zu sehen sind.

2. Dann Schritte 5-7 wie in der Abdruck-vom-Glas-Version.

Abb.5

IRIS SCANNER

IRIS-SCANNER

2014 wurde vom CCC eine Irisattrappe von Angela Merkel angefertigt.

Digitalkamera mit Infrarot-/Nachtmodus
Drucker
Kontaktlinse
Pinzette


leicht


15min


5-10€

1. Als erstes ein Foto von den Augen der betreffenden Person im Infrarotmodus machen.

2. Als nächstes das Foto ausdrucken.

3. Die Kontaktlinse auf das Auge des ausgedruckten Fotos legen (siehe Abbildung unten).

4. Das zu hackende Gerät mit dem Irisscanner kann nun mit dem ausgedruckten Foto entsperrt werden.

Abb. 6

GESICHTS-ERKEN-NUNG

2D-ERKENNUNG

Diese Anleitung kann bei Geräten mit Gesichtserkennungssoftware ohne 3D-Funktion und mit Blinzelschutz verwendet werden.

Digitalkamera
Drucker (optional)
Papier (optional)
Stift (optional)


leicht


2-15min


1€

1. Ein Foto von dem Gesicht der betreffenden Person machen.

2. Foto direkt vom Anzeigedisplay des Geräts vor die Kamera des zu entsperrenden Geräts halten.

3. Falls bei Schritt 2 Probleme auftauchen sollten, das Gerät zu entsperren, das Foto ausdrucken und den Ausdruck vor die Kamera des zu entsperrenden Geräts halten.

4. Falls das Gerät zusätzlich mit Lebenderkennung durch Blinzeln geschützt ist, einen Stift von oben nach unten über das Foto bewegen, um das Blinzeln zu imitieren.

IPHONE X - FACE-ID

Die folgende Anleitung kann verwendet werden, um die Face-ID Funktion des iPhone X zu knacken. Diese arbeitet mit 3D-Gesichtserkennung. (Stand: September '18) Auf den folgenden Seiten sind zwei Versionen von Masken zu sehen, mit welchen die Gesichtserkennung des iPhone X bereits geknackt wurde. Diese Anleitung bezieht sich auf die Maske auf Seite 33.

Computer
spezielles 3D-Programm
3D-Drucker unter Verwendung
von Sandstein
Digitalkamera mit Infrarot-/Nachtmodus
Drucker
Papier
Schere
Steinfarbe (optional)


schwer


ab 9h


ca. 200€

1. Fotos des Gesichts der betreffenden Person aus verschiedenen Perspektiven machen. Mithilfe des speziellen 3D-Programms die Fotos in ein virtuelles 3D-Objekt verarbeiten.

2. Das 3D-Modell mit einem 3D-Drucker unter Verwendung von Sandstein ausdrucken. PLA (Polylactides) Plastik, welches oft beim 3D-Druck verwendet wird, ist bei Wellen von 940-950 Nanometer (nm) transparent. In dieses Spektrum fällt Infrarot (780-30.000 nm), welches die Kamera des iPhones X für die Gesichtserkennung mit Face-ID verwendet.

3. Optional kann der einfärbige 3D-Druck noch mit Steinfarbe angemalt werden um die Kontraste im Gesicht stärker hervorzuheben.

4. Anschließend ein Foto von den Augen der betreffenden Person im Infrarotmodus machen.

5. Die Augen in der richtigen Größe ausdrucken, zuschneiden und auf das Modell an die Stelle der Augen kleben.

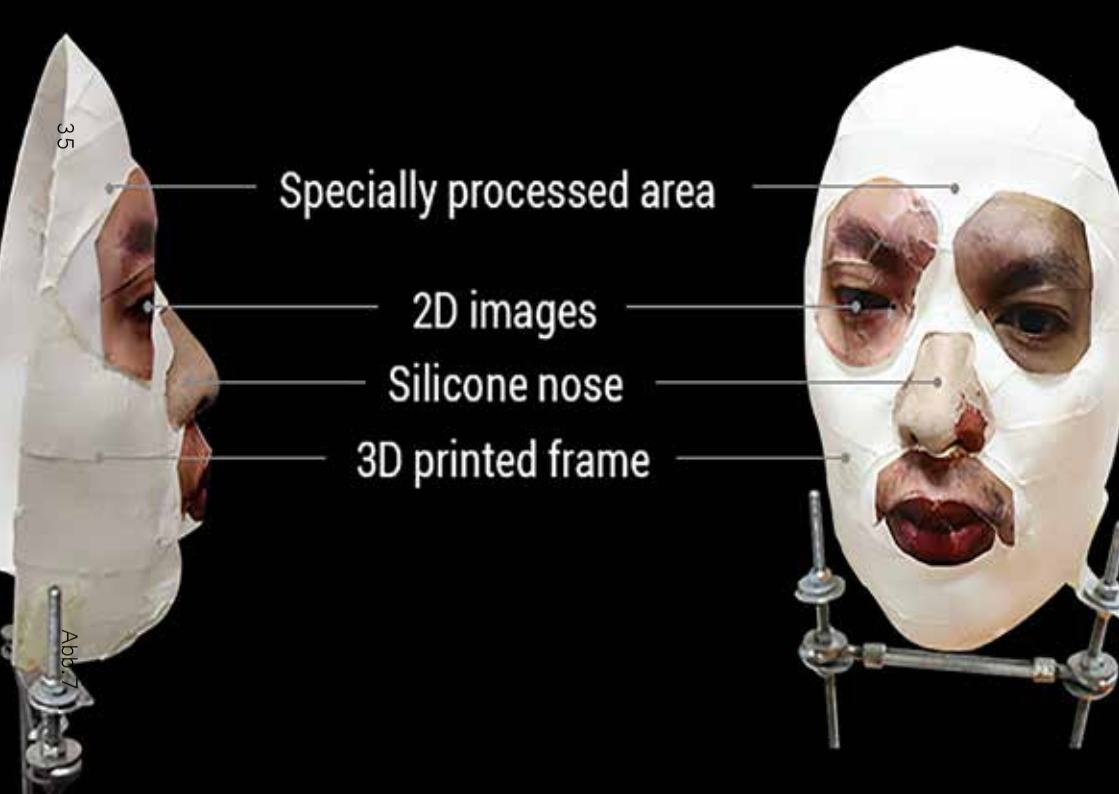
Specially processed area
2D images
Silicone nose
3D printed frame

Abb. 7

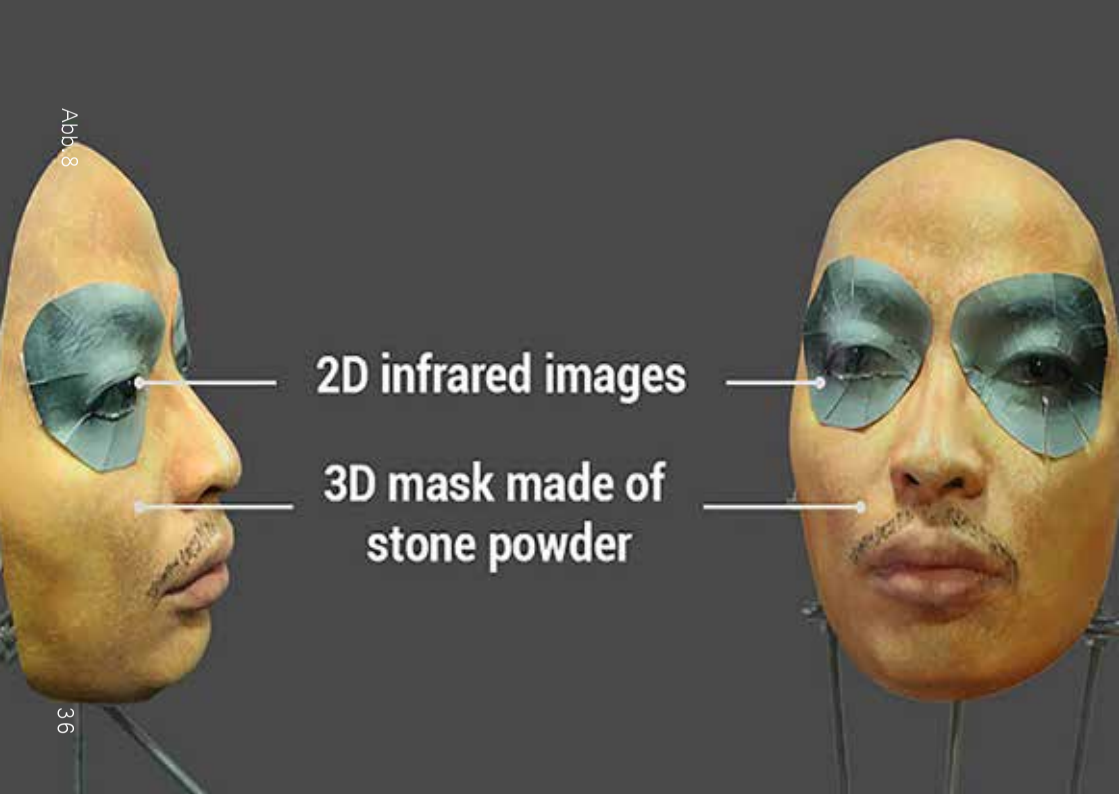

Abb. 8

SCHMINKTIPPS

Zur Abwehr von Gesichtserkennungssoftware, die nicht zur Authentifizierung, sondern zur Überwachung gedacht ist – wie beispielsweise das seit August 2017 bestehende Pilotprojekt am Bahnhof Südkreuz in Berlin – können sich folgende Schminktipps eignen.

Gesichtsschminke
Schwamm (optional)
Schminkpinsel (optional)

Gesichtsschminke öffnen und mit einem Schwamm, Pinsel, einem anderen Schminkapplikator oder dem Finger auf das Gesicht auftragen. Die folgenden Abbildungen auf den nächsten Seiten dienen als graphische Anleitungen.


leicht


15min

3€

1. Konturen vermeiden, da diese das Gesicht leichter erkennbar machen. Dunkle und helle Stellen im Gesicht in ihr Gegenteil verkehren.

2. Den Nasenrücken verdecken, da die Augen-Nasen-Stirn Region wichtig für die Gesichtserkennung ist.

3. Eines oder beide Augen teils verdecken, da die Symmetrie und die dunkle Kontur der Augen ein Hauptmerkmal des Gesichts darstellt.

4. Die elliptische Kopfform optisch verändern, indem beispielsweise Haare, Rollkragenpullover und andere Accessories dafür benutzt werden.

5. Asymmetrie, hilft die von der Gesichtserkennungssoftware erwartet Symmetrie der linken und rechten Gesichtshälfte zu unterwandern und somit diese zu täuschen.

Abb.9

Abb. 10

Abb. 11

QUELLEN

INTRO

Müller, Wolf: Sicherer Kanal von Alice zu Bob. Authentifizierung: Sein=Biometrie, in: IT-Sicherheit Grundlagen (Folien), Humboldt Universität zu Berlin, Computer Science Departement, Systems Architecture Group, S.11-13, 15, 19, 29-31

FINGERABDRUCK

verschlüsseln.org: Fingerabdrücke entfernen / unkenntlich machen?
Link: http://www.verschlüsseln.org/fingerabdruecke-entfernen-unkenntlich-machen/
(Zugriff: 20.09.18, 19:09 MEZ)

Kleinz, Torsten: CCC publiziert die Fingerabdrücke von Wolfgang Schäuble [Update], in: heise.de
Link: https://www.heise.de/security/meldung/CCC-publiziert-die-Fingerabdruecke-von-Wolfgang-Schaeuble-Update-193732.html
(Zugriff: 25.10.18, 16:35 MEZ)

“CCC Anleitung Fingerabdruck fälschen”- Youtube
Link: https://www.youtube.com/watch?v=OPtzRQNHzl0
(Zugriff: 07.09.18, 16:57 MEZ)

“Hacker kopiert Fingerabdruck von normalem Foto! - Clix-oom - Science & Fiction” - Youtube
Link: https://www.youtube.com/watch?v=CqJTWwq26FI (Zugriff: 07.09.18, 16:59 MEZ)

IRISSCANNER

“Die Sendung mit dem Chaos - Iris Scanner im Samsung Galaxy S8” - Youtube
Link: https://www.youtube.com/watch?v=4VrqufsHpS4 (Zugriff: 07.09.18, 17:00 MEZ)

GESICHTSERKENNUNG

“Galaxy S8: So hebelt man die Gesichtserkennung aus” - Youtube
Link: https://www.youtube.com/watch?v=FZPrC6QEGDY (Zugriff: 07.09.18, 17:01 MEZ)

“Bkav’s New Mask Beats Face ID in “Twin Way”: Do not Use Face ID in Business Transactions” - Youtube
Link: https://www.youtube.com/watch?time_continue=217&v=rhiSBc061JU (Zugriff: 28.09.18, 14:09 MEZ)

“Trying to Hack iPhone Face ID” - Youtube
Link: https://www.youtube.com/watch?v=54PHOyGoPnM
(Zugriff: 07.09.18, 17:04 MEZ)

“How Bkav tricked iPhone X’s Face ID with a mask” - Youtube
Link: https://www.youtube.com/watch?v=i4YQRLQVixM
(Zugriff: 07.09.18, 17:06 MEZ)

Harvey Adam: “CV Dazzle, Camouflage from face-detection”, Posted 2011-09-01
Link: https://ahprojects.com/cvdazzle/
(Zugriff: 29.01.19, 21:40 MEZ)

ABBILDUNGEN

Abb. 1 / Abb. 2 / Abb. 3 / Abb. 4
Bild: Kanna Loni

Abb. 5
Bild: Starbug
Link: https://www.heise.de/security/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html
(Zugriff: 07.09.18, 17:16 MEZ)

Abb. 6
Bild: Starbug
Screenshot aus: “Die Sendung mit dem Chaos - Iris Scanner im Samsung Galaxy S8” - Youtube
Link: https://www.youtube.com/watch?v=4VrqufsHpS4
(Zugriff: 07.09.18, 17:00 MEZ)

Abb. 7 / Abb. 8
Bild: Bkav
Link: http://www.bkav.com/d/top-news/-/view_content/content/103968/bkav%92s-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions (Zugriff: 13.12.18, 13:31 MEZ)

Abb. 9
Zeichnungen: Ilona Eidinger
Grafik: Kanna Loni
angelehnt an: Adam Harvey
Link: http://www.fredaktion.de/fakingsleep/wp-content/uploads/schminke-gegen-gesichtserkennung.jpg
(Zugriff: 07.09.18, 17:24 MEZ)

Abb. 10 / Abb. 11
Bild: Grigory Bakunov
Link: https://telegra.ph/Novyj-makiyazh-korolya-07-14
(Zugriff: 28.09.18, 13:58 MEZ)