ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

An
Das Bundesministerium des Innern

Nationales Forschungszentrum für angewandte Cybersicherheit

Prof. Dr. Christoph Busch

Hochschule Darmstadt
Haardtring 100
64293 Darmstadt
Tel. +49-6151-16-30090

christoph.busch@h-da.de

2020-01-27

Stellungnahme zum Gesetzentwurf zur Stärkung der Sicherheit im Pass- und Ausweiswesen

Sehr geehrte Damen und Herren,

Ich bin dankbar für den Entwurf des Gesetzes zur Stärkung der Sicherheit im Pass- und Ausweiswesen vom 9. Dezember 2019. Der Entwurf ist richtig und wichtig und wird ermöglichen, dass Deutschland zu den Europäischen Vorreitern im Live-Enrolment (Schweden und Norwegen) endlich aufschließen kann.

zur Technik:
Ich kann Ihre Annahme bestätigen, dass derzeit m.W. alle Produkte zur automatisierten Gesichtserkennung durch Morphing-Angriffe verwundbar sind. Es ergeben sich hohe Übereinstimmungswerte für beide im Lichtbild „enthaltenen“ Personen, die denen von unveränderten Lichtbildern entsprechen.

Es gibt zwei Alternativen zur Prävention von Morphing-Angriffen:

1.) Live-Enrolment in Deutschland und allen anderen EU-Ländern
2.) Elektronische Übertragung von digital signierten Lichtbildern direkt von autorisierten Photographen an die Passbehörde (ebenfalls in allen EU-Ländern)

zu 1.): das ist die langfristig sinnvollste Lösung.
zu 2.): dies könnte z.B. durch de-mail realisiert werden und würde die Bedenken der Photographen-Lobby entkräften. Deren Bedenken kann ich zwar verstehen - sie sind aber nicht mehr zeitgemäß. Und m.W. werden die Digitalisierungs-Bemühungen der Bundesregierung ja auch von den Oppositionsparteien getragen. Warum sollte man hier eine Ausnahme machen?

Im direkten Vergleich ist die Alternative 1.) klar zu favorisieren. Erstens aus Gründen der Sicherheit des Verarbeitungsprozesses, da Alternative 2.) möglicherweise Einbringpunkte für manipulierte/gemorphte Lichtbilder zulassen würde. Zweitens sind auch bei Alternative 2.) bisher nicht kalkulierte Kosten für die sichere digitale Bildübertragung (und dem damit verbundenen logistischen Aufwand) anzunehmen.

Unabhängig von 1.) und 2.) ist es notwendig, Morphing-Attack-Detection (MAD) Verfahren zu entwickeln, die für den Einsatz an der Grenze zur Detektion von Pässen mit gemorphten Lichtbildern z.B. aus Drittstaaten geeignet sind. siehe: https://christoph-busch.de/projects-mad.html
Es gibt mittlerweile etliche Forschungsaktivitäten, um gemorphte Lichtbilder zu erkennen. Die Detektionsleistung und insbesondere die Falschalarmraten solcher MAD-Verfahren sind derzeit ungenügend und für den operativen Einsatz noch nicht geeignet. siehe:
https://pages.nist.gov/frvt/reports/morph/draft_frvt_morph_report_2020jan24.pdf

Änderungsvorschlag:
Abweichend von Abschnitt B Besonderer Teil, sollte das Gesetz m.E. nicht *einen* Anbieter von Live-Enrolment vorsehen, sondern einen Standard vorgeben - z.B. eine BSI-TR unter Berücksichtigung von ISO/IEC NP 24358 *Face-aware capture subsystem specifications*, das derzeit in Entwicklung ist. So könnten *mehrere* Lieferanten / Betreiber unter Einsatz von verschiedenen Produkten zum Einsatz kommen, wenn diese Produkte nach der zu definierenden TR zertifiziert wurden. Zudem könnten bisher tätige Photographen als Dienstleister der Passbehörden in den Betrieb der Kioske eingebunden werden und so einen Marktanteil behalten. Daher sollte es in §1(5) lauten:
NEU: Das Bundesministerium des Innern, für Bau und Heimat bestimmt den Passhersteller sowie die Lieferanten von Geräten zur Aufnahme und elektronischen Erfassung von Lichtbild und Fingerabdrücken und macht deren Namen im Bundesanzeiger bekannt. Die Lieferanten von Geräten müssen die Kriterien erfüllen, die dazu vom BSI in einer technischen Richtlinie formuliert werden.

Weitere Änderung der Formulierung:
Für die Übergangsphase (bis zum Zeitpunkt, an dem in allen Passbehörden Live-Enrolment eingesetzt ist) sollte die Abgabe von gemorphten Lichtbildern explizit *verboten* sein. Das Einbringen eines verschmolzenen Lichtbildes in ein Personaldokument ist m.E. bisher nicht strafbar. Hier ist zu prüfen, ob PaßG §4(3) ggfls. wie folgt geändert werden kann:
ALT: "Auf Grund der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004, auf dem das Lichtbild, Fingerabdrücke, die Bezeichnung der erfassten Finger, ..."

NEU: "Auf Grund der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004, auf dem das Lichtbild, welches den Passbewerber und *nur* diesen repräsentiert, Fingerabdrücke, die Bezeichnung der erfassten Finger, ..." Oder alternativ NEU als zusätzlichen Satz: "Die Verwendung von manipulierten Lichtbildern ist nicht zulässig. Die Verschmelzung von Lichtbildern mehrerer Personen (Morphing-Angriff) in der Passbeantragung ist strafbar.“

zur Begründung des Live-Enrolment:
Wie im FAZ-Beitrag "Ein Pass für Zwei" von Piotr Heller am 20. Januar berichtet, ergab eine Umfrage unter den Experten auf der Security Printers Konferenz, dass eine relevante Anzahl von Pässen mit gemorphten Lichtbildern in den letzten 5 Jahren detektiert wurden. Darüber hinaus gibt es Hinweise auf eine hohe Dunkelziffer. Diese hohe vermutete Dunkelziffer ist auch durch die fehlenden Detektionsmöglichkeiten von gemorphten Lichtbildern zu erklären. Es gibt derzeit keine verlässliche Möglichkeit, ein gemorphtes Bild als solches zweifelsfrei zu erkennen.

Wir reden seit viereinhalb Jahren über Migration. Ich glaube, dass das nur der Anfang von dem ist, was wir in den nächsten Jahrzehnten als Migration erleben werden. Ein Grund ist, dass der Klimawandel in Afrika viele Menschen dazu zwingen wird, ihre Länder zu verlassen.

Die Menschen in Afrika haben Zugang zum Internet. Sie lesen die Nachrichten aus Europa und sie lesen auch unsere Publikationen, die sich im Allgemeinen mit dem Thema Biometrie befassen. Das weiß ich, da ich Fragen zu unseren Publikationen bekomme. Es ist naheliegend, dass Migranten auch über Morphing-Angriffe Bescheid wissen und in Zukunft eine Flugreise (mit entsprechend manipuliertem Pass) einer Schlauchboot-Seereise vorziehen werden.

Aus diesem Grund schreiben Sie zu recht im Entwurf: "*Die Funktion des Passes als Dokument zur Identitätskontrolle ist damit im Kern bedroht*." Das ist noch eine vorsichtige Formulierung! Sollte sich die Kenntnis über die Verwundbarkeit der Gesichtserkennung bei Morphing-Angriffen ausbreiten, dann kann man die derzeitigen Prozesse an der Grenze nur noch als "Abschreckung" vor Angriffen, aber nicht mehr als "Kontrolle" und Abweisung von unerlaubten Grenzübertritten bezeichnen.

Vor dem Hintergrund der massiven Verbreitung biometrischer Systeme an den Grenzen müssen Präventionsmaßnahmen gegen Morphing sowohl die Vermeidung des Einbringens von manipulierten Lichtbildern in nationale Personaldokumente (hier: verpflichtende Aufnahme der Passbilder *in* den Behörden) als auch die sichere Detektion von gemorphten Bildern in Dokumenten aus Drittstaaten (hier: Forschung und Entwicklung) umfassen.

Mit freundlichen Grüßen

Prof. Dr. Christoph Busch