PassGlobe: Ein Shoulder-Surfing resistentes Authentifizierungsverfahren für Virtual Reality Head-Mounted Displays

Tobias Länge*
Philipp Matheis*
tobias.laenge9@kit.edu
philipp.matheis9@kit.edu
Karlsruher Institut für Technologie (KIT)
Karlsruhe, Deutschland

Reyhan Düzgün
reyhan.duezguen@kit.edu
Karlsruher Institut für Technologie (KIT)
Karlsruhe, Deutschland

Peter Mayer
peter.mayer@kit.edu
Karlsruher Institut für Technologie (KIT)
Karlsruhe, Deutschland

Melanie Volkamer
melanie.volkamer@kit.edu
Karlsruher Institut für Technologie (KIT)
Karlsruhe, Deutschland

Abbildung 1: Beim Authentifizierungsverfahren *PassGlobe* müssen mehrere Orte auf einer Weltkugel ausgewählt werden, um sich zu authentifizieren. Die Weltkugel kann mit den Händen gedreht und mit einem Pointer eine Stelle ausgewählt werden.

ZUSAMMENFASSUNG

Mit Virtual Reality (VR) kann in virtuelle Welten eingetaucht und mit einer immersiven 3-D Umgebung interagiert werden. Das virtuelle Erlebnis wird dabei durch Head-Mounted Displays (HMDs) realisiert. Der zunehmende Einsatz von VR durch Unternehmen und Privatpersonen in unterschiedlichen Bereichen setzt sichere und nutzerfreundliche Authentifizierungsverfahren voraus. Dabei ist die Gefahr von Shoulder-Surfing Angriffen während der Authentifizierung besonders groß, da man während des VR-Erlebnisses von der realen Umgebung komplett isoliert ist. In dieser Arbeit wird existierende Literatur zu VR-Authentifizierung anhand vorher definierter Anforderungen evaluiert und das graphische Authentifizierungsverfahren *PassGlobe* vorgeschlagen, welches resistent gegenüber Shoulder-Surfing Angriffen ist.

SCHLAGWÖRTER

Authentifizierung, Virtual Reality, Virtual Reality Head-Mounted Displays, Shoulder-Surfing

1 EINLEITUNG

Sowohl im privaten als auch im kommerziellen Bereich finden VR-Head-Mounted Displays (HMDs) immer weitere Verbreitung. So werden diese nicht nur als Unterhaltungsmedium, sondern auch für Trainings [3] oder zur 3D-Darstellung in der Produktentwicklung [2] verwendet. Die Nutzung wird vermutlich auch in Zukunft weiter steigen, da Firmen wie beispielsweise Meta große Projekte, wie das Metaverse[1], für VR umsetzen wollen. Werden auf diese Weise VR-HMDs immer weiter in unser alltägliches Leben integriert, spielt die Sicherheit dieser Geräte eine wichtige Rolle. Dazu werden sichere und nutzbare Authentifizierungsverfahren für VR-HMDs benötigt, um den Zugang zu diesen Geräten zu schützen. Da diese Geräte auch in Gegenwart anderer Personen genutzt werden, und sich die Bewegungen während der Authentifizierung nicht verstecken lassen, stellen Shoulder-Surfing-Angriffe ein besonderes Risiko bei VR-HMDs dar [11]. Deshalb sind etablierte

*Beide Autoren haben gleichermaßen zu dieser Arbeit beigetragen.

MuC'22, 04.-07. September 2022, Darmstadt

https://doi.org/10.18420/muc2022-mci-ws01-462

[1] https://about.facebook.com/meta/ (Abrufdatum: 2022-01-28)

Verfahren, wie eine klassische PIN-Eingabe, nicht geeignet. In dieser Arbeit stellen wir grundlegende Anforderungen für Authentifizierungsverfahren für VR-HMDs auf. Anhand dieser analysieren wir existierende Authentifizierungsverfahren im VR-Kontext. Basierend auf den daraus resultierenden Erkenntnissen haben wir ein neuartiges, graphisches Authentifizierungsverfahren, *PassGlobe*, entwickelt um den Anforderungen gerecht zu werden. Neben klassischen wissensbasierten Authentifizierungsverfahren werden häufig biometrische Verfahren, wie Fingerabdruck-Scans, eingesetzt. In aktuellen Mobilgeräten wird jedoch zusätzlich immer ein wissensbasiertes Authentifizierungsverfahren verwendet, falls das biometrische Verfahren fehlschlägt. Aus diesem Grund sehen wir auch für VR-HMDs ein sicheres, wissensbasiertes Authentifizierungsverfahren als notwendig an. Deshalb beschränken wir uns in dieser Arbeit auf wissensbasierte Verfahren.

2 ANNAHMEN UND ANFORDERUNGEN

Zur Bewertung existierender Authentifizierungsmethoden im VR-Bereich, haben wir Anforderungen aufgestellt. Dabei liegt der Fokus auf der Sicherheit der Authentifizierungsverfahren, insbesondere dem Schutz vor Shoulder-Surfing-Angriffen.

2.1 Annahmen

Um die Anforderungen definieren zu können, mussten wir zuerst einige Annahmen an das System treffen. Da in Standalone-VR-Headsets ähnliche Hard- und Software wie in modernen Smartphones eingesetzt wird und wir von einem vergleichbaren Nutzungsverhalten ausgehen, nehmen wir ähnliche Eigenschaften an. Als Erstes gehen wir davon aus, dass das Authentifizierungsverfahren genutzt wird, um das VR-HMD zu entsperren. Alle weiteren Passwörter und Anmeldeinformationen können in einem Passwortmanager gespeichert werden, welcher ebenfalls durch das Authentifizierungsverfahren geschützt wird. Zudem nehmen wir an, dass bei besonderen Vorgängen, wie dem Bezahlen, eine erneute Authentifizierung benötigt wird. Drittens wird das Gerät durch ein Hardware-Sicherheitsmodul wie in Smartphones vor Rate-Angriffen geschützt. Dadurch kann schon eine PIN effektiv vor Angriffen schützen. Als Letztes gehen wir davon aus, dass während der Authentifizierung nur die nutzende Person selbst die Bildschirminhalte sehen kann. Dies ist eine Besonderheit von VR-HMDs im Gegensatz zu anderen Geräten, da diese direkt vor den Augen getragen werden.

2.2 Anforderungen

Zur Bewertung ob ein Authentifizierungsverfahren für den allgemeinen VR-Einsatz geeignet ist, haben wir mehrere Anforderungen aufgestellt. Dies sind drei Anforderungen bezüglich der Bedienbarkeit und zwei Sicherheitsanforderungen.

Interaktionsmethoden. Die gängigen VR-HMDs verwenden Bewegungscontroller mit unterschiedlichen Buttons zur Eingabe. Um sicherzustellen, dass die Authentifizierungsverfahren auf den verschiedenen Geräten genutzt werden können, haben wir basierend auf einer Betrachtung der gängisten VR-HMDs einige Anforderungen an die Interaktion mit dem Gerät aufgestellt: Zur Interaktion mit dem Authentifizierungsverfahren können ein HMD mit Bewegungserkennung und zwei Bewegungscontroller mit jeweils zwei Buttons, einer Trigger-Taste und einem Analog-Stick oder Touchpad zur Navigation in vier Richtungen verwendet werden. Außerdem dürfen Bewegungen nur im Sichtfeld des HMDs stattfinden, da sonst manche Tracking-Verfahren die Hände nicht korrekt erfassen können.

Diskrete Interaktion. Bei der Interaktion mit VR sind Bewegungen der Hände und des Kopfes in einem gewissen Rahmen üblich. Da VR-HMDs auch in Umgebung anderer Menschen eingesetzt werden, sollte sich die Authentifizierung in einem ähnlichen Rahmen abspielen. Deshalb fordern wir den Verzicht von auffälligen Bewegungen (z. B. sehr schnelle oder weite Bewegungen) oder Geräuschen (z.B. Sprachbefehle), da dies als unangenehm empfunden werden könnte.

Keine Spezial-Hardware. Manche Verfahren zur Authentifizierung nutzen spezielle Hardware, beispielsweise Eye-Tracking [6, 11]. Diese ist jedoch nicht in allen HMDs verfügbar, weshalb wir solche Verfahren als ungeeignet erachten.

Shoulder-Surfing-Resistenz. In der Regel kann bei der Benutzung von VR-HMDs die Umgebung nicht wahrgenommen werden, weshalb Shoulder-Surfing-Angriffe besonders einfach sind [11]. Somit sind Beobachtungen, sowohl direkt durch eine Person, als auch mithilfe von Kamera-Aufzeichnungen, unbemerkt möglich. Deshalb fordern wir, dass Authentifizierungsverfahren für VR-HMDs resistent gegen Shoulder-Surfing-Angriffe sind. Dabei definieren wir ein Verfahren als resistent, falls allein durch Beobachtungen keine Informationen über das eingegebene Passwort erlangt werden können und sich der Passwortraum somit durch Beobachtungen nicht einschränken lässt.

Passwortraum. Im Bereich von Smartphones umfasst der Passwortraum üblicherweise $10^5 - 10^6$ Möglichkeiten [1]. Dies legen wir auch als Anforderung für den VR-Bereich fest, da wir ebenfalls den Einsatz von Rate-Limitierungs-Verfahren annehmen, wie in 2.1 beschrieben. Somit ist unsere Anforderung an den Passwortraum, dass dieser ohne Anpassungen $10^5 - 10^6$ Möglichkeiten unterstützt.

3 LITERATUR-ANALYSE

In diesem Abschnitt werden Authentifizierungsverfahren für VR-HMDs aus der Literatur analysiert und die gefundenen Papiere anhand unserer Kriterien bewertet. Verfahren, welche die Anforderung *Keine Spezial-Hardware* nicht erfüllen, werden nicht weiter betrachtet. Die anderen Ansätze werden im folgenden kurz aufgegriffen und bewertet. Am Ende des Kapitels werden die Ergebnisse der Analyse zusammengefasst.

Seamless and Secure VR [8]. In der Arbeit von George et al. [8] werden zwei Authentifizierungsmethoden evaluiert. Zum einen eine 4-Stellige PIN und eine Umsetzung des Android-Patterns, bei welchem 5 – 6 Punkte auf einem 3x3 Grid miteinander verbunden werden müssen. Diese Verfahren wurden mit verschiedenen Interaktions-Methoden für VR implementiert. Da die Eingabemethoden der üblichen Interaktion mit VR-HMDs entsprechen, bewerten wir die Anforderungen bezüglich der Bedienbarkeit für alle Verfahren als erfüllt. In der von George et al. durchgeführten Studie beträgt die Quote der erfolgreichen Shoulder-Surfing-Angriffe über

alle Verfahren hinweg 18 % und somit wird es von uns als nicht Shoulder-Surfing-resistent bewertet.

Die Anforderung bezüglich des Passwortraums ist sowohl bei der PIN als auch dem Pattern erfüllt, da sich beide auf 10^5 erweitern lassen. Das Pattern lässt sich auf bis zu 140.704 (= $1.4 * 10^5$) Möglichkeiten[2] bei fixer Passwortlänge erweitern.

RubikAuth [11]. Die Arbeit von Mathis et al. [11] befasst sich mit einem für VR konzipierten Authentifizierungsverfahren namens *RubikAuth*. Bei diesem Verfahren hält die nutzende Person einen virtuellen Würfel mit Zahlen von 1-9 auf fünf verschiedenen Seiten in der Hand. Die Eingabe der Zahlen erfolgt durch drei unterschiedliche Methoden: *Controller tapping*, *Head pose* und *Eye gaze*. Die vierstellige PIN kann vollständig auf einer Seite des Würfels eingegeben werden oder auf mehrere Seiten verteilt. Die Eingabevariante *Eye gaze* verwendet Eye-Tracking-Hardware, weshalb diese die Anforderung *Keine Spezial-Hardware* nicht erfüllt.

Da theoretisch alle Bewegungen durch eine Kamera erfasst werden könnten, kann das Passwort durch entsprechende Beobachtungen vollständig ermittelt werden und somit bewerten wir das Verfahren als nicht Shoulder-Surfing-resistent. Der Passwortraum beträgt zwischen 32.805 Möglichkeiten, falls alle vier Stellen der PIN auf einer Seite eingegeben werden, und bis zu 2.099.520 Möglichkeiten, falls vier verschiedenen Seiten verwendet werden.

RoomLock [6, 7]. In den Arbeiten von George et al. [6, 7] werden verschiedene Varianten eines Verfahrens beschrieben, bei dem die nutzende Person Objekte in einem virtuellen Raum in der richtigen Reihenfolge auswählen muss. Dabei gibt es mehrere Eingabemethoden und 3 Varianten, welche die Positionen der nutzenden Person und der Objekte bestimmen. Mehrere Eingabemethoden nutzen Eye-Tracking Hardware und erfüllen deshalb nicht die Anforderung *Keine Spezial-Hardware*.

Bei einer der drei Positions-Varianten, $Position_{object}$, werden die Objekte zufällig im Raum platziert. Dadurch ist es theoretisch allein durch Beobachtungen nicht möglich zu erkennen, welches Objekt ausgewählt wird. Jedoch kann das gleiche Objekt mehrfach im Passwort vorkommen, wodurch diese Information über das Passwort erlangt werden kann. Deshalb erfüllt dieses Verfahren unser Kriterium der Shoulder-Surfing-Resistenz nicht. Wären nur unterschiedliche Objekte im Passwort erlaubt oder würden die Objekte nach jeder Eingabe zufällig verteilt werden, würde das Verfahren dieses Kriterium erfüllen. Bei der Variante $Position_{user}$ wird nur die Startposition der nutzenden Person randomisiert und bei der Basis-Variante wird keine Randomisierung verwendet. Bei beiden Varianten ist es möglich das Passwort durch Beobachtungen zu erlangen, wie auch die Studie von George et al. zeigt. Im Rahmen der Studie war der Passwortraum kleiner als 10^5 Möglichkeiten, lässt sich aber beispielsweise durch ein längeres Passwort oder eine größere Anzahl an Objekten erweitern.

3DPass [9]. In der Arbeit von Gurary et al. [9] wird ein Authentifizierungsverfahren namens *3DPass* vorgestellt. Bei diesem befindet sich die nutzende Person in einem virtuellen Haus und kann sich frei bewegen. Das Passwort zur Authentifizierung besteht aus den betretenen Räumen und dem Interagieren mit Objekten (z. B. Lichtschalter). In der Umsetzung von Gurary et al. wurde ein Xbox 360 Controller verwendet. Nach unserer Einschätzung lässt sich die Steuerung jedoch problemlos der Anforderung *Interaktionsmethoden* entsprechend anpassen ohne das Verfahren grundlegend zu ändern. Da sich bei diesem Verfahren theoretisch alle Eingaben zur Rekonstruktion des Passworts beobachten lassen, bewerten wir es als nicht Shoulder-Surfing resistent.

[2]https://github.com/delight-im/AndroidPatternLock (Abrufdatum: 2022-01-20)

Tabelle 1: Bewertung existierender Verfahren aus der Literatur basierend auf unseren Anforderungen in 2.2. ✓: Anforderung vollständig erfüllt. (✓): Anforderung teilweise erfüllt (siehe Bewertung in Abschnitt 3). ×: Anforderung nicht erfüllt.

Verfahren	Interaktionsmethoden	Diskrete Interaktion	Shoulder-Surfing-Resistenz	Passwortraum
PIN [8]	✓	✓	×	✓
Pattern [8]	✓	✓	×	✓
RubikAuth [11]	✓	✓	×	✓
RoomLock [6, 7]	✓	✓	×	✓
3DPass [9]	(✓)	✓	×	✓
SWIPE [12]	✓	✓	×	✓
PIN [16]	(✓)	✓	×	✓
Pattern [16]	(✓)	✓	×	✓
3D-Pattern [16]	(✓)	✓	×	×
ZeTA-VR [5]	(✓)	✓	✓	✓
Multi-attribute [14]	(✓)	✓	✓	✓

Pattern authentication in Virtual Reality [12]. In der Arbeit von Olade et al. [12] wurden mehrere Eingabemethoden für ein SWIPE-Pattern in VR durch eine Studie evaluiert. Dabei wurden sowohl die Usability als auch die Shoulder-Surfing-Resistenz untersucht. Von den vier vorgestellten Varianten erfüllen nur zwei die Anforderungen *Keine Spezial-Hardware*, da die anderen zusätzliche Hardware benötigen. Die Passwörter konnten in der Studie durch Beobachtungen erlangt werden und somit erfüllen die Verfahren nicht unser Kriterium der Shoulder-Surfing-Resistenz. Der Passwortraum lässt sich auf 10^5 Möglichkeiten erweitern (vgl. Analyse von *Seamless and Secure VR*).

3D-Pattern [16]. In der Arbeit von Yu et al. [16] werden drei Authentifizierungsverfahren evaluiert. Dabei handelt es sich um ein 2D-PIN-Feld, ein 2D-Android-Pattern und ein 3D-Pattern, welches durch Verbinden der Ecken eines Würfels funktioniert. In der Studie wird zur Interaktion das System *Leap Motion* verwendet. Wir gehen jedoch davon aus, dass sich das Verfahren mit wenigen Anpassungen auch auf VR-Controller übertragen lässt und demnach die Anforderungen bezüglich der Bedienbarkeit erfüllt werden können. Da sich bei diesem Verfahren theoretisch alle Eingaben zur Rekonstruktion des Passworts beobachten lassen, bewerten wir es

als nicht Shoulder-Surfing-Resistent. Das 3D-Pattern besteht aus 8 Elementen, die nach unserem Verständnis nicht doppelt gewählt werden können. Somit kann der Passwortraum dieses Verfahren nicht auf 10^5 erweitert werden.

ZeTA VR [5]. In der Arbeit von Duezguen et al. [5] wird vorgestellt, wie das ZeTA-Protokoll [10] im AR/VR-Kontext umgesetzt werden könnte. Bei diesem Verfahren besteht das Passwort aus logischen Verknüpfungen von Konzepten. Die Authentifizierung erfolgt dann durch eine Reihe von Challenges, bei denen angegeben werden muss, ob der abgefragte Begriff eine semantische Beziehung zum Passwort hat. Es gibt zum Zeitpunkt dieser Arbeit noch keine Implementierung oder Usability-Evaluation des Verfahrens. In der Arbeit werden drei mögliche Interaktionsmethoden vorgeschlagen, von welchen mindestens eine die Anforderungen bezüglich der Bedienbarkeit erfüllt. Aufgrund der Funktionsweise des Verfahrens mit zufälligen Begriffen kann nicht beobachtet werden, welche Frage beantwortet wurde. Somit ist es nur möglich herauszufinden, ob die Challenge mit Ja oder Nein beantwortet wurde. Da die Challenge-Begriffe so gewählt sind, dass Ja- und Nein-Antworten gleich häufig auftreten, bringt diese Information jedoch keinen Vorteil. Deshalb ordnen wir das Verfahren als Shoulder-Surfing-Resistent ein. Bei diesem Verfahren ist der Passwortraum hauptsächlich von der Anzahl an Challenges abhängig, die die nutzende Person beantworten muss.

Multi-attribute User Authentication [14]. Die Arbeit von Wang und Gau [14] beschreibt ein Challenge-Response-Verfahren, bei welchem die nutzende Person zur Authentifizierung Objekte mit zum Passwort passenden Attributen auswählen muss. Das vorgestellte Verfahren wurde bisher in keiner Studie evaluiert. Basierend auf der Beschreibung der Interaktionen gehen wir davon aus, dass eine Umsetzung in VR möglich ist, welche die Anforderungen bezüglich der Bedienbarkeit erfüllt. Die Größe des Passwortraums lässt sich durch mehr Attribut-Typen, Attribut-Werte und Objekte vergrößern. Aufgrund der zufälligen Generierung und Positionierung der Objekte während der Authentifizierung gehen wir davon aus, dass keine Merkmale des Passworts beobachtet werden können und das Verfahren somit Shoulder-Surfing-Resistent ist.

ReconViguRation [13]. In der Arbeit von Schneider et al. [13] werden verschiedene VR-Overlays für eine physische Tastatur vorgestellt. Eines der Overlays dient zur sicheren Eingabe von Passwörtern, indem in der VR ein zufälliges Tastaturlayout über die physische Tastatur gelegt wird. Für die Umsetzung dieses Verfahrens wurde eine physische Tastatur und ein zusätzliches Tracking-System (OptiTrack Prime 13) verwendet. Somit erfüllt das Verfahren nicht die Anforderung *Keine Spezial-Hardware*, da zusätzliche Hardware benötigt wird.

Zusammenfassung. Die Ergebnisse der Analyse werden in Tabelle 1 zusammenfassend dargestellt. Die einzigen Verfahren, die unser Kriterium der Shoulder-Surfing-Resistenz erfüllen sind *Zeta VR* und *Multi-attribute User Authentication*. Da jedoch beide Verfahren erst eine Datenbank mit den Begriffen und ihren semantischen Beziehungen benötigen und vor allem bei *Multi-attribute User Authentication* bisher nur eine abstrakte Beschreibung des Verfahrens vorhanden ist, lassen sich die Verfahren nur schwer umsetzen. Außerdem müssen bei *Zeta VR* viele Challenges hintereinander beantwortet werden, um die geforderte Größe des Passwortraums zu erreichen, was mit einer hohen Authentifizierungsdauer einhergeht. In dieser Arbeit wollen wir daher ein neues Authentifizierungsverfahren vorstellen, das ebenfalls diese Anforderung erfüllt.

4 PASSGLOBE: KONZEPT UND IMPLEMENTIERUNG

Idee. Basierend auf unseren Anforderungen und den Erkenntnissen aus der Literatur Analyse haben wir ein neues, Shoulder-Surfing resistentes Authentifizierungs-Konzept entwickelt. Unser Verfahren *PassGlobe* wurde durch graphische Authentifizierungsverfahren wie *PassPoints* [15] inspiriert, bei dem mehrere Punkte auf einem Bild als Passwort fungieren. Um jedoch auch resistent gegen Shoulder-Surfing-Angriffe zu sein, konnte das Bild nicht einfach in VR als 2D-Fläche dargestellt werden, da sich sonst anhand der Bewegungen die Positionen auf dem Bild erkennen lassen. Eine zufällige Verschiebung des Bildes in einem Bereich des virtuellen Raums würde dies auch nicht verhindern, da sich mit genug Beobachtungen anhand der Randfälle die Passwort-Positionen immer genauer bestimmen lassen. Alternativ könnte das Bild in der gesamten Sphäre um die nutzende Person zufällig platziert werden, was wir jedoch hinsichtlich der Bedienbarkeit als nicht geeignet erachten, da durch das Umschauen sowohl die Eingabedauer als auch der Konzentrationsaufwand steigen. Deshalb wird bei *PassGlobe* das Bild auf eine Kugel projiziert, welche dann rotiert werden kann. So ist durch Beobachtungen nicht erkennbar, welcher Ort auf der Kugel gewählt wurde, da die Kugel vor jeder Eingabe in eine zufällige Ausrichtung rotiert wird. Im Vergleich zu anderen möglicherweise geeigneten Verfahren wie *RoomLock* in der Variante $Position_{object}$ ohne Wiederholungen (siehe Abschnitt 3) oder einer PIN mit randomisiertem Eingabefeld bietet dieses Verfahren einige Vorteile. Bei diesen Verfahren sind die Positionen der Elemente im Alphabet immer zufällig, wodurch man diese erst finden muss. Bei *PassGlobe* hingegen bleibt die Textur auf der Kugel immer gleich, wodurch alle Positionen relativ zu einander unverändert bleiben. Dadurch erhoffen wir uns, dass es Nutzenden einfacher fällt die Orte wiederzufinden.

Aufgrund der Form ist es naheliegend als Bild eine Weltkarte zu verwenden, auf welcher sich die Nutzenden orientieren können. Wir vermuten, dass dies auch bei der Suche helfen kann, wenn sich eine Person auf der Weltkarte schon auskennt. Da nicht zu erwarten ist, dass bei der Eingabe immer exakt die richtige Position getroffen wird, gibt es einen gewissen Toleranzbereich um den tatsächlichen Passwortort. Abhängig von der Größe des Toleranzbereichs, verändert sich die Größe des Passwortraum pro Stelle. Im Vergleich mit PIN-Verfahren mit nur 10 Möglichkeiten pro Stelle kann bei *PassGlobe* ein kürzeres Passwort verwendet werden um die gleiche Rate-Resistenz zu erreichen.

Passwortvergabe. Bei Verfahren wie *PassPoints* wurde bereits das Problem von Hotspots beschrieben [4]. Auch bei *PassGlobe* besteht die Gefahr, dass Nutzende sich bei der Erstellung des Passworts auf bestimmte Punkte konzentrieren. Um dies zu verhindern, wird bei der Passwort-Erstellung in *PassGlobe* der gleiche Mechanismus wie in *Persuasive Cued Click Points* [4] verwendet. Dabei haben

Abbildung 2: Weltkarte für das *PassGlobe*-Verfahren. [3]

die Nutzenden nicht alle Orte auf der Kugel zur Auswahl, sondern nur einen zufälligen Bereich, in welchem dann der Passwortort gewählt werden kann. Nach Auswahl des ersten Passwortorts wird erneut ein zufälliger Bereich bestimmt, in welchem der nächste Ort gewählt werden kann.

Passworteingabe. Zu Beginn der Authentifizierung wird die Kugel in eine zufällige Ausrichtung rotiert und anschließend können die Nutzenden sie mit ihren (virtuellen) Händen beliebig ausrichten. Wurde der Passwortort gefunden, kann mithilfe eines Pointers an der Hand eine Markierung auf der Kugel platziert werden (s. Abb 1). Diese kann beliebig oft neu platziert oder durch nochmaliges anklicken bestätigt werden. Danach wird die Kugel erneut zufällig rotiert und mit der Eingabe des nächsten Passwortortes wird analog fortgefahren. Nach Eingabe aller Stellen überprüft das System, ob alle Eingaben innerhalb des Toleranzbereichs liegen.

Implementierung. Ein Prototyp wurde in der 3D-Engine *Unity* umgesetzt und mit dem VR-HMD *Valve Index* getestet. Die Kugel wurde als physikalisches Objekt mit fixer Position implementiert. Dadurch kann sie durch Berührungen und Bewegungen der Hände wie eine echte Kugel rotiert werden, ohne ihre Position im Raum zu verändern. Die Größe des Toleranzbereichs wurde so gewählt, dass der Passwortraum 10^5 Möglichkeiten entspricht und das Passwort möglichst kurz ist. Dies lässt sich mit einem 2-stelligen Passwort und einer Aufteilung der Kugel in 316 Teile erreichen. Als Textur für die Kugel wurde die in Abbildung 2 dargestellte Karte verwendet, bei welcher viele Meeresflächen und sonst einfarbige Gebiete mit Tieren oder anderen Objekten gefüllt wurden. Diese Bereiche wären sonst als Passwortorte ungeeignet, da es keine markanten Stellen gibt, mit deren Hilfe man sich die Position merken könnte.

5 DISKUSSION UND AUSBLICK

In dieser Arbeit wurde gezeigt, dass die bisher umgesetzten Authentifizierungsverfahren für VR-HMDs vor Shoulder-Surfing keinen ausreichenden Schutz bieten. Unser neuartiges Verfahren *PassGlobe* hingegen, ist resistent gegen Shoulder-Surfing-Angriffe, da sich die Kugel nach jeder Eingabe zufällig dreht. In Zukunft möchten wir noch eine Studie durchführen, um das Verfahren in Bezug auf Effizienz und Effektivität zu untersuchen und mit anderen Lösungen zu vergleichen. Dabei wollen wir auch überprüfen, ob der Schutz vor Shoulder-Surfing in der Praxis gewährleistet ist, da das Nutzerverhalten die Sicherheit einschränken könnte. Würden die Nutzenden beim Suchen nach einem Ort zum Beispiel immer erst die Weltkugel mit dem Äquator parallel zum Horizont ausrichten, damit es der üblichen Darstellung auf Weltkarten entspricht, so könnte dies bei einer Beobachtung Informationen über das Passwort preisgeben. Entsprechend kann dann der Breitengrad des eingegebenen Ortes durch Beobachtungen bestimmt werden, wodurch sich der Passwortraum auf die Längengrade reduziert. Dies wollen wir ebenfalls in Zukunft empirisch überprüfen.

[3] https://www.behance.net/gallery/25805325/Collins-Childrens-World-Map/modules/169538963, Abrufdatum 2021-11-26, Lizenz: CC BY-NC 4.0, Autor: Steve Evans

DANKSAGUNGEN

This research was supported by funding from the topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

LITERATUR

[1] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies* (Washington, DC) *(WOOT'10)*. USENIX Association, USA, 1–7.

[2] Leif P Berg and Judy M Vance. 2017. Industry use of virtual reality in product design and manufacturing: a survey. *Virtual reality* 21, 1 (2017), 1–17.

[3] Daniel W. Carruth. 2017. Virtual reality for education and workforce training. In *2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA)* (Stary Smokovec, Slovakia). IEEE, Piscataway, New Jersey, 1–6. https://doi.org/10.1109/ICETA.2017.8102472

[4] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C. Van Oorschot. 2012. Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism. *IEEE Transactions on Dependable and Secure Computing* 9, 2 (2012), 222–235. https://doi.org/10.1109/TDSC.2011.55

[5] Reyhan Duezguen, Peter Mayer, Sanchari Das, and Melanie Volkamer. 2020. Towards Secure and Usable Authentication for Augmented and Virtual Reality Head-Mounted Displays. arXiv:2007.11663 [cs.CR]

[6] Ceenu George, Daniel Buschek, Andrea Ngao, and Mohamed Khamis. 2020. GazeRoomLock: Using Gaze and Head-Pose to Improve the Usability and Observation Resistance of 3D Passwords in Virtual Reality. In *Augmented Reality, Virtual Reality, and Computer Graphics*, Lucio Tommaso De Paolis and Patrick Bourdot (Eds.). Springer International Publishing, Cham, 61–81.

[7] Ceenu George, Mohamed Khamis, Daniel Buschek, and Heinrich Hussmann. 2019. Investigating the Third Dimension for Authentication in Immersive Virtual Reality and in the Real World. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)* (Osaka, Japan). IEEE, Piscataway, New Jersey, 277–285. https://doi.org/10.1109/VR.2019.8797862

[8] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. In *In Proceedings of the Network and Distributed System Security Symposium (NDSS 2017)* (San Diego, California, USA). NDSS, NDSS, San Diego, California, USA. https://doi.org/10.14722/usec.2017.23028

[9] Jonathan Gurary, Ye Zhu, and Huirong Fu. 2017. Leveraging 3d benefits for authentication. *International Journal of Communications, Network and System Sciences* 10, 8 (2017), 324–338. https://doi.org/10.4236/ijcns.2017.108B035

[10] Andreas Gutmann, Karen Renaud, Joseph Maguire, Peter Mayer, Melanie Volkamer, Kanta Matsuura, and Jörn Müller-Quade. 2016. ZeTA-Zero-Trust Authentication: Relying on Innate Human Ability, Not Technology. In *2016 IEEE European Symposium on Security and Privacy (EuroS P)* (Saarbruecken, Germany). IEEE, Piscataway, New Jersey, 357–371. https://doi.org/10.1109/EuroSP.2016.35

[11] Florian Mathis, John H. Williamson, Kami Vaniea, and Mohamed Khamis. 2021. Fast and Secure Authentication in Virtual Reality Using Coordinated 3D Manipulation and Pointing. *ACM Trans. Comput.-Hum. Interact.* 28, 1, Article 6 (Jan. 2021), 44 pages. https://doi.org/10.1145/3428121

[12] Ilesanmi Olade, Hai-Ning Liang, Charles Fleming, and Christopher Champion. 2020. Exploring the Vulnerabilities and Advantages of SWIPE or Pattern Authentication in Virtual Reality (VR). In *Proceedings of the 2020 4th International Conference on Virtual and Augmented Reality Simulations* (Sydney, NSW, Australia) *(ICVARS 2020)*. Association for Computing Machinery, New York, NY, USA,

45–52. https://doi.org/10.1145/3385378.3385385

[13] Daniel Schneider, Alexander Otte, Travis Gesslein, Philipp Gagel, Bastian Kuth, Mohamad Shahm Damlakhi, Oliver Dietz, Eyal Ofek, Michel Pahud, Per Ola Kristensson, Jörg Müller, and Jens Grubert. 2019. ReconViguRation: Reconfiguring Physical Keyboards in Virtual Reality. *IEEE Transactions on Visualization and Computer Graphics* 25, 11 (2019), 3190–3201. https://doi.org/10.1109/TVCG.2019.2932239

[14] Jiawei Wang and BoYu Gao. 2021. *Analysis of Multi-attribute User Authentication to Against Man-in-the-Room Attack in Virtual Reality.* Springer International Publishing, Cham, Switzerland, 455–461. https://doi.org/10.1007/978-3-030-78642-7_61

[15] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies* 63, 1 (2005), 102–127. https://doi.org/10.1016/j.ijhcs.2005.04.010 HCI research in privacy and security.

[16] Zhen Yu, Hai-Ning Liang, Charles Fleming, and Ka Lok Man. 2016. An exploration of usable authentication mechanisms for virtual reality systems. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)* (Jeju, Korea (South)). IEEE, Piscataway, New Jersey, 458–460. https://doi.org/10.1109/APCCAS.2016.7804002