Hochschule für Telekommunikation Leipzig
University of Applied Sciences

Hochschule für Telekommunikation Leipzig (FH)
Institut für Telekommunikationsinformatik

Abschlussarbeit zur Erlangung des akademischen Grades
Bachelor of Science

Thema:	„Inwiefern bietet die Authentifikation ohne Passwort Vor- und Nachteile gegenüber Webanwendungen hinsichtlich Nutzerfreundlichkeit, Datenschutz und Sicherheit?“

Vorgelegt von:	Ertugrul Sener
Geboren am:	17.10.1998
Geboren in:	Berlin

Vorgelegt am:	8. September 2020

Erstprüfer:	Prof. Dr. Erik Buchmann Hochschule für Telekommunikation Leipzig Gustav-Freytag-Straße 43-45 04277 Leipzig
Zweitprüfer:	Juri Lobov T-Systems International GmBH Holzhauser Straße 1-4 13509 Berlin

1 Vorwort

Vor Ihnen liegt die Bachelorarbeit zur Forschungsfrage „Inwiefern bietet die Authentifikation ohne Passwort Vor- und Nachteile gegenüber Webanwendungen hinsichtlich Nutzerfreundlichkeit, Datenschutz und Sicherheit“.

Diese habe ich als Abschlussarbeit im Rahmen meines dualen Studiums für angewandte Informatik an der Hochschule für Telekommunikation Leipzig in Zusammenarbeit mit der Telekom Security im Chapter Software Development angefertigt. Das Ziel ist es vorhandene Authentifizierungsstrategien kritisch zu bewerten und eine eigene prototypische Lösung vorzulegen, die bestmöglichst die Kriterien der Sicherheit, des Datenschutzes und der Nutzerfreundlichkeit erfüllt und über eine Kombination dessen gleichzeitig die damit einhergehenden Nachteile ausgleicht.

Die Fragestellung habe ich zusammen mit meinem Prof. Dr. Erik Buchmann und meinem betrieblichen Vorgesetzten Juri Lobov entwickelt. Ich bin davon überzeugt, dass die Kombination aus theoretischem Forschungshintergrund und längjähriger praktischer Erfahrung mir bei einer umfangreichen Beantwortung der Forschungsfrage behiflich sein wird.

Daher möchte ich meinen Begleitern bereits im Voraus für ihre Unterstützung bei der Erarbeitung meiner Arbeit und der Betreuung danken.

Ebenfalls möchte ich meinen Kollegen bei der Telekom Security danken, die mir jederzeit Unterstützung anbieten. Sowohl bei der technischen Umsetzung als auch bei Formulierungen und der Ausarbeitung und Verbesserung des Inhaltes der Arbeit.

Ich wünsche Ihnen viel Freude beim Lesen.

Ertugrul Sener
Berlin, 18. August 2020

Selbstständigkeitserklärung

Hiermit erkläre ich, Ertugrul Sener, dass die von mir an der *Hochschule für Telekommunikation Leipzig (FH)* eingereichte Abschlussarbeit zum Thema

„Inwiefern bietet die Authentifikation ohne Passwort Vor- und Nachteile gegenüber Webanwendungen hinsichtlich Nutzerfreundlichkeit, Datenschutz und Sicherheit?“

selbstständig verfasst wurde und von mir keine anderen als die angegebenen Quellen und Hilfsmittel verwendet wurden.

Leipzig, den 8. September 2020

Ertugrul Sener

Inhaltsverzeichnis

Abkürzungsverzeichnis

BSI Bundesamt für Sicherheit in der Informationstechnik 13

HTTPS Hypertext Transfer Protocol Secure 14

TOTP Time based one time password 19

U2F Universal second factor 15

URL Uniform Resource Locator 15

W3C World Wide Web Consortium 15

WebAuthn Web Authentication 15

Abbildungsverzeichnis

Tabellenverzeichnis

Quellcodeverzeichnis

2 Einleitung

2.1 Motivation

Die Motivation für die Erarbeitung der Forschungsfrage ergab sich am 29. Juni 2020, als eine Rundmail von dem Data Breach Monitoring-Tool von Firefox die Bildschirme erreichte, welches einen neuen Datenleck bei Wattpad meldete. Wattpad ist eine Webseite, bei welcher Nutzer Geschichten frei für die Öffentlichkeit schreiben und publizieren können. Kompromittiert wurden neben den klassichen daten wie Passwörtern, IP-Adressen, E-Mail-Adressen und Geburtsdaten auch sehr persönliche Informationen wie geografische Standorte, ein Kurzprofil des Nutzers, das Profilbild, die Social-Media-Profile und sogenannte Session-Tokens jeglicher Dienste des Benutzers. Entnehmen kann man dies mehreren Artikeln, bei der allerdings die größe der Datenmengen zwischen 250 und 280 Millionen Einträgen variieren. Eine genaue Zahl liefert der Artikel der riskbasedsecurity mit 268.830.266 (nach der Entfernung von Duplikaten) kompromittierten E-Mail Addressen, die sich laut des Artikels in einer einzigen Datenbank befanden. [7] Die Bedrohung für jeden einzelnen dieser Nutzer ist nun allgegenwärtig, da nun ihr Passwort im Umlauf ist - Das sie womöglich auch für andere Dienste verwenden. Dieses Problem gibt es nun schon seit einigen Jahren und Wattpad ist nicht der Einzige sogenannte 'Data Breach' der letzten Jahre. Technische Probleme (Sicherheitslücken, Versäumnisse) und Angriffsszenarien kriegt die informationsafine Menscheit der Neuzeit gut organisiert, doch dann scheitert es in riesigen Unternehmen oft an der Wahl eines Passwortes. Bei Disskusionen im Internet, wird sich häufig aufgrund der selben Gründe gegen eine zwei Faktor Authentifizierung und Passwort-Manager ausgesprochen. Die 2FA sei zu umständlich und ein Passwort-Manager aufgrund des Masterpasswortes und dem Angst vor Verlust zu riskant. Das potenzielle Risiko welches durch Passwörter allerdings im Vergleich zu diesen neueren Verfahren aufkommt, wird häufig ignoriert. Individuelle Passwörter für jeden Dienst seien unmöglich merkbar und eine zwei Faktor Authentifizierung sei zu kompliziert um sie für jeden Dienst, wenn möglich, einzusetzen. Die Frage, die sich stellt ist es, ob man mit einer Kombination aus den vorhandenen vielfältigen Authentifizierungsmöglichkeiten eine beqeueme aber gleichzeitig auch sichere Authentifizierungsvariante schaffen könnte, bei denen es dem Anwender kinderleicht möglich sein soll sich gegenüber einer Webseite zu authentifizieren. Das Merken von langen Passwörtern sollte mitunter vermieden werden, da diese bei Kompromittierung publik werden und danach ein potenzielles Risiko für jeden anderen genutzten Dienst des Nutzers darstellen. Das Passwort als ersten Faktor der Kategorie 'Wissen' ist unter Beachtung gewisser Vorgaben nicht auszuschließen.

2.2 Problemdefinition

Lange reichte der Benutzername und das Passwort aus, um einen Benutzer sicher zu identifizieren. Heutzutage gelangen sensible Informationen immer öfter an Dritte. Dabei ist es nicht zwingend notwendig, dass die Authentifizierungsquelle, also jene Quelle bei der die Daten persistiert sind und die die Authentifizierung bei Eingabe durchführt, diese Daten irrtümlich herausgibt. Durch sogenannte Metadaten, das sind Informationen und Merkmale zu Daten, ist es Angreifern häufig möglich das Passwort zu erraten bzw. zurückzusetzen. Wenn also der Benutzername lautet 'MichaelJacksonFanForever' ist die Antwort auf die Sicherheitsfrage zum Lieblingskünstler nicht weit entfernt. Gleichzeitig neigen Menschen zu leicht merkbaren Passwörtern, die sie mehrfach für verschiedene Dienste verwenden. Dies stützt eine kürzlich durchgeführte repräsentative Studie der Bitkom Reserach [1] im Auftrag des Digitalverbands Bitkom. So nutze etwa jeder dritte Onlinenutzer (36%) dasselbe Passwort für mehrere Dienste. Auch wenn gleichzeitig 63% der Befragten angaben, bei der Erstellung von Passwörtern auf "einen Mix aus Buchstaben, Zahlen und Sonderzeichen" zu achten, beweist diese Befragung an 1.000 Internetznutzern, dass die Frage nach der Sicherheit von Passwörtern auch im Jahre 2020 immernoch Relevanz hat. Eine ähnliche Studie hat die Bitkom zum Thema 'Nachlässigkeit bei Passwörtern' am 08.11.2016 [2] gemacht, bei der die prozentuale Verteilung an unsicheren Passwortnutzern die befragt wurden nur einen Prozent höher liegt. Das heißt konkret, dass sich innerhalb von 4 Jahren keine messbare Besserung ergeben hat. Das Bewusstsein über die Internetpräsenz und der Schutz dessen scheinen immernoch keine große Aufmerksamkeit vom modernen Nutzer zu erhalten. Das Problem mit unsicheren Passwörtern ist allerdings so alt wie das Internet.

2.3 Stand der Forschung

2.3.1 Unsichere Passwörter

In der fünften Ausgabe der Zeitschrift "Wirtschaftsinformatik & Management" 2018 mit dem Titel "Schwache Passwörter - Nutzer spielen weiterhin Vogel Strauß" schrieb der Autor Geralt Beuchelt: "Der Umgang mit Passwörtern ist so ähnlich wie eine Diät: Eigentlich weiß man genau, was richtig ist - Macht aber oft genug das Gegenteil. Und nicht selten ist der Grund Bequemlichkeit. Warum selber kochen, wann nach einem langen Tag eine Pizza lockt? Und warum lange, umständliche Passwörter verwenden, wenn es einfach zu merkende, die man für alle Accounts verwendet, doch auch tun¿'. [3] Die symbolische Pizza steht für die Mehrfachverwendung von teils schwachen Passwörtern für alle genutzten Dienste inklusive des 'Verwaltungsdienstes' wie der Mail, welches als meist einziges Identifikationsmerkmal dient, über die weitere Dienste betroffen

sein können. Der Begriff des Passwortes stammt aus dem militärischen Bereich des 16. Jahrhunderts, wobei tatsächlich das einzelne Wort gemeint war, welches einem Zutritt zu Gebäuden verschaffte. Damit verwandt ist das Kennwort, welches nicht das Passieren sondern die Kennung des gemeinsamen Geheimnisses betont. Damit ist gemeint, dass der Passierer mit einem Kennwort auch automatisch als Geheimnisträger identifiziert wird. Als allerdings Computer immer leistungsfähiger wurden, wurde der Begriff der Passphrase etabliert, um die Notwendigkeit längerer Passwörter hervorzuheben. Weitere Schlüsselwörter für das heutzutage bekannte Passwort sind: Schlüsselwort, Kodewort (auch: Codewort) oder die Parole. Die Länge gillt gemeinhin als die allumfassende Sicherheit von Passwörtern. Dem widerspricht die klare Trennung zwischen Länge und Komplexität von Passwörtern durch das Bundesamt für Sicherheit in der Informationstechnik, die sinngemäß in ihrer Empfehlung zum Thema 'sichere Passwörter' schreiben, dass die Länge von Passwörtern nicht dessen Komplexität und Sicherheit gegen Angriffe widerspiegelt [4].

2.3.2 Passwort Policys

Das gewählte Passwort soll für einen selbst leicht merkbar, für einen Computer oder menschlichen Angreifer allerdings schwer zu erraten sein. So empfielt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Passwörter zu verwenden, die möglichst nicht aus Tastaturmustern bestehen wie 'asdfgh' oder '1234abcd'. Allgemein wird ein 20 bis 25 Zeichen langes Passwort aus zwei Zeichenarten einem 8 bis 12 Zeichen langem Passswort aus 4 Zeichenarten in Punkto Komplexität gleichgesetzt. [4]
Das Wort 'Policy' ist in diesem Zusammenhang als 'die Regel' zu verstehen und in der Wortkombination sind Passwort Policys die Regeln, die zu einem sicheren Passwort führen. Derart Regeln gibt das BSI vor. So seien der Kreativität bei Passwörtern keine Grenzen gesetzt [4]. Zum Beispiel könne man einen leicht zu merkenden Satz nehmen, diesen mit Bindestrichen verbinden und von jedem Wort den ersten Buchstaben entfernen. Die Frage die sich dabei stellt ist es, ob dieser Satz dann auch die Tippgeschwindigkeit des Nutzers beeinträchtigt, weil relativ viele Denkprozesse während des Tippens stattfinden müssen. Ein Passwort soll leicht merkbar sein, für einen Angreifer allerdings schwer zu brechen. Grundsätzlich gillt, auch das ist nur im Idealfall so, je länger ein Passwort ist, desto besser. Dies bedeutet wie bereits oben angeschnitten allerdings nicht, dass das Passwort 'aaaaaaaaaaaaaaaaaaa' ein mathematisch sicheres Passwort ist. Die Länge des Passwortes ist nur einer von vielen Faktoren, die am Ende zur Komplexität und der daraus resultierenden beitragen. Im Idealfall besteht das lange Passwort aus mehreren Zeichenarten. Eine weitere Empfehlung ist es, keine Sonderzeichen an den Anfang oder das Ende des Passwortes anzuhängen, um es für einen Angreifer schwerer erratbar zu machen. Dies lässt sich damit begründen, dass sobald ein Angreifer die restlichen Zeichen des Passwortes erraten konnte oder durch Metadaten anderer Dienste (wie oben in dem Michael-Jackson Beispiel) kennt, das

Durchprobieren von allen verfügbaren Sonderzeichen für die erste und letzte Stelle der Zeichenkette keine große Leistung erfordert. Sie machen das Passwort mathematisch zwar sicherer (Mehr Zeichenarten bedeuten mehr Zeichen insgesamt und dadurch mehr Kombinationsmöglichkeiten für Passwörter), bei gegebenen Umständen sind diese einzelnen Sonderzeichen allerdings obsolet und können weggelassen werden. Passwort Policys können allerdings auch teilweise wertvolle Informationen für einen potenziellen Angreifer bieten. Denn was Angreifer durch sehr strikte Passwort Policys unteranderem erkennen können, ist die Mindest- und Maximalzeichenlänge. Dabei wird der Angreifer zum Beispiel aus der Regel 'Das Passwort muss mindestens 8 und maximal 16 Zeichen lang sein.' alle Kombinationen für weniger als 8 Zeichen und mehr als 16 Zeichen bei der Erratung eliminieren können. Weitere Regeln wie 'Das Passwort muss mindestens ein Sonderzeichen beinhalten' können zusätzliche Informationen bieten. Daher sind Passwort-Policys zwar ein sehr wichtiges Werkzeug, um Nutzer zu sicheren Passwörtern zu zwingen. Durch das Bequemlichkeitsproblem des Nutzers können allerdings immernoch einfach zu erratende Passwörter entstehen. Verhindern lässt sich dies nicht ganz. Die Informationen die Nutzer beim Anmelden bekommen, nutzen Angreifer dann zum Knacken jener Passwörter. Die Faustregel lautet: Je mehr Metadaten, desto besser. (Aus Sicht des Angreifers)

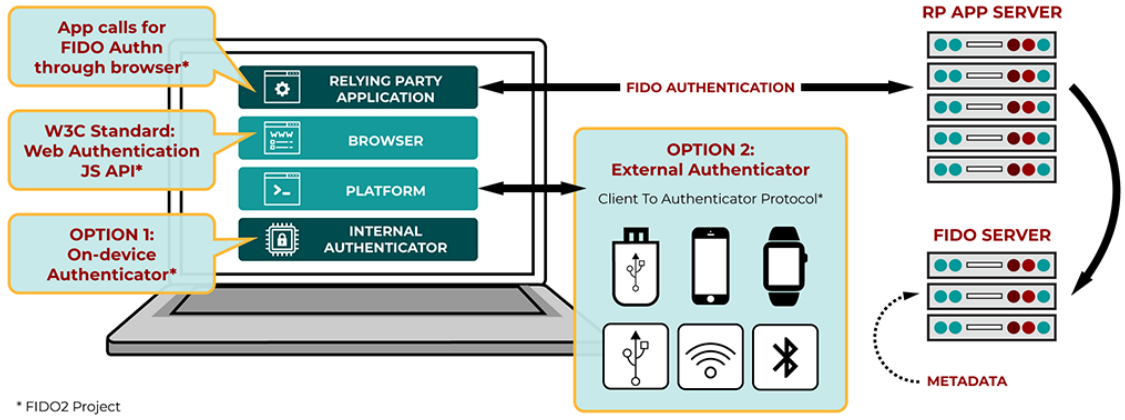
2.3.3 Übertragungsproblem

Das Problem mit der Unsicherheit von Passphrasen oder auch Passwörtern beginnt allerdings jedes Mal aufs Neue, sobald man ein Passwort eintippt. So ist die Bedrohung nicht mit der Wahl eines mathematisch sicheren Passwortes gebannt. Das wissenbasierte Verfahren, welches sich einer Zeichenkette bedient die man in ein Feld eintippt, ist per sé dann unsicher sobald einer der Geheimnisträger (Menschen mit Kenntniss über die Parole) kompromittiert bzw. infiziert ist. So gibt es verschiedenste Angriffsvektoren um das Passwort eines Users für einen speziellen Dienst herrauszufinden. Von personalisierten (oder auch allgemeinen) Phishing Mails, zu Shoulder Surfing bis hin zu Trojanern und Keyloggern auf dem System Desjenigen. Diese können vom Angreifer teilweise remote ausgeführt werden, für manche Angriffe benötigt der Angreifer allerdings physischen Zugriff aufs System. Ein weiteres großes Problem ist die Übertragung von Passwörtern über die klassiche User-Browser-Schnittstelle. Dabei wird das Passwort im Browser des Clients gehasht und dann an den Server übertragen. Die sichere Kommunikation anhand des Hypertext Transfer Protocol Secure (HTTPS) findet erst bei der Übertragung zum Server statt, die Eingabe des Passwortes an den Browser allerdings ist ungeschützt. Diese Übertragung von Buchstaben kann mitgelesen werden. Das Hashen löst das Problem das ein Angreifer im selben Netzwerk mitlauschen und das Passwort über einen sogenannnten Man-in-the-middle Angriff entwendet. Somit sich der Identität des Passwortbesitzers bedient und sich bei anderen Diensten als Diesen ausgibt. Es bleibt allerdings immernoch das Problem des Wiederholungsangriffs. Der Angreifer

muss womöglich also nicht ein Mal das Passwort im Klartext lesen können. Es genügt, den Hash und den Benutzernamen im Request abzufangen um diese dann in einem seperaten Aufruf vom eigenen Rechner an die selbe Uniform Resource Locator (URL) zu senden. Diese Art des Angriffs nennt man einen Replay Attack. Es handelt sich um das Imittieren von Benutzereingaben durch einen Angreifer, bei der der Angreifer die Passphrasen nicht im Klartext kennt. Durch den Zugang zum Dienst ist es ihm somit (je nach Implementierung des Dienstes) möglich, sensible Daten des Nutzers einzusehen die nicht für den Angreifer bestimmt sind. Die Frage nach der 'Relevanz' von sensiblen Daten sollte obsolet werden, wenn man an die Möglichkeiten denkt, die der Angreifer mit ihnen nun in der Hand hällt. Mit diesen könnte er den Nutzer zum Beispiel erpressen um an noch mehr Daten oder Geld des Nutzers zu kommen.

2.3.4 FIDO2 - Alternative zum Passwort

FIDO steht für 'Fast Identity Online' (Schnelle Identität im Netz). Sie ist das Ergebnis einer Kooperation des World Wide Web Consortium (W3C) und der FIDO Alliance. FIDO2 basiert auf vorhandenen Protokollen wie Web Authentication (WebAuthn) für die Browser-Server-Kommunikation und CTAP für die Browser-Authenticator-Kommunikation. Auf der offiziellen Webseite der yubico, einem der Hauptentwickler und Publizierer des Vorgängerprotokolls Universal second factor (U2F) wird die FIDO2 - U2F, also die zwei Faktor Authentifizierung spezifiziert durch U2F das immernoch im FIDO2 Protokoll beheimatet ist, wie folgt beschrieben: "an open authentication standard that enables internet users to securely access any number of online services with one single security key [...]. FIDO2 is the latest generation of the U2F protocol" [5]. Während das Vorgänger - Protokoll U2F von Google und Yubico ins Leben gerufen wurde, ist FIDO2 ein offener dezentraler Kommunikationsstandart für die passwortlose Kommunikation welches die Authentifizierung für sowohl Privatnutzer als auch Unternehmen beqeuem und gleichzeitig sicher machen soll.



Um die Sicherheit des Nutzers zu gewährleisten kombiniert FIDO2 die Methoden des UAF und des U2F. Bevor wie bei gängigen Zweifaktoren wie eines PINs oder sechsstelligen Schlüssels der Schlüsselaustausch stattfinden kann, muss der User der Anwendung oder des Dienstes eine lokale Verifikation durchführen. Diese soll sicherstellen, dass es sich bei der Person, die die Authentifikation durchführt und der Person, die den Schlüssel vorher registriert hat, um die selbe Person handelt. Diese Verifikation kann zum Beispiel ein Knopf auf einem USB - Stick sein, auf den der Web-Service wartet - Bevor er die Challenge an den Nutzer sendet. So lange also ein Angreifer keinen physischen Zugang zu diesem USB - Stick erhält, ist das Verfahren sicher. Sollte es doch vorkommen, dass der Angreifer Zugriff auf den Stick erhält und den Knopf drückt, setzt die sozusagen zweite Phase ein. Die Webseite sendet dem User eine Challenge, welche der User lokal mit seinem Schlüssel auf dem Computer lösen kann. Die Webseite erhält dann das Ergebnis und vergleicht dieses mit dem eigenen Ergebnis. Gibt es ein Match, sendet der Server der Webseite die zugehörige Response zur Challenge an den User zurück und lässt ihn passieren. Wie die Abbildung zeigt gibt es neben der externen Authentifikation durch Smart-Watch, USB- Stick oder Smartphone auch die Option der 'on-device-authentication'. Damit ist die Authentifizierung durch einen PIN oder einen eingebauten Fingerabdruck-Sensor (über biometrische Daten aller Art) gemeint, die allerdings nicht extern angeschlossen ist sondern sich auf dme Gerät befindet. Auf die initiale Schlüsselerstellung und weitere Details zum FIDO Protokoll, die für diese Arbeit relevant sind, gehe ich im nächsten Kapitel: 'Grundlagen' ein.

2.4 Zielsetzung

Ziel dieser Abschlussarbeit ist es einen Nachweis dafür zu liefern, dass Authentifikation in 2020 sowohl sicher als auch bequem sein kann und das sich diese Punkte nicht gegenseitig ausschließen. Ziel ist es auch, den Leser in die Sicht des Angreifers auf Systeme einzuweisen, sodass im Idealfall automatische Schutzreaktionen wie das Wählen von sicheren Passwörtern hervorgerufen, wenn nicht sogar eine der beschriebenen FIDO2 Verfahren wie der erste oder sogar der Zweite Faktor, verwendet werden. Der Prototyp soll die verschiedenen Authentifizierungsmöglichkeiten veranschaulischen und präsentieren, um dem Nutzer die Wahl auf eines der Verfahren zu erleichtern. Gleichzeitig ist natürlich ein hauptsächliches Ziel dieser Arbeit auch die Grenzen von 'modernen' Authentifizierungsverfahren aufzuzeigen und auch zu zeigen, inwiefern eine Kombination dieser vorhandenen Verfahren, Probleme löst. Ein weiteres Ziel soll es sein, in gewisser weise kategorisch darzulegen, welches Verfahren für welchen Nutzertypen geeignet ist. Die Idee dahinter ist, dass es eine klare Trennung in der Nutzung von Accounts zwischen Entwicklern, Unternehmern und dem 'Casual Websurfer' gibt. Was alle drei Arten von Computernutzern allerdings gemeinsam haben ist: Sie besitzen persönliche Daten, an die kein Angreifer bzw. eben kein Dritter gelangen soll. Der Schutz dieser Daten sollte jedem Individuum selbst wichtig sein, um in den nächsten

5 bis 10 Jahren auf Besserung zu hoffen. Nicht nur technisch muss die Menscheit mit dem neuen digitalen Zeitalter umgehen und sich absichern können, sondern auch auf die menschliche Komponente achtgeben. Es sollte dennoch erwähnt sein, dass diese Arbeit nicht darauf abzielt jede einzelne Authentifikationsstrategie und Möglichkeit aufzuzeigen und zu bewerten sondern eher die klassichen und weiterverbreitetsten Verfahren aufzuzeigen, auf die die restlichen Verfahren meist basieren. So ist der Yubikey am Ende auch nur eine Möglichkeit zur Umsetzung von einer Challenge-Response-basierten Authentikation anhang von privaten Schlüsseln welches bereits im FIDO Standart definiert ist. Auch ist es ein Nicht-Ziel dieser Arbeit das Resultat auf eine einzige perfekte Lösung zu dezimieren und diese zum neuen Standart zu erklären. Viel mehr möchte ich meinen Lösungsansatz präsentieren und disskutieren und darauf aufbauend Vorschläge für die Nutzung von bestimmten Personengruppen abgeben.

3 Grundlagen

3.1 Datenschutz

3.1.1 ISO 27001

3.1.2 IT-Grundschutz

3.2 Authentifizierungsmethoden

3.2.1 Authentifizierungsmöglichkeiten

3.2.2 Zeitbasierte Passwörter

3.2.3 Private Schlüssel

4 Methodik

4.1 Aufbau des Prototypen

Das Ziel des Prototypes ist es, wie eingangs erwähnt, vorhandene Authentifizierungsverfahren abseits der klassischen UserID / Passwort Methode zu begutachten und dessen Schwächen aufzudecken. Darauf aufbauend wurde die Methodik für die Findung eines Verfahrens welches die Kriterien der Sicherheit, des Datenschutzes und der Bequemlichkeit besser erfüllt, gewählt. Der Prototyp beschreibt eine einfache Webseite, die aus dem Internet erreichbar sein wird und zwei Eingabefelder und einen Loginbutton besitzt. Die unterschiedlichen Methoden der Authentifizierung wählt man über ein Dropdownmenü, welches sich zwischen Login-Button und Username / Passwort Feld befindet. Je nach Authentifizierungsverfahren werden kleine Popup-Boxen sichtbar, die die weiteren Schritte für die Authentifikation erläutern. Ein Teil des Prototypen soll die gewählten Methoden demonstrieren. Neben einer erfolgreichen Demonstration der Authentifizierung sollen nach jeder Methode auch Kennwerte ausgegeben werden. Einer davon soll zum Beispiel die Zeit von der ersten Eingabe in ein Eingabefeld bis zur Authentifizierung zählen und anzeigen.

Neben den vorhandenen Methoden soll die eigene Architektur aufgebaut werden, die sich an vorhandenen Authentifikationsmöglichkeiten bedient. Die UserID und das Passwortfeld bleiben stets im Vordergrund, müssen allerdings nicht zwingend für jedes der Verfahren genutzt werden, so kann es zum Beispiel bei einer besitzbasierten Authentifikation bereits reichen, den Besitz (z.B einen USB, welcher einen Schlüssel beherbergt) im Computer einstecken zu haben und auf den Loginbutton zu drücken.

4.2 Auswahl der Authentifizierungsverfahren

Neben des altbekannten Time based one time password (TOTP) Verfahrens, wird das Secure Element und die E-Mail Authentifikation betrachtet. Dabei bedienen sich diese Verfahren aller drei Möglichkeiten der Authentifikation, dem Wissen, dem Besitz und der körperlichen Merkmale. Das Dropdownmenü zeigt die Authentifikation über biologischen Merkmale (Touch ID oder Face ID) nur sofern das Gerät, auf welchem der

Prototyp bedient wir, einen entsprechenden Sensor und die entsprechende Software zur Verarbeitung besitzt.

4.3 Kriterien zur Bewertung des Prototypen

4.4 Architektur

5 Prototypischer Lösungsansatz

5.1 Bequemlichkeitsproblem

5.2 Kriterien für erfolgreiche Authentifikation

5.3 Implementierung des Prototypen

6 Auswertung

6.1 Messung der Kriterien am Prototypen

6.1.1 Nicht behandelte Kriterien

6.1.2 Fehleranfälligkeit

6.2 Implementierung

6.3 Ablauf und Durchführung

7 Ausblick und Fazit

A Anhang

A.1 Ergänzende Informationen

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln. Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln. Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.