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 Javascript basierten Web-Anwendungen hinsichtlich Nutzerfreundlichkeit, Datenschutz und Sicherheit?“

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

Vorgelegt am:	23. August 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 „Inwiefern bietet die Authentifikation ohne Passwort Vor- und Nachteile gegenüber Javascript basierten Web-Anwendungen 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. Ziel war 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 dieser Bachelorarbeit.

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 Javascript basierten Web-Anwendungen hinsichtlich Nutzerfreundlichkeit, Datenschutz und Sicherheit?“

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

Leipzig, den 23. August 2020

Ertugrul Sener

Inhaltsverzeichnis

Abkürzungsverzeichnis

TOTP Time based one time password 15

Abbildungsverzeichnis

Tabellenverzeichnis

Quellcodeverzeichnis

2 Einleitung

2.1 Motivation

Die Motivation für die Arbeit erschloss sich mir am 29. Juni 2020, als eine Rundmail von dem Monitoring-Tool von Firefox herumging, 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 Passwörtern auch IP-Adressen, E-Mail-Adressen, Geburtsdaten und sehr persönliche Informationen wie geografische Standorte, ein Kurzprofil, das Profilbild, die Social-Media-Profile und alle verknüpften Accounts jeglicher Dienste des Benutzers. Die Datenmenge umschloss etwa 300 Millionen Einträge, bei denen die Passwörter zwar gesalted sind, allerdings das Knacken dieser bereits durch eine Hackercommunity in Angriff genommen wurde und etwa 10% bereits 'entschlüsselt' wurden. Die Frage die sich stellte war es, ob persönliche Daten von mir nun im Umlauf waren. Glücklicherweise nutze ich einen Passwort-Manager und mein Passwort war zufallsgeneriert und ich kannte es selbst nicht einmal, da es zu kompliziert war um es sich zu merken. Dieses Leck hatte in meinem Freundeskreis, unter denen einige auf Wattpad registriert waren, rumgesprochen und mir stellte sich immer mehr eine Kernfrage: Wie kann es im Jahre 2020 immernoch sein, dass Menschen die selben Passwörter für Dienste verwenden und diese nicht ausreichend kompliziert wählen? Immerhin gibt es dieses Problem nun schon seit einigen Jahren und dennoch ändert sich augenscheinlich nichts an der Situation. Technische Probleme und Angriffsszenarien kriegt die informationsafine Menscheit gut organisiert, doch dann scheitert es in riesigen Unternehmen an der simplen Wahl eines Passwortes. Bei mehreren Disskusionen in meinem Umfeld, kamen die selben Argumente gegen eine zwei Faktor Authentifizierung und Passwort-Manager hervor. Passwörter seien unmöglich für alle Dienste merkbar und eine zwei Faktor Authentifizierung sei zu kompliziert um sie für jeden Dienst, wenn möglich, einzusetzen. Die Forschungsfrage kam daher, dass ich mich fragte, 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 Dienst darstellen.

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 Besserung ergeben hat. Das Problem mit unsicheren Passwörtern ist allerdings so alt wie das Internet.

2.3 Stand der Forschung

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.

2.4 Zielsetzung

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.

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 aus einer Kombination dieser Methoden besteht. 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.

4.2 Auswahl der Authentifizierungsverfahren

Bei der Wahl der Verfahren muss besonders darauf geachtet werden, dass man versucht, die drei Methoden Wissen, Besitz und körperliche Merkmale möglichst gleichermaßen bedient und großflächig in der Industrie genutzte verwendet. Beim Besitz wurde sich für die Time based one time password (TOTP) Authentifikation entschieden, da Smartphones heutzutage keine Rarität darstellen und das Verfahren durch Apps wie den Google Authenticator und die vielen Webseiten die diese nutzen an Popularität gewonnen hat.

Auf der Wissensebene wurde die E-Mail als zusätzlicher Schutz gewählt, da ein physischer Zugang zum Mailaccount das Wissen über das Passwort und die korrekten Einloggdaten (womöglich auch ein zweiter Faktor oder eine Multifaktor-Authentifizierung) erfordert. Auf der Ebene der biologischen Merkmale wurde der Fingerabdruck gewählt, welcher allerdings nur auf Geräten angezeigt wird, die auch einen entsprecheneden Sensor für Fingerabdrücke besitzen.

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.