Lufthansa Systems

DHBW
Duale Hochschule
Baden-Württemberg
Mannheim

Duale Hochschule Baden-Württemberg
Mannheim

Bachelorarbeit

Analyse und Integration einer passwortlosen Authentifizierung im Unternehmenskontext

Studiengang Cyber Security

Verfasser:	Luka Tsipitsoudis
Matrikelnummer:	4110112
Kurs:	TINF20CS1
Bearbeitungszeitraum:	06.06.2023 – 29.08.2023
Abgabedatum:	29.08.2023
Betreuer:	Stefan Köster

Ehrenwörtliche Erklärung

Ich versichere hiermit, dass ich meine Projektarbeit mit dem Thema: „*Analyse und Integration einer passwortlosen Authentifizierung im Unternehmenskontext*“ selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Ort, Datum

Abstract

Deutsch

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

LSY Lufthansa Systems GmbH & Co. KG

1 Einführung

Diese Arbeit beschäftigt sich mit passwortlosen Authentifizierungsverfahren. Im Folgenden werden zunächst die Problemstellung und das Ziel der Arbeit erläutert. Anschließend wird der Aufbau der Arbeit beschrieben und auf verwandte Arbeiten eingegangen:

1.1 Problemstellung & Ziel der Arbeit

Die Problemstellung dieser Arbeit bezieht sich auf den aktuellen, passwortlosen Ansatz der Authentifizierung im Unternehmenskontext der Lufthansa Systems GmbH & Co. KG (LSY). Trotz ihrer hohen Etablierung und Verbreitung bieten passwortlose Authentifizierungsverfahren nicht nur Vorteile, sondern auch eine hohe Anzahl an Angriffsvektoren.

Ziel dieser Arbeit ist es daher passwortlose Authentifizierungsverfahren genauer zu betrachten. Verschiedene passwortlose Verfahren werden vorgestellt und ihre Vor- und Nachteile aufgezeigt. Dabei soll ein besonderes Augenmerk auf den Vergleich der Angriffsvektoren von passwortlosen und passwortbasierten Verfahren gelegt werden. Einer der passwortlosen Verfahren wird begründet ausgewählt und detailiierter betrachtet. Dabei wird analysiert, ob das Verafahren für die LSY geeignet ist und welche Anpassungen vorgenommen werden müssen. Betrachtet werden insbesondere die Aspekte der Sicherheit und der Benutzerfreundlichkeit. Der Fokus liegt auf der Frage, ob passwortlose Verfahren eine Alternative darstellen, welche Passwörter gänzlich ersetzen.

1.2 Aufbau der Arbeit

1.3 Referenzierte Arbeiten

2 Grundlagen

2.1 Einführung in cFront

2.2 CIA-Triade

2.3 Arten der Authentifizierung

2.4 Multi-Faktor-Authentifizierung

2.5 Passwortbasierte Authentifizierung

- Die heutzutage am häufigsten genutzte Methode zur Authentifizierung ist die passwortbasierte Authentifizierung **chanda2016password**.
- Dabei handelt es sich am häufigsten um alphanumerische Passwörter, welche aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen **chanda2016password**.
- Passwörter können durch verschiedene Angriffe kompromittiert werden. Angreifer können Zugriff auf die Datenbank erhalten, in welcher die Passwörter gespeichert sind. Aber auch auf persönlicher Ebene können Passwörter erlangt werden. Aufgeschriebene Passwörter können in fremde Hände geraten. Auch Social Engineering kann genutzt werden, um Passörter mit Hilfe von Phishing oder Keyloggern zu erlangen. Häufig lassen sich Passwörter allerdings auch mit Hilfe von Brute-Force- oder Dictionary-Attacken kompromittieren **chanda2016password**.
- Brute-Force-Attacken versuchen alle möglichen Kombinationen von Zeichen, welche ein Passwort enthalten kann, auszuprobieren. Je höher dabei die Anzahl an möglichen Kombinationen ist, desto aufwändiger wird es ein Passwort zu erraten.

- Je länger ein Passwort, desto schwieriger zu knacken. Länge auch wichtiger als Zeichenraum **chanda2016password**.
- Hier auch kurz auf die Mathematik dahinter eingehen.
- Studien zeigen, dass Nutzer dazu neigen gleiche oder ähnliche Passwörter für verschiedene Zugänge zu nutzen **chanda2016password**.
- Verfügen Angreifer über ein Passwort eines Nutzers, können häufig auch andere Zugänge übernommen werden **chanda2016password**.
-

2.5.1 Speicherung

- Passwörter können auf verschiedene Arten gespeichert werden. Dadurch können verschiedene Angriffsvektoren entstehen **chanda2016password**.
- Plaintext am schlechtesten. Werden die Passwörter in lesbarer Form gespeichert, können Angreifer alle Passwörter auslesen, sobald sie Zugriff auf die Datenbank haben. Dabei muss kein weiterer Aufwand betrieben werden **chanda2016password**.
- Verschlüssellung besser, aber nicht optimal. Verschlüssellung ist zurückführbar. Gelangen Angreifer an den benötigten Schlüssel, können sie alle Passwörter entschlüsseln und auslesen **chanda2016password**.
- AM besten Hashing mit Salt. Sobald ein Passwort gehasht wurde, kann es nicht mehr zurückgerechnet werden. Durch einen individuellen Salt kann ebenfalls verhindert werden, dass Angreifer die Passwörter mit Hilfe von Rainbow-Tables entschlüsseln können **chanda2016password**.
- auch noch zwei salts möglich - einer public einer private. schützt vor offline angriffen **chanda2016password**.
- Vielleicht hier noch ganz kurz auf Hash Funktionen eingehen?

2.5.2 Faktor Mensch

- Von Menschen erstellte Passwörter sind keine echten Zufallswerte. Das liegt insbesondere daran, dass Nutzer sich Passwörter merken können müssen. Daher beinhalten Passwörter häufig Informationen, welche einen Bezug zum Nutzer haben. Dazu gehören beispielsweise Namen, Geburtsdaten, Adressen oder andere persönliche Informationen. Auch Passwörter, welche einfache Tastaturmuster beinhalten sind sehr beliebt. Dazu zählen beispielsweise „qwertz“ oder „123456“ **chanda2016password**.
- Es ist sehr schwierig für Nutzer sich verschiedene komplexe Passwörter zu merken. Daher neigen Nutzer dazu, einfache Passwörter zu nutzen oder Passwörter für verschiedene Zugänge zu wiederholen **chanda2016password**.
- Das macht von Menschen erstellte Passwörter anfälliger für Angriffe, da diese einfacher zu erraten sind **chanda2016password**.
-

2.6 Passwortlose Authentifizierung

2.6.1 Magic Link

2.6.2 One Time Password (OTP)

2.6.3 Biometrische Daten

2.6.4 Public Key Cryptography

2.7 Yubikey

2.8 Fido2

2.8.1 Webauthn

2.8.2 CTAP2

2.8.3 Sicherheit

3 Umsetzung

3.1 Aktueller Stand der LSY

3.2 Integration eines Yubikeys in die LSY

3.3 Nutzung des passwortlosen Verfahrens im Unternehmenskontext

3.4 User Feedback

3.5 Zeitmessung

3.6 Nutzung des passwortlosen Verfahrens im privaten Kontext