Hochschule Wismar
University of Applied Sciences
Technology, Business and Design
Faculty of Engineering, Department EE & CS

Master-Thesis

Security Evaluation of Multi-Factor Authentication in Comparison
with the Web Authentication API

Submitted by: July 31, 2019

from: Tim Brust
        born 03/31/1995
        in Hamburg, Germany

First supervisor: Prof. Dr.-Ing. habil. Andreas Ahrens
Second supervisor: Prof. Dr. rer. nat. Nils Gruschka

Purpose of this thesis

The purpose of this master-thesis is to introduce, analyze and evaluate existing multi-factor authentication solutions in regards of their technical functionality, usability in web projects and potential security risk.

Those multi-factor authentication solutions should be compared to the Web Authentication API in order to identify if the Web Authentication API is a suitable replacement or a complementary addition to the multi-factor authentication solutions.

Abstract

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special contents, but the length of words should match the language.

Kurzreferat

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special contents, but the length of words should match the language.

Contents

1 Introduction

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special contents, but the length of words should match the language.

1.1 Methods of authentication

There are multiple different methods or forms respectively that can be used to authenticate a user against someone or something. Traditionally only knowledge, possession and trait are considered the different forms of authentication[1], but other sources also count methods like location- or time-based authentication[2]. Therefore this thesis accounts them, too.
In the following sections each of those methods is described briefly.

1.1.1 Knowledge

The most common method of authentication is knowledge so therefore something the »the user knows«. Commonly used in web project are passwords. Other forms of knowledge are for example banking Personal identification number (PIN), a passphrase, secret/recovery questions or a One-time password (OTP). The security relies on the fact that the knowledge method is considered a secret that only the user knows.[3]

1.1.2 Possession

Another form of authentication is the possession, i.e. »the user has«. The most common example is a key for a lock. Other forms are for example a bank card or a security token, both realized in hardware and/or software.

---

[1] See BB17, p. 140.
[2] ZKM12.
[3] See Eck14, p. 467.

1.1.3 Biometrics

Besides the knowledge and possession factors, another one is the biometrics. This factor is classified as something »the user is« and commonly includes the fingerprint, facial or iris scan. In theory many other characteristics like the gait, the ear, DNA or even the human odor could be used as a biometric factor.[4]
These intrinsic factors are sometimes refereed to as traits or inherits, too.[5]

While it seems naturally to authenticate a person with a biometric, it also comes with a couple of challenges. Both the false rejection rate (FRR), i.e. a user is rejected even though it's a legitimate authentication attempt and false acceptance rate (FAR), i.e. an imposter is granted access, need to be accounted. Compared to knowledge and possession factors the enrollment of the biometric and the continuous update of the sample is more complicated and expensive.
On the other hand though, it's more complicated to steal this factor than the others.

1.1.4 Others/Location

While the mentioned forms above are considered a standard in the literature, others forms exists, too. Those include e.g. the location of the user or a time-based authentication.[6]

1.2 Difference between authentication and verification and MFA vs 2SV

One could argue that the sometimes the different authentication factors can be reduced to the same (OTP as something the user knows, since it relies on a secret). In this case the authentication is technically correct not a Multi-factor authentication (MFA) but a multi-step verification, since the same factor is used multiple times. Since this fine differentiation is not important for the thesis the term MFA is used throughout.

1.3 Differentiation of factors

1.3.1 Password

Just knowledge. Often weak, re-used. Meant to be remembered. One factor only. Protection by the server often not given, user's are writing it down etc.

---

[4]See JRN11, pp. 30–34.
[5]See DRN17, p. 186.
[6]See DRN17, p. 191.

1.3.2 MFA

More general term for 2FA. Can combine e.g. password with another method (like possession of hardware key, App) or trait (like TouchID, FaceID)

OOB

Out-of-band (OOB)

1.3.3 WebAuth

New API World Wide Web Consortium (W3C)

2 One Factor

2.1 Threats

2.1.1 What you know (Password)

2.1.2 What you habe (Possession)

2.1.3 What you are (Biometrics)

3 Multi-factor authentication

In this chapter a list of different MFA solutions is described in detail.

3.1 OTP

3.1.1 HMAC

Keyed-Hashing for Message Authentication (HMAC) Code is an extension of a Message Authentication Code (MAC) and standardized in Request For Comments (RFC)z and National Institute of Standards and Technology (NIST) abc.

HTOP

HMAC-based One-time Password algorithm, counter based. RFC 899. Configurable length (6-10). Default SHA1. Truncation of HMAC

TOTP

Time based instead of counter based. RFC 123 and Initiative For Open Authentication (OATH).

pros

1. Collisions in MD5 or SHA1 are no problem, already stated/analyzed in the RFC

cons

"Just an algorithm"

1. synchronization

2. invalidation

3. nobody knows how the algorithm is implemented (RFC = no standard)

4. Differences (e.g. Steam - only 5 digits, limited Alphabet)

5. Brute Force if server does not limit

6. Not phishing resistant

3.2 Smart Cards

3.3 Hardware Tokens

4 Security

4.1 Introduction

In this chapter the introduced MFA solutions are analyzed in regards of their security aspects, ranging from algorithms to transportation risks.

4.2 HOTP and TOTP

In this section the security of both HMAC-based One-time Password algorithm (HTOP) and Time-based One-Time Password algorithm (TOTP) is being analyzed.

4.2.1 Algorithm

As both the HTOP and the TOTP are based on the HMAC algorithm by building the OTP over the HMAC function of the secret key and the counter with a truncation, the underlying HMAC algorithm needs to be evaluated.
The important part here is the chosen cryptographic hash algorithm. Mostly Secure Hash Algorithm (SHA)-1 is used, since it's the default of the RFC. Given that both SHA-1 and MD5 are considered insecure one has to ask if they are still considered secure in the OTP context.
Because the collision resistance of the chosen cryptographic hash algorithm is not important for the security of the OTP generation those algorithms do not expose a threat.
The Federal Office for Information Security (BSI) lists these algorithms as secure for HMAC[1]

Citations: []

It is more important that the algorithm is implemented correctly, in the past e.g. Google did not issue OTP values with a leading zero. Besides that, the minimum length of the OTP values are six digits, meanwhile the RFC supports up to 10.
For example Steam, decided to use a different alphabet and character length.

A theoretical vulnerability is to use the time sync offset feature because it enables an attacker to use a token that's much longer valid than it should be. (as discussed in section xx - time sync/drift)

---

[1]Sic19.

4.2.2 Transportation

Given that the generation of the OTP is considered secure the more important region to analyze is the transportation of these OTP. In this section the transportation mediums SMS, E-Mail and App are considered.

SMS

The biggest advantage of SMS as a transportation medium is every mobile, ranging from an old Nokia to a new iPhone XS, is capable of receiving SMS. All major mobile phone operation systems come with a SMS application pre-installed, so no external apps are required.
SMS are around 1999 and highly accepted and easy to use.

While there are some key advantages with SMS transportation it also comes with a lot of downsides. Besides the cost aspect of SMS traffic, both for the sender and potentially for the receiver due to roaming fees, too, the current state of SMS traffic is considered insecure.
The SMS traffic relies on the Signalling System No. 7 (SS7) network which was developed in the 1970s. It has multiple security flaws that allows an attacker to eavesdrop or modify the in- and out-coming traffic.[2]

In contrast to the web and email the user is not very aware of phishing attacks in the SMS context. Studies however show that a new technique called forward phishing is already in use. In this scenario the attacker sends the victim a (spoofed) SMS from the fakes service provider to reply with the OTP code for security measures.[3]

Another negative aspect of SMS transportation is the routing. Many companies rely on third-party providers in order to send the SMS to the user. Often these providers like name some are using countries where SMS are very cheap, but on the other hand the SS7 security measures like SMS home routing and not enforced. This results in a higher security risk of the SMS being compromised while reaching the user. Also, the third party providers are given access to the OTP which enables the risk of a malicious insider because the security measures might be weaker than the original company.

Especially for Android there exists multiple SMS trojans which are capable of intercepting the SMS, too.

Given all these facts SMS transportation should be avoided at all costs[4], since there are multiple flaws in the SS7 network itself and the process how the SMS reaches the user. It's also not resistant against phishing or mobile phone trojans.

BILDER für Phishing und Interception und Malware

---

[2]Wel17; HO17; Puz17.

[3]Jak18; Sia+17.

[4]Jak18.

cons

1. Delivery time

2. SIM Swapping, cloning, hijacking, ...

App

pros

1. Works offline

2. cheaper

cons

1. Secret can be phished while setup (either on phone or computer)

2. Trusted apps? OSS?

3. Vulnerabilities –> e.g. Authy

E-Mail

pros

cons

5 WebAuth

5.1 History and evolution

5.2 Technical implementation and details

5.2.1 Browser support

5.2.2 Usability

5.3 Security aspects

5.3.1 Problems

- Identify theft if not as 2FA and key is lost (e.g. Yubikey without fingerprint sensor)

6 Comparison

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special contents, but the length of words should match the language.

12

7 Conclusion

Bibliography

[BB17]   Lee Brotherston and Amanda Berlin. *Defensive Security Handbook: Best Practices for Securing Infrastructure.* Sebastopol, CA, USA: O'Reilly Media, 2017. ISBN: 9781491960356.

[DRN17]   Dipankar Dasgupta, Arunava Roy, and Abhijit Nag. "Multi-factor authentication." In: *Advances in User Authentication.* Springer, 2017, pp. 185–233.

[Eck14]   Claudia Eckert. *IT-Sicherheit: Konzepte - Verfahren - Protokolle.* 9. Auflage. Munich, Germany: De Gruyter, 2014. ISBN: 978-3-486-77848-9.

[HO17]   Silke Holtmanns and Ian Oliver. "SMS and One-Time-Password Interception in LTE Networks." In: *2017 IEEE International Conference on Communications (ICC).* May 2017, pp. 1–6. DOI: `10.1109/ICC.2017.7997246`.

[Jak18]   Markus Jakobsson. "Two-factor inauthentication – the rise in SMS phishing attacks." In: *Computer Fraud & Security* 2018.6 (2018), pp. 6–8. ISSN: 1361-3723. DOI: `10.1016/S1361-3723(18)30052-6`.

[JRN11]   Anil K. Jain, Arun A. Ross, and Karthik Nandakumar. *Introduction to Biometrics.* New York, NY, USA: Springer, 2011. ISBN: 978-0-387-77325-4. DOI: `10.1007/978-0-387-77326-1`.

[Puz17]   Sergey Puzankov. "Stealthy SS7 Attacks." In: *Journal of ICT Standardization* 5.1 (2017), pp. 39–52.

[Sia+17]   Hossein Siadati et al. "Mind your SMSes: Mitigating social engineering in second factor authentication." In: *Computers & Security* 65 (2017), pp. 14–28. ISSN: 0167-4048. DOI: `10.1016/j.cose.2016.09.009`.

[Sic19]   Bundesamt für Sicherheit in der Informationstechnik. "Kryptographische Verfahren: Empfehlungen und Schlüssellängen." In: *Technische Richtlinie TR-02102-1, Bundesamt für Sicherheit in der Informationstechnik* 1 (2019).

[Wel17]   Bill Welch. "Exploiting the weaknesses of SS7." In: *Network Security* 2017.1 (2017), pp. 17–19. ISSN: 1353-4858. DOI: `10.1016/S1353-4858(17)30008-9`.

[ZKM12]   F. Zhang, A. Kondoro, and S. Muftic. "Location-Based Authentication and Authorization Using Smart Phones." In: *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.* June 2012, pp. 1285–1292. DOI: `10.1109/TrustCom.2012.198`.

List of Figures

Listings

List of Tables

Glossary

S

SS7 A telephony signaling protocol

W

W3C The international standards organization for the World Wide Web

Acronyms

B

BSI Federal Office For Information Security

F

FAR False Acceptance Rate

FRR False Rejection Rate

H

HMAC Keyed-Hashing For Message Authentication

HTOP HMAC-based One-time Password Algorithm

M

MAC Message Authentication Code

MFA Multi-factor Authentication

N

NIST National Institute Of Standards And Technology

O

OATH Initiative For Open Authentication

OOB Out-of-band

OTP One-time Password

P

PIN Personal Identification Number

R

RFC Request For Comments

S

SHA Secure Hash Algorithm

SS7 Signalling System No. 7, *Glossary:* SS7

T

TOTP Time-based One-Time Password Algorithm

W

W3C World Wide Web Consortium, *Glossary:* W3C

Declaration of Academic Integrity

Hereby, I declare that I have composed the presented paper independently on my own and without any other resources than the ones indicated. All thoughts taken directly or indirectly from external sources are properly denoted as such.

Hamburg, July 31, 2019

Tim Brust

Theses

Max 1 page with discussion-worthy key aspects of this thesis.
6-12 theses!