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 19, 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

1. Possession
2. Trait
3. Knowledge
4. (Location)

1.2 Differentiation of factors

1.2.1 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.

1.2.2 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)

1.2.3 WebAuth

New API W3C

2 One Factor

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.

3 Two-factor

Wording: Two-Factor Auth vs Two-Factor Verification

3.1 OTP

3.1.1 HMAC

HMAC Code is an extension of a MAC and standardized in RFCz and 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 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 HTOP and 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 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 BSI lists these algorithms as secure for HMAC[1]

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)

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 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][3][4]

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.[5][6]

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[5], 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

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.

7 Conclusion

Bibliography

[1] Verfahren, Kryptographische: Empfehlungen und Schlüssellängen. In: *Technische Richtlinie TR-02102-1, Bundesamt für Sicherheit in der Informationstechnik (BSI), Stand* 8 (2017), S. 2017–01

[2] Welch, Bill: Exploiting the weaknesses of SS7. In: *Network Security* 2017 (2017), Nr. 1, 17 - 19. http://dx.doi.org/https://doi.org/10.1016/S1353-4858(17)30008-9. – DOI https://doi.org/10.1016/S1353–4858(17)30008–9. – ISSN 1353–4858

[3] Holtmanns, S. ; Oliver, I.: SMS and one-time-password interception in LTE networks. In: *2017 IEEE International Conference on Communications (ICC)*, 2017. – ISSN 1938–1883, S. 1–6

[4] Puzankov, Sergey: Stealthy SS7 Attacks. In: *Journal of ICT Standardization* 5 (2017), Nr. 1, S. 39–52

[5] Jakobsson, Markus: Two-factor inauthentication – the rise in SMS phishing attacks. In: *Computer Fraud & Security* 2018 (2018), Nr. 6, 6 - 8. http://dx.doi.org/https://doi.org/10.1016/S1361-3723(18)30052-6. – DOI https://doi.org/10.1016/S1361–3723(18)30052–6. – ISSN 1361–3723

[6] Siadati, Hossein ; Nguyen, Toan ; Gupta, Payas ; Jakobsson, Markus ; Memon, Nasir: Mind your SMSes: Mitigating social engineering in second factor authentication. In: *Computers & Security* 65 (2017), 14 - 28. http://dx.doi.org/https://doi.org/10.1016/j.cose.2016.09.009. – DOI https://doi.org/10.1016/j.cose.2016.09.009. – ISSN 0167–4048

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

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

OTP One-time password

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 19, 2019

Tim Brust

Theses

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