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: August 1, 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 introduce or take new methods into account like location- or time-based authentication.[2] Therefore this thesis accounts for them, too and describes the methods in the following sections briefly and a detailed analysis of the security, potential risk and threats is done in section 2.1.

1.1.1 Knowledge

The most common method of authentication is knowledge, i.e. »something the user knows«. Commonly used in information technology (IT) are passwords. Other forms of knowledge are for example a personal identification number (PIN) used e.g. banking (ATM’s, credit cards) or telephony (SIM card), a passphrase, secret or 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. »something the user has« (physically). The most basic example is a key for a lock. Other forms are for example a bank or ID card which can use techniques like radio-frequency identification

[1] See TW75, p. 299; See BB17, p. 140; And08, p. 47.
[2] ZKM12; See DRN17, p. 191.
[3] See Eck14, p. 467.

(RFID), an onboard chip or magnetic stripes to store the information. In IT security tokens are often used, which can be a hardware (e.g. a YubiKey or an RSA SecurID) or software (e.g. a smartphone application) token. They can either be disconnected, connected (e.g. via USB or as a smart card) or contactless (e.g. via near-field communication (NFC), Bluetooth Low Energy (BLE) or RFID).[4]

The security of this method relies on the fact that only a legitimate user has access to the possession factor and that no intruder has access or can e.g. make a copy. The biggest risk is the lost or theft of the possession, although e.g. some security tokens are itself protected with a form of authentication like the fingerprint of the legitimate user.

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.[5]
These intrinsic factors are sometimes referred to as traits or inherits, too.[6]

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 the false acceptance rate (FAR), i.e. an imposter is granted access, need to be accounted for the usage. Compared to knowledge and possession factors the enrollment of the biometric and the continuous update of the sample is more complicated and expensive.[7]

On the other hand, it's more complicated to steal, share or copy this factor than the others. The usability varies because of the quality of the used biometrics module, the chosen biometric itself and the availability of the biometric.

1.1.4 Further methods of authentication

While the mentioned authentication forms above are considered a standard in the literature, other forms exist, too. Those include e.g. the location of the user. The location-based approach grants or denies the access based on the current location. This can either be physical (e.g. via GPS) or digital with e.g. an IP-address.[8]

Yet another form is the time-based authentication. A common example is the time restricted access to a banking safe, which can only be opened at specific times of the day, it's secured by a time lock. In IT this form of authentication helps to protect

[4] See Tod07, p. 24; DLE19; See Kei17, pp. 8–11.
[5] See JRN11, pp. 30–34.
[6] See DRN17, p. 186.
[7] See JRN11, pp. 18–24.
[8] ZKM12.

against e.g. phishing attacks from abroad, because the access is granted or denied based on the time and general routines where e.g. a user logs on.[9]

1.2 Wording differences between multi-factor, multi-step, authentication and verification

The naming of the chosen authentication or verification methods by companies is often confusing or difficult to understand. Companies use terms like two-factor authentication (2FA), often just calling it 2FA,[10] while others are talking about two-step-verification, sometimes written as 2-Step Verification too.[11].

One could argue that the different authentication factors can be reduced to a single one, e.g. that an OTP is »something the user knows«, since it relies on a secret that *could* in theory be memorized, too.
In this case the term multi-factor authentication (MFA) or 2FA is technically incorrect, since it's instead a multi-step authentication, because the same factor is used multiple times.

Besides that (user) verification is a part of the authentication process, this fine differentiation of verification vs. authentication and multi-step vs. multi-factor is not important for this thesis and the term MFA is used throughout.

[9] See DRN17, p. 191.

[10] Sup19a.

[11] Sup19b; Pla; Goo; Mic19.

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.

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)

1. re-usage
2. phishing -> stealing in general
3. secret might be known by others, too (e.g. security questions)

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.

[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.

7 Conclusion

7.0.1 View?

OAuth 2.0, KERERBOS, radius based, LDAP, AD, OpenID Connect, SAML

Bibliography

[And08] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems.* 2nd ed. Indianapolis, USA: Wiley, 2008. ISBN: 9780470068526.

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

[DLE19] Thomas Dressel, Eik List, and Florian Echtler. "SecuriCast: Zero-touch Two-factor Authentication Using WebBluetooth." In: *Proceedings of the ACM SIGCHI Symposium on Engineering Interactive Computing Systems.* EICS '19. Valencia, Spain: ACM, 2019, 6:1–6:6. ISBN: 978-1-4503-6745-5. DOI: 10.1145/3319499.3328225.

[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.

[Kei17] Konstantinos Markantonakis Keith Mayes. *Smart Cards, Tokens, Security and Applications.* 2nd ed. Cham, Switzerland: Springer International Publishing AG, 2017. ISBN: 978-3-319-50498-8, 978-3-319-50500-8.

[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).

[Tod07] Dobromir Todorov. *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*. Auerbach Publications, 2007. ISBN: 1420052195,9781420052190,9781420052206.

[TW75] Rein Turn and W. H. Ware. “Privacy and Security in Computer Systems: The vulnerability of computerized information has prompted measures to protect both the rights of individual subjects and the confidentiality of research data bases.” In: *American Scientist* 63.2 (1975), pp. 196–203. ISSN: 00030996.

[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.

Internet sources

[Goo] Google. *Google 2-Step Verification.* URL: https://www.google.com/landing/2step/ (visited on 08/01/2019).

[Mic19] Microsoft. *How to use two-step verification with your Microsoft account.* July 25, 2019. URL: https://support.microsoft.com/en-us/help/12408/microsoft-account-how-to-use-two-step-verification (visited on 08/01/2019).

[Pla] PlayStation. *2-Step Verification.* Website. URL: https://www.playstation.com/en-us/account-security/2-step-verification/.

[Sup19a] Apple Support. *Two-factor authentication for Apple ID.* July 30, 2019. URL: https://support.apple.com/en-us/HT204915 (visited on 08/01/2019).

[Sup19b] Apple Support. *Two-step verification for Apple ID.* May 29, 2019. URL: https://support.apple.com/en-us/HT204152 (visited on 08/01/2019).

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

Symbols

2FA Two-factor Authentication

B

BLE Bluetooth Low Energy

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

I

IT Information Technology

M

MAC Message Authentication Code

MFA Multi-factor Authentication

N

NFC Near-field Communication

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

RFID Radio-frequency Identification

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, August 1, 2019

Tim Brust

Theses

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