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 12, 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

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

Keyed-Hash Message Authentication Code is an extension of a Message Authentication Code (MAC) and standardized in RFCXYz 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 phising resistant

3.2 Smart Cards

3.3 Hardware Tokens

4 Security

4.1 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.

4.2 (T)OTP

4.2.1 Transportation

SMS

pros

1. Every mobile is capable of receiving SMS (from old Nokia’s ranging to new iPhone Xs)
2. No apps required, works everywhere (worldwide)
3. easy to use

cons

1. Relies on the SS7 security, which is broken
2. SMS eavesdropping is very easy
3. Forward phishing attacks are possible, too
4. Mobile phone trojans can intercept all incoming SMS
5. costs millions for bigger companies (each SMS is charged)
6. Roaming costs

7. Delivery time
8. Routing mainly unknown
9. Third party companies send the SMS - countries very it's cheap (Africa, ...) are used - how are those data protection laws

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] Dasgupta, Dipankar ; Roy, Arunava ; Nag, Abhijit: Multi-factor authentication. In: *Advances in User Authentication*. Springer, 2017, S. 185–233

[2] Turner, James M.: The keyed-hash message authentication code (hmac). In: *Federal Information Processing Standards Publication* (2008), S. 198–1

[3] Biryukov, Alex ; Lano, Joseph ; Preneel, Bart: Recent attacks on alleged SecurID and their practical implications. In: *Computers & Security* 24 (2005), Nr. 5, 364 - 370. http://dx.doi.org/https://doi.org/10.1016/j.cose.2005.04.006. – DOI https://doi.org/10.1016/j.cose.2005.04.006. – ISSN 0167–4048

[4] Biryukov, Alex ; Lano, Joseph ; Preneel, Bart: Cryptanalysis of the Alleged SecurID Hash Function. In: Matsui, Mitsuru (Hrsg.) ; Zuccherato, Robert J. (Hrsg.): *Selected Areas in Cryptography*. Berlin, Heidelberg : Springer Berlin Heidelberg, 2004. – ISBN 978–3–540–24654–1, S. 130–144

[5] Han, W. ; Wang, Y. ; Cao, Y. ; Zhou, J. ; Wang, L.: Anti-Phishing by Smart Mobile Device. In: *2007 IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007)*, 2007, S. 295–302

[6] Halpert, Benjamin: Mobile Device Security. In: *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*. New York, NY, USA : ACM, 2004 (InfoSecCD '04). – ISBN 1–59593–048–5, 99–101

[7] Dressel, Thomas ; List, Eik ; Echtler, Florian: SecuriCast: Zero-touch Two-factor Authentication Using WebBluetooth. In: *Proceedings of the ACM SIGCHI Symposium on Engineering Interactive Computing Systems*. New York, NY, USA : ACM, 2019 (EICS '19). – ISBN 978–1–4503–6745–5, 6:1–6:6

[8] Mourad, Hassan: The Fall of SS7-How Can the Critical Security Controls Help? In: *SANS Institute InfoSec Reading Room* (2015)

[9] Ulqinaku, Enis ; Lain, Daniele ; Capkun, Srdjan: 2FA-PP: 2Nd Factor Phishing Prevention. In: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. New York, NY, USA : ACM, 2019 (WiSec '19). – ISBN 978–1–4503–6726–4, 60–70

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

[11] 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

[12] 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

[13] Halpin, Harry: The W3C web cryptography API: motivation and overview. In: *Proceedings of the 23rd International Conference on World Wide Web* ACM, 2014, S. 959–964

[14] Likitha, Soorea ; Saravanan, R.: Cryptanalysis of a Multifactor Authentication Protocol. In: Sa, Pankaj K. (Hrsg.) ; Bakshi, Sambit (Hrsg.) ; Hatzilygeroudis, Ioannis K. (Hrsg.) ; Sahoo, Manmath N. (Hrsg.): *Recent Findings in Intelligent Computing Techniques*. Singapore : Springer Singapore, 2019. – ISBN 978–981–10–8639–7, S. 35–42

[15] Jacomme, C. ; Kremer, S.: An Extensive Formal Analysis of Multi-factor Authentication Protocols. In: *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, 2018. – ISSN 2374–8303, S. 1–15

[16] Ometov, A. ; Petrov, V. ; Bezzateev, S. ; Andreev, S. ; Koucheryavy, Y. ; Gerla, M.: Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications. In: *IEEE Network* 33 (2019), March, Nr. 2, S. 82–88. http://dx.doi.org/10.1109/MNET.2019.1800240. – DOI 10.1109/MNET.2019.1800240. – ISSN 0890–8044

[17] Wang, Kailong: Analyzing Security and Privacy in Design and Implementation of Web Authentication Protocols. In: Sun, Jing (Hrsg.) ; Sun, Meng (Hrsg.): *Formal Methods and Software Engineering*. Cham : Springer International Publishing, 2018. – ISBN 978–3–030–02450–5, S. 441–445

[18] Krawczyk, Hugo ; Bellare, Mihir ; Canetti, Ran: RFC 2104: HMAC: Keyed-hashing for message authentication. In: *Internet Engineering Task Force* 252 (1997)

[19] M'Raihi, David ; Machani, Salah ; Pei, Mingliang ; Rydell, Johan: Rfc 6238-totp: Time-based one-time password algorithm. In: *Tools. ietf. org* (2011)

[20] M'Raihi, D ; Bellare, M ; Hoornaert, F ; Naccache, D ; Ranen, O: *RFC 4226: HOTP: An HMAC-based one-time password algorithm*. 2005

[21] Thomas, Kurt ; Li, Frank ; Zand, Ali ; Barrett, Jacob ; Ranieri, Juri ; Invernizzi, Luca ; Markov, Yarik ; Comanescu, Oxana ; Eranti, Vijay ; Moscicki, Angelika ; Margolis, Daniel ; Paxson, Vern ; Bursztein, Elie: Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA : ACM, 2017 (CCS '17). – ISBN 978–1–4503–4946–8, 1421–1434

[22] Cristofaro, Emiliano D. ; Du, Honglu ; Freudiger, Julien ; Norcie, Gregory: Two-Factor or not Two-Factor? A Comparative Usability Study

of Two-Factor Authentication. In: *CoRR* abs/1309.5344 (2013). http://arxiv.org/abs/1309.5344

[23] Xie, Qi ; Dong, Na ; Wong, Duncan S. ; Hu, Bin: Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol. In: *International Journal of Communication Systems* 29 (2016), Nr. 3, 478-487. http://dx.doi.org/10.1002/dac.2858. – DOI 10.1002/dac.2858

[24] Petsas, Thanasis ; Tsirantonakis, Giorgos ; Athanasopoulos, Elias ; Ioannidis, Sotiris: Two-factor Authentication: Is the World Ready?: Quantifying 2FA Adoption. In: *Proceedings of the Eighth European Workshop on System Security*. New York, NY, USA : ACM, 2015 (EuroSec '15). – ISBN 978–1–4503–3479–2, 4:1–4:7

[25] Mulliner, Collin ; Borgaonkar, Ravishankar ; Stewin, Patrick ; Seifert, Jean-Pierre: SMS-Based One-Time Passwords: Attacks and Defense. In: Rieck, Konrad (Hrsg.) ; Stewin, Patrick (Hrsg.) ; Seifert, Jean-Pierre (Hrsg.): *Detection of Intrusions and Malware, and Vulnerability Assessment*. Berlin, Heidelberg : Springer Berlin Heidelberg, 2013. – ISBN 978–3–642–39235–1, S. 150–159

[26] Aloul, F. ; Zahidi, S. ; El-Hajj, W.: Two factor authentication using mobile phones. In: *2009 IEEE/ACS International Conference on Computer Systems and Applications*, 2009. – ISSN 2161–5322, S. 641–644

[27] Ghazizadeh, Eghbal ; Cusack, Brian: Evaluation Theory for Characteristics of Cloud Identity Trust Framework. In: *Cloud Computing-Technology and Practices*. IntechOpen, 2018

[28] Barkadehi, Mohammadreza H. ; Nilashi, Mehrbaksh ; Ibrahim, Othman ; Fardi, Ali Z. ; Samad, Sarminah: Authentication systems: A literature review and classification. In: *Telematics and Informatics* 35 (2018), Nr. 5, 1491 - 1511. http://dx.doi.org/https://doi.org/10.1016/j.tele.2018.03.018. – DOI https://doi.org/10.1016/j.tele.2018.03.018. – ISSN 0736–5853

[29] 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

[30] 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

[31] Shivraj, V. L. ; Rajan, M. A. ; Singh, M. ; Balamuralidhar, P.: One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In: *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*, 2015, S. 1–6

[32] Dmitrienko, Alexandra ; Liebchen, Christopher ; Rossow, Christian ; Sadeghi, Ahmad-Reza: On the (In)Security of Mobile Two-Factor Authentication. In: Christin, Nicolas (Hrsg.) ; Safavi-Naini, Reihaneh (Hrsg.): *Financial Cryptography and Data Security*. Berlin, Heidelberg : Springer Berlin Heidelberg, 2014. – ISBN 978–3–662–45472–5, S. 365–383

[33] Eldefrawy, M. H. ; Alghathbar, K. ; Khan, M. K.: OTP-Based Two-Factor Authentication Using Mobile Phones. In: *2011 Eighth International Conference on Information Technology: New Generations*, 2011, S. 327–331

[34] Dmitrienko, Alexandra ; Liebchen, Christopher ; Rossow, Christian ; Sadeghi, Ahmad-Reza: SECURITY ANALYSIS OF MOBILE TWO-FACTOR AUTHENTICATION SCHEMES. In: *Intel Technology Journal* 18 (2014), Nr. 4

[35] Guirat, Iness B. ; Halpin, Harry: Formal Verification of the W3C Web Authentication Protocol. In: *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security*. New York, NY, USA : ACM, 2018 (HoTSoS '18). – ISBN 978–1–4503–6455–3, 6:1–6:10

[36] Halpin, Harry: Semantic Insecurity: Security and the Semantic Web. In: *PrivOn 2017 - Workshop Society, Privacy and the Semantic Web - Policy and Technology*. Vienna, Austria, Oktober 2017, 1-10

[37] Ulybyshev, D. ; Bhargava, B. ; Villarreal-Vasquez, M. ; Alsalem, A. O. ; Steiner, D. ; Li, L. ; Kobes, J. ; Halpin, H. ; Ranchal, R.: Privacy-Preserving Data Dissemination in Untrusted Cloud. In: *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, 2017. – ISSN 2159–6190, S. 770–773

[38] Cairns, Kelsey ; Halpin, Harry ; Steel, Graham: Security Analysis of the W3C Web Cryptography API. In: Chen, Lidong (Hrsg.) ; McGrew, David (Hrsg.) ; Mitchell, Chris (Hrsg.): *Security Standardisation Research*. Cham : Springer International Publishing, 2016. – ISBN 978–3–319–49100–4, S. 112–140

[39] Angelogianni, Anna: *Analysis and implementation of the FIDO protocol in a trusted environment*, University of Piraeus, Diplomarbeit, 2018

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

[41] Christopher Hadnagy, Michele F.: *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*. 1. Wiley, 2015. – ISBN 1118958470,9781118958476

[42] Harrington, Jan L.: *Network Security: A Practical Approach (The Morgan Kaufmann Series in Networking)*. Morgan Kaufmann, 2005. – ISBN 0123116333,9780123116338

[43] Keith Mayes, Konstantinos Markantonakis (.: *Smart Cards, Tokens, Security and Applications*. 2. Springer International Publishing, 2017. – ISBN 978–3–319–50498–8, 978–3–319–50500–8

[44] Eckert, Claudia: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. 10. Auflage. De Gruyter, 2018. – ISBN 978–3110551587

[45] LeBlanc, Jonathan ; Messerschmidt, Tim: *Identity and Data Security for Web Development: Best Practices*. O'Reilly Media, 2016 https://www.amazon.com/Identity-Data-Security-Web-Development/dp/1491937017?SubscriptionId=AKIAIOBINVZYXZQZ2U3A&tag=chimbori05-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=1491937017. – ISBN 1491937017

List of Figures

Listings

List of Tables

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 12, 2019

Tim Brust

Theses

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