Fakultät für Ingenieurwissenschaften

Exposé zur Master-Thesis

Sicherheitsevaluation von Multi-Faktor-Authentifizierung im Vergleich zur Web Authentifizierungs API

Security evaluation of multi-factor authentication in comparison with the Web Authentication API

eingereicht von:	Tim Brust geboren am 31.03.1995 in Hamburg Studiengang IT-Sicherheit und Forensik
Matrikelnummer:	246565
Erstgutachter:	Prof. Dr.-Ing. habil. A. Ahrens
Zweitgutachter:	

Hamburg, den 25. Januar 2019

1 Problemstellung und Motivation

Der sichere Umgang mit Passwörtern stellt für viele Anwender noch ein Problem dar.[1] Häufig werden Passwörter von verschiedenen Seiten wiederverwendet, teilweise auch die privaten Passwörter mit denen aus dem beruflichen Umfeld vermischt. Dies erzeugt ein hohes Risiko für die (vertraulichen) Daten der Nutzer. Hinzu kommt, dass weniger als die Hälfte der Deutschen im Jahr 2019 Multi-Faktor-Authentifizierung nutzen und nur 10% der Deutschen in 2018 einen Passwortmanager genutzt haben. Aktuell merken sich über die 70% der Befragten die Passwörter noch im Kopf oder schreiben sie in Klartext auf einen Zettel.[2]
Zeitgleich steigt die Anzahl an erfassten Fällen von Cyberkriminalität weiter an[3] und auch zum Beispiel Phishing bleibt ein großes Risiko. Zwar können Multi-Faktor-Authentifizierungen gegen Bedrohungen wie Brute-Force oder geklaute Passwörter Abhilfe schaffen, aber gegen gut getarnte Phishing-Attacken sind diese nutzlos. Des Weiteren gilt beispielsweise der SMS Verkehr nicht mehr als sicher, trotz dessen werden viele zweite Faktoren über diesen unsicheren Weg übermittelt. Diesen negativen Trends steht jedoch eine neue Programmierschnittstelle gegenüber – die Web Authentication API. Diese befindet sich in Entwicklung für die weit verbreiteten Browser wie Chrome, Edge, Safari und Firefox. Sie ermöglicht eine sichere Registrierung, Login und Zwei-Faktor-Authentifizierung ganz ohne das Generieren, Merken oder Aufbewahren von Passwörtern durch die Nutzung von asymmetrischen Kryptosystemen. Die privaten Schlüssel können sowohl auf externen Geräten wie USB Sticks gespeichert werden, als auch durch eingebaute Sensoren in den Geräten wie Fingerabdruckscanner gespeichert und geschützt werden.

[1] Nier, H. (2017, Januar 23). Der große Passwort-Stress [Digitales Bild]. Zugriff am Januar 23, 2019, von https://de.statista.com/infografik/7705/der-grosse-passwort-stress/.

[2] ARD, & Infratest dimap. (n.d.). Was tun sie, um sich vor einem Missbrauch Ihrer persönlichen Daten zu schützen?. In Statista - Das Statistik-Portal. Zugriff am 23. Januar 2019, von https://de.statista.com/statistik/daten/studie/955802/umfrage/massnahmen-von-internetnutzern-zum-schutz-vor-datenmissbrauch-in-deutschland/.

[3] Bundeskriminalamt. (n.d.). Polizeilich erfasste Fälle von Cyberkriminalität im engeren Sinne* in Deutschland von 2004 bis 2017. In Statista - Das Statistik-Portal. Zugriff am 23. Januar 2019, von https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/.

2 Zielsetzung und Abgrenzung

2.1 Zielsetzung

Zielsetzung dieser Master Thesis ist eine Einführung in die Multi-Faktor-Authentifizierung und verschiedene gängige Faktoren (Besitz, Wissen, Merkmal) inklusive der technischen Funktionsweise, Nutzungsmöglichkeiten im Web und potenziellen Sicherheitsproblemen. Die Web Authentication API soll als Alternative bzw. mögliche Ergänzung hierzu vorgestellt werden. Dabei muss die Frage geklärt werden, inwiefern diese die Sicherheit und den Nutzerkomfort erhöhen kann. Dabei spielt die Bewertung der Sicherheit der Web Authentication API eine entscheidene Rolle.

2.2 Zielgruppe

Die Zielgruppe dieser Master Thesis sind technisch versierte Leser, die ein Verständnis für Datenschutz und -sicherheit besitzen und die (mathematische) Funktionsweise hinter Algorithmen wie RSA, elliptischen Kurven und symmetrischen Schlüsselaustausch kennen. Des Weiteren richtet sich diese Master Thesis an interessierte (Web-) Entwickler, die den Einsatz alternativer oder ergänzender Registrierungsverfahren und Multi-Faktor-Authentifizierungen durch den Einsatz von asymmetrisches Kryptosystemen verstehen und ihre Vor- und Nachteile nachvollziehen wollen.

2.3 Abgrenzung

Bestehende Algorithmen und Konzepte werden, soweit nicht für den Verlauf der Arbeit benötigt, nicht näher erläutert. Außerdem soll diese Master-Thesis keine reine Kryptoanalyse werden, sondern auch auf andere Aspekte wie die Benutzbarkeit durch die Benutzer, technische Umsetzbarkeit und Unterstützung eingegangen werden, um zu evaluieren inwiefern die Web Authentication API genutzt werden kann. Die Bereiche OAuth 2.0 bzw. OpenID Connect sowie Single Sign On (SSO) sind ebenfalls nicht Fokus dieser Arbeit.

3 Stand der Forschung

Die Themenbereiche wie Cyberkriminalität, Multi-Faktor-Authentifizierung und sichere Passwörter sind ausreichend erforscht, ebenso die dahinter zum Einsatz kommenden Algorithmen und mathematischen Grundlagen. Dazu zählen auch bekannte Schwachstellen und etwaige Lösungen für diese. Vorarbeiten im Bereich Universal Two Factor (U2F) existieren ebenfalls, jedoch ohne den Bezug zur Web Authentication API und ihrem Einsatz.[1,2]

Da sich Web Authentication API aktuell noch in der Entwicklung befindet, ist der Stand der Forschung im Vergleich zu den bekannten Multi-Faktor-Authentifizierungsverfahren weniger fortgeschritten. Die aus dem FIDO Standard resultierende Web Authentication API nutzt zwar bekannte mathematische Grundlagen, die technische Umsetzung und Einbindung in produktive Systeme ist aber weitestgehend noch nicht erfolgt. Ebenso gibt es bisher kaum Analysen zu ihrer Sicherheit und den möglichen Schwächen.

[1] Korkmaz, M. (2017). Grundlagen der FIDO-Authentifizierung und Vergleich mit traditionellen Authentifizierungsverfahren (Doctoral dissertation, Hochschule für Angewandte Wissenschaften Hamburg). Zugriff am 23. Januar 2019, von http://edoc.sub.uni-hamburg.de/haw/volltexte/2017/4020/pdf/Bachelorarbeit_MuratKorkmaz.pdf

[2] Angelogianni, A. (2018). Analysis and implementation of the FIDO protocol in a trusted environment (Master's thesis, University of Piraeus). Zugriff am 23. Januar 2019, von http://dione.lib.unipi.gr/xmlui/handle/unipi/11387

4 Vorgehen

Zunächst soll in dem ersten Abschnitt dieser Master Thesis der Leser in Grundlagen von Passwörtern und Authentifizierung eingeführt werden. Hierfür werden die verschiedenen Bereiche

1. Passwörter ohne zweiten Faktor (“One-Faktor-Authentication“)
2. Multi-Faktor-Authentifizierung
3. Web Authentication API

kurz vorgestellt und voneinander abgegrenzt.

Anschließend wird auf die Probleme und Risiken von “One-Faktor-Authentication“ eingegangen. Im dritten Abschnitt werden die verschiedenen Faktoren (beispielsweise zeitbasierte Faktoren, SMS oder biometrische Merkmale) näher analysiert und ihre technische Funktionsweise beschrieben. Außerdem werden die Faktoren jeweils auf ihre Sicherheit und Schutz gegen mögliche Angriffe wie Phishing oder Man in the middle (MITM) untersucht.
Darauf aufbauend wird die Web Authentication API im vierten Abschnitt detailliert beschrieben. Hierbei wird im Detail auf die technische Funktionsweise eingegangen und vor welchen Angriffsmöglichkeiten der Einsatz schützen kann, jedoch auch welche etwaigen Sicherheitsrisiken vorhanden sind. Hierfür wird auf einen technischen Proof of Concept zurückgegriffen und die Web Authentication beispielhaft implementiert.

Im fünften Abschnitt wird die Web Authentication API mit der Multi-Faktor-Authentifizierung verglichen. Dabei wird untersucht, inwiefern sich die Web Authentication API als Ersatz für Multi-Faktor-Authentifizierung eignet und/oder ob diese komplementär eingesetzt werden können.
Abschließend erfolgt eine Bewertung anhand der gewonnenen Erkenntnisse aus dem vorherigen Abschnitt sowie ein Fazit mit Ausblick.

5 Vorläufige Gliederung

- Abstract
- Inhaltsverzeichnis
- Abbildungsverzeichnis, Tabellenverzeichnis, Quellcodeverzeichnis, Abkürzungsverzeichnis
- Einleitung
- einstufige Authentifizierung
- Multi-Faktor-Authentifizierung
  - Faktoren (Besitz, Wissen, Merkmal)
  - Sicherheitsprobleme
- Web Authentication API
  - Geschichte (FIDO, U2F)
  - Technische Umsetzung und Browser Unterstützung
  - Sicherheitsprobleme
- Vergleich von Multi-Faktor-Authentifizierung und der Web Authentication API
  - Kriterien und Vergleich
- Bewertung, Fazit und Ausblick
- Literaturverzeichnis
- ggf. Glossar
- Anhang
- Ehrenwörtliche Erklärung

6 Literatur

[AZEH09] 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

[Beu18] BEUCHELT, Gerald: Schwache Passwörter — Nutzer spielen weiterhin Vogel Strauß. In: *Wirtschaftsinformatik & Management* 10 (2018), Oct, Nr. 5, S. 18–21. http://dx.doi.org/10.1007/s35764-018-0094-x. – DOI 10.1007/s35764–018–0094–x. – ISSN 1867–5913

[CHS16] CAIRNS, Kelsey ; HALPIN, Harry ; STEEL, Graham: Security analysis of the W3C web cryptography API. In: *International Conference on Research in Security Standardisation* Springer, 2016, S. 112–140

[DDC18] DAS, Sanchari ; DINGMAN, Andrew ; CAMP, L J.: Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key. In: *2018 International Conference on Financial Cryptography and Data Security (FC)*, 2018

[Eck14] ECKERT, Claudia: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. De Gruyter Oldenbourg, 2014. – ISBN 9783486778489

[GB17] GILMAN, Evan ; BARTH, Doug: *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media, 2017. – ISBN 9781491962190

[Kwo02] KWON, Taekyoung: Impersonation attacks on software-only two-factor authentication schemes. In: *IEEE Communications Letters* 6 (2002), Aug, Nr. 8, S. 358–360. http://dx.doi.org/10.1109/LCOMM.2002.802034. – DOI 10.1109/LCOMM.2002.802034. – ISSN 1089–7798

[LM16] LEBLANC, Jonathan ; MESSERSCHMIDT, Tim: *Identity and Data Security for Web Development: Best Practices*. O'Reilly Media, 2016. – ISBN 1491937017

[Ngu15] NGUYEN, Kim: Neue Wege der hardware-basierten Authentisierung und Identifikation: FIDO, PKI und mehr. In: BUB, Udo (Hrsg.) ; DELESKI, Viktor (Hrsg.) ; WOLFENSTETTER, Klaus-Dieter (Hrsg.): *Sicherheit im Wandel von Technologien und Märkten*. Wiesbaden : Springer Fachmedien Wiesbaden, 2015. – ISBN 978–3–658–11274–5, S. 49–54

[SM18] SCHWARTZ, Michael ; MACHULAK, Maciej: *Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software*. Apress, 2018. – ISBN 9781484226001

[Spi16] SPITZ, Stephan: Mobile Multifaktor – Authentisierung. In: *Datenschutz und Datensicherheit - DuD* 40 (2016), Apr, Nr. 4, S. 203–205. http://dx.doi.org/10.1007/s11623-016-0578-x. – DOI 10.1007/s11623–016–0578–x. – ISSN 1862–2607

[Sta15] STANISLAV, Mark: *Two-Factor Authentication*. It Governance Publishing, 2015. – ISBN 9781849287326

[UBVV+17] 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