D. Reinhardt, H. Langweg, B.C. Witt, M. Fischer et al. (Hrsg.): Sicherheit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Göttingen 2020 129

Usability, Sicherheit und Privatsphäre von risikobasierter Authentifizierung

Stephan Wiefling[1]

Abstract: Risikobasierte Authentifizierung (RBA) ist eine adaptive Sicherheitsmaßnahme zur Stärkung passwortbasierter Authentifizierung. Sie zeichnet Merkmale während des Logins auf und fordert zusätzliche Authentifizierung an, wenn sich Ausprägungen dieser Merkmale signifikant von den bisher bekannten unterscheiden. RBA bietet das Potenzial für gebrauchstauglichere Sicherheit. Bisher jedoch wurde RBA noch nicht ausreichend im Bezug auf Usability, Sicherheit und Privatsphäre untersucht. Dieser Extended Abstract legt das geplante Dissertationsvorhaben zur Erforschung von RBA dar. Innerhalb des Vorhabens konnte bereits eine Grundlagenstudie und eine darauf aufbauende Laborstudie durchgeführt werden. Wir präsentieren erste Ergebnisse dieser Studien und geben einen Ausblick auf weitere Schritte.

Keywords: Passwort; Authentifizierung; Risikobasierte Authentifizierung

1 Einleitung

Passwortbasierte Authentifizierung hat eine lange Tradition [MT79] und ihre Schwachstellen sind seit langer Zeit bekannt. Diese Schwachstellen reichen von Wiederverwendung gleicher Passwörter [FH07] über kurze Längen [DMR10] bis hin zu Phishing [DTH06]. In letzter Zeit stellen Diebstähle großer Benutzernamen-Passwort-Datenbanken und die damit verbundene automatisierte Eingabe dieser Daten bei anderen Onlinediensten (Credential Stuffing) eine immer größere Gefahr für passwortbasierte Authentifizierung dar [Ak19, WKB14]. Ebenso tragen neue intelligente Passwortratemethoden zu immer effizienteren Angriffen auf Online-Passwörter bei [Wa16].

Trotzdem bleiben Passwörter weiterhin die vorherrschende Authentifizierungsmethode bei vielen Onlinediensten. Aus diesem Grund sind Inhaber von Onlinediensten angehalten, ihre Nutzer mit zusätzlichen Maßnahmen vor Angriffen zu schützen. Eine dabei häufig angebotene Maßnahme ist die Zwei-Faktor-Authentifizierung (2FA) [QHD18]. Diese stellt sich unter Nutzern jedoch als unbeliebt heraus. Weniger als 10% aller aktiven Nutzer des Onlinedienstes Google hatten 2FA im Januar 2018 aktiviert [Mi18], obwohl Google diese Technologie seit 2011 aktiv bei ihren Nutzern bewirbt [Sh11]. Ein Grund für die niedrige Akzeptanz könnte darin liegen, dass Nutzer die kontinuierliche Abfrage zweier unterschiedlicher

[1] TH Köln, Data & Application Security Group, Betzdorfer Straße 2, 50679 Köln, Deutschland / Ruhr-Universität Bochum, Mobile Security Group, Universitätsstrasse 150, ID 2 / 127, 44780 Bochum, Deutschland
stephan.wiefling@th-koeln.de

doi:10.18420/sicherheit2020_12

Authentifizierungsfaktoren als zusätzliche Bürde empfinden [Kr15]. Ein alternativer Ansatz zur Stärkung passwortbasierter Authentifizierung ist risikobasierte Authentifizierung (RBA), welche passwortbasierte Authentifikation mit geringer Nutzerinteraktion stärken kann.

2 Risikobasierte Authentifizierung (RBA)

RBA wird häufig in Kombination mit passwortbasierter Authentifizierung eingesetzt [Fr16]. Diese Technologie soll vor Angreifern schützen, welche in Kenntnis der Zugangsdaten (Benutzernamen und Passwort) sind oder diese mit wenigen Versuchen erraten können. Beispiele dafür sind Credential Stuffing [WKB14], Phishing [DTH06] oder Machine-Learning-basiertes gezieltes automatisiertes Erraten von Passwörtern [Wa16].

Bei der Passworteingabe beobachtet RBA Merkmale, die in dem Kontext verfügbar sind. Mögliche Merkmale reichen von Netzwerkinformationen (z.B. IP-Adresse oder IP-basierte Geolocation) über Geräteinformationen (z.B. verwendeter Browser) bis zu biometrischen Eigenschaften (z.B. Tippverhalten). Basierend auf diesen Merkmalen berechnet RBA eine Risikobewertung, welche typischerweise einer der drei Kategorien *niedriges*, *mittleres* und *hohes Risiko* zugeordnet wird. Bei einem niedrigen Risiko (z.B. gleiches Gerät und gleicher Ort wie immer) wird nach dem Absenden der Zugangsdaten der Zugriff gewährt. Bei einem mittleren Risiko (z.B. ungewöhnliches Gerät an einem anderen Ort) wird der Nutzer nach zusätzlicher Authentifizierung gefragt. Eine solche Authentifizierung kann beispielsweise die Verifikation der hinterlegten E-Mail-Adresse sein [WLID19a]. Wird die zusätzliche Authentifizierung erfolgreich erbracht, so wird der Zugriff gewährt. Bei einem hohen Risiko (z.B. IP-Adresse ist für Spam bekannt) wird hingegen der Zugriff verweigert. Diesen Fall sollten Onlinedienste allerdings nur in sehr seltenen Fällen durchführen, um legitime Nutzer nicht ungewollt auszuschließen.

3 Forschungsstand

Die aktuell publizierte Forschung im Bereich RBA beschränkt sich größtenteils auf die Konzepte und Vorstellung neuer RBA-Systeme. Die von den Systemen zur Risikobewertung herangezogenen Merkmale unterscheiden sich dabei grundsätzlich voneinander. So verwendet beispielsweise das RBA-Verfahren von Freeman et al. die IP-Adresse und den User-Agent-String [Fr16]. Bei Steinegger et al. sind es hingegen der Browser-Fingerprint, fehlerhafte Login-Versuche sowie die IP-basierte Geolocation [St16]. Tabelle 1 zeigt eine Auflistung der vielfältigen in der Literatur erwähnten Merkmale, die im Kontext von RBA vorstellbar sind.

Der Einsatz von RBA beschränkt sich aktuell auf große Onlinedienste [WLID19a]. Darüber hinaus empfiehlt das National Institute of Standards and Technology (NIST) in ihren Digital Identity Guidelines RBA als Maßnahme gegen onlinebasiertes Passwortraten [Gr17].

Merkmal	**RBA Referenzen (mit Ausnahme von [AvO16])**	**Informationstiefe zur Unterscheidbarkeit** [AvO16]
IP-Adresse	[Fr16, GOB13, CM12, AuH11, HH14, St16]	Hoch
User-Agent-String	[Fr16, HH14, SPJ15]	Hoch
Sprache	[Fr16, HH14, CM12]	Hoch
Displayauflösung	[DHO17, SPJ15]	Hoch
Login-Zeit	[Fr16, HH14, GOB13, SPJ15, CM12]	Niedrig
Evercookies	[HH14]	Sehr hoch
Canvas-Fingerprinting	[DHO17, Mo12, St16]	Medium
Maus-/Tastenanschlag Dynamik	[Tr12, So19]	- (*Niedrig bei Scrollrad-Fingerprinting*)
Fehlgeschlagene Loginversuche	[HH14, St16]	-
Protokoll-Fingerprinting	-	Hoch
Audioverarbeitung	-	Medium
WebRTC	-	Medium
Zählen von Rechnern hinter NAT	-	Niedrig
Batterie-Information	-	Niedrig
Ad-Blocker-Erkennung	-	Sehr niedrig

Tab. 1: Auswahl möglicher Merkmale, die zur RBA-Risikobewertung herangezogen werden können (angelehnt an [WLID19a]). Alle Merkmale können durch die Benutzung eines Webbrowsers ohne Erweiterungen ermittelt werden.

Folglich nimmt die Bedeutung dieser Technologie immer weiter zu. Allerdings halten bislang die Unternehmen, die RBA einsetzen, ihre Erfahrungen mit RBA vor der Öffentlichkeit zurück. Dies erschwert eine flächendeckende Einführung von RBA. Dabei besitzt diese Technologie auch für kleine und mittelgroße Webseiten das Potenzial, die Sicherheit für ihre Nutzer zu erhöhen.

Die Usability einer neuen Technologie hat einen großen Einfluss auf die Akzeptanz und Verbreitung dieser Technologie [AA18]. Allerdings wurden die Usability-Aspekte von RBA bislang noch nicht erforscht. In gleicher Weise trifft dies auf die Privatsphärenaspekte zu.

4 Forschungsvorhaben

Ziel des Dissertationsvorhabens ist das weitreichende Verständnis von RBA in den dort noch unerforschten Bereichen der Usability, Sicherheit und Privatsphäre. Mit der Forschung an RBA soll eine großflächige Anwendung der Technologie, auch bei kleinen und mittelgroßen Onlinediensten, ermöglicht werden. Zusammengefasst widmet sich das geplante Dissertationsvorhaben den folgenden Fragestellungen:

- Wie muss RBA umgesetzt sein, damit diese Authentifizierung von Nutzern *effektiv*, *effizient* und *zufriedenstellend* [IS17] durchgeführt werden kann?
- Welche Merkmale müssen gesammelt werden, damit RBA die Nutzer in zufriedenstellendem Maße vor Angriffen schützen kann?

- Wie können diese Merkmale gesammelt und ausgewertet werden, um eine möglichst große Privatsphäre bei gleichbleibender Sicherheit von RBA zu erreichen?

5 Erste Ergebnisse

Als Grundlage für weitere Studien wurde der Einsatz von RBA bei acht großen Onlinediensten mithilfe von Black-Box-Tests erforscht [WLID19a]. Dafür wurden 28 virtuelle Identitäten und 224 Nutzeraccounts auf diesen Onlinediensten erstellt. Danach haben wir Nutzerverhalten mithilfe eines Automatisierungsframeworks in menschenähnlicher Weise erzeugt und damit die Onlinedienste auf normales Verhalten trainiert [WGLI19]. Nach 20 Sitzungen auf den Onlinediensten wurden anschließend einzelne Merkmale der virtuellen Identitäten variiert und die Reaktionen der Dienste auf diese Veränderungen getestet. Basierend darauf konnte auf Gestaltung und Funktionsweisen der getesteten RBA-Varianten geschlossen werden und somit der Stand der Technik in Bezug auf RBA ermittelt werden.

Aufbauend auf den Ergebnissen wurde eine Between-Group Laborstudie konzipiert, in welcher die Usability- und Sicherheitswahrnehmungen von RBA untersucht wurden. Diese Wahrnehmungen wurden mit 2FA und rein passwortbasierter Authentifikation (Nur-Passwort) verglichen. Die Ergebnisse der im Einreichungsprozess befindlichen Studie zeigen unter Anderem mit signifikanten Ergebnissen, dass RBA gebrauchstauglicher als 2FA und sicherer als Nur-Passwort angesehen wird.

6 Zusammenfassung

RBA wird in Zukunft immer wichtiger für Webseitenbetreiber werden. Gründe dafür liegen, neben der NIST-Empfehlung, in erhöhten Sicherheitsrisiken durch neue Angriffsmethoden wie Credential Stuffing oder verbesserte Passwortratemethoden. Aus diesem Grund ist die Erforschung für ein ganzumfassendes Verständnis dieser Technologie von großer Bedeutung.

Die ersten Ergebnisse des Dissertationsvorhabens heben bereits die Notwendigkeit für RBA-Forschung hervor. So wurde im Rahmen der Grundlagenstudie eine für lange Zeit existente Sicherheitslücke im RBA-Verfahren von Facebook entdeckt, welche in einem Responsible-Disclosure-Prozess geschlossen wurde [WLID19a, WLID19b]. Auch die im Einreichungsprozess befindlichen Studienergebnisse zeigen Probleme von RBA auf, die die Usability dieser Technologie negativ beeinflussen könnten, sofern diese Probleme nicht entsprechend angegangen wurden.

Trotz allem zeigen die ersten Ergebnisse bereits, dass RBA stärkere Sicherheit bei erhöhter Usability bereitstellen kann. Inwiefern das auch unter Wahrung der Privatsphäre und DSGVO-konform passieren kann, wird der weitere Verlauf des Dissertationsvorhabens zeigen.

Amazon, Facebook, GOG.com, Google, iCloud, LinkedIn, Steam und Twitch

Danksagung Das Projekt URIA (Usability of Risk-based Implicit Authentication) wird durch das Graduiertenkolleg „Human Centered Systems Security“ (NERD.NRW) vom Land Nordrhein-Westfalen gefördert.

Literaturverzeichnis

[AA18] AlHogail, Areej; AlShahrani, Mona: Building Consumer Trust to Improve Internet of Things (IoT) Technology Adoption. In: Advances in Neuroergonomics and Cognitive Engineering, Jgg. 775. Springer International Publishing, Cham, Juni 2018.

[Ak19] Akamai: Credential Stuffing: Attacks and Economies. [state of the internet] / security, 5(Special Media Edition), April 2019.

[AuH11] Akhtar, Nadeem; ul Haq, Farid: Real time online banking fraud detection using location information. In: Computational Intelligence and Information Technology. Springer, 2011.

[AvO16] Alaca, Furkan; van Oorschot, P. C.: Device fingerprinting for augmenting web authentication: classification and analysis of methods. In: ACSAC ’16. ACM Press, 2016.

[CM12] Cser, Andras; Maler, Eve: The Forrester Wave: Risk-Based Authentication, Q1 2012. 2012.

[DHO17] Daud, Nor Izyani; Haron, Galoh Rashidah; Othman, Siti Suriyati Syd: Adaptive authentication: Implementing random canvas fingerprinting as user attributes factor. In: ISCAIE ’17. IEEE, 2017.

[DMR10] Dell’Amico, Matteo; Michiardi, Pietro; Roudier, Yves: Password strength: An empirical analysis. In: INFOCOM ’10. IEEE, 2010.

[DTH06] Dhamija, Rachna; Tygar, J. D.; Hearst, Marti: Why Phishing Works. In: CHI ’06. ACM, April 2006.

[FH07] Florencio, Dinei; Herley, Cormac: A Large-scale Study of Web Password Habits. In: WWW ’07. ACM, New York, NY, USA, Mai 2007.

[Fr16] Freeman, David; Jain, Sakshi; Dürmuth, Markus; Biggio, Battista; Giacinto, Giorgio: Who Are You? A Statistical Approach to Measuring User Authenticity. In: NDSS ’16. Internet Society, Februar 2016.

[GOB13] Golan, Lior; Orad, Amir; Bennett, Naftali: System and method for risk based authentication. Oktober 2013. US Patent 8,572,391.

[Gr17] Grassi, Paul A; Fenton, James L; Newton, Elaine M; Perlner, Ray A; Regenscheid, Andrew R; Burr, William E; Richer, Justin P; Lefkovitz, Naomi B; Danker, Jamie M; Choong, Yee-Yin; Greene, Kristen K; Theofanos, Mary F: Digital identity guidelines: authentication and lifecycle management. Bericht NIST SP 800-63b, National Institute of Standards and Technology, Gaithersburg, MD, Juni 2017.

[HH14] Hurkala, Adam; Hurkala, Jaroslaw: Architecture of Context-Risk-Aware Authentication System for Web Environments. In: ICIEIS ’14. September 2014.

[IS17] ISO/TC 159/SC 4: Ergonomics of human-system interaction. ISO 9241-420:2011, 2017.

[Kr15] Krol, Kat; Philippou, Eleni; De Cristofaro, Emiliano; Sasse, M. Angela: "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. USEC '15. Internet Society, Februar 2015.

[Mi18] Milka, Grzergor: Anatomy of Account Takeover. In: Enigma 2018. USENIX Association, Januar 2018.

[Mo12] Molloy, Ian; Dickens, Luke; Morisset, Charles; Cheng, Pau-Chen; Lobo, Jorge; Russo, Alessandra: Risk-based Security Decisions Under Uncertainty. In: CODASPY '12. ACM, Februar 2012.

[MT79] Morris, Robert; Thompson, Ken: Password security: A case history. Communications of the ACM, 22(11), November 1979.

[QHD18] Quermann, Nils; Harbach, Marian; Dürmuth, Markus: The State of User Authentication in the Wild. In: WAY '18. August 2018.

[Sh11] Shah, Nishit: Advanced sign-in security for your Google account. Official Google Blog, Februar 2011. https://googleblog.blogspot.de/2011/02/advanced-sign-in-security-for-your.html.

[So19] Solano, Jesus; Camacho, Luis; Correa, Alejandro; Deiro, Claudio; Vargas, Javier; Ochoa, Martín: Risk-Based Static Authentication in Web Applications with Behavioral Biometrics and Session Context Analytics. In: ACNS '19. Springer International Publishing, 2019.

[SPJ15] Spooren, Jan; Preuveneers, Davy; Joosen, Wouter: Mobile device fingerprinting considered harmful for risk-based authentication. In: EuroSec '15. ACM Press, 2015.

[St16] Steinegger, Roland H.; Deckers, Daniel; Giessler, Pascal; Abeck, Sebastian: Risk-based authenticator for web applications. In: EuroPlop '16. ACM Press, 2016.

[Tr12] Traore, Issa; Woungang, Isaac; Obaidat, Mohammad S.; Nakkabi, Youssef; Lai, Iris: Combining Mouse and Keystroke Dynamics Biometrics for Risk-Based Authentication in Web Environments. In: ICDH '12. IEEE, November 2012.

[Wa16] Wang, Ding; Zhang, Zijian; Wang, Ping; Yan, Jeff; Huang, Xinyi: Targeted Online Password Guessing: An Underestimated Threat. In: CCS '16. ACM, Oktober 2016.

[WGLI19] Wiefling, Stephan; Gruschka, Nils; Lo Iacono, Luigi: Even Turing Should Sometimes Not Be Able To Tell: Mimicking Humanoid Usage Behavior for Exploratory Studies of Online Services. In: NordSec '19. Springer Nature, November 2019. Open Access: https://nbn-resolving.org/urn:nbn:de:hbz:832-epub4-14221.

[WKB14] Wang, Xinran; Kohno, Tadayoshi; Blakley, Bob: Polymorphism as a Defense for Automated Attack of Websites. In: ACNS '14. Springer International Publishing, S. 513–530, 2014.

[WLID19a] Wiefling, Stephan; Lo Iacono, Luigi; Dürmuth, Markus: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: IFIP SEC '19. Springer International Publishing, Juni 2019. Open Access: https://nbn-resolving.org/urn:nbn:de:hbz:832-epub4-13694.

[WLID19b] Wiefling, Stephan; Lo Iacono, Luigi; Dürmuth, Markus: Risk-based Authentication website. 2019. https://riskbasedauthentication.org.