Multi-factor Authentication as a Service for Web Applications with User-based Risk Profiles

David Morais[1,3], André Zúquete[2[0000−0002−9745−4361]], and António Mendes[3]

[1] University of Aveiro, Aveiro, Portugal
{davidmorais35,andre.zuquete}@ua.pt
[2] DETI / IEETA / LASI, University of Aveiro, Aveiro, Portugal
[3] WIT SOFTWARE, Porto, Portugal
antonio.mendes@wit-software.com

Abstract. With the recent growth of Internet of Things (IoT), cloud platforms and the exponential increase in online exchanges encompassing sensitive information pertinent to users, it has become necessary to implement strong authentication methods to minimize the risk of user impersonation and, consequently, enhancing the protection of private information. In this paper, a solution is proposed which employs risk assessment aligned with a Multi-Factor Authentication (MFA) system, in a platform that can be easily integrated in applications in order to delegate the authentication process to an external platform. While pushing forward the concept of Adaptive Authentication as a Service, the main goal is to protect against user impersonation and illegitimate access to accounts, while keeping the intrinsic protection of MFA systems and rendering phishing attacks inconsequential with the aid or risk-based adaptability.

Keywords: Authentication as a Service · Multi-factor Authentication · Risk-based Adaptation.

1 Introduction

Authentication is increasingly becoming a concern of multiple solutions to prevent illegitimate access to accounts and grant access control to their users. In spite of this, security is being neglected by some and, as it happens, a vast majority of the solutions on the market still employ passwords as a standalone authentication method.

Without surprise, some developers realized this status quo, which lead to the growth spurt of Multi-Factor Authentication (MFA) [4]. Additionally, an increasingly popular authentication architecture has emerged, known as Risk-Based Authentication (RBA) [5] or Adaptive Authentication. It adapts the strength of the authentication scheme to the risk associated with a user, using historical and contextual information (such as IP addresses, login times or user agents).

In addition to provide a secure and flexible way to perform MFA, the goal was to protect end-users against social engineering attacks and known vulnerabilities, while maintaining the compatibility with multiple web applications.

2 Main Contributions

The solution culminates in an external, risk-based MFA system, where the adaptive authentication process can be delegated to the proposed platform via HTTP redirects, similarly to what the OAuth 2.0 [2] standard does for authorization. Despite this, the authentication system is not an Identity Provider (IdP) [3]. It was conceived for dealing centrally, but separately, with user authentications required by several web applications. We provide authentication as a service, just like IdPs, but we do not manage unique user identity profiles.

The proposed approach allows the creation of per-user risk models, that are dynamically trained whenever successful authentications are performed. Thus, helping to adjust and improve the model in real time, which consequently means that there is no need to pre-train them. The usefulness of the Density Based Spacial Clustering of Applications with Noise (DBSCAN) algorithm [1] in the context of risk assessment was also proven, computing the risk of a login attempt based on the significant resemblances it has with the user's past authentications. This is especially important, given the fact that it is an unsupervised clustering algorithm, which has significant advantages over the ones commonly used in this field.

All of this was achieved with extreme customization, allowing client applications to select which factors to employ and individually alter the weight of each context feature used in the risk assessment for their domain.

3 Experimental Results

To fully test the extend of the algorithm, some metrics were collected in terms of precision, recall and accuracy of the models. For that, a control set of 10 users was chosen manually from a data-set [6], being representative of the "normal" use-case. From the remaining users, four different categories were created, each with 10 users, and representative of extreme use-cases, in order to assert that the system is still viable in those contexts. Each model was trained with 80% of the genuine data, and the remainder of the data-set was used to make predictions in order to obtain metrics, which were then averaged for each category and compared with the control set results.

Additional, some tests regarding realistic authentications were performed, using a risk model with a week's worth of past authentications from the aforementioned data-set. Four authentication scenarios were used to evaluate the risk calculated individually by the machine-learning algorithm, the total risk computed by the risk engine, and the risk perceived by the end user.

Acknowledgements

This research was funded by National Funds through the FCT - Foundation for Science and Technology, in the context of the project UIDB/00127/2020.

References

1. Ester, M., Kriegel, H.P., Sander, J., Xu, X.: A density-based algorithm for discovering clusters in large spatial databases with noise. In: Proc. of the Second Int. Conf. on Knowledge Discovery and Data Mining. p. 226–231 (1996)
2. Hardt, D.: The OAuth 2.0 Authorization Framework. RFC 6749, IETF (Oct 2012), http://tools.ietf.org/rfc/rfc6749.txt
3. Maler, E., Reed, D.: The Venn of Identity: Options and Issues in Federated Identity Management. IEEE Security & Privacy **6**(2), 16–23 (2008). https://doi.org/10.1109/MSP.2008.50
4. Sinigaglia, F., Carbone, R., Costa, G., Zannone, N.: A survey on multi-factor authentication for online banking in the wild. Computers & Security **95** (2020). https://doi.org/10.1016/j.cose.2020.101745
5. Wiefling, S., Lo Iacono, L., Dürmuth, M.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: Dhillon, G., Karlsson, F., Hedström, K., Zúquete, A. (eds.) 34th IFIP TC 11 Int. Conf. (SEC 2019), IFIP Advances in Information and Communication Technology, vol. 562. Springer, Lisbon, Portugal (2019). https://doi.org/10.1007/978-3-030-22312-0_10
6. Wiefling, S., Jørgensen, P.R., Thunem, S., Lo Iacono, L.: Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. ACM Transactions on Privacy and Security **6**(1) (2022). https://doi.org/10.1145/3546069