Multi-Factor Authentication as a Service for Web applications with User-based Risk Profiles

David Morais
University of Aveiro,
WIT Software

André Zúquete
DETI / IEETA / LASI,
University of Aveiro

António Mendes
WIT Software

2023

Introduction

With the recent growth of Internet of Things, cloud platforms and the exponential increase in online exchanges encompassing sensitive information pertinent to users, it has become necessary to implement strong authentication methods. A solution is proposed which employs risk assessment aligned with a Multi-Factor Authentication (MFA) system, 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 impersonation and illegitimate access, while keeping the intrinsic protection of MFA systems and rendering phishing attacks inconsequential with the aid or risk-based adaptability.

Implemented Solution

Conceived for dealing centrally, but separately, with user authentications required by several web applications, we provide authentication as a service, just like Identity Providers, but we do not manage unique user identity profiles. As seen in Figure 1, the authentication can be delegated via HTTP redirects, similarly to what OAuth does for authorization.

The proposed approach creates per-user risk models, that are dynamically trained whenever successful authentications are performed. Thus, adjusting and improving models in real time, employing DBSCAN, with no need to pre-train them.

Experimental Results

Lets us assume that the same user, after establishing a risk profile, tries to login from different scenarios as shown in Table I. These show how different shifts in the authentication context impact the associated risk.

Overall the results are rather good, especially in the cases where significant changes in the context result in an exponential jump in risk scores. They were much better than prior attempts with other algorithms, such as SVM and One-class SVM.

To further test and validate the performance of the algorithm, some metrics were collected in terms of precision, recall and accuracy of the models.

Main Contributions

- **Authentication as a service** – delegating the adaptive authentication through redirects;
- **Dynamic per-user models** – usefulness of DBSCAN in unsupervised risk assessment;
- **Flexible & Configurable** – configurations and support for MFA and risk assessment.

Table I: Login scenarios with respective risk scores.

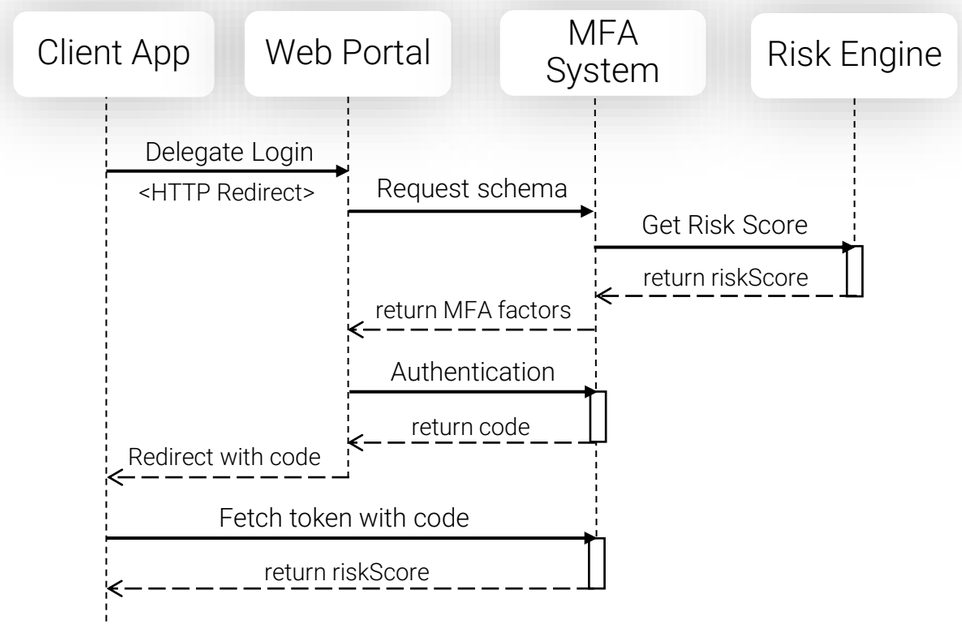
Scenario	I	II	III	IV
IP Address	10.3.55.70	10.3.55.70	10.3.55.87	92.221.109.162
ISP	AT&T	AT&T	Vodafone	Spectrum
Location*	Sandnes	Oslo	Sandnes	Artur Nogueira
Time zone	NO	NO	NO	BR
Browser*	Chrome	Firefox	Firefox	Firefox
OS*	Chromecast	Windows	Windows	Windows
Timestamp	19:44:56	19:51:54	09:46:20	03:15:29
Failed Attempts	0	0	3	3
DBSCAN Score	25.0%	34.1%	50.0%	100.0%
Risk Score	18.0%	24.0%	65.0%	100.0%

*Values simplified due to space constraints.

Conclusions

Adaptive authentication has proven to be an incredible aid on exacerbating the security of any authentication process, considering the context in which a login attempt is made. The authentication scheme can hence be dynamically altered in order to assure the needed security for a given risk score.

Figure 1: Authentication high-level flow.



universidade de aveiro
theoria poiesis praxis

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

INFORUM
SIMPÓSIO DE INFORMÁTICA

References

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)

Hardt, D.: The OAuth 2.0 Authorization Framework. RFC 6749, IETF (Oct 2012), http://tools.ietf.org/rfc/rfc6749.txt

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