Multi-Factor Authentication Simulator

Ben Barrow

2024

1 Chapter 1

1.1 Project Context

Authentication is the method by which a secure system, such as a computational device, application or database, can verify a user's access rights to its resources [1]. The first use of an authentication method like this stems from passwords used on time-shared computers, attributed to Fernando J. Corbató in 1961 [2]. Initially, devices were authenticated using Single Factor Authentication (or SFA) comprised of just one layer of input, typically passwords [3]. Authentication is generally considered to fall under one of three categories [4]:

- User Knowledge - Password, PIN, Security Questions
- User Ownership - Smart Card, Key Fob, Number Generator
- User Features - Fingerprints, Irises, Voice Detection, Other Bio-metrics

As methods of attacking these systems developed [5], the outdated nature and weakness of SFA [6] led to the development of Two-Factor Authentication, which supplemented the initial layer with an additional layer [7], such as utilizing mobile phones for additional security [8].

Finally, Multi-Factor Authentication was developed, namely 'A method of authenticating the identity of a user' which can include 'providing a plurality of factor-based data instances corresponding to a user' [9]. More simply, it is the evolution of Two-Factor Authentication, providing increased robustness in its sources [10] and therefore more adaptability in application [11]. The combination of these authentication techniques can be further sorted into three levels, or Authenticator Assurance Levels [12], based on the level of security that they provide. This security is generally framed in the level of certainty the system has of the user's claimed identity, with higher levels providing increased certainty.

1.2 Project Motivations

Since COVID-19, a larger effort to transfer services to the internet (source) has led to an increased number of older users on the internet (source), but

the availability of educational tools for these users has not kept pace with the developments in this field (source).

1.3 Project Aim and Objectives

This project will aim to develop an artefact that can be used to educate users on the different authentication methods that they can use. It will attempt to cater to an older audience, to cover the knowledge gap that has accumulated for this demographic. The resulting artefact should make the user aware of both the options they have when creating accounts and the level of security that their chosen configuration will provide. To accomplish this, the following objectives will be observed:

Obj.1. The artefact can authenticate a user by using a single factor or combination of multiple factors.

Obj.2. The artefact can support the use of a range of authentication options.

Obj.3. The artefact can allow for the configuration as how a user should be authenticated and under what conditions.

Obj.4. The artefact can give an indication of an authentication assurance level based on how a user is authenticated.

Obj.5. The artefact will be designed with an older generation of users in mind, focusing on usability and ease of use.

1.4 Project Methods

The project will start with (1) Multi-Factor Authentication Research, followed by (2) Artefact Design, (3) Artefact Development, (4) User Observation and Feedback and finally (5) Analysis of Feedback and Observation.

1.4.1 Multi-Factor Authentication Research

This research will largely comprise of identifying and collecting an appropriately sized list of common authentication frameworks. It will allow the artefact to be effective in its execution while maintaining a reasonable scope for work inside the deadline.

1.4.2 Artefact Design

The design component will involve creating wireframes for the final designs of the artefact, as well as completing essential design documents for the underlying hierarchy and code.

1.4.3 Artefact Development

The development component will comprise the completion of several tickets, with an assessment at the end of this period around how much of each success criterion was met. Testing can then occur as the final step in this stage, allowing for direct observation of the present and expected results.

1.4.4 User Observation and Feedback

User Observation and Feedback will be key in allowing for the identification of the successful completion of the 5th objective. Feedback will be collected from users both in and outside the key demographic to provide evidence for the usability of the resultant artefact.

1.4.5 Analysis of Feedback and Observation

This final step will involve comparing and contrasting the Project Objectives with the finished project, allowing for a fair assessment of the goals and objectives outlined earlier in the development.

References

[1] Stocksdale G, NSA glossary of terms used in security and intrusion detection in *SANS Institute Resources*, 1998 Apr

[2] R. M. Fano; F. J. Corbató, Time-Sharing on Computers in *Scientific American, Vol. 215, No. 3*, pp. 128-143, September 1966

[3] Bonneau, J.; Herley, C.; Van Oorschot, P.C.; Stajano, F, Passwords and the evolution of imperfect authentication in *Communications of the ACM* 58.7, pp. 78–87, 2015

[4] Velásquez, Ignacio, et al, Authentication Schemes and Methods: A Systematic Literature Review in *Information and Software Technology, vol. 94*, pp. 30–37, Feb. 2018

[5] Adeyinka Olalekan, Internet Attack Methods and Internet Security Technology in *2008 Second Asia International Conference on Modelling & Simulation (AMS)*, May 2008

[6] Sint, Khin; Sint Kyaw, Analysis on the Strength and Weakness of Current Authentication Systems to Overcome Their Limitations in *International Journal of Scientific Engineering and Technology Research*, pp. 463-468, 2019.

[7] Harini, Narasimhan;T. R. Padmanabhan, 2CAuth: A new two factor authentication scheme using QR-code in *International Journal of Engineering and Technology 5.2*, pp. 1087-1094, 2013

[8] Aloul; Fadi; Syed Zahidi; Wassim El-Hajj, Two-factor authentication using mobile phones in *2009 IEEE/ACS international conference on computer systems and applications*, pp. 641-644, 2009.

[9] Scheidt, E.M.; Domangue, E, Multiple Factor-Based User Identification and Authentication. *U.S. Patent 7,131,009*, 31 October 2006.

[10] Tellini, Niklas; Vargas, Fredrik, Two-Factor Authentication: Selecting and implementing a two-factor authentication method for a digital assessment platform, 2017

[11] Banyal, Rohitash Kumar, et al, Multi-Factor Authentication Framework for Cloud Computing in *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation*, 1 Sept. 2013

[12] Grassi, Paul A., et al, Draft nist special publication 800-63b digital identity guidelines in *National Institute of Standards and Technology (NIST) 27*, 2016