Three factor authentication

Conference Paper · December 2017

DOI: 10.23919/ICITST.2017.8356384

CITATIONS
11

READS
2,829

2 authors, including:

Aspen Olmsted
Simmons University
95 PUBLICATIONS **252** CITATIONS

SEE PROFILE

Three Factor Authentication

William Kennedy, Aspen Olmsted
Department of Computer Science
College of Charleston
Charleston, SC
wakenned@g.cofc.edu, olmsteda@cofc.edu

***Abstract*—Authentication, security, and confidentiality are some of the most important topics of cyber security. There have been many solutions presented to users for strengthening the security of login password-based authentication methods. Primarily this has been through the use of two-factor authentication methods. Two-factor authentication is the combination of single factor authentication mechanisms. The growing popularity and acceptance of two-factor methods are driven by the increasing need for privacy and security in this technological age. The success and popularity of adapted security measures are largely dependent on their ease of implementation and convenience to the user. The focus of this research is to address and analyze the implications of using a three-factor authentication model for added security in websites and mobile apps. This paper will present an app we created which could provide a potential method for three-factor authentication that could potentially ensure added authentication assurances without loss of convenience.**

Keywords- Authentication; Security; Three Factor Authentication; Mobile; Web; Access Control

I. INTRODUCTION

User authentication is the main building block for any secure cooperative computing system. Security concerns are on the rise in all areas of industry such as banks, healthcare institutions, industry, etc. Due to the proliferation of mobile devices and the heightened interaction between mobile applications and web services, the authentication of users is more frequent for mobile devices than for desktop users [1]. In many instances of multi-factor authentication, both a mobile device and a desktop are necessary and go hand in hand for adequate authentication. One of the drawbacks of multifactor authentication is that user ID's and passwords are abundant, with many users stating that they have more user IDs and passwords than they can remember [2]. This cost of convenience makes the proposed implementation of higher security measures and added authentication factors worrisome to many users and providers.

To better understand the factors in play with authentication, it is first necessary to understand what authentication is. Authentication and the various measures of authentication are used to verify that a specific user or process is who they say they are. It is that simple. There are four standard ways that users are authenticated:

- Something you know – This is the most basic form of authentication with which most users are familiar. This standard is usually presented as a username or password which is known only to the user.
- Something you have – This form of authentication is represented by the user having possession of a physical entity or device. This can be represented as a physical token such as the user's smartphone or other media device generating a temporary and sometimes single use authentication code.
- Something you are – This form of authentication is represented as a biometric signature such as a fingerprint, retina scan, or facial recognition. This is generally seen as one of the strongest forms of authentication when conducted properly [3].
- Someplace you are – This form of authentication corresponds to where a user or process is located, and in response gives or denies access to resources accordingly. This standard can be conducted through the use of a range of IP addresses or geographic location points [3].

For multifactor authentication to be conducted properly, one or multiple of these standards are coupled to heighten security standards. In this work, we will present an app we created which joins three of these standards in order to give a higher level of security and authorization to the user. The organization of this paper is as follows: Section II reviews the related work. Section III describes the motivation for this research. Section IV describes the implementation and results of the created app. Conclusively, Section V will provide a conclusion and discussion of future work.

II. RELATED WORKS

Li et al. [4] first introduced the concept of using biometrics as a factor in a three-factor authentication system in order to help the grim situation of network security. In this paper, they proposed using passwords, smart cards, and biometrics as a viable solution towards three-factor authentication. It was through this proposal and the analysis of the progression of modern technology and the in-depth look into the drawbacks of fewer security measures which prompted the use of facial recognition as part of the app to be developed for this project. The discussion of the speed/flow of biometrics, as opposed to other authentication factors, was very influential to the progression of this research. The presented scheme could resist many kinds of attacks and protect the hosts multimedia and web resources, which in response, made it very attractive as a potential starting off point.

In Native Autonomous Process Authentication, Olmsted analyzed the promise of multifactor authentication when it came to users while also analyzing the issues that arise when applications try to give credentials to autonomous software processes. Autonomous software processes when allowed credential privileges leave gaps for malicious incursions and attacks [3]. The importance of this paper was paramount as it proposed that in order to have a more secure system, autonomous background processes should not be allowed credentials which in hindsight they should not possess in the first place, as issues can arise.

In Two-Factor Authentication: Cybersecurity for Today's World, HCPro discusses the importance of security in the healthcare industry with "two-factor authentication being the backbone of even a basic cybersecurity program" [2]. The emphasis on weighing convenience and speed over security was part of the main discussion and analysis of this paper. The importance of this paper towards my continued research and app development centered on making the process as seamless as possible with having as few clicks as possible connected to multiple processes.

III. Motivation

The motivation of this paper is to investigate an orderly approach to the design of a secure three-factor authentication app with the protection of user privacy in the most time efficient and convenient way allowable. The hypothesis is that an app can be developed that performs three-factor authorization without being overly complicated or time-consuming. The app will use three-factor authentication to incorporate the increased advantages of an authentication based on a password, username, and facial recognition through possession of a mobile device [5].

IV. Implementation and Results

The design of the app took place in MIT App Inventor 2 beta. The app was designed to consist of two pages in this early stage and to work primarily on Android. The login page functions to take in a username and password. With this app being in the prototype phase the login credentials were hard coded. This means that the user would not be able to create their own account at this time; but would at a later date be able to, when the app can be fleshed out. The user would log in to this page with the username and password, and then the camera would queue up and take their picture, performing a facial recognition check.

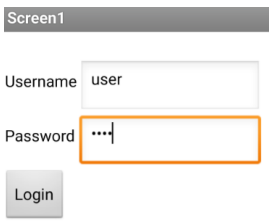

Figure1. Login Screen

The facial recognition functionality was provided through an extension called CamVision1 which works with MIT App Inventor 2. The next step was incorporating the Microsoft Cognitive Service, which allowed for the addition of a computer vision API which would be necessary for the facial recognition process. Once the facial recognition is completed, the app takes you to the second screen which presents a successful login message.

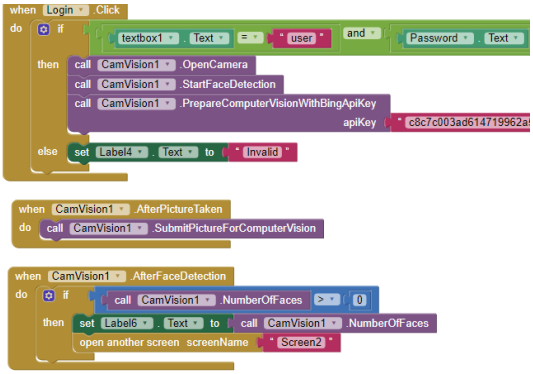

Figure2. MIT App Inventer 2 Blocks

The app performed as desired with user interaction consisting of the input of a username and password and then having their picture taken all at the expense of a single click of the mouse. The convenience and simplicity of this three-factor authentication app exceeded all expectations for ease of use. The cost of convenience is at its most minimum as presented through the apps one click sign in capabilities.

V. Conclusion and Future Work

The implementation of a future market standard of a three-factor authentication method seems all but assured with the use of biometrics and other authentication methods when used in an efficient way. With efficiency comes confidence and with confidence comes reliability. The increased reliability of a more secure platform with three-factor authentication is hard to ignore. With further research, the app can be developed to allow for users to create their own accounts, and for the account development of each user to save credentials and biometric reference tags.

References

[1] D. DeFigueiredo, "The Case for Mobile Two-Factor Authentication," *IEEE Security & Privacy, vol. 9, no. 5,* pp. 81-85, Sept-Oct 2011.

[2] HCPro, *Briefings on HIPAA*, vol. 17, no. 1, pp. 1-5, January 2017.

[3] J. N. M. K. J. L. X. Z. Xiong Li, "Rhobust three-factor remote usesr authentication scheme with key agreement for multimedia systems," *Security and Communication Networks,* 2016.

[4] Y. X. A. C. J. Z. R. D. Xinyi Huang, "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems," *IEEE,* vol. 22, no. 8, pp. 1390-1397, 2010.

[5] A. Olmsted, "Native Autonomous Process Authentication," in *Proceedings of World Congress on Internet Security 2016 (World-CIS 2016),* London, UK, 2016.