Strategies: An Inclusive Authentication Framework

Natã Barbosa
Syracuse University
School of Information Studies
nmbarbos@syr.edu

ABSTRACT

This paper briefly describes a proposed interaction workflow that is currently being developed as part of a research effort towards providing better solutions for accessible authentication, strongly guided by contextual inquiry and evidence-based guidelines. The approach described herein is being developed and tested to be foundations for tests and findings of the research, consequently evolving along the research progress towards providing a scalable, deployable, secure, usable for everyone, and last, but not least, privacy preserving platform for web authentication.

Categories and Subject Descriptors

D.4.6 [**Security and Protection**]: Security and Protection – *Access Controls, Authentication, and Verification*

General Terms

Human Factors, Authentication

Keywords

Authentication; Contextual Inquiry; Disability; Privacy

1. INTRODUCTION

The interaction workflow proposed in this framework is aiming to reduce the difficulties that people with disabilities currently face when authenticating to several web pages and web services. By focusing heavily on improving the user experience of web authentication, the hopes over the outcomes of the work under way are that of solving user experience problems while providing a secure and scalable mechanism that can be deployed by websites around the world, towards easing the process of authentication.

Specific goals of this project include, but are not limited to (1) design accessible authentication that is secure, fast and usable for everyone; (2) design new authentication mechanisms that are privacy-preserving (i.e., service providers do not know what disability condition a user has); and (3) evaluate these new mechanisms with users with disabilities in longitudinal field trials.

The framework is being designed from the beginning to be extensible, meaning that it will allow for new strategies to be implemented for catering certain types of disabilities. The main characteristics of said interaction workflow are: (1) the gap between the user disability and the task of authentication is filled/eased with a suitable mechanism of communication between the browser (most likely a JavaScript Application Programming Interface) and the user, such suitable mechanism is to be compatible with the user's disability (perhaps machine learning can be implemented in order to guess the first-time suitable mechanism); (2) once the initial Device-API pairing is successfully completed, the user is no longer required to type passwords. Instead, they make use of a broader range of authentication possibilities that are available through mobile devices (e.g. accelerometer, microphone, camera, gyroscope, GPS) to prove identity to the phone. The user is then able to communicate seamlessly with the mechanism once the suitable mechanism has been successfully identified (3) the web application server knows nothing about this process, the process is triggered by a script included into a webpage; (4) suitable mechanism of communication between human and computer must be able to address user's disability; (5) user authentication to the mobile device should make use of one or combined biometrics and/or other factors (e.g. location) from mobile device resources (e.g. voice, face, gesture, gait).

ASSETS '14, Oct 20-22 2014, Rochester, NY, USA

ACM 978-1-4503-2720-6/14/10.

http://dx.doi.org/10.1145/2661334.2661413

2. INTERACTION WORKFLOW

2.1 First-Time Authentication

The following steps describe the process of having a user authenticate the first time using the proposed workflow. (1) the JavaScript API requests user approval to have a device (e.g. smartphone) start the authentication process. A unique token is sent to the user using a suitable mechanism that the user can understand (suitable mechanism can be guessed by machine learning/usage profile at the first time?); (2) user passes on the token to user's phone (or phone can detect the user token through a suitable mechanism); (3) phone asks for user credentials; (4) user enters credentials on the phone; (5) user submits form with credentials; (6) credentials are stored locally on the phone (local storage) for subsequent authentication; (7) form fields are filled based on credentials entered on the phone. The suitable mechanisms not defined in the interaction workflow should (1) be able to communicate with the user; and (2) allow for user input that can prove for identity. The suitable mechanism should take user's disability into account.

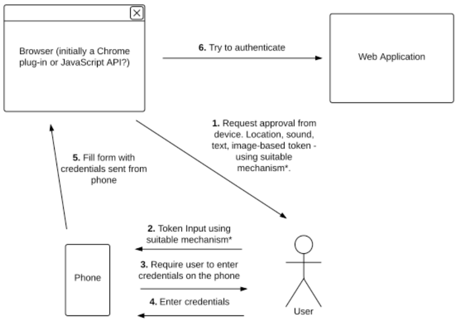
Browser (initially a Chrome plug-in or JavaScript API?)
6. Try to authenticate
Web Application
1. Request approval from device. Location, sound, text, image-based token - using suitable mechanism*.
5. Fill form with credentials sent from phone
2. Token Input using suitable mechanism*
3. Require user to enter credentials on the phone
4. Enter credentials
Phone
User

Figure 1. First Time Authentication

2.2 Subsequent Authentication

After previously having sent credentials through the aforementioned workflow, the process for authentication is almost the same, except for the fact that the user is no longer required to enter credentials on the phone if the credentials are the same as the ones used at first time authentication (i.e. the password has not changed), according to the workflow in Figure 2.

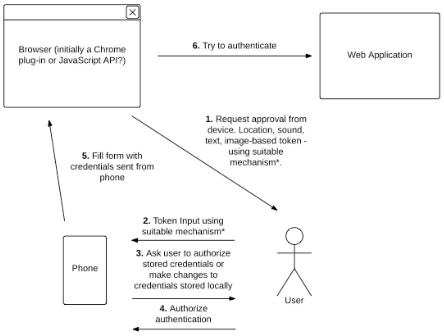
Browser (initially a Chrome plug-in or JavaScript API?)
6. Try to authenticate
Web Application
1. Request approval from device. Location, sound, text, image-based token - using suitable mechanism*.
5. Fill form with credentials sent from phone
2. Token Input using suitable mechanism*
3. Ask user to authorize stored credentials or make changes to credentials stored locally
4. Authorize authentication
Phone
User

Figure 2. Subsequent Authentication

3. USER SCENARIO AND STRATEGIES

A user with low vision accesses the Facebook login page. A script on the page tells the user that they can use their phone to authenticate. This message/token is sent through a visual message that is readable by the screen reader or by playing a sound. The user picks up his smartphone and enters the token or makes the phone listen to the token. The smartphone lets the user know that the token is valid and shows the form to enter credentials on smartphone's screen. The user types credentials and authenticates to his Facebook profile. The next day, the user goes through the same one-time token validation process, except that they no longer need to enter their credentials as they are now stored on the phone. The phone asks the user if they want to use stored credentials or enter new credentials (in case a password has been changed). The user authorizes stored credentials to be sent or enters new credentials and authenticates to his Facebook profile. It is also important to remember that the token is not used for authentication purposes, but it is used for establishing communication. Once a token is used (i.e. communication is established), that token can no longer be used for starting the process of authentication. The user scenario described above implements some of the potential strategies that can be plugged into the framework, but it is important to highlight that the main advantage of this framework is that it can accommodate different strategies for addressing different disabilities. In the scenario above, the user with low vision could simply scan the token through QR code on the screen, or make the phone listen to the one-time token generated by the web page through the phone's microphone. In order for the user to authenticate to the phone in any subsequent authentication, they could simply shake their phone in a certain way, allowing for the smartphone to authenticate the user based on phone's motion or even speak a passphrase that would allow their phone to send their credentials over the network, instead of having to type passwords. Smartphones provide a broad range of interaction that can be used to prove for one's identity, and the purpose of using smartphone is to allow for developers to implement different strategies that can be used given the hardware available (e.g. GPS, gyroscope, accelerometer, camera, microphone).

4. EARLY IMPLEMENTATION

At the time of this writing, the framework is implemented under a minimum systems architecture scheme that will allow the interaction workflow to be tested. The framework will support authentication using both smartphones and phones that are not smartphones, here called "Dumbphones". The architecture proposed in this document is being developed to be foundations of the framework that is subject of this paper and is further described in Figure 3.

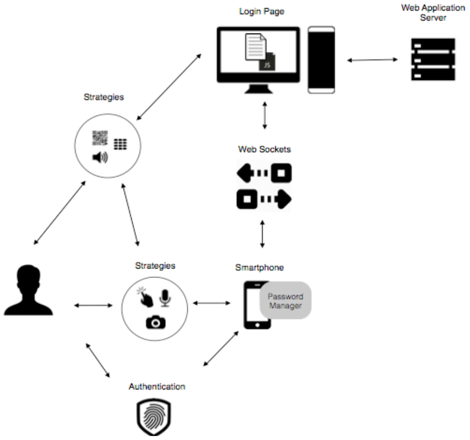

Figure 3. Framework Architecture – Using Smartphones

For "Dumbphones" the process is slightly different because resources on the phone are limited (i.e. no internet, no local storage). However, the same strategies approach can be used to establish communication with the web sockets server (e.g. SMS server to get and send token to web sockets server).

5. ONGOING WORK

The current status of the architecture uses the user's smartphone as a password manager. The implementation is being developed to accommodate different strategies of communication with the user. For example, in the current implementation, it is possible to inform the token to the user through text, sound, and QR code. The underlying infrastructure will allow for different strategies of communication to be easily integrated, as different disabilities will require different approaches. The framework is already foundations for executing early user testing so that assumptions can be validated and uncertainties eliminated. In the future, insights might also allow for implementation such that no credentials will be required (i.e. new ways to prove one's identity can be used on the web). Early user interviews have provided insights to support "dumbphones". This is only the beginning of tapping into the potential of an approach that can accommodate several communication and user interaction needs through the use of different strategies.

6. ACKNOWLEDGMENTS

I thank the guidance of my faculty advisor Dr. Yang Wang as well as the discussion with and feedback from Bryan Dosono, Jordan Hayes, Tarun Rajput, Huichuan Xia, Dr. Kevin Du, and Dr. Joon Park. I am also grateful to the support from the School of Information Studies at Syracuse University. This paper is based upon work developed under a Sub-recipient Agreement that is sponsored by the US Department of Education, Award Number H33A130057. Any opinions, findings, conclusions or recommendations expressed herein are those of the author(s) and do not necessarily reflect the views of the United States Department of Education or Carnegie Mellon University