BEHAVIOR CHARACTERISTICS OF MOBILE WEB APPLICATIONS AUTHENTICATED USERS

Alin Zamfiroiu [1*]
Carmen Rotună [2]

ABSTRACT

The Internet facilitates nowadays interaction and collaboration between persons located at very long distances from each other. It also facilitates interactions between software systems located at great distances. The key concept is the identification of the subject involved in the interaction. It is necessary to validate whether the person performing certain activities on a software system is the person entitled and not an unauthorized one.
In this paper we propose a study of the actual context in user authentication domain, in various online applications.
Therefore, the purpose of this document is to provide stakeholders (software developers) the characteristics on users conduct within online mobile applications. Based on these features, specific profiles can be created for each user. By using the completed profiles, we can achieve recognition models based on user behavior.

KEYWORDS: *characteristics, behavior, users, online applications, mobile applications*

1. INTRODUCTION

According to [1], mobile devices are increasingly used and popular. More and more software developers began to create applications dedicated to these devices. Thus, most online applications have an online mobile version.

Traditional authentication model, where authentication is password based, creates major inconveniences for mobile devices, where devices limitations and consumers behaviour require an integrated, convenient and also secure solution.

Password-based authentication represents, very often, a solution vulnerable to attacks. By adding a second factor as part of the authentication process, increased security is achieved.

Thus, this paper proposes the implicit authentication, while using observations on user behavior within the application.

[1*] corresponding author, Senior Researcher, The National Institute for Research & Development in Informatics Bucharest, university assistant, Department of Economic Informatics and Cybernetics, Bucharest University of Economic Studies, Romania, zamfiroiu@ici.ro
[2] Scientific Researcher, The National Institute for Research & Development in Informatics Bucharest, Romania, carmen.rotuna@rotld.ro

Considering the above mentioned reasons, the implicit authentication is particularly suitable for mobile devices and laptops. But this authentication method may be implemented for any type of device.

The device usage pattern varies from one person to another. This type of information can be useful to create a more detailed profile for each user.

Implicit Authentication:

- acts as a second factor and supplements password authentication;
- acts as a primary authentication method, replacing password authentication entirely;
- provides additional security for financial transactions such as purchases by credit card, acting as a barrier against fraud.

The method for determining the score from previous authentications is based on the identification and analysis of user behavior characteristics.

In the proposed model, when behavior analysis determines a level below a certain threshold, the user is required to authenticate explicitly by entering a passcode.

The threshold that will require explicit authentication may vary for different applications, depending on the intended security level.

There are solutions to reduce the authentication concerns (Single Sign-On - SSO), but these identify the device, not the rightful user.

Therefore, SSO does not defend well against theft or exchanging devices, where the devices are shared voluntarily.

According to studies on authentication process perception for mobile devices, it appears that a transparent authentication experience is recommended, which enhances security. Users were receptive to biometric authentication and behavioral indicators.

Implicit authentication forms are for example location-based access control, biometric methods, dynamic typing model and keyboard shortcuts.

Recently, the accelerometers of some devices have been used for user identification and profiling.

Implicit authentication uses a variety of data sources for authentication decisions. For example, modern mobile devices offer rich data collections on user behavior, such as:

- location and co-location;
- accelerometer measurements;
- WiFi, Bluetooth or USB connections;
- biometric style measurements, such as entering text and voice data;
- contextual data such as calendar entries content.

Also, auxiliary, user information could be another source of data for implicit authentication.

The mobile device itself can take the authentication decisions to determine if a password is required to unlock the device or a given application. In this case, data can be stored locally, which is beneficial for privacy. It is also possible to use local authentication to access remote services, for example, using the SIM card, the user can sign and send an authentication decision to the service provider. It must be considered, however, that although this approach protects user privacy, it does not protect against devices theft. If the device is stolen, an attacker can obtain the information stored in memory and find information about the user.

All approaches, even those where data is held locally have the potential for confidentiality breaches.

Modeling user profile should contain all his behavior patterns, for example, how frequently he makes phone calls to numbers from phonebook or the order of placing calls to certain phone numbers.

In general, the user model may also take into account combinations of indicators.

User behavior usually depends on the time of the day and the day of the week. People are generally at work in the same location on working days, but their location varies during weekends.

According to [2] standard password-based authentication is vulnerable immediately after login, as there is no mechanism to verify continuously the user's identity. This can be a serious problem, especially for sensitive platforms, offering facilities to their users based on username and password only. Therefore, a method that allows user continuous authentication is extremely helpful.

An alternative to password-based authentication method is biometric data based method.

Biometric identification methods address users identification by using their physical characteristics (eg. the face, fingerprint, iris) or behavioral traits (ie. dynamic keyboard shortcuts, mouse dynamics, etc.).

2. ONLINE PLATFORMS AUTHENTICATION METHODS

The most common authentication types available for online applications, differ in the level of security provided by combining the factors involved in the process. The security level of an application varies depending on the category of the authentication factors:

- **User and password-based authentication** - the most common example of authentication is based on a single factor password authentication. The security of the password depends on the diligence of the person who sets up an account: the system administrator or user. Best practices include creating a strong password and ensuring that no one can access it. One of the main issues about setting a password is that most users either do not understand how to create strong memorable passwords, or underestimate the need for security. Additional policies, that increase complexity, lead to high volumes of requests for passwords related issues in the enterprise environment. This problem can result in the use of simplistic rules for creating passwords, and as a result, reduced length and complexity passwords tend to be used most frequently. These passwords can be cracked within a few minutes, making them almost as ineffective as if no password is used or if a password is written on a paper and discovered by a malicious person. Therefore, safety measures are needed to prevent these situations, such as creating less predictable passwords. Password testing predicts the ease with which it could be broken by: guessing it, "brute force" attacks, "dictionary" attacks or other common methods.

Given the increasing speed in machine processing, "brute force" attacks pose a real threat to passwords. Using, for example, general purpose parallel graphic processing (GPGPU) hackers can produce more than 500 million passwords per second, even using low-performing hardware. Depending on the particular software, "rainbow tables" are useful to reverse the cryptographic algorithms and can be used to crack 14 characters alphanumeric passwords in about 160 seconds. This is done by comparing the password database with a table of all possible encryption keys.

Social engineering methods are also a major threat to password-based authentication systems. To reduce the likelihood of such an attack, an organization must involve everyone and spread awareness, from management to their employees, given the fact that the complexity of the password has no importance, if an attacker tricks a user to divulge it. Even IT personnel, if not properly trained, can be exploited through invalid passwords related requests. All employees must be aware of phishing tactics, in which fake e-mails and websites can be used to acquire sensitive information from one recipient. Other threats, such as Trojans, can be received also in e-mail messages. As a conclusion, password authentication is one of the easiest methods to hack.

Password-based security may be appropriate to protect systems that do not require a high level of security, but even in these cases, constraints should be applied to protect them. For any system that needs increased security, stronger authentication methods should be used.

Strong authentication is sometimes considered synonymous with multifactor authentication. However, single factor authentication is not necessarily week in all cases. Many biometric authentication methods, for example, are strong when implemented properly.

- **Biometric Authentication** - biometric verification is considered a sub-group of biometric authentication. Biometric technologies involved, rely on how individuals can be uniquely identified by one or more biological distinctive features, such as fingerprints, hand geometry, the structure of the retina or iris, voice, dynamic keyboard usage, DNA or signatures.

  Biometric authentication is based on the use of a proof of identity as part in a process of authorizing a user to access a system. Biometric security technologies are used for a wide range of electronic communications, including enterprise security, trade and online banking.

  Biometric authentication systems compare biometric data from user with the authentic, verified data, stored by the system. If they are identical, the authentication is confirmed and the access is granted. This process is sometimes a part of a multifactor authentication system. For example, a smartphone user might connect with his personal identification code, and then provide a retina scan to complete the authentication process.

Nowadays there are several methods for collecting and reading biometric data to ensure strong authentication. Any of the biometric identification methods has certain characteristics that make it suitable for use in an authentication process. Some are fast, others can be used without the subject's knowledge and others are very difficult to forge.

Biometric authentication methods examples:

a. digital signature;
b. fingerprint;
c. facial recognition;
d. retina scan;
e. iris scan;
f. hand geometry;
g. voice analysis.

- **Two-factor Authentication (2FA)**

"Two-factor" Authentication (also known as 2FA) is a type of multi-factor authentication based on unambiguous identification of users by combining two different components. These components can be something the user knows, something the user has, or something that is inseparable from the user. Two-factor authentication requires two types of credentials before an user can connect to an account or system, confirming that the entity that wants to access the account is indeed the rightful user.

Figure 1. Two-factor Authentication [4]

Using this system to validate a person's identity, is based on the assumption that it is unlikely for an unauthorized entity to provide the two factors required for access. If, in an attempt to log in, at least one component is missing or incorrectly provided, the user's identity is not established with certainty and therefore the access request is rejected.

2FA security system reinforces the fact that the rightful user must provide two items for identification from different categories. Typically, proof of identity is composed of two items: something memorable a security code or password and a physical evidence, such as an identity card. The second factor authentication increases security because even if an intruder steals a password, it should also access the physical device to enter the user's account.

Examples of factors involved in two-factor authentication are:

a. a password sent as text;
b. a PIN number;
c. Captcha usage.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of challenge-response test, which consists of reading and reproduction of text, used to determine whether or not the user is human. This user identification procedure has a shortcoming for those whose daily work is slowed down by the distorted words, which are difficult to read. A person on average takes about 10 seconds to solve a typical CAPTCHA.

Tokens are used to validate user's identity (as in the case of a client attempting to access the bank account). A token is similar to an electronic key accessing a system. It is used in addition to or instead of a password, to prove that the person is who claims to be. Some devices can also store other information, such as a digital signature, or biometric data like, for example, fingerprints:

1. Digital Certificate;
2. Smart card;
3. USB Device;
4. One Time Password.

Two-factor authentication by implementing HOTP or TOTP:

1. **HOTP** (HMAC - One Time Password algorithm) described in RFC4226 standard, is based on two fundamental things: a shared secret and a moving factor (counter). This algorithm is based on events, which means that every time a password is generated, the moving factor will be increased based on the events, so subsequently generated passwords should be different every time;

2. **TOTP** (Time-based One-Time Password Algorithm - RFC6238) is an algorithm that calculates a unique password from a shared secret key and current time using a cryptographic hash function to generate a one-time password.

- **Multi-factor Authentication**

Multi-factor authentication (MFA) is a method of access control where a user is granted access only after providing, several separate items from the following categories, in an authentication process: something a user knows (knowledge factor), something a user has (factor possession) and something the user is (factor inherence).

In multi-factor authentication use case, several factors are used to enhance the security of transactions compared to two-factor authentication.

Figure 2. Multi-factor Authentication

- **Three-factor authentication (3FA)**

  Adds another security factor and prevents counterfeiting authentication. Typically, a biometric feature measurement is added. Such a system checks, for example if the person intending to login knows the password, possesses the identity card and if fingerprint match the stored records.

- **Four-factor authentication (4FA)**

  4FA authentication increases security through the use of four unique factors for authentication. It turns the intent to compromise an account into an impossible mission, since a hacker should be using a portable device to break a password, while connected to a USB token cloned, and to match the rightful account owner retina scan and fingerprint.

- **Five-factor authentication (5FA)**

  A five factors based authentication system is based on the three factors frequently used (knowledge, possession and inherence), plus location and time. In such a system, a user must reproduce something he knows or remembers, prove that it possesses an item with authentication capabilities, provide a biometric sample, his location must be correct, and all this in a timeframe accepted and verified in order to gain access to the system.

3. MOBILE WEB APPLICATIONS

Web applications for mobile devices are software applications developed to run in browsers for mobile devices, with restrictions concerning hardware resources and software resources.

Mobile devices provide users the benefits of connecting to the internet anywhere and anytime.

The specific characteristics of web applications for mobile devices are designed in accordance to mobile devices limitations:

- the size of the display screen - a usual web application is developed for a classical computer, which has a larger monitor size; for mobile devices, web applications must be adjusted to the display size of the device used;
- resolution is very important for images and text displaying; text within the web application must be readable also from mobile devices;
- connecting to the Internet - when mobile devices are connected to the Internet via wireless, the user is likely to move out of network range, so internet connection is lost, therefore, web applications must coordinate this action and not require a permanent connection.

Following an empirical analysis, a list of recommendations for designing mobile web applications was developed, presented in Table 1:

Table 1. Recommendations for mobile devices web applications

Hierarchy	The division of displayed information, so that it may be rearranged according device's screen size
	Highlighting the important content
	The user must not press more than 2-3 times to get the desired information
Links	Assign shortcut keys for each link on a page
	If a link used within the web application is not usable on a mobile device, the user should know about this situation
	Ability to automatically dial a phone number that is written in the web application content
Navigation	Minimizing scrolling process through web pages of mobile applications
	Positioning the most used sections at the top of the page to be readily accessible for mobile users
	Include navigation buttons at the top of each page
	Include navigation buttons at the bottom of each page
Footnote information	Include a link to the desktop version of web application
	Include a link to the feedback page
Page titles, navigation links, and URL	Page title and links must not exceed 15 characters
	Use only alphanumeric characters
Page content	Highlighting the important content
	The most important topics are positioned at the top of the web application's main page
Page arrangement	Do not use frames or tables
	Do not use absolute sizes
Forms	Use the dropdown lists, radio buttons and checkboxes to minimize user interaction with the application
	Use default values, where possible
Images and colors	Use reduced dimension pictures
	For spacing do not use graphics or animation.
	An image should not exceed 80% of the device screen width
Screen size	Two sites with different sizes for mobile and desktop devices are recommended

All mobile devices browsers share the following characteristics:

- Bookmarks to save important user pages;
- Save page option, used to save web application pages in device memory so the user can access these pages even when the device cannot connect to the Internet;
- History, saving the last web page browsed on that drive;
- web page full screen mode so that web page content can be displayed on a larger area of the mobile device;
- increase or decrease content font size, for users who want larger text content or want to view more content in a single page;
- return button to previous page of the web application;
- based on the web applications characteristics and user interaction mode, can be determined the interaction characteristics which will help create user profiles.

4. ANALYSIS OF USERS BEHAVIOR CHARACTERISTICS

In web applications for mobile devices case, we can take into account specific characteristics of traditional web applications, but also other mobile-specific features such as:

- text typing speed; the speed is significantly different on mobile devices compared to typing on a computer keyboard and varies from one user to another;
- the area covered when typing; each user has a push pattern on the mobile device, depending on the size of the user's fingers; this feature depends also on the user's physical appearance;
- the amount of time a key is pressed; alike the case of a computer keyboard, it should be measured how much time a specific button is pressed on the virtual keyboard;
- how the keyboard display is closed when no longer necessary; the user can achieve this through touch action, just outside the keyboard area or by using the device’s botton for leaving the current activity, in this case the virtual keyboard;
- touch screen area to run (scroll) a page, or a text; similar to the area where a user holds the cursor, mobile device screen is divided into several sectors, saving the sector used to run the page content within the app, Figure 3 and Figure 4.

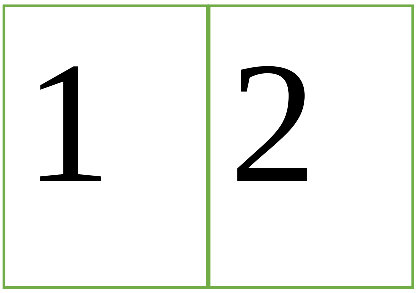

Figure 3. Dividing the screen into two sectors to run the page

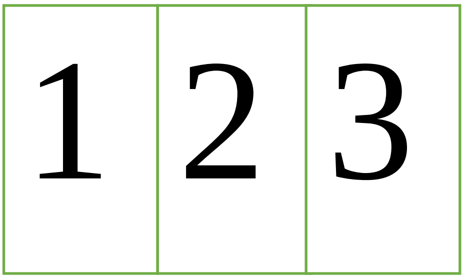

Figure 4. Dividing the screen into three sectors to run the page

- zooming required to read text; each user prefers a certain degree of text magnification, so that it reads comfortable the text displayed in the application;
- editing mode; the user can use a single finger, two fingers from different hands, or use multiple fingers to write text using the virtual keyboard; this characteristic applies only to users who use devices with virtual keyboard; for other devices with physical keyboard it may not apply;
- how the user holds the mobile device when reading (landscape or portrait);
- how the user holds the mobile device when writing (landscape or portrait).

These characteristics must be measured for all online application users and, based on these measurements, achieve a profile for each user.

For each property in the set, a series of measurements will be conducted after the user is authenticated and a working session is created. The results are then saved in a database as presented in table II.

Table 2. Measurements realized for a t number of sessions

Session	TS	CK	ZRT	RM	WM
S_1^u	TS_1^u	CK_1^u	ZRT_1^u	RM_1^u	WM_1^u
S_2^u	TS_2^u	CK_2^u	ZRT_2^u	RM_2^u	WM_2^u
…	…	…	…	…	…
S_i^u	TS_i^u	CK_i^u	ZRT_i^u	RM_i^u	WM_i^u
…	…	…	…	…	…
S_t^u	TS_t^u	CK_t^u	ZRT_t^u	RM_t^u	WM_t^u

Where:

S_1^u – is the session 1 for the user U<
TS – text typing speed;
CK – how the keyboard display is closed;
ZRT – zooming required to read text;
RM – how the user holds the mobile device when reading;
WM – how the user holds the mobile device when writing.

5. CONCLUSIONS

In this study an analysis of the current state of authentication domain within online applications was conducted.

A research was conducted on how users interact within web applications for mobile devices. Further, were determined characteristics of user interaction in online applications. In the end of the study it was performed an analysis on the user behavior characteristics.

These characteristics are measurable, and optional to be included in user behavior analysis module.

In a future research, models concerning the user profile based on the identified characteristics will be developed. The models will vary depending on the metering model and the capabilities of the web platforms developed using different programming languages.

ACKNOWLEDGMENT

This work was been carried out as part of the Nucleu project: PN 16 09 01 02 – Cercetări privind autentificarea online în cadrul aplicațiilor software bazată pe comportamentul utilizatorilor (Research on online authentication in software applications based on users behavior).

REFERENCES

[1] E. Shi, Y. Niu, M. Jakobsson, R. Chow, Implicit Authetication through Learning User Behavior, Information Security. Springer Berlin Heidelberg, 2011. 99-113.

[2] J. Roth, On Continuous User Authentication via Typing Behavior, IEEE Transactions On Image Processing, July 28, 2014.

[3] V. R. Yampolskiy, Action-based user authentication, Int. J. Electronic Security and Digital Forensics, Vol. 1, No. 3, 2008.

[4] FTC seeks public comments on facial recognition, 2012, https://crisisboom.com/2012/01/10/ftc-seeks-public-comments-on-facial-recognition/

[5] Fingerprint sensors, facial recognition and biometric surveillance to propel biometrics market, http://www.donseed.com/4278-2/

[6] IBTimes, 2015, UN: Biometric iris scanners transforming Syrian refugee programme by preventing fraud, http://www.ibtimes.co.uk/un-biometric-iris-scanners-transforming-syrian-refugee-programme-by-preventing-fraud-1527362

[7] 5 Things You Should Know About the FBI’s Massive New Biometric Database, 2012, https://crisisboom.com/2012/01/11/fbi-biometric-database/

[8] NIST Authentication Guideline. 2016, https://pages.nist.gov/800-63-3/sp800-63-3.html#sec4

[9] Strong Authentication Best Practices, https://safenet.gemalto.com/multi-factor-authentication/strong-authentication-best-practices/

[10] Biometric authentication: what method works best?, http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16

[11] Understanding Digital Certificates, https://technet.microsoft.com/en-us/library/bb123848(v=exchg.65).aspx

[12] Retina scan, http://whatis.techtarget.com/definition/retina-scan