ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 1, 84-92 (2019)

www.astesj.com

Special Issue on Recent Advances in Engineering Systems

ASTESJ

ISSN: 2415-6698

Web Authentication: no Password; Listen and Touch

Viorel Lupu[*]

Research & Development, Online Services SRL, Buzău, 120191, Romania

ARTICLE INFO

Article history:
Received: 15 December, 2018
Accepted: 22 January, 2019
Online : 26 January, 2019

Keywords:
Web
Security
Authentication
Multi-Factor
Image-Password
Voice notification
Mobile phone
Password
Disabilities
Smart-Headphones

ABSTRACT

Just as electricity has an essential role in our lives, the internet network and especially web services have become of vital importance nowadays. Without security service layers, apparently small things like checking a child's school schedule on web may turn the daily routine into a nightmare. Web services users are still required to use many combinations of usernames and passwords. Despite technologically advances that bring many benefits to those owning top of range smartphones, complex combinations of identifiers and passwords are still required for basic security. Top tier smart mobile phones also add device-specific vulnerabilities to the risk of misuse or may expose sensitive data like biometrics. To meet users' expectations, authentication systems must be safe, fast, efficient, intuitive and easy to use, especially on mobile phones. User satisfaction, reduced fraudulent authentication issues, increased security, reduced management costs, regulatory compliance are main goals for the new advanced web technologies systems. This paper presents some real-time multi-factor authentication methods that uses voice calls to communicate random passwords to registered users. The ultimate goal is to relieve web service users from the stress of memorizing complex combinations, or copying text strings for user identifiers and passwords from paper or external memory devices like mobile phones. The new features are presented for a web service after migration from the traditional authentication system to the one with the proposed new method. This work is an extension of the paper entitled "Securing Web Accounts by Graphical Password and Voice Notification" published in 2018 IEEE International Conference on Engineering, Technology and Innovation (ICEITMC).

1. Introduction

Any authentication service must be designed, built and operated on a basis of user centric vison [1]. These design standards, associated with data protection requirements [2, 3] may imply costs, time, technologies and human resources that are beyond reach for many small companies which provide simple and useful web sites like school timetables. Users must obey the site's rules and the method of authentication. They must use given usernames and long, maybe complex or random passwords. There are several options, such as saving the login data in the browser or writing them elsewhere. If the web service is provided by an authority such as a bank or a governmental agency, the importance of a proper user access goes higher as risks of identity frauds are also high [3]. Every website that is part of our digital life, which requires and maintains personal data is equally important; without adequate security measures, any of these websites can be a weak bastion after which we might become cyber-victims.

In terms of security, when talking about Internet web services, appropriate means of authentication must be provided so that only authorized users have access to them. At the same time, Internet web services have to be easily accessible. New vulnerabilities or changes of standard requirements may occur during operations affecting the security environment completely.

Web authentication is a process that relies most on human-computer interaction. The authentication system directly influences the quality of Internet web services, in terms of usability. There is a tradeoff between the complexity of the authentication system and the service usability [4, 5].

Internet web services based on the usage of sensitive data, require high quality security systems, often a combination of SSL protocol enabled connections and multi-factor authentication systems. Low-cost single-factor authentication systems based on text strings must be reconsidered. They are no longer feasible neither for user identity nor for passwords. The RFC 2196

[*]Viorel Lupu, +40744545600, viorel.lupu@onlineservices.ro

https://dx.doi.org/10.25046/aj040109

recommendations have posed new restrictions on the user, as more vulnerabilities have been revealed [4, 5, 6 and 7].

On the other hand, it is difficult for the human user to remember long or complex identifiers and passwords, not to mention in stressful environments or in physically challenged contexts, in which such authentication methods are proved to be inappropriate. As a result, human user often resorts to storing identifiers and passwords in browsers memories or in easily accessible, visible files. They tend to use predictable graphic passwords and, sometimes, the same identifiers and passwords are in use for multiple websites [4, 6].

Also, we would argue that text-based authentication systems are not suitable for smartphones. Often smartphone users find it difficult to remember, read and type text during the authentication process, such as for example a simple 'copy-paste' action of a unique text passcode received by SMS, an operation which may prove to be a challenging task on a mobile phone.

Multifactor authentication is considered the best practice for authentication [4] today. Users have to provide more and more information to the authentication system in order to authenticate successfully. Authentication standards like Universal Authentication Framework (UAF) or Universal Second Factor Authentication (U2F) proposed by Fast Identity Online Alliance (FIDO) are based on latest knowledge about public key cryptography [4, 5], biometrics, mobile devices, server technologies, best practices in the field etc. in order to provide an open and public accessible framework [8].

Internet services authentication systems have to assure that secure protocols run properly: digital certificates need to be valid [5], software updates need to be at the latest version etc. System time is also very important. Web servers keep time in different ways and more or less accurate. Synchronizing the web server local time with an external time server over the Internet it is a standard practice nowadays. If the time source is manipulated or not updated, everything may go astray mostly because digital certificates, the basis for secure web communications, contain time references. Cloudflare deploys a new authenticated time service called *Roughtime*, in an effort to secure certain timekeeping services. The publicly available service is based on an open-source project of the same name that was started by Google [9, 10].

Authentication failures result in inestimable damage and there are plenty of examples: Sony Pictures Entertainment corporation (announced on December the 3rd 2014), Yahoo (on December the 15th 2016, where 3 billion accounts were compromised in a series of incidents), Equifax (on September the 7th 2017, where 148 million data sets with personal data were stolen, including social security number, with a recovery cost of $400 million dollars) or for Marriott International (announced on November the 30th 2018, where about 500 million guests, including full names, date of birth, passport information, payments, preferences etc.). [11]. It is estimated that a third of U.S. businesses have had a customer information breached in 2017, including the information needed to authenticate their customers [12]. All these events might create a spiral of more and more security incidents that would make use of this data.

Authentication failure has new dimensions such as social engineering, mobile phone thefts and most important, revealed by recent trends, SIM-Swap or cloning the GSM Subscriber Identity Module (SIM) card. Cybercriminals look for future victims using social media websites. On such websites, it seems easy to find personal details of the victim (e.g. the date of birth, the e-mail address, the mobile phone number, etc.). Finally, it is not so hard to convince the GSM operator to make an emergency transfer of the GSM number to a new SIM (in the criminal hands). Then the authentication system works as expected. But not in favor of real users [13, 14], as the real user just discovers that his/her mobile phone is dead. From a technical point of view these fraudulent actions seem beyond the scope of the authentication process.

The security system should not rely entirely on the security components of the operating system. Recent security vulnerabilities (the case of Meltdown and Spectre) leak data as encryption keys, passwords [15], security identifiers, images etc., data that should be protected by the operating system. Instead, it is disclosed without user consent. The process of solving those vulnerabilities is a long one, as it will have to deal with hardware architecture redesign [15].

Nowadays, security is a serious concern for the entire society, being the result of technology, people and policies working together. In this sense, the new GDPR have been imposed in the EU since May the 25th 2018 [2]. In Europe, "companies must alert government authorities within 72 hours of a known breach and may be fined up to 4 percent of their global revenue under data protection laws" [17].

This study proposes a different solution for real-time, multi-factor authentication: image selection [17, 18 and 19] guided by voice via phone call notifications [20, 21]. This paper presents a detailed analysis, results, related works and comments on the implementation decisions, as well as on user reactions. Our aim is to improve the authentication process with better user experience and comfort. Also, we intend to extend its usability in high stress conditions (public hospitals, police and justice departments, public administration) and for the elderly or people with disabilities.

2. Background

Forms are commonly and efficiently filed with the use of secure web forms, be it small or medium size enterprises (SMEs), corporations or government entities. In the situation analyzed in this paper, the web forms in use run on a national authority's centralized web services application due to the need for real-time sensitive medical records such as those used in the field of human organ transplants. The operators reporting the data, taking into account the strict medical specialization and the legal implications, are medics accredited for the respective field. Each medical unit enrolled in the national transplant system has at least one accredited medic on staff. During the analyzed period, there were over 60 accredited medics in the program. Reports were filed on a daily basis, but also following certain unforeseen events.

The secure web forms are filled in using computer terminals placed in the operative staff common rooms of the respective hospitals, as terminals used for patient registration. Terminal access is permitted to all the medical staff in the hospital. Thus, the transplant database system is potentially at risk of exposure to unauthorized personnel. The credentials were disseminated to high school level medical personnel, which were operating data. Many times, the Internet address, user name and password were written on post-it note stuck on the terminal' screens, further allowing access for curious individuals to presumably protected data. Even though such post-it's were not used in all locations, there were notebooks or unprotected files containing these credentials.

The described situation does not represent an exception; it is often met in other environments, where the legal implications may be less serious. There were also security conscious operators who used their private computer terminals or mobile devices for these reports. In the effort to limit the data exposure, several technologies and methodologies were evaluated, being clear that the use of text strings as passwords is difficult to use on mobile devices [4, 5 and 22].

An attractive and convenient alternative is the use of personal mobile devices in comparison to investing in new equipment. Nowadays, the personal mobile telephone is ubiquitous, being a smart device, permanently connected to the internet and provided with an array of sensors used for increased security. High resolution video cameras, near field communication (NFC) readers, fingerprint readers, geo-location (GPS) receivers are already embeded in current smart phones, open the opportunity to use multi-factor security solutions. Starting with 2009, the smart phone market absorbed more than 173 million units, out of which almost 2 million have an embedded NFC reader (www.statista.com). NFC terminals have the ability to read NFC chips embedded in many types of supports such as implants, ID cards, labels and rings.

The NFC technology embedded into mobile devices, based on the Near Field Communication Data Exchange Format (NDEF) allows the automatic reading of a secure web site address and users identifiers. According to the NDEF specification, a URI record for the secure website using https://domain/aplication/UserId format [20] allows the user to open automatically the web application by approaching the NFC support to the smart mobile device. Thus, increasing security, user comfort, though the potential problems could be even greater in case these NFC supports are lost or stolen.

We have also analyzed the possibility of sending one-time, unique random passwords to authorized users, based on preregistered personal mobile phone numbers. The option of sending the password through Short Message System (SMS) is almost intuitive. Banks use this system for two-factor authentication for several decades. In 2005 it was demonstrated that the use of this system can be compromised since the SMS as a communication technology is quite vulnerable [19, 22]. This vulnerability is inherited from the telephony signaling system, also called SS7, developed in 1975 and in use ever since. Due to this, the SMS is no longer a recommended communication channel in authentication systems.

Cybercriminals rapidly penetrate weak security policies on mobile devices using a combination between social engineering, Internet available advanced software technologies and the use of sniffers for text strings sent on clear text communication channels. Their target is to clone SIM card in order to take over the victim's mobile telephone number, build a replica of the security environment on a malicious device for later use in hijacking all victim's Internet accounts where the phone number is registered for multifactor authentication (e.g. bank account). Methods that were unimaginable several years ago are now available to anyone who wants to dabble with them [13, 14].

Images or sounds can be an alternative to text passwords. Image-based authentication seems to be promising especially due to the fact that the human mind retains images and image associated actions better in comparison to written text strings [4, 6, 7, 17 and 23]. The replacement of the text password with a graphic one does not increase the level of security of the authentication method, being equivalent to the use of a four-digit PIN number [23].

The Interactive Voice Response (IVR) systems have been around in call centers since the 1970s and are presently used to transmit voice codes. For example, Microsoft runs an international system for software license activation using a similar IVR technology that receives and transmits the activation codes to be typed by the user.

The system analyzed in this paper implemented the use of a graphic password, which is communicated through the telephone network.

3. A new method for web authentication

The suggested authentication method aims to increase system security and user satisfaction. Taking into consideration that users easily recall images [4, 6 and 18] and image-related actions, the proposed authentication system displays images and processes user actions (as screen touch or clicks). The images are selected to be meaningful to the users. With voice guidance through a telephone call, the users have to choose between them. Processing the user's actions, the authentication system assembles an indicator and compares it with the random one-time password constructed into voice indications.

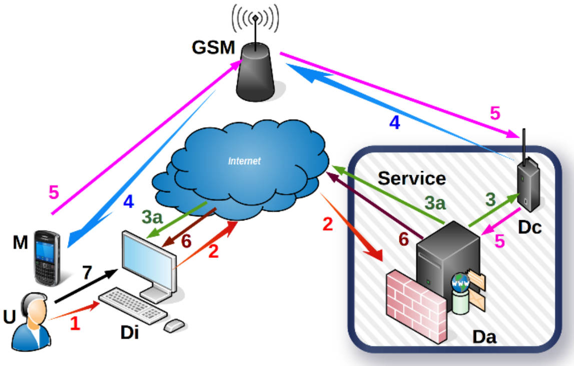


Figure 1: Web authentication system

The proposed authentication method (Figure 1) has two main phases. The first phase consists of the user's identification and starts the authentication session. The second randomly generates the password, initiates a phone call and authenticates the user. If the authentication system receives a known user identity, then the second phase is automatically started.

The first phase is of a special importance, derived from the fact that there are a lot of devices capable of initiating secure web sessions, from simple, classic personal computers to the latest mobile smart-devices with biometrics. The classic old-style computer browser provides options to save website address and user identifiers. Specially crafted computers like laptops may be equipped with additional specialized hardware to read fingerprints, NFC cards or to process images and sounds. With latest smartphones, user identifiers may be stored and better protected e.g. by fingertips and encrypted file systems. The authentication system has to detect from the authentication request who is the potential user and from what device the authentication request is made. If that device is already registered and all secure attributes are up to date, then the authentication procedure goes forward.

The authentication process is carried out following several steps [21] as illustrates in Figure 1:

1. A secure web session (2) is established with the server system after the user's (U) action (1) upon the Internet terminal (Di). The user's action (1) is carried out either by typing the URI (Da), or by using the device's video camera visual to recognize a QR code, or entering proximity of the terminal with an NFC ID card issued by the organization running the web service, if the respective terminal has an embedded NFC reader.

2. When the SSL session is opened (2), it provides a number of details about the Internet terminal (Di) that initiated the session and about the particular user (U). If those details are read off the NFC card's chip or the browser's memory, then the system automatically continues to the next step. As such, the user has to provide an identifier related to a user recognized by the web system (Da) and a password to confirm the authentication request. The request confirmation password can be in the form of a text string, graphic image set or an audible sound, depending on the particular security policy.

3. If the secure web session is initiated with the user's identifier and a known confirmation password, the web service generates a unique one-time random password and directs (3) the telephone call initiation device (Dc) to establish a connection with the user's (U) telephone number (4) on record. Simultaneously with the telephone connection, the web system (Da) will securely update (3a) the display on the requesting terminal (Di).

4. The communication device (Dc) initiates the telephone call using the public telecom network (4) (i.e. GSM). The web service (Da) monitors the status of the telephone call (5) using the communication device (Dc). The system waits for the call to be answered before starting dictation. The telecom network can also transmit other events regarding the status of the call such as if the line is busy or the mobile phone is outside the coverage area etc. Once the user answers, the communication device (Dc) will play the voice indications appropriate for the respective unique password.

5. The user (U) answers the call or not. Events detected by the communication device (Dc) in the public telecom network are sent in real-time (5) to the web system (Da). The web system will close the web session if the telephone call fails for any reason (i.e. line is busy).

6. The web system (Da) securely communicates the status of the call with the user's terminal. Thus, when the user answers the call (5), the terminal receives and displays the set of images (6). Figure 2 is an example of a set of images displayed on the user's terminal.

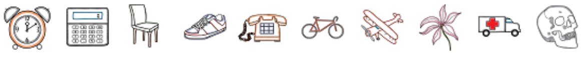


Figure 2: Example of a set of images for one-time-password

5. Following the indications received in the call (5), the user selects (7) the relevant ones amongst the other images (Fig. 2) displayed on the internet terminal, thus communicating the unique password to the web servers. The system validates the password and authenticates the user if during the call the latter has selected the appropriate images in the instructed order. Afterwards, the authenticated user may continue the web session. Any deviation from these restrictions leads to the closing of the web session by the web service.

The aforementioned web authentication method has the following advantages:

The password used to start the whole process (step 1) does not directly authenticate the user. It is merely a password confirming the user's intent to authenticate into the system. If unauthorized individuals use the respective password, the process cannot be continued since they do not possess the authorized user's mobile phone terminal. The initiation of every web session generates a telephone call and in consequence, the real user receives unsolicited calls, knowing that his account is being abused. The real user can take steps and change the confirmation password. In case of malicious authentication requests, the system eliminates abuse before an imposter can access the system.

Using NFC ID cards, rings or implants, the user is relieved of the need to memorize identifiers or confirmation passwords, which can be constructed of very long strings that are practically impossible to memorize, leading to increased system security.

In the absence of NFC support on protected access devices (i.e. mobile telephone terminals with biometric sensors), the identification strings may be stored in the browser's memory or in password manager type applications. The terminal's web browser (Di) may also save the Internet address and credentials of the secure website. The website address may be displayed in the form of an icon on the display of the Internet terminal, as to ease the user's task to memorize such details. The secure web session once initiated using the icon can also provide the user's identifier and confirmation password.

If public access web terminals are used, the confirmation password can be image-based thus avoiding the possibility that the respective terminals may memorize the confirmation password in the browser or password manager applications. Still, this type of password may be visually exposed to people in close proximity or to video surveillance systems.

The images used by the user to build the password based on the telephone call instructions are displayed on the internet terminal in the step 6, only if the user answers the call. This workflow reduces the exposure of the images to unauthorized users, increasing the security of the web service.

The telephone calls can be processed by the operating system (OS) of the smartphone. Thus, we can apply policies based on time periods or in correlation to other data such as geo-fencing (GPS position), GSM network name, Wi-Fi network SSID etc. as to semi-automatically reject unwanted calls.

The communication device (Dc) can produce the sounds necessary for voice calls through synthesis (text to speech) or by combining pre-recorded sounds. The pre-recorded sounds can be the result of professional recordings. Moreover, by mixing voice with background noise, the resulting sounds can be recognized by the users as authentic web service instructions.

This authentication method is terminal OS (operating system) and web browser independent (e.g. Linux, Windows, Android, IOS with Chrome, Firefox, Edge, Opera etc.). Suggested authentication method does not rely entirely on the operating system security components. It is crucial that the Secure Socket Layer (SSL) based on digital certificates etc. to be fully functional.

The implemented and studied system is being improved continuously. The public access terminals available to all operative hospital staff have been fitted with specialized USB connected NFC readers. With these readers and NFC ID cards, the authorized medical staff have quicker access to secured web forms used to report sensitive data, at the same time being less exposed to different security risks such as phishing attacks. As a result, the system became safer, more comfortable and much more productive.

4. Findings

The proposed web authentication service has been implemented [20] and runs continuously since December 2016 to serve the central transplant agency and authorized hospitals across one European Union member state. Beginning with September 2017 the usage of the new authentication system has become mandatory. Every authorized hospital is represented by an accredited specialist who daily reports medical events and data to the national authority, 24/7.

Web service usage data were collected continuously in log files. Data collected for this analysis is based on the regular system usage by 60 authorized operators in the timeframe between September 2017 and April 2018. In this time span, the number of operators increased. The analysis in this paper is based on all the web traffic for 20.000 successful authenticated sessions.

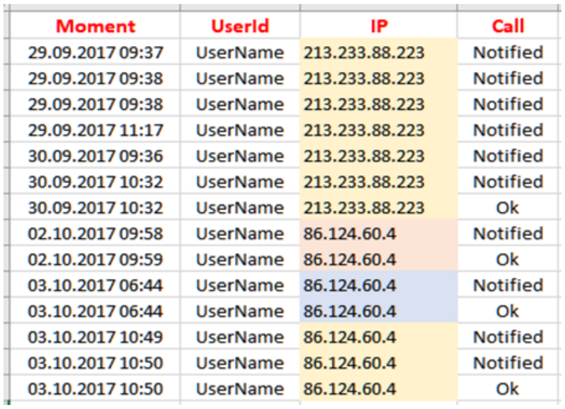
The proposed authentication method was implemented on short notice and without staff training, taking into account that it was virtually impossible to stop activities in hospitals only for this specific training. Thus, each operator has discovered the new authentication method when a new medical event or new data had to be reported to the central entity or when, in some cases, a lot of unsolicited phone calls from the web service (a phone-call for every authentication request) have been received. These unsolicited phone calls forced the specialist to change his/her password which as a consequence of the new authentication method become a confirmation password. Many specialists have learned to use private web sessions and not to store the user name and password in Internet browsers when using computers available to all the department staff. Subsequently, they received NFC ID cards and NFC readers. The Internet web service was re-engineered for a special non-public sign-in web page which started the secure web session and the authentication process by automatically reading the NFC link. This administrative procedure reduces web traffic in general, but did not affect the selected sessions for this analysis, because the use of the NFC ID card automatically generated a secure web session for a known user identifier (if it is still valid) to start the phone call process.

For this analysis all web site logs were saved and processed. The web server logs any web request, writing in the logs the client's IP address, protocol and the time moment when the web request was made, as well as the files that were requested on the server, the details of the browser, etc. [28]. Telephone communication logs contains telephone numbers, call events and timestamps. In this analysis all this data is correlated from web site logs, telephone communication logs and data from the web site database to filter user authentication requests and necessary details about the authentication process.

Web server logs contain a large number of unauthorized sessions because of the web services' public exposure. The current analysis does not take into account all unauthorized sessions. For any user, the authentication process model starts with the first GET (a method from the HTTP protocol [29]) web request for the web sign-in page retrieved from the web server log. These GET web requests are filtered for those requests that send valid user identifiers, accepted confirmation passwords and are continued with phone calls.

Then data is filtered and consolidated by web sessions having a unique client set of IP address, user identifier, session timeframe and phone call. In this stage, the user identity and telephone number are associated from the central database. Telephone calls log complete the analyzed authentication process model with call events. All sessions with an unsuccessful phone call are discarded i.e. sessions when the phone calls ended with busy signals, rejected calls, dial error, busy network or not answered at all, including phone calls with out of network coverage signals or if the user hanged-up before the end of the voice message. Then, searching the web server logs for session authentication failure or success events all necessary information is collected and processed. Now the entire authentication process is modelled. Resulted authentication process models are then ordered by user and timestamps. Figure 3 illustrates sample data processed by this model for one user (where real user identifier was obfuscated with *UserName* for security reasons).

As illustrated in figure 3, the user's authentication activity pattern reveals the fact that this particular user has tried to authenticate many times without success, especially because he/she was too slow to select the indicated images within the required amount of time. The first three lines of data reveal the fact that he/she has tried to authenticate three times on the 29th of September 2017 starting from 9:37 AM with no authentication success. Then, there is a new failed try after nearly two hours, same day at 11:17 AM. The next day, on the 30th of September the user has tried to authenticate two times from 9:36 AM and succeed the authentication one hour later, at 10:32 AM. On the 2nd of October, two days later, the user was able to succeed from the first try, at 9:58 AM. The IP address reveals that, starting with the 2nd of October, the web sessions are initiated from another network device.



Moment	UserId	IP	Call
29.09.2017 09:37	UserName	213.233.88.223	Notified
29.09.2017 09:38	UserName	213.233.88.223	Notified
29.09.2017 09:38	UserName	213.233.88.223	Notified
29.09.2017 11:17	UserName	213.233.88.223	Notified
30.09.2017 09:36	UserName	213.233.88.223	Notified
30.09.2017 10:32	UserName	213.233.88.223	Notified
30.09.2017 10:32	UserName	213.233.88.223	Ok
02.10.2017 09:58	UserName	86.124.60.4	Notified
02.10.2017 09:59	UserName	86.124.60.4	Ok
03.10.2017 06:44	UserName	86.124.60.4	Notified
03.10.2017 06:44	UserName	86.124.60.4	Ok
03.10.2017 10:49	UserName	86.124.60.4	Notified
03.10.2017 10:50	UserName	86.124.60.4	Notified
03.10.2017 10:50	UserName	86.124.60.4	Ok

Figure 3: Authentication process modeled from log files

Calculating the averages for all the users, the average number of failed authentications attempts is 250% higher as compared to the authenticated ones, in the first month of use. In the following months, similar to the phenomenon described in Figure 3, the average values decrease. The value is 70% in the second month of use. Notice the decrease in the following months: 45% in the third month, 10% in the fourth month and 4% in the fifth month. These average values form the graph in Figure 4, confirm the fact that in time the users learn the new authentication mechanism and become productive.

The graph in Figure 4 also contains failed authentication attempts launched from public access terminals. The data analysis shows on one hand that the public access system was exposed to unauthorized use and, on the other hand, that part of the medical staff who knew the system and accessed it without respecting the legal procedures, have finally understood that that it was no longer possible to do so. These authentication attempts have been reduced considerably by implementing the new method.

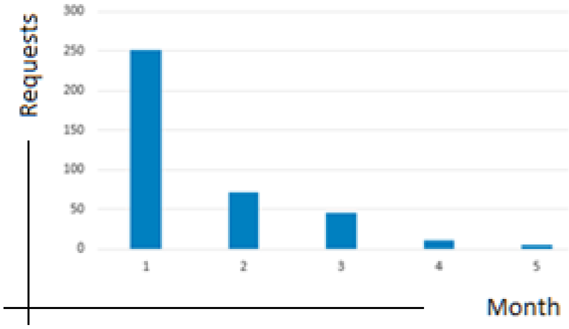


Figure 4: Learning cycle (5 months)

From analyzing the use of data, it has been revealed that users need an average of 30 seconds to authenticate, the difference being calculated between the authentication request timestamp and the start of the secure web session. The 30 second interval is composed of the time needed to place the telephone call (10 seconds) and 20 seconds needed for the user to answer the call and to select the images indicated verbally during the call. Those 30 seconds are the price paid for an increased security system and this time frame is comparable, as well as less time consuming than multifactorial authentication by other means (by text message, where the user must wait to receive the message, to open the application and must memorize the received code in order to later type it into the web interface).

While running the new system we also found that users are creative in finding new solutions to circumvent strict rules. As such, they requested that their personal telephone number to be changed in the database to the one publicly accessible in the department or have temporarily redirected their calls to other telephone numbers, of work colleagues usually. These practices are barely legal. However, we found fewer examples of such behavior as compared to the previously mentioned cases with post-it notes placed on the terminal's display in the operative medical staff room, that facilitated access to anyone who would breach the system. In order to counteract these use cases, we needed better organization frameworks, better user training and the use of advanced technologies that, for example, can detect automatic call forwarding.

One of the measures we applied, was to expedite the implementation of equipment necessary for the use of NFC technologies, such as the implementation of specialized NFC readers and user NFC ID cards. Thus, the users no longer knew the authentication web page URI, the unique user identifier nor the confirmation password. In order to initiate the session, they just needed to have the NFC ID in close proximity to the reader. The NFC ID cards improve the user comfort, they contribute to the increased system security, but, at the same time, they increase the implementation costs. The NFC ID cards were readily accepted by the medical staff, which later realized how easy they are to use.

Still, call redirection, unsecured mobile telephone theft, SIM card cloning are still major vulnerabilities for the system, especially if the voice notification subsystem uses an internationally recognized language and the images are directly indicated.

5. Related work

Since the user mentally establishes the connection between sounds and images, indirect indication is possible. For example, images can display animals while sounds describe their favorite food. In the set of animal icons, the rabbit will be chosen when the word "carrot" is heard.

The use of mother tongues can improve system security. A flower is indicated by vocalizing the expression "smells good". It is difficult for an unauthorized, non-native speaker to choose the flower icon when hearing *lukter godt* or *miroase bine* while this comes natural for a native speaker.

Indirect indications require special attention when it comes to expressing emotions. It might be harder for an unauthorized person to guess the correct images, when those images are selected in relevance to the experiences and according to the expected emotions of the actual user. Voice indications may sound cryptic because the meaning behind any symbol needs previous user initiation to understand and act in the required timeframe. An example of this kind of set of images are illustrated in figure 5.

These methods may have a difficulty level so high that unauthorized users are unable to guess correct image passwords even if they control both the authentication workstation and the user's phone. This method of authentication emphasizes the fact that the user's prior knowledge is an important element to be considered in multifactor authentication processes.

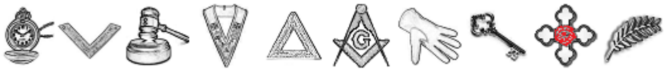


Figure 5: Example of a set of images

Security may also be enhanced within the proposed method of authentication using some traps as a result of some simple changes to the set of the displayed images or to the voice indications. This kind of changes require targeted training to user groups. This way, users will be instructed not to select any image following the first voice indication. The first voice indication in the call is a trap for users that do not know this detail. Another simple change is to use trap images. Trained users can easily avoid them even if they are urged to select them. In the image set from Figure 5, a trap image may be the icon of the key. A user with no training might touch that icon, following the voice indication and the authentication would fail.

Language that is familiar to the user (i.e. the local dialect) as well as false verbal instructions and/or trap images can provide insurmountable obstacles for unauthorized users. These methods have the advantage of being categorized as "what the user knows" [4, 5] and are not equipment-dependent (since they are compatible with fixed-line, analogue telephony) and with some necessary adjustments they can be used as an authentication method for users with severe deficiencies (such as visually impaired persons).

The web service interface must be carefully designed and implemented to hide the correlation between a trap and a failed authentication. Repeated tries must not help the unauthorized user to discover the reason why the authentication fails.

No technique is infallible and, in the domain area of security, authentication, or content protection, continuous efforts must be made to be at least one step ahead of cybercriminals. The suggested authentication method was developed on the basis that the users, the most important entity of the system, make mistakes. In order to reduce the effects of human mistakes and to help users in their overall effort to maintain the data safe, a simple security device has been added to the system. Figure 6 presents the updated authentication system; the added security device is labeled CA in the form of audio headphones.

The enhanced voice notification flow (figure 6) contains a smart-headphone (CA) as compared to the original flow (figure 1). These smart-headphones must be capable to function as regular headphones connected to the mobile phone and smart enough to detect special encoded data sub-channel in the audio stream. When such a stream is detected, the smart headphones automatically converts encoded data into comprehensible sounds according to the user's language. In other words, the headset hides a security component that users need to have in order to succeed in the authentication process.

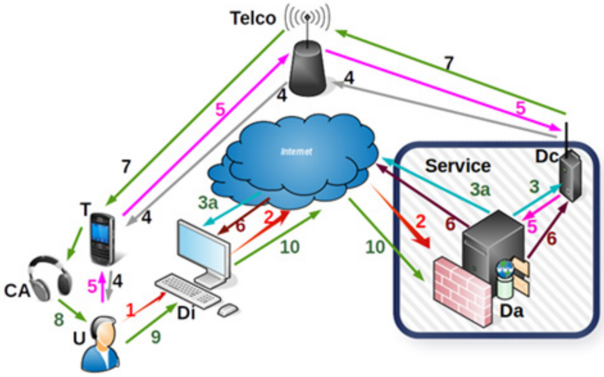


Figure 6: Enhanced web authentication system

In the enhanced authentication method, the telephone voice call contains an encrypted audio stream sub-channel, unintelligible to humans. This way the enhanced authentication method is more robust if the phone call is redirected, the mobile phone is lost, cloned etc. keeping the one-time random passwords voice indications just for certified users. One must have the smart-headphones connected to be able to listen the voice indications.

These especially designed smart headphones may be subject to the addition of more security features like biometrics or other security features that restrict smart headphone use outside of the particular scope (e.g. the user must touch the headphones to allow decryption of the audio stream, a gesture unknown to a malicious person who manages to have both the smartphone and the smart headphones, since the shape of the smart headphones and their functionality seem normal/common).

Following these ideas, a prototype of these smart headphones was made. The voice notification system has been parameterized to transmit data using well-known dual tone multi-frequency signaling (DTMF) analogue telephony technology. DTMF streams are transmitted over phone calls, simultaneously and in the same frequency band as the voice channel. DTMF audio streams are easily decoded as bit streams using low power CMOS chips (e.g. MT8870). Bit streams are transmitted to a connected low power microsystem built as a System on a Chip (SOC). SOC processes all data streams and finally produces voice indications into the headphone speakers.

The proposed enhanced authentication process flow (Fig. 6, Fig. 7) is started by the user (1) in interaction with a browser. The browser sends the user identifier, the user confirmation password and the details about the device that initiates browser request (e.g. NFC device identifier) to the server, over an SSL Internet connection. The server prepares a random one-time-password (OTP) and engages (3) the modem to call the known user and, at the same time, instructs (3a) the browser to display relevant information.

The modem tries to call the known user's phone number (4). If user's phone is busy or if there is a telephone network congestion or if the user answers or rejects the call (5) then the server either closes the web session or continues it by sending to the modem (6) a code derived from the OTP and to the browser a web page to display the set of images (6a).

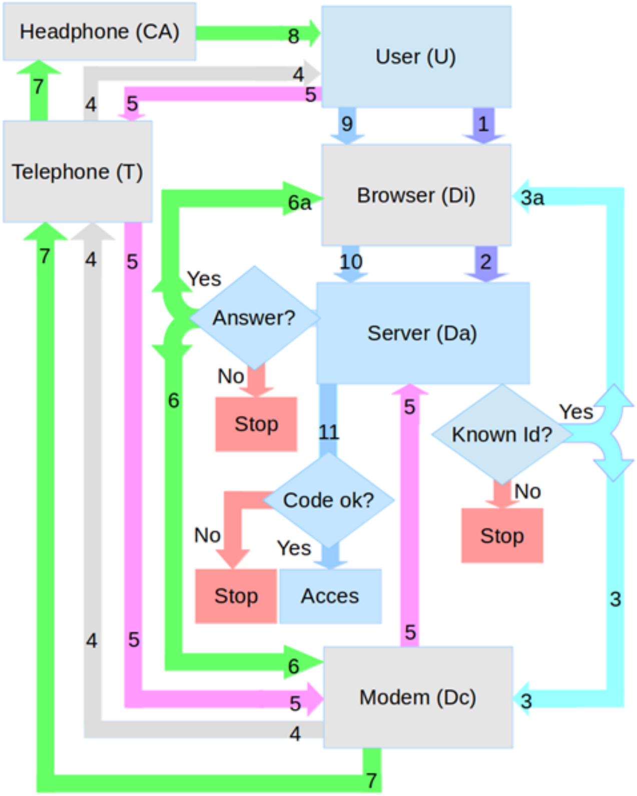


Figure 7: Enhanced authentication process flowchart

The modem starts the audio playback and mixes the DTMF encoded indications in the audio stream (7). The DTMF encoded string is detected, decoded and played back (8) by the smart headphones. The user acts (9) on displayed images based on his knowledge and according to the voice indications received through the smart headphones. The browser sends the user actions (10) (click or touch events) back to the server, in real-time. The server analyses the user web session continuously and verifies if all the required conditions are met (11) in order to authenticate the current user successfully.

Although the presented architecture (Fig. 6) contains a hidden security element in an audio headset, with virtualization technologies everything may become software based in a carefully architected mobile system. User comfort increases with virtualized devices, but the system management layer will have to address new security risks. These technological options must be thoroughly studied before being implemented as a public service.

Conclusion

As the analysis presented in this paper shows, the new authentication methods redefine the user interaction with the web system during the authentication process. These new methods create an independent channel of communication between the user and the system, through the public telephone network in order to dictate a unique, random single-use password. The presented methods remove some important security vulnerabilities such as SIM card cloning, used to take fraudulent control of web accounts.

We have analyzed in detail the operation of a medical system that implements the new manner of web authentication, presenting a series of data and use models which on one hand confirm the usefulness of these methods and on the other hand stand at the basis of future improvements. Before implementation, the analyzed medical system was plagued with unauthorized access sessions by individuals using public access terminals available in hospitals. After the implementation we have found a drastic reduction of unauthorized access coming from this type of terminals.

The central authority running the analyzed web service implemented the use of NFC ID cards and distributed specialized NFC readers for the necessary terminals. The use of NFC ID cards has become standard, noticing increased speed in the authentication process. Now, users no longer need to memorize Internet web site address, personal identifiers nor passwords in order to initiate the secured web sessions used to signal the authentication intent of the user.

Even though the paper presents a system based on random single use passwords (OTP) that are equivalent to 4-digit PIN numbers, they do not represent a restriction. The system analyzed in this paper uses such passwords because they are sufficient to obtain the desired effect, without disrupting unnecessarily the fragile balance between security, functionality and comfort.

In accordance to the presented method, the authentication process produces plenty of other useful data besides that collected during the password creation phase. The continuous analysis of the system's identification data using a Deep Learning algorithmic process could increase security as a whole by applying custom user profile policies. The user profiles contain data that refers to the timeframe needed for the voice indications to be recognized and actions to be taken for successful authentication. These ideas have not been implemented nor analyzed yet, but are considered for further development.

As the latest advances in computing (including better, more powerful processors, large and very fast storage systems e.g. solid-state drives (SSD), artificial intelligence, deep learning technologies) are accessible to the public but also to cybercriminals, further efforts must to be undertaken to enhance every component of the security system in order to fight cyber-crime. This work tries to emphasize the role of people and culture in the authentication process. The main ideas presented in this paper have been implemented / tested and analyzed in detail. As one would expect, the subject open to future research, as knowledge, innovation, technological advances in Information Technologies, communications, miniaturization and low energy consumption devices will bring new, more secure and user-friendly solutions.

Conflict of Interest

The author declares no conflict of interest.

References:

[1] ISO 9241 Ergonomics of Human-System Interaction Standard, https://www.iso.org, 2018.

[2] EU General Data Protection Directive (GDPR), https://www.eugdpr.org/, 2018

[3] Paul A. Grassi, Michael E., Garcia James L. Fenton, "Digital Identity Guidelines", NIST Special Publication 800-63-3, https://doi.org/10.6028/NIST.SP.800-63-3, 2018

[4] D. Dasgupta, A. Roy, A. Nag, "Advances in User Authentication", ISSN:2363-6149, 2017

[5] Richard E. Smith. "Authentication – From Passwords to Public Keys", ISBN: 0-201-61599-1, 2002

[6] D. Charruau, S.M. Furnell & P.S. Dowland, "PassImages : An alternative method of user authentication" in Advances in Networks, Computing and Communications 2, ISBN: 9781841021409, 2004

[7] S. Chiasson, A. Forget, R. Biddle, P.C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords" https://link.springer.com/article/10.1007/s10207-009-0080-7, 2009

[8] FIDO Alliance, https://fidoalliance.org/, 2018

[9] Lily Hay Newman, "Cloulldflare and Google Will Help Sync the Internet's Clocks - and Make You Safer", https://www.wired.com/story/cloulldflare-google-roughtime-sync-clocks-security/, retrieved Nov. 2018

[10] Roughtime Project, https://roughtime.googlesource.com/roughtime, 2018

[11] Nicole P., Amie T., Adam S., "Marriott Hacking Exposes Data of Up to 500 Million Guests", The New Work Times, https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html, accessed 2018-12-01

[12] State of Authentication Report 2017, FIDO Alliance, https://fidoalliance.org/, 2018

[13] "Silicon Valley Execs Targeted in 'SIM Swap' Hacking, $1 Million in Crypto Stolen", https://www.newsbtc.com/2018/11/22/silicon-valley-execs-targeted-in-sim-swap-hacking-1-million-in-crypto-stolen/, 2018

[14] "$14 Million in Cryptocurrency Allegedly Stolen By SIM Swappers, Authorities Report", https://www.cryptoglobe.com/latest/2018/09/14-million-in-cryptocurrency-allegedly-stolen-by-sim-swappers-oklahoma-city-authorities-report/, 2018

[15] Paul Kocher et.al., "Spectre Attacks: Exploiting Speculative Execution" https://spectreattack.com, 2018

[16] N. Perloth, A. Tsang, A. Santano, Marriott Hacking Exposes Data of Up to 500 Million Guests https://www.nytimes.com Nov. 30, 2018

[17] Z. Zhao, G. Ahn, J. Seo, H. Hu, "On the Security of Picture Gesture Authentication" 22nd USENIX Security Symposium ISBN: 978-1-931971-03-4, 2013

[18] Arti Bhanushali, et al., "Comparison of graphical password authentication techniques" International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, 2015

[19] William E. Burr et al. "Electronic authentication guideline" NIST Special Publication 800-63-2, 2013

[20] NFC Forum, "Essentials for Successful NFC Mobile Ecosystems", 2008

[21] Online Services srl, “Constructive assembly and method for granting authorized access to an Internet service platform”, PCT/RO2017/000002 Patent pendig, 2016

[22] Entersekt, “OTP security past its expiration date” https://www.entersekt.com, 2014

[23] Entersekt, “Securing the mobile banking channel” https://www.entersekt.com, 2014

[24] Sonia Chiasson, “Usable Authentication and Click-Based Graphical Passwords” ISBN: 978-0-494-47475-4, 2009

[25] M. Mathuri Pandi, A. Valarmathi, “A secured graphical password authentication system” International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 5 ISSN: 2278-0181, 2013

[26] Amish Shah, Partth Ved, Avani Deora, Arjun Jaiswal, Mitchell D'silva, "Shoulder-surfing resistant graphical password system" Procedia Computer Science 45, pp. 477 – 484, 2015

[27] Vinit Khetani, Jennifer Nicholas, Anuja Bongirwar, Abhay Yeole, “Securing web accounts using graphical password authentication through watermarking” International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 6 ISSN: 2231-2803, 2004

[28] "Logging in W3C httpd". World Wide Web Consortium. 1995-10-12. Retrieved 2018-11-20.

[29] R. Fielding et. al., “Hypertext Transfer Protocol – HTTP/1.1”, The Internet Society (1999).