www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16419-16426

Digital Remembrance Based User Validation for Internet of Things [IoT]

Sunain Kowser,
4th Sem, M.Tech,
BGSIT,
sunainkowser@gmail.com

Abstract—The increasing number of devices within the IoT is raising concerns over the efficiency and exploitability of existing authentication methods. The weaknesses of such methods, in particular passwords, are well documented. Although alternative methods have been proposed, they often rely on users being able to accurately recall complex and often unmemorable information. With the profusion of separate online accounts, this can often be a difficult task. The emerging digital remembrance concept involves the creation of a repository of remembrance specific to individuals. We believe this abundance of personal data can be utilized as a form of authentication. In this paper, we propose our digital remembrance based two-factor authentication mechanism, and also present our promising evaluation results. Keywords—Digital remembrance, authentication, IoT, security

I. INTRODUCTION

As the Internet of Things (IoT) concept continues to grow, a greater number of personalized services are becoming embedded within our environment, which requires a greater level of interaction with our personal devices. With the rapid growth in mobile and wearable technology, we are seeing devices increasingly becoming a method of authentication (e.g. smartphones and RFID enabled cards). For example, many smartphones can now be used as a payment method [1]. However, for security or accountability purposes, interaction with such services often requires user authentication. Unfortunately, many of the existing authentication mechanisms are considered impractical, outdated or weak. The problems with current authentication strategies will continue to hamper computing, until a more feasible approach is developed.

There are a wide variety of authentication strategies that are currently in use. However, there are issues with many of them, which is why many researchers are focusing on developing new methods, specifically for IoT. The traditional use of a single alphanumeric password has long been considered outdated and insecure. Yet it still remains the most popular form of authentication (including as part of multi-factor authentication mechanisms). There have been other proposed methods including the use of user specific questions (e.g. place of birth), secret questions and answers, pin numbers or selected images, amongst many others. The major weak link in most authentication mechanisms is the users themselves. The average user has 26 online accounts [2], requiring them to memorize a plethora of different pins, passwords and secrets, with often more than one required for some accounts (e.g. online banking). It is therefore unsurprising that many users reuse their passwords and secret answers. Many existing authentication challenge questions are generic, and the answers to which can easily be found online using websites suchas 192.com or from screening user's online profiles (e.g. company profiles or social media accounts). These types of authentication are highly susceptible to social engineering and phishing attacks.

There have been numerous attempts to address this issue. The latest initiative is the introduction of multi-factor authentication, which facilitates the use of various factors, which can include mobile devices, one-time-use password generators and RFID cards, amongst others. Largely, these authentication mechanisms are scientifically sound; however, in the real-world the main challenge is getting users to adopt and integrate these mechanisms into everyday life.

An emerging area of computing is the concept of digital remembrance, which is the idea of preserving user remembrance into a physical format stored in an online repository. Such data is often stored in photographic, video and audio formats, usually with embedded meta-data (e.g. geotagging). These remembrances are highly specific to individual users and could potentially be an untapped resource of authentication challenge material. The main difference is that users are far more likely to remember specific events from their own lives, than a random secret answer that has been set in haste. The abundance and diversity of digital memory data means that there is a plethora of unique authentication challenges that can be created.

In this paper, we propose a digital remembrance based twofactor user authentication mechanism for mobile devices. This mechanism aims to provide a practical and reliable form of authentication for modern users. The highly specific nature of digital remembrance allows for its use as authentication material, and its complexity can be varied depending upon the nature of the service being accessed. It is also able to mitigate the cyber-physical risks associated with emerging mobile biometric mechanisms (e.g. fingerprint theft and duplication). As an additional benefit, digital memory data allows for the use of more interactive forms of authentication (e.g. multiple choice or interactive maps). Therefore, making it more difficult for attackers to undertake shoulder surfing, social engineering and phishing attacks, as well more traditional attacks such as using brute-force or rainbow tables. To the best of our knowledge, there have been no other authentication mechanisms proposed that use digital remembrance to provide user authentication.

The remainder of this paper is structured as follows. Section II will provide background information and existing research on authentication and digital remembrance. Section III presents the initial design of the authentication mechanism, whilst Section IV presents the evaluation of our design. Section V outlines some potential applications for the mechanism, and finally, the paper concludes in Section VI.

II. BACKGROUND

A. Multi-Factor Authentication

Multi-factor authentication is a more robust form of access control, whereby users identify themselves in a staged process using different personal factors. The most commonly used factors are as follows:

- Knowledge Factor: Referred to as ‘something you know’, this is information known by the user that they must provide to progress in their authentication. Such information may include passwords, PINs and answers to secret questions.

- Possession Factor: Referred to as ‘something you have’, which is something that the user must have in their possession in order to progress with the authentication. Such information may include one-time password (OTP) generator, ID card or a smartphone.

- Inheritance Factor: Referred to as ‘something you are’, which are biological characteristics of the user that are compared for authentication. Such comparisons may include fingerprint scan, retina scan, facial recognition or voice recognition.

- Location Factor: Referred to as ‘somewhere you are’, this uses the user’s current location as a form of authentication. The use of GPS-enabled smart devices has enabled the ease of geographical location confirmation.

- Time Factor: Time is often used as logical support to other authentication factors. For example, by comparing the geographical locations of login attempts, fraudulent logins can be detected if vast geographical distances are observed within a short time-frame.

There have been numerous multi-factor authentication mechanisms proposed, for a wide variety of purposes. Some of the most recently proposed mobile-based authentication mechanisms are as follows. TouchIn [3] is a two-factor authentication mechanism for multi-touch mobile devices. Users draw a geometric curve of their own choice (knowledge factor) using one or multiple fingers. An authentication template is created based on characteristics extracted from this input, such as finger pressure and hand geometry (inheritance factor). Another example is by Abdurrahman et al. [4], who propose a mobile-based multi-factor authentication mechanism based on a pre-shared number (knowledge factor), GPS Location

(location factor) and time stamp (time factor). The approach is designed as a cost-effective alternative to SMS-based multifactor authentication.

The importance of using multi-factor authentication techniques has been highlighted in the media recently, by the news surrounding the LastPass hack [5]. However, throughout our literature review, we have been unable to find a mobile multifactor authentication mechanism similar to ours that is based on the user's own digital remembrance.

B. Digital Remembrance

The area of human digital remembrance was first conceptualized in 1945 with the idea of Bush's Memex [10]. This device was a place for storing books, records, and communications and was envisioned as an "enlarged intimate supplement to memory" [10]. In today's society, the proliferation of smart and wearable devices has made this idea a reality. In turn, this has paved the way for 'lifelogging', which refers to theprocess of using such devices to automatically record aspects of our lives in digital form [11]. When we record our lives we are creating lifelogs or human digital remembrance (HDMs) of human experiences. These logs are a digital representation of ourselves that evolve and grow alongside us and are a form of pervasive computing that consists of "a unified digital record of the totality of an individual's experiences, captured multimodally through digital sensors and stored permanently as a personal multimedia archive" [12]. In other words, they are a combination of many types of media, audio, video and images that have been recorded using a range of devices and sensors [13], [14]. As the IoT develops, the range of information that we have access to and can incorporate into our lifelogs is growing daily. However, as we gain access to more data, management of this information becomes more difficult and structuring accurate HDMs is a challenge.

However, past research into the elements of human memory can be drawn upon so that HDM data can be structured into a reasonable representation of a memory. Within our brain, there are five major memory systems (procedural, perceptual representation, short-term, episodic and semantic memory) that regulate everything from languages to skills and knowledge [15]. Episodic memory, in particular, is related to remembrance about personally experienced occasions. Their primary concern is about the subject's experiences of temporally dated episodes or events, and the temporal-spatial relations between them [15], [16]. When we remember an event, we usually tend to remember temporal episodes and recall where we were, the time of the event and what happened. Therefore, when creating HDMs, it is important to structure this information into events or happenings that accurately corresponds to our lives in a manner that facilitates remembering [17].

III. INITIAL DESIGN

In this section, we will provide an overview of the proposed authentication mechanism. The motivation behind this idea is that end-users are finding authentication increasingly complex, frustrating and unmemorable. This method aspires to provide users with a mechanism that allows them to authenticate themselves using their personal digital remembrance. Their remembrance is more likely to be retained in long term memory and will be far more recallable than pins, passwords or secret words.

This approach has many benefits, such as the abundance of material providing a plethora of unique authentication challenges (i.e. not repeating questions). The diversity of digital memory media (e.g. photos, videos and sound clips) and subsequent meta-data (e.g. geotagging, timestamps and camera manufacturer information) allows for various levels of authentication interactivity. Additionally, the level of detail present in digital memory data provides a high degree of flexibility in terms of adjusting the complexity or comprehensiveness of the authentication challenge, to suit the needs of the service providers.

There are several categories of potential authentication questions, including:

- Date/Time recognition : Assess whether the user is able to determine the time, date or chronology relating to a digital memory event (e.g. what year is this videoclip from? or which of the following images represent your location at 14:00pm on 01/01/2014?).

- Place recognition: Assess whether the user is able to determine the location of their digital

memory events (e.g. select the region on the map where this memory event took place, or select all of your digital memory images that are from your trip to Portugal in 2012). •

- People/Pets recognition: Assess whether the user is able to identify specific people or animals from their digital remembrance(e.g. type the name of the people/pets highlighted in the video still or image)

- Device recognition: Assess whether the user is able to identify the device used to capture digital remembrance (e.g. identify the manufacturer of the device used to take this photo).

- Habit recognition: Assess whether the user is able to identify their own behavioural habits (e.g. which of the routes shown on the map would you usually take on a Monday morning?).

- Audio recognition: Assess whether the user is able to recognise independent audio or audio tracks extracted from video files (e.g. type the names of the people that can be heard in the audio clip).

- Ownership recognition: Assess whether the user is able to recognise media that is from taken their digital memory, as opposed to stock images (e.g. select those images you recognise from your digital remembrance).

As the digital remembrance concept continues to evolve, there will be many more potential future categories that will emerge.

There are also several methods of collecting the authentication responses, which can provide various degrees of interaction, including:

- Choice selection: Answers are selected (multiple or single) using items (e.g. radio buttons or images) that represent the answers, which can be presented in the form of text, images, video clips or audio clips.

- Image part selection: Selecting parts of an image or video clip still as an answer (e.g. select a country from a map or select a person from an image).

- Alphanumeric input: A traditional text box input which requires users to manually type in the answers.

- Interactive categorisation: Dragging media into defined categorised folders to provide their answers (e.g. separating six images into two age respective folders).

The exact nature of the authentication challenge changes randomly, but each is designed to suit the required level of complexity and comprehensiveness.

A high-level overview of the proposed two-factor authentication mechanism design is shown in Fig 1. There are three main actors in the mechanism, these are the User's Smartphone (US), Service Provider (SP) and the Digital Memory Authentication Service (DMAS).

The US serves as an independent platform allowing communications with other actors. More importantly, as this is amobile user-authentication mechanism, its physical presence with the user also becomes an authentication factor.

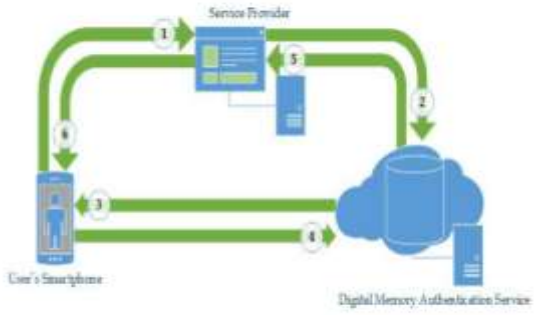


Fig. 1: Authentication mechanism overview

The SP provides a particular service to the user, but to access this service using mobile authentication, the user must first register their device with the SP. The SP does not have access to any of the user's digital memory data, nor any of the account details associated with it, so instead the SP uses a trusted third party (the DMAS) to handle this.

The DMAS hosts the user's digital remembrance in a cloud environment and provides part of the authentication using their memory data. Users are able to configure which remembrance they wish to allow to be used for authentication purposes. The DMAS implements many advanced techniques to generate unique authentication challenges, such as data mining, facial recognition, image analysis and data classification. The use of these techniques is imperative for the robustness of the authentication process. They can be used to determine the suitability of remembrance to be used for authentication challenges (e.g. identifying common landmarks which may make identifying locations easy). Another purpose is to assess the level of image disparity so as not to provide easy challenges (e.g. being asked to identify images from the North Pole amongst images from the Caribbean). To mitigate this problem, the DMAS uses image classifiers to select visually similar images. An extra dimension of difficulty can also be added, as the DMAS has the capability to manipulate images to create trick questions (e.g. superimpose people into images).

The high-level process of the mechanism is explained in the following steps, which correspond to the numbering shown in Fig 1. In the scenario illustrated, the user wishes to access a service using their smartphone, which has been registered with the SP, and both the user and SP already hold accounts with the DMAS.

1) The user requests access to SP's service, where the user's device has been registered previously. The identity of the physical device is first authenticated against the SP's records.

2) The SP negotiates an authentication session with the DMAS, specifying the comprehensiveness (e.g. number of questions) complexity (e.g. difficulty of the questions) for the desired authentication challenge.

3) Upon the user requesting the challenge, it is computed by the DMAS to match the SP's requirements and is then sent to the user. At this stage, all potentially useful meta-data has been stripped from any digital memory data used.

4) The user sends their response to the challenge back to the DMAS, which validates their answer.

5) The DMAS returns the authentication challenge result to the SP.

6) If the authentication result is successful, the user will be granted access by the SP.

This approach is capable of providing a robust mobile-based user authentication mechanism for IoT. The added benefit, particularly for IoT environments is that no single party can provide full authentication or access all the user's details. Therefore, if the mobile device is lost or stolen it cannot be used to gain unauthorised access.

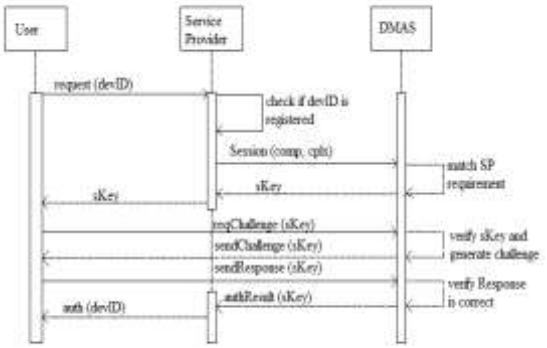
A. Detailed Explanation

The proposed authentication process should ideally be conducted over SSL, in order to maximise security by providing an additional layer of confidentiality and integrity assurance. Unfortunately, some IoT devices are computationally limited, which prohibits them from running SSL [18]. Therefore, to remain suitable for operation within an IoT environment, the mechanism needs to be able to function securely without relying on SSL.

In the proposed two-factor authentication mechanism, we firstly use the Possession Factor, which is provided by the physical presence of the US (assessed by the SP). The second is a Hybrid Knowledge Factor, which is achieved using the DMAS to generate user-specific Knowledge Factor challenges, whilst combining them with elements of both Location and Inheritance factors. In order to satisfy the two-factor requirements, neither authentication actor involved (i.e. SP or DMAS) is able to know all of the user's authentication information.

As all of the actors in the mechanism will have pre-existing relationships (e.g. prior account or device registration). We make the assumption that both the SP and the DMAS mutually trust each other, similar to those assumptions made by numerous existing mechanisms including SSL CA trust model [19], OpenID [20] and external account authentication (e.g. Facebook [21] and Google Identity Platform [22]). We also assume that the digital memory data used for authentication isn't in the public domain (e.g. on public-facing social media sites).

A detailed schematic of the authentication process is illustrated in the UML sequence diagram illustrated in Fig 2. In the diagram, symEnc() is a symmetric encryption function that uses a secret key shared between the actors at each end of the respective data flow arrow, devID is the device ID, hash() is a hash function, accKey is the SP's account key, cCPLX is the challenge complexity, cCOMP is the challenge comprehensiveness and sKey is the session key. request is the challenge request, uChal is the user's unique challenge, uResp is the user's response to the challenge, authRes is the authentication challenge result and authToken is the authentication token.



As illustrated in Fig 2, we use symmetric encryption to secure communications between the actors, as they all have pre-existing relationships. The SP provides the initial authentication factor (Possession) and then if this can be verified, a session key (sKey) is negotiated on behalf of the US, sothe DMAS's identity can be assured. The session key is used as a marker to prevent unauthorised replay attacks, in place of using nonces. Each sKey is timestamped, has a limited lifespan and is tied to the initiating IP address. A challenge/response mechanism is then used to authenticate the US against the DMAS. These challenges are computed by the DMAS using the user's digital remembrance and the SP's requirements. Once both authentication factors have been verified, the SP issues an authentication token to the US, allowing them to access the required service.

IV. EVALUATION

In order to evaluate the security characteristics of the authentication mechanism proposed in this paper, we used the Scyther Tool [23], [24] to provide a formal analysis. Scyther is an automatic security protocol verification tool, which is used to identify potential attacks and vulnerabilities. It has been used to verify numerous security protocols, such as [25]. We used Scyther to evaluate the following properties of our proposed mechanism:

- Secrecy: To ensure the confidentiality of credentials, keys, tokens and data is maintained i.e. no intruders are able to steal them.
- Replay attack resistance: To ensure resistance to attacks whereby communications between two genuine actors are intercepted and repeated by an intruder, thus allowing them to masquerade as an authentic actor.
- Reflection attack resistance: To ensure resistance to attacks where authenticating actors can be fooled into providing the answer to their own challenge.
- Man-in-the-middle attack resistance: To ensure resistance to attacks where malicious entities are able to intercept and modify communications between two genuine actors, without raising suspicion.

Fig 3 illustrates the results obtained from Scyther's analysis. As can be seen, Scyther has been unable to determine anyweaknesses or feasible attacks against our proposed mechanism. We repeated the Scyther verification ten times, using both the manually defined claims and Scyther's automatically generated claims, and the results remained the same.

V.POTENTIAL APPLICATIONS

The increasing demand for innovative forms of mobile authentication means that there are numerous potential applications for our proposed mechanism.

One such application area that the mechanism could be applied to is the emerging trend of BYOD within corporate settings. In those corporations that do not enforce a blanket ban, mobile devices (e.g. tablets or smartphones) only require the wireless key to access the network. Currently, in the majorityof cases it is too cumbersome to introduce authentication into such a setting. Therefore, there is a growing need for a more secure and practical process. Utilising the proposed mechanism would allow the physical

presence of the device to be used as one authentication factor, whilst the correct answer to digital memory based challenges to provide the other. This would provide a more robust access control mechanism, allowing for greater accountability within corporations with BYOD policies.

Another potential application area is that of online banking. Current systems require passwords, memorable words and one-time codes to login. However, instead of remembering complicated passwords, the user could enter their username and the last 4 digits of their debit card number but instead of then entering a password, the DMAS could provide a challenge based on particular remembrance. As online banking accounts are considered high risk, this would require authentication challenges that could match the higher complexity and comprehensiveness expected. Example challenges for both of the potential applications are shown in Fig 4 and 5.

Fig. 4: Example interactive question

Fig. 5: Example text-based question

VI. CONCLUSION

In this paper, we have presented a digital remembrance based authentication mechanism for mobile user authentication. We have provided a detailed overview of the mechanism and presented our initial evaluation. The result from our evaluation indicate that protocol would be adequately secure for authentication purposes. The lack of reliance on SSL means that it would also be suitable for use within an IoT environment. Thus suggesting that if implemented, it could provide a feasible and more effective form of authentication.

The novel approach of using personal digital remembrance for authentication is able to mitigate many of the risks associated with current password or generic question based methods (e.g. shoulder surfing, phishing and brute force). Several forms of emerging mobile authentication such as biometrics, are highly susceptible to physical attacks (e.g. fingerprint lifting) meaning that once such data (e.g. the fingerprint) has been obtained, the authentication mechanism is rendered obsolete. However, with our proposed mechanism this risk is greatly lowered, as the ability to replay, repeat or guess the challenges is significantly reduced. The degree of personalisation offered means that users are more likely to know the answer to the challenge, as opposed to forgetting answers or passwords set months previously. Additionally, the diverse range of highly personal remembrance,

provides a more flexible approach to authentication, as both complexity and comprehensiveness can be altered in the generation of unique challenges. We hope that the proposed mechanism is able to replace the generic and outdated approaches currently in use within mobile user authentication.

In our future work, we are hoping to expand our initial implementation into a fully working prototype. This will allow us to conduct further experiments and determine the full extent of the acceptance of the concept. We also aim to publish the details surrounding the functionality and mechanisms utilised by the DMAS server for authentication challenge creation.

REFERENCES

[1] J. Garside, "Smartphone swipe payment scheme unveiled — money — the guardian,"
[2] T. is Money, "Passwords: Why using a software 'safety box' can keep your online accounts secure — this is money,"
[3] J. Sun, R. Zhang, J. Zhang, and Y. Zhang, "Sightless two-factor authentication on multi-touch mobile devices," IEEE Conference on Communications and Network Security (CNS), pp. 436–444, 2014.
[4] U. Abdurrahman, M. Kaiiali, and J. Muhammad, "A new mobilebased multi-factor authentication scheme using preshared number, GPS location and time stamp," International Conference on Electronics, Computer and Computation (ICECCO), pp. 293–296, 2013.
[5] D. Gewirtz, "Lastpass hack reinforces importance of using multi-factor authentication,".
[6] R. Lennon, "Changing user attitudes to security in Bring Your Own Device (BYOD) & The Cloud," Proceedings of the 5th Romania Tier 2 Federation Grid, Cloud & High Performance Computing Science Conference (RO-LCG), pp. 49–52, 2012.
[7] Y. Xuechen, "LED Display Screen Monitoring Platform Based on IdentityAuthenticationwithUSBKey,"12th IEEE International Conference on Computer and Information Technology (CIT), pp. 905–909, 2012.
[8] R. Teymourzadeh, "Smart novel computer-based analytical tool for image forgery authentication," IEEE International Conference on Circuits and Systems (ICCAS), pp. 120–125, 2012.
[9] S. Michael, "Winbeta,"
[10] V. Bush, "As We May Think," The Atlantic Monthly, 1945.
[11] A. R. Doherty, N. Caprani, C. .Conaire, V. Kalnikaite, C. Gurrin, A. F. Smeaton, and N. E. OConnor, "Passively Recognising Human Activities Through Lifelogging," Comput. Human Behav., vol. 27, pp. 1948–1958, 2011.
[12] M. Dodge and R. Kitchin, "Outlines of a world coming into existence: pervasive computing and the ethics of forgetting," Environ. Plan.B Plan.Des., vol. 34, pp. 431–445, 2011.
[13] L. Kelly, "The Information Retrieval Challenge of Human Digital Remembrance," BCS IRSG Symposium: Future Directions in Information, 2007.
[14] C. Gurrin, D. Byrne, N. OConnor, G. J. F. Jones, and A. F. Smeaton, "Architecture and Challenges of Maintaining a Large-scale, Contextaware Human Digital Memory," 5th International Conference on Visual Information Engineering, pp. 158–163, 2008.
[15]E.Tulving,"WhatIsEpisodicMemory?"Curr.Dir .Psychol.Sci.,vol.2, pp. 67–70, 1993.