Review Paper On Various Methods Of Implicit Authentication

Shital J. Mehatre
Computer Science & Engineering
G.H.Raisoni College of Engineering & Management
Amravati, India
shitalmehatre21@gmail.com

Dinesh S. Datar
Information Technology
G.H.Raisoni College of Engineering & Management
Amravati, India
dinesh.datar@raisoni.net

***Abstract*—** The quest (search) for a reliable and convenient security system to authenticate a computer user has existed since the inadequacy of conventional password mechanism was realized, first by the security community, and then gradually by the public. Verifying the identity of a user before granting access to objects or services is an vital step in nearly all applications or environments. Some applications (e.g. pervasive environment) may impose additional requirements for user authentication mechanism, such as to be continuous and unobtrusive. New system is hoped being transparent and with very minimum user involvement denoted as implicit authentication system. This paper tackles the issue of ambient systems adaptation to users' needs while the environment and users' preferences evolve continuously.

Keywords- *security, implicit authentication, behavior modelling, good event, bad event,Privacy-preserving implicit authentication*

*****

I. INTRODUCTION *(HEADING 1)*

As mobile devices quickly gain in usage and popularity [1], more consumers are relying on these devices, particularly smartphones, as their primary source of Internet access. Continued and rapid increase of online applications and services results in an increase in demand for authentication. Traditional authentication via password input fall short/unsecure in the context of authentication. From secret knowledge like password up to physical traits as biometrics, current smartphone authentication systems are deemed inconvenience and difficult for users. Burdens on remembering password as well as privacy issues on stolen or forged biometrics have raised a futuristic idea of authentication systems. Implicit authentication is hoped being transparent and with very minimum user involvement, consists of legitimating a user depending on the user's usage profile, instead of relying on the user explicitly knows (patterns, tokens, passwords, private keys etc.). Implicit authentication relies not on what the user knows but is based upon user behaviour, and is accomplished by building so-called user profiles from various sensor data and makes identity theft by third parties more promising, it requires the server to learn and store the user's usage profile. In empirical evidence was given that the features collected from the user's device history are effective to distinguish users and therefore can be used to implicitly authenticate them (instead or in addition to explicit authentication based on the user's providing a password).

II. LITERATURE SURVEY

Two common techniques to addressing client management of an increasing number of service credentials exist in use:

1) The number of times the user needs to authenticate
2) Biometrics.

Solutions such as Single Sign-On (SSO) and password managers may reduce the problem related to frequent authentication, they do not identify the user but rather the device. Therefore, SSO does not defend well against theft and compromise of devices, nor does it address the problem of voluntary account sharing. According to a study on user perception of authentication on mobile devices, Furnell et al. [11] found that users want a transparent authentication techniques that increases security and "authenticates the user continuously/periodically throughout the time of day and day of week in order to maintain confidetiality in the identity of the user". Some form of implicit authentication exists already in the form of location-based access control [12, 5], or biometrics, notably keystroke dynamics and typing patterns . More recently, accelerometers in devices have been used to make user usage profile and identify users. Chang et al. [13] used accelerometers in television remote controls to identify individuals. These biometrics and location-based approaches are complementary to implicit authentication as it can potentially utilize biometrics as features in computing the authentication score.

III. DEFINITIONS

When talking about authentication, it is helpful to give some basic definitions regarding this matter. The process of authentication, verification, validates a claimed identity by matching it to a known set of identities [2]. Most people are creatures of habit - authentication answers the question "Am I who I claim to be?" [3]. The result of the one-to-one test has a binary output: The answer can be true or false. However, there are certain degrees, i.e. thresholds, of deciding whether the identity can be confirmed [4]. It is then assumed, that the dataset with the highest similarity represents the individual. Thus, identification returns a vector or tuple closest to the person's characteristics instead of binary answers.

IV. AUTHENTICATION METHODS

After defining the most important terms, some of the most common features that can be utilized to perform authentication are explained. There are many methods through which we can implicitly aauthenticate user. *In* this review paper we are mainly focusing on "Implicit Authentication Through Learning User Behavior".

a) Implicit Authentication Through Learning User Behavior

How can we "authenticate" users without bothering them or interfering with their daily routines/habits? In reality, many things authenticate us: something we know (answers to questions); something we have (a secure ID token); or something we are (biometrics such as fingerprints, voice, eyesight). But something often overlooked and easy to examine is our implicit habits or routines. We propose implicit authentication, an approach that uses observations of user behavior for authentication. Most people are creatures of habit - a person goes to work in the morning, perhaps with a stop at the temple, but almost always using the same route, same vehicle. Once at work, she might remain in the general vicinity of her office building until lunch time. In the afternoon, perhaps she picks up her child from play school. In the evening, she goes gym. Throughout the day, she checks her various email accounts. Perhaps she also uses online banking, e-shopping. Weekly visits to the grocery store, parlour, regular calls to family members, etc. are all rich information that could be gathered and recorded almost entirely using smartphones. These devices are capable of collecting a rich set of information, such as location, motion, communication, and usage of applications and would benefit from implicit authentication because of their text input constraints.

1) Modelling User Behavior

The density functions for each feature conditioned on the time-of-day and day-of-week, thereby forming a user model. Given a user model and some recently observed behavior, we can compute the probability that the device is in the hands of the legitimate user. This probability is used as an authentication score[5].

Following are some terms used in this method -

- Score: Used to make an authentication decision
- Threshold: Used to decide whether to accept or reject the user. Threshold can vary for different applications, depending on whether the application is security sensitive.
- Good event: Making a phone call to a family member, known number , numbers saved in contact list or browsing a familiar website.
- Bad event: Making a call to an unknown number or visiting an unknown URL

b) Gait

Another method for implicit authentication is an Arm Swing, the way in which user naturally swings hand while doing other work or walking. First approaches of analyzing the individual characteristics of human gait were found in the 1970s [6]. Since then, researchers have tried to automatically identify people from their walk. This method studies an unobtrusive mechanism of user authentication based on new biometric modality. Collect arm swing of the person by using a motion recording sensor, which records acceleration of the arm swing in three orthogonal directions. Using frequency domain analysis of the arm swing accelerations, we obtained anEqual Error Rate (EER) of 10% based on a preliminary data set including 120 arm swing. But this method is proposed as a weak biometric for user authentication.

c) Ear shape Biometrics

Authenticating user via image or video captured using smartphone camera during a call. Implicitly take ear image using front smartphone camera to recognize and authenticate users without them realizing. Consider both shape and texture information to represent ear image. Steps used for implementing are as follows –

- Firstly, all Local Binary Pattern (LBP) are combined
- Concatenate the collected patterns into a single histogram
- In order to get geometric features, use the idea of ear location center that is easily adjusted by smartphone user
- Combine previous steps to represent ear image as a descriptor
- The recognition is performed using a nearest neighbor classifier computed feature space

d) Privacy-Preserving Implicit Authentication

The first privacy-preserving implicit authentication system was presented, in which the server does not need to study the user's usage profile. It makes use of an *ad hoc* two-party computation protocol to compare the user's recent sampled features against an encrypted stored profile. Here a simpler protocol (Flexible and Robust) based on the principal of set intersection that has the advantages of:

- requiring only one cryptosystem;
- not exposing the relative order of recent feature samples;
- being capable of dealing with any type of features (numerical or non-numerical).

In fact, implicit authentication turns out to be a weak excuse to justify the storage and/or access by servers to the usage profiles of users. In [7] it was shown how to make implicit authentication compatible with the privacy of users. The idea is that the server only needs an encrypted version of the user's usage profile. In simple implicit authentication when a user wishes to use some application, he/she has to authenticate themselves in order to use that application. In this type of authentication, the history of a user's actions on the user's device is used to construct a user profile that consists of a set of features. But when we store the accumulated profile of the user in the user's device, an intruder might compromise the device and alter the stored profile in order to impersonate the legitimate user. So it is not safe. Hence, for security, the profile must be stored by some external entity. But this extends to another issue that the user's profile includes potentially sensitive information and storing it outside the user's device violates privacy. Implicit authentication systems try to mitigate the above privacy problem by using a third party, the carrier (i.e. the network service provider) to store the user's profiles.

In the privacy-preserving implicit authentication system proposed in [8], the user's device encrypts the user's usage profile at set-up time, and forwards it to the carrier, who stores it for later comparison.

- no security problem : because during normal operation the user's device does not store the user's profile (it just collects the fresh usage features).
- no privacy problem : because the carrier does not see the user's profile in the clear.

All the computation takes place at the carrier and both inputs are encrypted: indeed, the carrier stores the encrypted profile and the user's device sends the encrypted fresh sample to the carrier.

V. CONCLUSION AND FUTURE RESEARCH

In this paper, a view of authentication and implicit authentication has been described. Fortunately, current studies indicate that users would welcome the establishment of implicit authentication [9], [10]. But yet this mechanism is not completely secure because sometimes user behaves or have to behave diplomatically rather than habitual. Then user scores would be degraded. Hence we can conclude that implicit authentication might not be able to replace explicit authentication entirely, and although parts of it show some disadvantages, the principle is really promising in terms of both security and usability.

Future research will include account sharing capabilities and authentication of user in unconscious and diplomatic situation. Future work also includes supervised learning techniques for profiling and to develop models for other types of adversaries, including friends and family members. To get the data necessary, we can recruit the help of family members and friends to study how to game and defend the implicit authentication system.

REFERENCES

[1] S. Schroeder. Smartphones Are Selling http://mashable.com/2010/ 02/05/smartphones-sales/.

[2] J. Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez. Combining biometric evidence for person authentication. Advanced Studies in Biometrics, pages 1–18, 2005.

[3] E. Shi, Y. Niu, M. Jakobsson, and R. Chow. Implicit Authentication through Learning User Behavior http://midgard.cs.ucdavis.edu/ ˜niu/papers/isc2010full.pdf.

[4] L. Whitney. Smartphones to dominate PCs in Gartner forecast. http://news.cnet. com/8301-1001_3-10434760-92.html.

[5] R. Brunelli and D. Falavigna. User identification using multiple cues.

[6] R. Brunelli and D. Falavigna. Person identification using multiple cues. IEEE transactions on pattern analysis and machine intelligence, 17(10):955–966, 1995.

[7] N. A. Safa, R. Safavi-Naini and S. F. Shahandashti, "Privacy-preserving implicit authentication", in *IFIP SEC 2014-Intl. Information Security and Privacy Conference*, IFIP AICT 428, pp. 471–484, 2014.

[8] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song. Authentication in the clouds: a framework and its application to mobile users. In Proceedings of the 2010 ACM workshop on cloud computing security workshop, pages 1–6. ACM, 2010.

[9] A. Buchoux and N. Clarke. Deployment of keystroke analysis on a smartphone. In Proceedings of the 6th Australian information security management conference. Perth, Western Australia: SECAU-Security Research Centre, pages 40–47, 2008.

[10] S. Furnell, N. Clarke, and S. Karatzouni. Enhancing user authentication for mobile devices. Fraud & security, 2008(8):12–17, 2008.

Article in a conference proceedings:

[11] S. Furnell, N. Clarke, and S. Karatzouni. Beyond the pin: Enhancing authentication for mobile devices. Computer Fraud and Security, 2008.

[12] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location/GPS claims. In WiSe '03: 2nd ACM workshop on Wireless security, 2003.

[13] K. Chang, J. Hightower, and B. Kveton. identification using accelerometers in television remote controls. In International Conference on Pervasive Computing, 2009.