International Journal of Advanced Computer Science and Information Technology (IJACSIT)
Vol. 5, No. 2, 2016, Page: 25-34, ISSN: 2296-1739

www.elvedit.com

Social mobile authentication in pervasive environment

Authors

Mohamed Es Fih *contact@esfih.com*
Faculty of computer science, Universiti Technologi Malaysia *Versoix, Switzerland*

Suhaimi Ibrahim *suhaimiutmkl@gmail.com*
Advanced informatics school, Universiti Technologi Malaysia, University *Kuala Lumpur 55200, Malaysia*

Abstract

There is a common understanding in the mobile phone industry that smartphones are now the majority type of phone in use in the market. This understanding has to be confronted to the reality on the ground especially in developing countries. Although smartphones make the majority of the current sales, there are facts that demonstrate that smartphones are not yet the predominant device. Studies have shown that Android phones are used as dumb-phones which in effect or practice makes the phones as good as featured phone. Other references give us statistics as to the sales of smartphones vs. featured phones in the last 3 years and taken into consideration that most phones are sold with a 1 to 2 years contract, and the fact that many people tend to keep the same phone for more than 2 years this study concludes that it would be wrong to build a mobile marketing strategy purely on smartphones. The important information from these facts is not a discussion about whether there are more smart phones than other types of phones but rather a more constructive discussion: How can we leverage the presence of smart phones users to enhance the authentication of non smart phone users ? Beyond the devices, such type of authentication would require a social relationship between the 2 users in order to allow the authentication. This is called a "Social authentication method". Different researchers have proposed various schemes of social authentication, some based on a token number, others on a Bluetooth connexions between the 2 users to friend's face recognition for Facebook social authentication method. In this paper we will analyze the current mobile phone authentication context as well as the current social authentication proposals. We will then introduce a novel way of social authentication which we will detail.

Key Words Mobile, ecommerce, mobile commerce, ubiquitous, pervasive

Authentication, mobile commerce, mobile banking, mobile payment.

I. INTRODUCTION

Today internet users landscape is dominated by social networks. Recent research[1] has found that an average of 75% of internet users of all ages are connected on social websites. In other words, for every 4 internet users, 3 of them have online social relations. And the number of "connected" users that interact on social network is steadily growing. Electronic social interaction seems to allow almost anybody to connect with anybody. Furthermore many social network systems, such as LinkedIn, are based on the theory of the Six degrees of separation which states that any human can be connected to an other human via a maximum of 6 steps of introductions by commonly known contacts. A study by the Facebook data team [10] has shown that in 2011 already, any given user is approximately just 4 steps away from any other user of the platform. The social networks therefore provide a certain proximity for connecting with existing and new contacts. Facebook for degrees separation According to a recent web post from "WeAreSocial" [#9], there are about 3.6 billion of unique mobile users, among which half are active smart-phone social users. Interestingly, a study [#7] about an experimentation's data set collected by 100 volunteers equipped with Bluetooth cell phones in a specific work/study environment, has shown that "friends" physically meet at least once a day in average. An interesting development is the emergence of services that extend access to social networks even for users having basic phones and no internet access. Such is the case of Fonetwish, a company that is proposing a solution to connect and manage a Facebook account via USSD (Unstructured Supplementary Service Data). Screenshot of such "non-connected" Facebook service is shown in the figure below: Facebook by Fonetwish, which runs on the USSD protocol(Fonetwish) The combination of the sheer number of socially networked individuals, the high usage of mobile phones and the extension of social networks to non connected basic phones are a good foundation to seek and build an interaction between smart-phone and non-smart phone users for the purpose of mobile social authentication for the later.

A study by the Facebook data team [10] has shown that in 2011 already, any given user is approximately just 4 steps away from any other user of the platform. The social networks therefore provide a certain proximity for connecting with existing and new contacts.

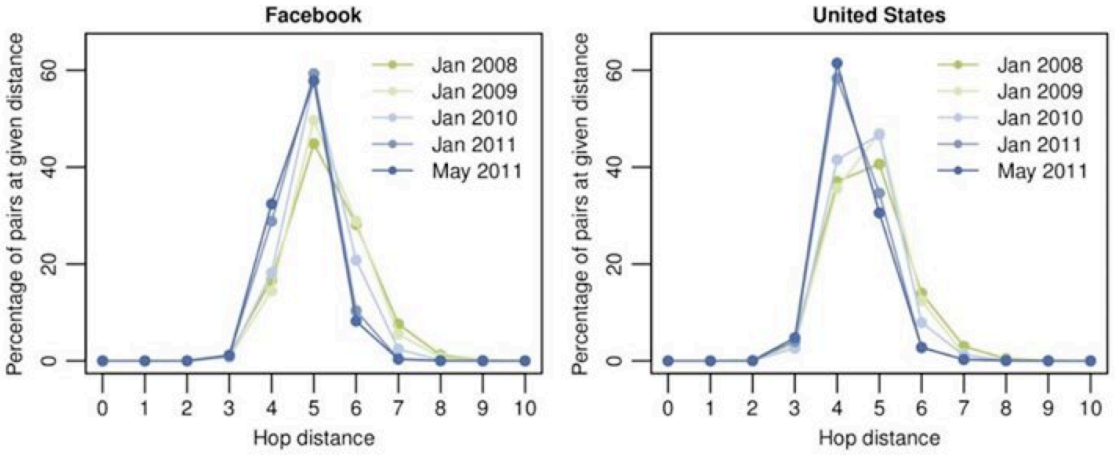

FIGURE I: Facebook 4 degrees social distance [10]

According to a recent web post from WeAreSocial [9], there are about 3.6 billion of unique mobile users, among which half are active smart-phone social users. Interestingly, a study [#encounters] about an experimentation's data set collected by 100 volunteers equipped with Bluetooth cell phones in a specific work/study environment, has shown that "friends" physically meet at least once a day in average.

An interesting development is the emergence of services that extend access to social networks even for users having basic phones and no internet access. Such is the case of Fonetwish, a company that is proposing a solution to connect and manage a facebook account via USSD (Unstructured Supplementary Service Data). Screenshot of such "non-connected" Facebook service is shown in the figure below:

FIGURE 2: Facebook via USSD [6]

The combination of the sheer number of socially networked individuals, the high usage of mobile phones and the extension of social networks to non connected basic phones are a good foundation to seek and build an interaction between smart-phone and non-smart phone users for the purpose of mobile social authentication for the later.

II. Connectivity context

There is a common understanding in the mobile phone industry that smartphones are now the majority type of phone in use in the market. This understanding has to be confronted to the reality on the ground especially in developing countries. Although smartphones make the majority of the current sales, there are references that demonstrate that smartphones are not yet the predominant and exclusive type of device and should not be taken so in any mobile marketing or mobile solution deployment strategy.

The online compendium of mobile statistics and research [12] informs us that many countries, although having a great penetration rate of mobile users, a large part of the population does not have a connected phone. In India for instance, where 62.5% of the population is equipped with a GSM subscription, only 3.4% of the population owns a 3G or 4G subscription. Likewise in Nigeria, where among the 76.3% of the population that has a GSM phone, only 7.5% have a 3G or 4G connections.

According to the 2015 ICT facts report [15], apart from the American and European continents, the remaining regions of the world have below 50% of mobile broadband users, with the African continent scoring a mere 17.4% as displayed in the figure below.

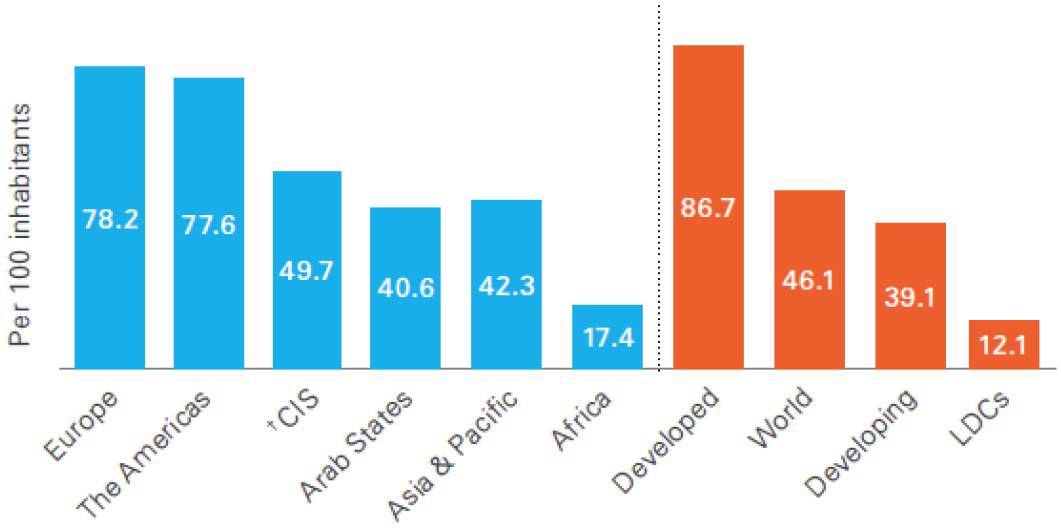

FIGURE 2: Mobile broadband subscriptions as of 2015 [15]

At this level, the 3G/4G connectivity (subscription) is not a prominent condition for most of the mobile users outside the Euro-American regions. Such a fact limits the use of advanced authentications methods which require not only smart phones, but more importantly an internet connexions.

According to the Pew Research Center [6], as of October 2014, about 80% of the American population is using their phone for sending and or receiving text messages (SMS). Whereas only 50% of them download and use Apps.

It appears from a Washington Post report [14] that even in the west, some users are intimidated by the complexity of the smart phones and or inhibited by the high commitments of 3G/4G subscription contracts. As a result Smartphones get more sophisticated, but their owners do not.

A Business Insider report [4] suggest that although Android phones greatly surpass iPhones in terms of number of holders, the Android phones are basically used as "dumb phones" meaning that a great portion of users do not buy and use Apps or access internet connected resources.

In view of the literature and reports from the industry listed above, we believe that a Mobile based project can not afford yet to build upon the assumption that the majority of users will carry smart phones and will have mobile-broadband subscriptions. However, we can agree about the mutual presence of different types of phones and connectivity levels among a given population.

And in view of the high usage of social networks across all regions and demographics, we believe that there is ground for leveraging the presence of connected smart-phone users to assist in the authentication of non-smart phones users, in a given space and time.

III. Related works

Borrowing from the Human Sciences disciplines the Social approach involves the interaction of the user with his acquaintances or social network, in order to improve his authentication to a system. This is referred to as the Fourth-Factor Authentication or somebody you know . It is a forth level added to the traditional Three-Factors Authentication: something you have (e.g a hardware token), something you are (e.g a fingerprint), and something you know e.g. a password [5].

In a very interesting study from 2006 entitled Fourth-Factor Authentication: Somebody You Know, John Brainard et Al. [2] have proposed this until-then uncommon social authentication approach. They use a process that they call Social Vouching. Vouching is a peer-level authentication in which one user, the helper, leverages his primary authenticator in order to assist a second user, the asker, to perform emergency authentication as a replacement for challenge questions or calls to a help-desk. In this particular study the solution of vouching is applied for the case when a user forgot her original password, she will call and ask her friend to vouch her (Human Social Authentication) by giving her a vouch-code that she will use to get the her new temporary password for her account. The vouching is based on a One time Password (OTP) RSA brand token, that the helper possess and uses to generate a temporary password for the asker. The graphic below explains the flow of such action, Alice being the Asker and Harry being the Helper:

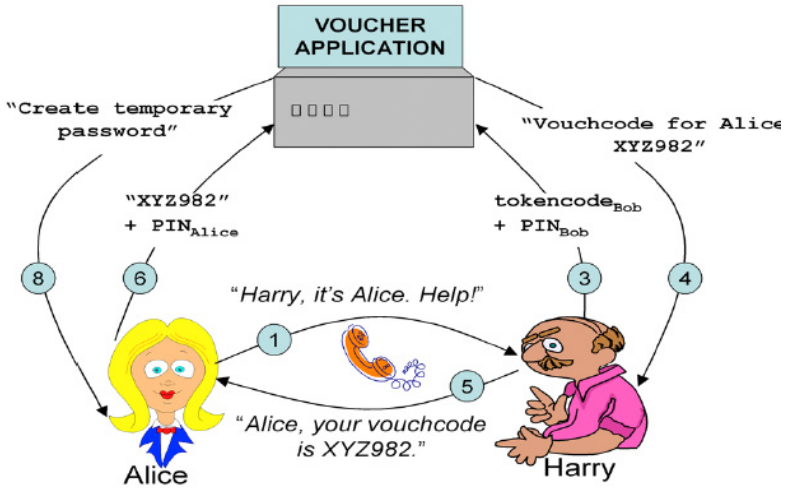

FIGURE 2: Social authentication based on OTP Token [2]

Based on the same logic [1] have proposed a Social Authentication Protocol for Mobile Phones. To authenticated a given user, their proposed system will require a vouching token from one of his social contacts who will recognize his friend (Human recognition) and prove that fact by giving a vouching token to the concerned user. This is exactly the same idea as the one defined by [2] but it has been automated between the users mobile phones, using Bluetooth sighting and Wifi connection in order to achieve the same result but without the need to make a phone call or the need to have an RSA OTP token. Given the fact that Bluetooth sighting range can be of up to 10 meters and thus can not guaranty the real physical sighting between the users, they propose to analyze the time it takes for a phone to discover and connect to the other users phone via Bluetooth and also they require the vouching user to confirm acceptation of the vouching request with his password or pin code.

Also proposed in their work is a method using phone calls to friends to obtain an authentication token. A first stage of declaring the list of friends that can vouch for a given user is required, and to enhance the security of this call based vouching they propose to record and analyze the calls patterns in order to identify potential impostors. The Reality Mining group within the Massachusetts Institute of Technology Media Lab has been recording and analyzing data on human behavior using Bluetooth Mobile Phones loaded with software that stores information about both the phones environment and its usage. In particular, the group has published a data set collected by 100 volunteers equipped with Bluetooth cell phones during the 2004-2005 academic year. One of the aim of this study was to use the Mobile Phones as a indicator or social interaction between the subjects. A large part of the study results relates to sociology but the usage of Mobile Phones makes it very relevant to our subject.

[2] have explored the behavior of participants in the same Reality Mining Project in the interest of extracting useful knowledge from social context recordings. Their definition of friends, two people whose phones come within proximity on ten or more separate days, is particularly useful to our work. Some of their relevant discoveries are: The longest period with no encounters reported is 4 hours and 24 minutes. Individuals encounter rates are reasonably predictable. Most pairs of people (71%) encounter on only one day. Encounters between friends account for two-thirds of all encounters. Such results show that friends or the social environment of a given user could be effectively available to process a Fourth-Factor Authentication. In view the predictable character of certain encounters a well designed system could even estimate and contact the nearest to be individual to invite him to help in an Authentication need. Naturally, some peoples activities are less predictable than others. In particular, he considered the entropy associated with location and daily schedules. He found that freshman undergraduates in the study had the most random schedules, followed by graduate students, then by the MIT faculty and staff who typically had low entropies. Such low entropy subjects are predictable. Using Bayes rule conditioned on the time of day and any available location information, Eagle was able to predict whether a given user will see a given subject within the hour with accuracies of up to 90%. Eagles findings are extremely valuable information for our research since our Mobile Commerce transactions can happen in environments specifically located in time and space: The markets.

[1] have studied the Feasibility of a Socially Aware Authentication scheme based on the extensive research available in the Reality mining data set (2008). They have come to the conclusion that the fourth factor element can be used as an enabling technology, facilitating the use of the traditional three factors where they are most appropriate. In their paper they confirm that based on the Reality Mining Group data, a social interaction between users for Authentication purpose is very likely to take place many times in the day as the users spend time together or interact with mostly the same people at the same places and at roughly the same time frame of a day. For terminology aspects lets name as Witness any friend or acquaintance that could help a user to proceed with a Social Authentication for a Mobile Transaction.

[12] has proposed a scheme employing a cognitive agents approach. The key advantage of this approach is that the authentication process is kept less intrusive to customer by automatically authenticating the customer using a set of metrics generated over transaction sensitivity, beliefs, and environment context. We can look at this approach in a Socio-Cognitive way and add a Social Cognitive Agent which will analyze the social context of the user.

The Social Authentication approach is slightly younger than the other approaches however it is receiving a fast growing interest especially in view of the current WEB 2.0 world where Social Networks such as Face-book and Twitter has gathered users in the number of hundred of Millions and have deployed a number of Mobile applications to keep their users hooked to their Web Social Life. This could be a gold mine for pushing Social Authentication to a mass deployment. Such assumption is confirmed by recent researches like [7] who proposes a Model to predict Social ties and their strength from the Mobile Phone call and connection history. Even more recently a trend is set such as the work of [6] who address the issues of security in the Social Mobile Applications, but more importantly they propose a protocol for a secure and private way of discovering friends who are potentially in a geographical proximity. This trend of Secure Friend Discovery could be applied for the purpose of Witness Discovery for Social Authentication purpose for instance.

IV. OUR APPROACH

Our proposed Social Authentication model uses the smart and connected phone of a third party user which is referred to by [2] as the "trustee" to enhance the authentication of the main user, referred to as the "holder". The graphic below gives a visual representation of the process, with Anna being the "trustee" and John being the "holder".

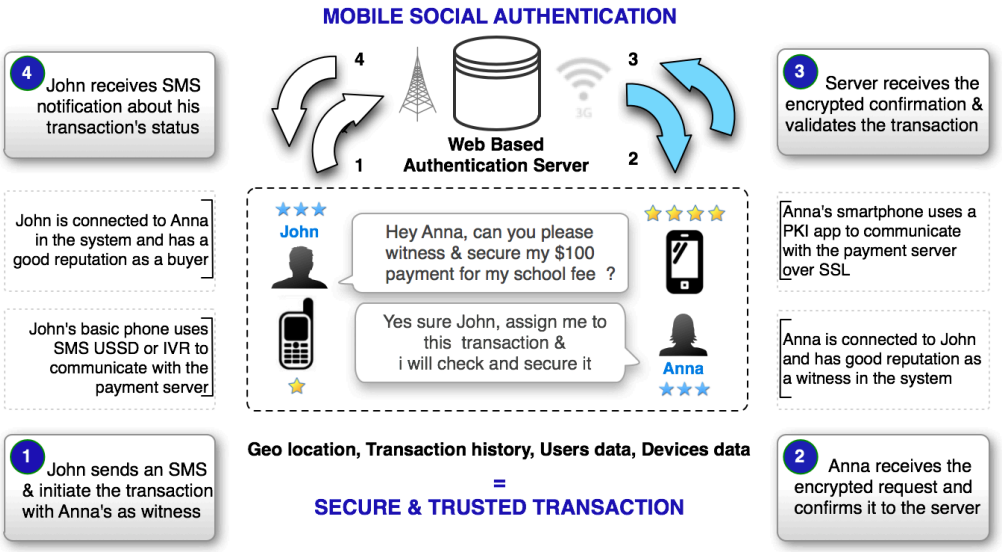

FIGURE 2: Social authentication based on OTP Token [2]

a. John via an SMS initiates the transaction request to the server nominating Anna as his witness. This initiation could also be done via an IVR call or USSD menu in order to enhance speed and security of this step. Prior to this step, John has physically met or called Anna over the phone to inform her about the amount and beneficiary information of the transaction he wants to do and the need for her to assist him in the authentication process. So Anna is aware of the amount and approximate time of the transaction.

b. The authentication server verifies John's request by analyzing the caller ID, the geo-location as well as the beneficiary of the transaction and compares it to the records to confirm the genuinely of the request. If the request is un-usual, the server will initiate an IVR call or a USSD menu to John reading back to him the received request and asking him to confirm the veracity by entering his user's pin code.

c. The server checks that John and Anna are “connected” and that Anna is indeed an appointed “trustee” of John. 2. Anna receives the encrypted request and confirms it to the server. The request that comes from the server is signed using the server's private key and encrypted with Anna's public key therefore insuring that the communication is authentic and comes in full integrity. Upon verification of the amount and destination of the payment, as well as the time window, Anna would confirm back to the server her approval as a “trustee” for this transaction to happen. Here Anna's phone will use the initial encrypted message and adds upon it her signature and encrypts it with the server's pubic key. 3. Server receives the encrypted confirmation from Anna. Server verifies the incoming confirmation using it's private key and Anna's public key

d. After deciphering the message the server compares the resulting received content with the initial request sent to Anna for her perusal. If it matches, the server approves the transaction. John receives SMS notification about his transaction's status (a) All stakeholders in the transaction receive a confirmation of the transaction using their respective communication channel with the server. John is encouraged to check with his beneficiary that the transaction was received on the other end (by phone call).

Our solution was proposed for testing and feedback to a group of specialists and was rated according to 6 criteria about which we present the results here under:

TABLE 1: Social authentication scoring by industry experts

APPROACHES	Parent Criteria	Coverage		Deployability		Security		AVERAGE SCORE
	Criteria	Mobile Type	Connectivity	Usability	Costs	Channel	Level of Security	
SOC	Social Authentication	100	100	33	100	100	67	**83**

Overall the specialists have scored our method well with a final average of 83, which is above the average of averages of all the methods (58). They also confirmed the added value it brings in terms of coverage, which other methods cold not provide especially for the segment of basic phone users without Internet connections.

V. Conclusion

Our initial proposal has shown potential by proposing the concept of leveraging a smartphone user to secure the authentication of a non-connected phone. This approach may be further experimented and future works of the author include the development of an Adroid app which will use PKI certificates for the witness/help to encrypt and sign a transaction he was requested to witness. Such organization could potentially give to our proposition the level of "non-repudiation" which is the highest level of authentication in the industry and has legal value to the same level as a paper based signature.

REFERENCES

[1] Muthucumaru Maheswaran Bijan Soleymani. Social authentication protocol for mobile phones. IEEE, 2009.

[2] John Brainard. Fourth-factor authentication: Somebody you know. CCS 06: Proceedings of the 13th ACM. Conference on Computer and Communications Security, pages 168–178, 2006b.

[3] Businessinsider.com. Google's dirty secret: Android phones are basically used as dumbphones. Technical report, Business Insider, 2014. URL http://www.businessinsider.com/apple-android-market-share-ecommerce-2014-1.

[4] Kolodgy C. Biometrics: You are your own key. InfoWorld, 2001.

[5] Pew Research Center. Social networking fact sheet, 2014.

[6] Dong et al. Secure friend discovery in mobile social networks. Technical report, IEEEE, 2011.

[7] Zhang et al. Predicting social ties in mobile phone networks. Technical report, IEEE, 2010.

[8] Simon Kemp. Digital, social and mobile worldwide in 2015. January 2015. URL http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/.

[9] Marco Rosay Lars Backstrom, Paolo Boldiy. Four degrees of separation. WebSci 12 Proceedings of the 4th Annual ACM Web Science Conference, pages Pages 33–42, 2012.

[10] A.G. Miklas. Exploiting social interactions in mobile systems. In UbiComp 2007: Ubiquitous Computing: 9th International Conference, 2007.

[11] Mobithinking, 2014. URL https://mobiforge.com/research-analysis/global-mobile-statistics-12

[12] B. Sathish Babu Pallapa Venkataram. An authentication scheme for ubiquitous commerce: A cognitive agents based approach. IEEE, 2008.

[13] Rosenwald. Smartphones get more sophisticated, but their owners not. WashingtonPost, 2014.

[14] Brahima Sanou. Ict facts and figures. The International Telecommunication Union ITU, 2015.

[15] Robert W. Reeder Stuart Schechter, Serge Egelman. It's not what you know, but who you know. a social approach to last-resort authentication. CHI09: Proceeding of the twenty-seventh

AUTHORS' BIOGRAPHY

Based in Geneva Mohamed is the eSolutions Advisor for the International Trade Center (ITC), a joint agency of the WTO and the UN. Prior to ITC Mr Es Fih has been an e-Entrepreneur and a specialist in internationalization of businesses and has assisted in the setup and globalization of about 1,800 companies in more than 40 jurisdictions. Such exposure has provided Mr Mohamed with an extensive understanding of the fiscal and legal issues required to understand and control the whole life cycle of a cross-border transaction. Having seen the "Inner & Outer" sides of the e-payment industry, as a web agency and as a compliance officer for financial institutions, Mr Mohamed is currently pursuing a PHD in Malaysia