An Adaptive Multimodal Biometric Framework for Intrusion Detection in Online Social Networks

Ja'far Alqatawna

King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan

Summary
In this paper we propose an adaptive intrusion detection framework which can be applied to various Online Social Networking Platforms (OSNPs). The idea is based on the fact that most OSNPs are extremely interactive which implies that the activities of the users in these platforms can generate substantial information which can be used to build behavioral models to continuously authenticate users and detect any intrusion attempt. The framework is adaptive in the sense it can use several sources to obtain authentication information based on the type of the device used to access a particulars OSN. These sources include keystroke dynamics, mouse dynamics, touch dynamics, and other behavioral activities.

Key words:
Intrusion Detection, Continuous Authentication, Biometrics, Multimodal, Keystroke Dynamics, Mouse Dynamics, Security Mechanism, Online Social Networks

1. Introduction

Online Social Networks (OSNs) such as Facebook, Tweeter and Instagram have become very popular and an intact part of most of our everyday actions. It seems that the instance publishing of the user generated content and the mimic of real social relationships lay behind this increased popularity. The OSNs give their users a very convenient digital medium for communication, meeting friends and sharing a large amount of information. Consequently, OSNs adopters have evolved to a significant portion of the internet users with the highest engagement rate [1]. This has opened up new opportunities that cannot be missed by businesses and/or governmental agencies. Viral marketing, customer behavior analysis and opinion mining are just a few examples of such opportunities.

Most OSNs can be characterized as a profile based service [2]. This means that the user needs to create a profile to be able to use the service. Such profile is used to store user information, interact with other users and record all his/her activities. Moreover, OSNs are extremely interactive; users post text messages, upload pictures and share links, videos and other multimedia contents. These user's activities create a huge amount of information with strong personal and behavioral characteristics which can be utilized to authenticate the user.

On the other hand, OSNs are subject to several security and privacy threats. A study showed that in the context of OSNs phishing attack by which user is tricked to share sensitive information is four times more effective than blind attempts [3]. Although Access to the user profile is commonly controlled by some sort of password-based authentication, threats such as account/machine hijacking, Man-In-The-Middle (MITM), phishing and password guessing are prevalent[3][4][5][6]. All these threats can lead to an intrusion attack which is unauthorized access and control of user profile and its related information. This encourages researchers to investigate more effective methods to protect OSNs.

In contribution to this domain, we suggest a multimodal biometric intrusion detection framework for OSNPs. In this framework, a profile-based intrusion detection approach is combined with several continuous biometric authentication functions including keystroke, mouse and touch dynamics. Proper implementation of such framework would increase the accuracy of intrusion detection in OSNs.

The rest of the paper is organized as follow. Section 2 provides a theoretical background for the proposed framework. Section 3 presents the multimodal intrusion detection framework and its components. In section 4 we discuss some practical implications for designing and implementing the proposed framework. Conclusion and future direction are given in section 5.

2. Theoretical Background

As we have discussed in the introduction, OSNs are subject to several security threats that can lead to security intrusion which according to the RFC 2828 can be defined as "a security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so" [7]. In this section we will discuss the theoretical background of our proposed intrusion detection framework. It will cover intrusion detection, static authentication and continuous authentication.

Manuscript received April 5, 2015
Manuscript revised April 20, 2015

2.1 Intrusion Detection

Intrusion represents unauthorized access to system resources including physical access and logical access to the resources. One of the early attempts to build a model for intrusion detection was report by Denning in [8]. Denning hypothesized that security intrusion can be detected by continuously monitoring a system's logs for abnormal patterns of system usage and suggested a model included profiles for representing the behavior of subjects with respect to objects in terms of metrics and statistical models. Such models can be constructed by observing different type of metrics including event counters, interval timer and resource measure. Let us, for instance, consider a counter that counts the number of failed login attempts over a period of time. If this counter exceeds a predefined threshold, this will be considered an intrusion. In general several statically models can be used to detect intrusions:

1- **Operational Model**: for a given observation $\mathcal{X}_{1,}...,\mathcal{X}_{n}$ deciding anomalies in $\mathcal{X}_{n+1}$ can be done by comparing a new observation against a predefined limit. This is commonly known as threshold-based anomaly.

2- **Mean and Standard Deviation Model**: it can be used with event counters, interval timers, and resource measures accumulated over a fixed time. The model assumes that all we know about $\mathcal{X}_1,\ldots,\mathcal{X}_n$ are mean and standard deviation:

$$\bar{x} = \sum_{i=1}^{i=n} x_i \qquad (1)$$

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{i=n}(x_i - \bar{x})^2} \qquad (2)$$

Anomalies in $\mathcal{X}_{n+1}$ occur if it falls outside a confidence interval that is (d x σ) from the mean for some parameter *d*.

3- **Multivariate Model**: very useful to correlate two or more variables which can give greater confidence in defining abnormalities and detecting intruder.

4- **Markov Process Model**: a transition matrix can be generated to characterize the transition probabilities between state variables. A new observation is considered anomaly if its probability as determined by the previous state and the transition matrix is too low.

5- **Time Series Model**: can be used to detect abnormal timing, for instance, evens that take place very fast or very slow.

Anomaly Detection and Signature Detection are two general approaches applied in several intrusion detection methods [9]. Statistical anomaly detection can either threshold detection or profile based. In the threshold detection a limit is defined for the frequency of particular events independently from the user. On the other hand, the profile based detection focuses on user's activities to develop a behavioral model that uniquely defines the user. In signature detection, rules which represent attack patterns are defined and used to check if a given behavior represents an intrusion attempt.

OSNs can be characterized as a profile based service. Users' profiles generate substantial information which can be used to build behavioral models to characterize individual user's behavior and detect any intrusion attempt. Therefore, Profile based intrusion approach will be more appropriate for the proposed framework.

2.2 User Authentication

According to the RFC 2828 authentication is defined as the process of verifying an identity claimed by or for a system entity [7]. When an entity presents an identifier to the security system, the system will request authentication information which represents a binding between the identified and the entity. Authentication is either static or dynamic. The two approaches are discussed below.

2.2.1 Static Authentication

Static authentication is performed one time at the login stage. The authentication information is commonly based on something the user knows such as password, PIN Code or answer to a secret question. However, this traditional authentication method is subject several security attacks [10]. For instance, a study conducted by [11] showed that users are likely to choose very short (1-5 characters) password; this allows attacker to exhaustively test all possible passwords. Moreover, the same study showed that users tend to choose guessable and dictionary words such as their names, birthdates and place names which are

easily breakable using simple dictionary attack. The limitations of password-based authentication method have encouraged the development and the adoption of other authentication means such as such as biometric authentication and token-based authentication. These methods are either used separately or combined with a password mechanism to achieve multifactor authentication.

2.2.2 Continuous Authentication

As traditional static authentication is only performed at a login stage which leaves the system without a security control to verify the user identify during his active session. This have encouraged many researchers to look for innovative methods to continuously verify user identity [12][13][14][15]. The basic idea here is to collect real time authentication information from the user and constantly use this information to re-verify his claim identity. Many behavioral biometrics can be used to acquire such authentication information [12]. The behavioral biometrics utilized in the proposed framework will be discussed in the next section.

2.2.3 Biometric Authentication

Biometric authentication depends on the fact that humans can generate authentication information from a set of unique biological characteristics that they have in their bodies. These include static biometrics such as fingerprint, retinal pattern, iris, and hand geometry; and dynamic characteristics such as voice, hand writing, and keystroke pattern. The advantage of such method is that it does not depend on a something that the user should remember (e.g. Password or PIN) or a something the user should have (e.g. smartcard or token). However, some biometrics authentication methods require an extra hardware and their cost is not justifiable for large scale deployments.

Among the promising biometrics methods which can be applied for the purpose of continuous authentication are keystroke dynamics, mouse dynamics and touch dynamics. These are discussed below:

Keystroke Dynamics: Biometric authentication based on Keystroke dynamics has recently started to gain the attention of many researchers because it represents a cost-effective password-free authentication mechanism which does not required additional hardware [16][17][18]. The method depends on the rhythm of individual keyboard typing which represents a unique and a robust biometric measure. The most common utilized keystroke features are the time a key is pressed (dwell time) and the time between “key up” and “key down” (flight time). In some cases these features are combined with the pressure generated while pressing the keyboard buttons to increase the accuracy of identification, however, such approach requires additional hardware which could prevent the wide spread use of this authentication method.

Mouse Dynamics: Authentication using the patterns of mouse movements and events is another unobtrusive biometric modality that does not require complicated infrastructure [19]. Ahmad [20] discussed several mouse actions that can be used to extract identification features; these include mouse movement, drag and drop, point and click and silence. These actions can be described using properties such as movement direction, duration, traveled distance.

Touch Dynamics: With the emergence of smart devices that are fitted out with a touch screen; touch dynamics can be an alternative to keystroke dynamics and mouse dynamics [21][22][23]. In additional to the timing features that are commonly used in keystroke dynamics, pressure and size have been suggested to be used in touch dynamics authentication system [24]. Sayed et al. [12] have suggested that touch screen gestures such as flicks, scrolls, taps, pinch and zoom can be used to create a user behavioral model. They have also pointed that these actions can be characterized using properties such as speed, direction, acceleration and pressure.

3. Proposed Intrusion Detection Framework

In this section we will present our proposed intrusion detection framework which can be applied to various online social network platforms (OSNP). The idea is based on the fact that most OSNPs are extremely interactive which implies that the activities of the users in these platforms can generate substantial information which can be used to build behavioral models to continuously authenticate users and detect any intrusion attempt.

A typical OSNP is subject to intrusion because it verifies user identity at the login stage only. This leaves the users account vulnerable to several security threats including session hijacking, machine hijacking, phishing and password guessing. Such situation is illustrated in figure 1.

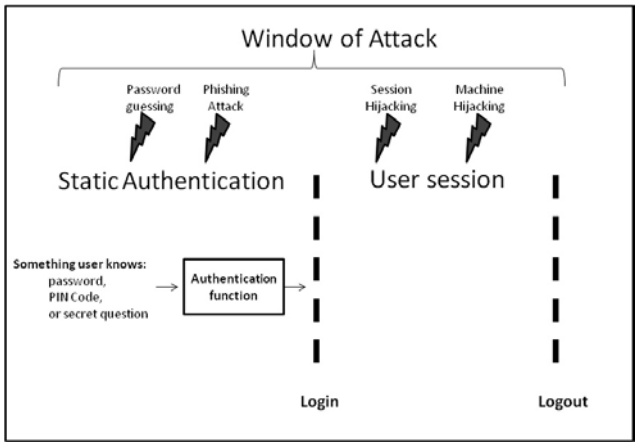

Fig 1: A typical OSNP which is vulnerable to several security threats.

To overcome the weaknesses of the above OSN, our framework applies the concept of defense-in-depth which suggests that multiple security mechanisms should be layered; hence, if one security layer fails the system will not be compromised. Therefore, the framework combines Profile-based Anomaly Detection with two types of user authentication techniques; a typical static authentication function at the login stage (e.g. using something a system user knows such as password, PIN code or secret question) and a set of continuous authentication functions during the user's active session. See figure 2 and figure 3.

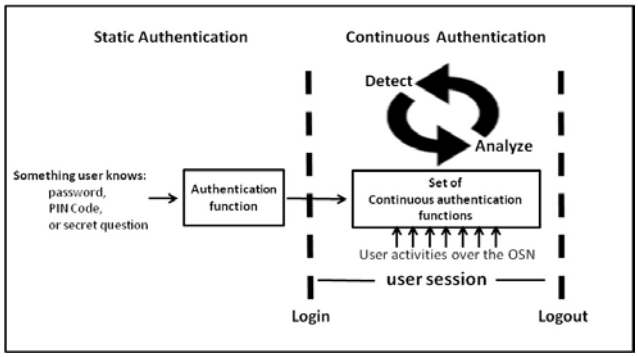

Fig2: Monitoring user behavioral and continuously authenticate him to detect any intrusion attempt.

The framework is adaptive in the sense it can use several sources to get authentication information based on the type of the device used to access a particulars OSN. These sources include keystroke dynamics, mouse dynamics, touch screen dynamic, and other behavioral activities. The framework has four components: ***Profile-based anomaly detector, user devise detector***, ***static authentication function***, and set of ***biometric continuous authentication functions***. The aforementioned components are shown in figure 3 and will be discuss in the following subsections.

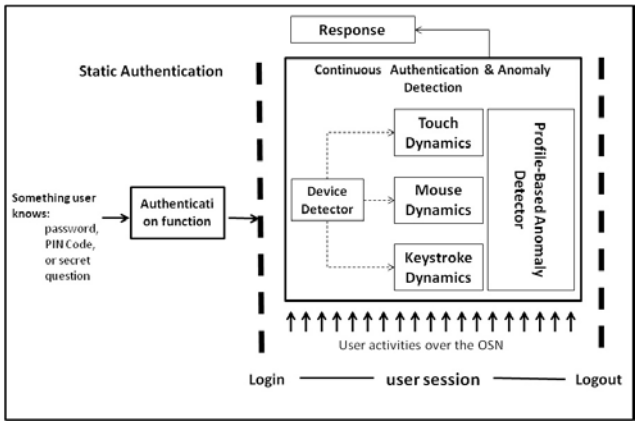

Fig 3: Framework Components.

3.1 Profile-based Anomaly Detector

Most OSNPs are profile based, which means that a user needs to register to the particular OSNP in order to use it. The created profile represents a node in the OSN and it is the primary way to communicate with other profiles in that OSN. All the activities of the user are generated inside this profile and as OSNPs are extremely interactive we expect substantial amount of information that can be use to characterized the user behavior. The Profile-based Anomaly Detector will utilize this profile to characterize the normal individual user behavior by analyzing his past activities and then detect any significant deviations which might represent an intrusion. Several statistical metrics can be use to model the user behavior, for instance, counter of several activities such as login and logout over a period of time or time interval between two related events.

3.2 User Device Detector

User device detector is responsible for detecting the type of the device a particular user is using to access his profile and choosing the appropriate continuous authentication accordingly. While users may access their OSNs using different devices, some of the continuous authentication functions might not be available. If the user accesses his profile from a personal computer, the keyboard and the mouse will be available and can be utilized. However, with the widespread of the Personal Digital Assistant (PDA) such as smart phones and tablets, only a touch screen will be available. Therefore, the user device detector gives the framework an adaptability which applies the principle of defense in depth in a dynamic way.

3.3 Static Authentication Function

This function represents the first line of defense and it is a typical security mechanism in any OSNP. For the sake of simplicity and cost cutting, such component is usually realized through something the user knows such as password, PIN code or secret question. However, extra care should be given to this mechanism as it is vulnerable to many security attacks such as password guessing, social engineering and phishing. Several countermeasures can be applied to strengthening the password based authentication including strong password policy to define the password structure and limit the number of login attempt, proactive password checking and educating the users.

3.4 Continuous Authentication Functions

While static authentication verifies the user identity at the login stage only, the risk of intrusion is still there. One possibility is that the user ID and password are in fact stolen which cannot be detected by the static authentication method. Moreover, the user session might be hijacked, for instance, by attacker who managed to get the session ID by exploiting Cross-Site Scripting (XSS) attack which is very common over many OSNPs. Also, intrusion can simply take place if the user keeps his device unattended while logged into his profile, the attack which is commonly known as machine hijacking. The proposed framework deals with these threats by enforcing several biometric and continuous authentication functions which are selected dynamically based on the type of the device used to access the user profile. These functions are described in the following subsections.

3.4.1 Keystroke Dynamics

Many user activities over the OSNs require inputting a text which in many cases comes from a physical keyboard. Activities such as entering the password at the login stage, posting a massage in the user profile, commenting on other user messages and chatting with friends all require typing. These activities generate typing patterns which are unique to each user and hold identification qualities. Modeling user's typing rhythm on the keyboard can be used to continuously authenticate the user and detect intruders. Features such as pressing time, latency between key presses can be used to build keystroke model. For the proposed framework to utilize keystroke dynamics as a continuous authentication method, OSN's users will be ask at the registration phase to provide several typing patterns to allow the system to build authentication model and train appropriate classifier. Once this achieved, the classier can be used during the active user session to detect any imposter.

3.4.2 Mouse Dynamic

Another source of biometric authentication information is the mouse dynamics which represent the various mouse's movements and activities perform by the user and can be used to uniquely identify him. Whenever the user uses a laptop or a PC to access his profile in a particular OSN, part of his activities will be generated using the mouse. Mouse features such as clicks, drag and drop, movement coordinates and speed can be used to model the user behavior and then continuously authenticate him.

3.4.3 Touch Dynamics

With increased popularity of the touch screen devices especially smart phones, large segment of OSN's users are using these devices to access their profiles. In such cases physical keyboard and mouse will not be available and cannot be used for authentication. However, the user's activities using the touch screen can be collected and used to generate authentication model. The user model can be created from the touch keyboard stroke, or screen gestures such screen flicks, scroll, taps, pinch and zoom.

4. Practical Implications

Intrusion Detection Systems (IDSs) usually face an accuracy problem. This is due the overlap between the legitimate user behavior and the intruder behavior [9]. The IDS accuracy can be measure in term of *false positive rate* (FPR) which represents the rate of legitimate user identified as intruders and *false negative rate* (FNR) which represents the rate of intruders identified as legitimate users. As show in figure 4, a loose interpretation of the intruder behavior will increase FPR, on the other hand, a tight interpretation will lead to higher FNR.

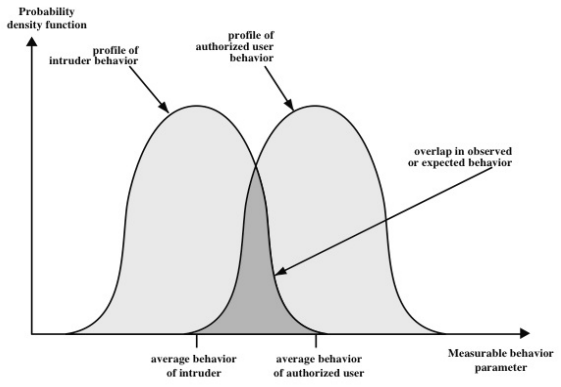

Fig 4: Profiles of behavior of intruders and authorized users [9].

Similarly biometric authentication methods have accuracy problem. This due to the fact that the bio-template generated by the user for authentication might not exactly the same as bio-template generated at the enrollment stage. Therefore, the system uses a matching score that quantifies the similarity between the two templates. As shown in figure 5, selecting the decision threshold affects both FPR and FNR.

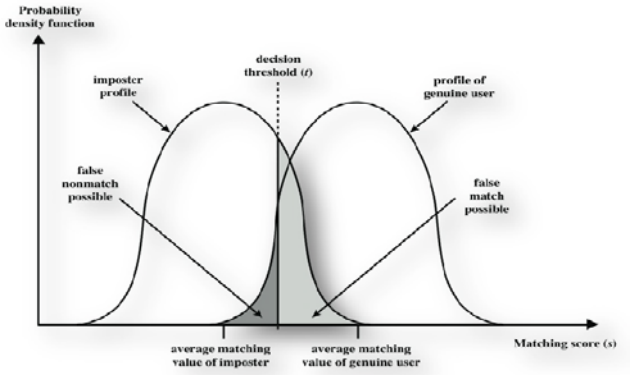

Fig 5: Profiles of biometric characteristic of an imposter and an authorized user [9].

Bailey et al. [25] argued that biometric authentication accuracy rates are worse than traditional authentication methods. They suggested a system that combines user data from keyboard, mouse, and graphical user interface interactions. Their results showed that combining the modalities increases the accuracy of authentication. Fridman et al. [26] pointed that some biometrics may provide more data than other; therefore, they suggested the use of multimodal continuous authentication where several classifiers fused together which would provide accrue and robust verification.

In our proposed framework profile-based intrusion detection combined with several continuous authentication functions including keystroke, mouse and touch dynamics which would increase the accuracy of the detection.

5. Conclusion and Future Directions

Users' profiles over OSNPs are subject to intrusion because static authentication is the only security control employed by these platforms to verify user identity. While security check is only perform at the login stage, this control leaves the users' accounts vulnerable to several security threats including session hijacking, machine hijacking, phishing and password guessing. To overcome these security issues we proposed a multimodal biometric intrusion detection framework for OSNPs. The framework components were discussed along with its practical implications.

A possible future work is to test the applicability of the proposed framework in a particular OSNP such as Tweeter or Facebook. This will require analyzing user activities and profiles over the selected OSNP to identify the set of features that can be used to build the profile-based anomaly detection components. Another future direction is to test a several combinations of continuous authentication functions to check which combination will give better detection rate.

References

[1] Sadovykh, V., Sundaram, D., & Piramuthu, S. (2015). Do online social networks support decision-making?. *Decision Support Systems*, *70*, 15-30.

[2] Youssef, B. E. (2014). ONLINE SOCIAL NETWORK INTERNETWORKING ANALYSIS. *International Journal of Next-Generation Networks*, *6*(2).

[3] Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2011). Security issues in online social networks. *Internet Computing, IEEE*, *15*(4), 56-63.

[4] Kumar, D. V., Varma, P., & Pabboju, S. S. (2013). Security issues in social networking. *International Journal of Computer Science and Network Security*, *13*(6), 120-124.

[5] White, J., Park, J. S., Kamhoua, C. A., & Kwiat, K. A. (2014). Social network attack simulation with honeytokens. *Social Network Analysis and Mining*, *4*(1), 1-14.

[6] A Obiniyi, A., N Oyelade, O., & Obiniyi, P. (2014). Social Network and Security Issues: Mitigating Threat through Reliable Security Model. *International Journal of Computer Applications*, *103*(9), 1-7.

[7] Shirey, R. (2000). RFC 2828: Internet security glossary. *The Internet Society*.

[8] Denning, D. E. (1987). An intrusion-detection model. *Software Engineering, IEEE Transactions on*, (2), 222-232.

[9] Stallings, W., & Brown, L. (2008). Computer Security. *Principles and Practice*.

[10] Yan, J. (2004). Password memorability and security: Empirical results. *IEEE Security & privacy*, (5), 25-31.

[11] Klein, D. V. (1990, August). Foiling the cracker: A survey of, and improvements to, password security. In *Proceedings of the 2nd USENIX Security Workshop* (pp. 5-14).

[12] Syed, Z., Banerjee, S., & Cukic, B. (2014). Continual authentication. *Biometric Technology Today*, *2014*(6), 5-9.

[13] Mondal, S., & Bours, P. (2015). A computational approach to the continuous authentication biometric system. *Information Sciences*, *304*, 28-53.

[14] Roth, J.; Xiaoming Liu; Metaxas, D., "On Continuous User Authentication via Typing Behavior," *Image Processing, IEEE Transactions on* , vol.23, no.10, pp.4611,4624, Oct. 2014

[15] Xiaojun, C., Zicheng, W., Yiguo, P., & Jinqiao, S. (2013). A Continuous Re-Authentication Approach Using Ensemble Learning. *Procedia Computer Science*, *17*, 870-878.

[16] Monaco, J. V., Bakelman, N., Cha, S. H., & Tappert, C. C. (2012, August). Developing a keystroke biometric system for continual authentication of computer users. In *Intelligence and Security Informatics Conference (EISIC), 2012 European* (pp. 210-216). IEEE.

[17] Deng, Y., & Zhong, Y. (2013). Keystroke dynamics user authentication based on Gaussian mixture model and deep belief nets. *International Scholarly Research Notices*, *2013*.
[18] Teh, P. S., Teoh, A. B. J., & Yue, S. (2013). A survey of keystroke dynamics biometrics. *The Scientific World Journal*, *2013*.
[19] Shen, C., Cai, Z., Guan, X., & Maxion, R. (2014). Performance evaluation of anomaly-detection algorithms for mouse dynamics. *Computers & Security*, *45*, 156-171.
[20] Ahmed, A. A. E., & Traore, I. (2007). A new biometric technology based on mouse dynamics. *Dependable and Secure Computing, IEEE Transactions on*, *4*(3), 165-179.
[21] Liu, C. L., Tsai, C. J., Chang, T. Y., Tsai, W. J., & Zhong, P. K. (2015). Implementing Multiple Biometric Features for a Recall-Based Graphical Keystroke Dynamics Authentication System on a Smart Phone. *Journal of Network and Computer Applications*.
[22] Chang, T. Y., Tsai, C. J., & Lin, J. H. (2012). A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *Journal of Systems and Software*, *85*(5), 1157-1165.
[23] Fathy, M. E., Patel, V. M., Yeh, T., Zhang, Y., Chellappa, R., & Davis, L. S. (2014). Screen-based active user authentication. *Pattern Recognition Letters*, *42*, 122-127.
[24] Tasia, C. J., Chang, T. Y., Cheng, P. C., & Lin, J. H. (2014). Two novel biometric features in keystroke dynamics authentication systems for touch screen devices. *Security and Communication Networks*, *7*(4), 750-758.
[25] Bailey, K. O., Okolica, J. S., & Peterson, G. L. (2014). User identification and authentication using multi-modal behavioral biometrics. *Computers & Security*, *43*, 77-89.
[26] Fridman, L., Stolerman, A., Acharya, S., Brennan, P., Juola, P., Greenstadt, R., & Kam, M. (2014). Multi-modal decision fusion for continuous authentication. *Computers & Electrical Engineering*.

Ja'far Alqatawna is an Assistant Professor at King Abdullah II School for Information Technology, University of Jordan. He received his B.Eng degree in Computer Engineering from Mu'tah University, Jordan, followed by MSc. in Information and Communication Systems Security from The Royal Institute of Technology (KTH), Sweden. In 2010 He has been awarded his PhD. Degree in Computer Information Systems with specialisation in Information Security and e-Business from Sheffield Hallam University, UK. He was part of research project for investigating XACML as a policy language for distributed networks at Security, Policy and Trust Lab (SPOT) of the Swedish Institute of Computer Science (SICS), Sweden. His current research interests are in the field of e-Business security in which he try to look for multi-dimensional approaches that go beyond the technical dimension in order to develop trustworthy e-Business environment.