Towards a Context Aware Modeling of Trust and Access Control Based on the User Behavior and Capabilities

Abdallah Mhamed[1], Meriem Zerkouk[2], Anas El Husseini[1,3], Belhadri Messabih[2], and Bachar El Hassan[3]

[1] Institut Mines-Télécom / Télécom SudParis - CNRS UMR 5157 SAMOVAR, Evry, France
abdallah.mhamed@it-sudparis.eu
[2] University of Sciences and Technology Oran, Algeria
{zerkouk.meriem,bmessabih}@gmail.com
[3] Lebanese University, LASTRE Lab., Tripoli, Lebanon

Abstract. During the last decade, several context based security models has been proposed to take into account the user behavior aspect. However the studied context is mainly related to device and spatio-temporal features, which may led to a weak and inappropriate contextual modeling. By using the huge and various contextual data issued from the sensors deployed in smart environments, our objective is to provide a security framework suitable for dependant people. This paper shows our approach to model both trust and access control based on the deduced user behavior and capabilities.

Keywords: Smart environment, trust evaluation, authentication, access control, device usability, user behavior, user capability, context awareness.

1 Context, Motivations and Challenges

1.1 Security in Smart Environments

Pervasive systems contribute significantly to the deployment of personalized services in smart environments. When considering dependant users within their living spaces, security requirements still remain an open issue.

While pervasive environments raise new security challenges, they also bring new opportunities owing to ubiquitous technologies and ambient intelligence which provide valuable contextual information about the user and his environment.

Authentication and access control are the main security services which are required to check the identity of users and to grant access to the resources they need.

Context-aware based security is an emerging approach to deal with the new security problems introduced by the high dynamicity and heterogeneity of mobile devices that characterize pervasive and highly dynamic computing environments.

We believe that this can be really achieved owing to context awareness which allow us to benefit from sensing and mobile technologies to derive more accurate contextual data about the user profile and his environment.

J. Biswas et al. (Eds.): ICOST 2013, LNCS 7910, pp. 69–76, 2013.

1.2 User Authentication Devices

Usually the adoption of authentication devices relies on three factors [1]: effectiveness, cost and user acceptance. An underlying constraint of most existing authentication techniques is that they require the user to actively do something in order to be authenticated. When these devices are used by physical or mental impaired people, we have to consider two important additional factors:

- Usability: the ease with which people can interact with any device/technology.
- Non Intrusiveness: use in a discrete and transparent manner without any inconvenience for the user.

The various impacts of several different disabilities on the security and usability of many existing authentication means have been demonstrated in [2]. In some situations the authentication device can be considered as intrusive, and it is therefore desirable to have methods that may be applied transparently, without the need to interrupt with legitimate user activities. By using the anatomy of human head and the dynamics of human voice, the Head Authentication Technique (HAT) proposed in [3] is a non intrusive biometric technique to provide a continuous and transparent authentication.

Despite the huge previous research work, the problem of achieving adequate and effective user authentication still remains an ongoing challenge. Among the range of authentication techniques (based on secret knowledge, token or biometrics), no single method can be considered as applicable to all contexts and for all. Furthermore, the authentication process is mainly based on the provision of some credentials (PIN codes, passwords and even biometric templates) which can be forged or replayed and by the way is exposed to potential spoofing attacks.

Recently, a new approach has been emerged by using the behavioral features of users. A feasibility of having such authentication was studied by Al-Khazzar [4] who proposed an approach based on psychological mechanisms through a 3D graphical maze. A user authentication on mobile devices based on User's behavior and spatio-temporal context was adopted by Rocha [5]. A user behavioral model based on activities, environmental contexts, and user profile is proposed by Lima [6]. The continuous authentication system using behavioral analysis of users, proposed by Brosso [7] is built using the evidences of behavior to establish trust levels for a continuous authentication of the user during the application software.

2 Our Context Aware Framework

A pervasive environment is characterized by a richness of contexts in which users, devices and agents are mobile. The availability of contextual data provided by sensors can be used to extract behavior patterns of the mobile entities (users, devices, agents). Context awareness can bring a valuable help to understand the relation between users, devices and environments. Owing to the big range and variety of sensors deployed, the pervasive space can provide a very rich and valuable information set which can be used to derive the "dynamic profile" of users (social relationship and user behavior).

By combining the dynamic profile with the user capabilities, our research strategy is motivated by the following challenging tasks:

1°) to identify users discreetly and transparently,
2°) to provide an adaptable service of users based on their capabilities and behavior to ensure more personalization and suitable security.

The objective of our approach is the design and implementation of a context aware framework illustrated in Figure 1.

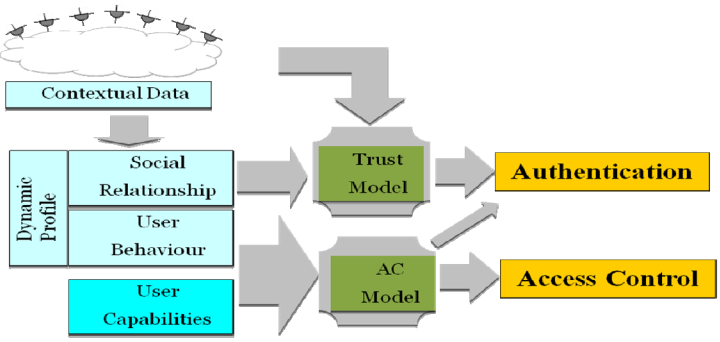

Fig. 1. Our Context Aware framework

The contextual data collected from sensors are used to derive user behavior patterns which will contribute to set up an implicit authentication process without using any intrusive device (Figure 2).

By the way, the user behavior can be combined with the user capabilities to build a dynamic trust and access control models.

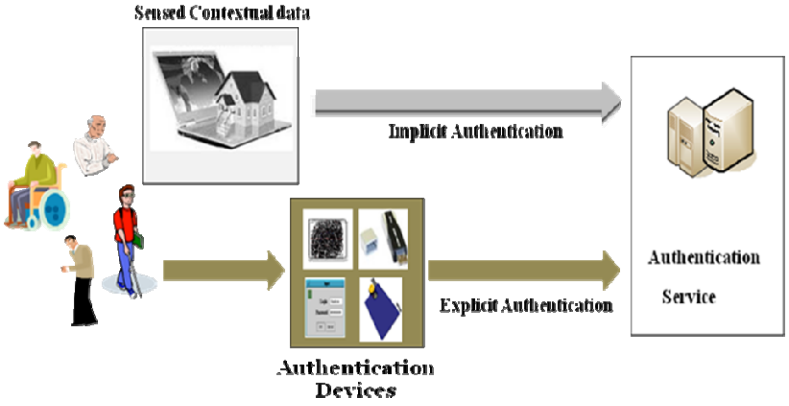

Fig. 2. A transparent authentication process

2.1 Contextual Trust

The contextual data open new opportunities for the establishment of trust relations between communicating entities. Trust models based on user abilities, user behavior, user preferences and contextual factors must be explored to improve trust models.

The recent literature brings some interesting ideas going towards the new vision of trust modeling and its contribution to built new context aware security frameworks. To handle the dynamic and variable nature relationships in pervasive environments, some new properties of trust were considered in [8]. Boukerche et al. proposed a novel trust evaluation prototype in which the updating process of trust value relies on the cooperation level of nodes. Honest behavior will be rewarded while malicious behavior will be penalized [9]. According to Tanveer Zia et al, the recent trust models migrate from a single dimension to multi-dimension trust calculation models by merging the history, the experience and the context of related entities [10]. The given review of trust models show that some basic elements of context such as time and context similarity are considered. However none of the existing works gives a common and unified consideration on all factors that influence the trust.

We have proposed a context-aware trust model based on user behavior by taking into consideration both the user profiles and context attributes [11]. We introduced a protection against the malicious threats affecting the trust evaluation process. We also improved the accuracy of trust metrics based on the right human behavior in situations that require trust.

2.2 Contextual Access Control

For pervasive systems, the access control is handled by the development of context aware based access control models which rely on context data to assign the permission to the users (roles) in the right situation which makes the model dynamic according to the change of context over the time. Extended Role Based Access Control (RBAC) models [12] are based on context awareness. Their aim is to improve RBAC by assigning the right access more dynamically. The access is based on the validity of the context by adding to RBAC a single contextual data which is spatial, temporal or environmental [13, 14, 15]. According to our literature review the current access control policies don't take into account the user impairments nor the behavior of users.

We have proposed a context-aware access control model based on user behavior and capabilities [16]. The model is based on ontology learning, enriching and evolution which support continuous learning of behavior and capability patterns.

3 Trust Modeling

The main features of our proposed trust model [11] are given below:

- It combines many of the good features presented in other models, like trust recommendations and the idea of trust distribution, and trust per service concept;

- It was essentially made for mobile devices with limited resources, which means it requires less overhead and uses less bandwidth;
- It combines the concept of trust evaluation and risk assessment,
- It ensures preserving the privacy of the users and devices, without disclosing personal information about users, like time of usage and location;
- It introduces the new concept of Judgment;
- It deploys a new scheme to detect any abnormal behavior of the nodes,
- It can provide different levels of trust based on requested services.

3.1 Trustworthiness

The calculation of a trustworthiness value includes the direct trust and the indirect trust. Direct trust is what is commonly called "Risk Assessment". It is used for dealing with newcomers which the entity has not yet any past records of trust evaluation. In case where trust is service-dependent, we added a multiplicative factor to the number of negative actions. This factor is called the Security Action Coefficient (***SAC***). This coefficient refers to the security level of a service.

Direct trust is obtained using:

$$DT = \frac{\Sigma PA_i}{\Sigma PA_i + SAC \times \Sigma NA_i} \ .$$

$\boldsymbol{PA_i}$ is the number of positive actions done by the given node and noticed by node $\boldsymbol{i}$. $\boldsymbol{NA_i}$ refers to the number of negative actions.

The indirect trust is given by: $IT = \frac{\Sigma Tw_i \times J_i}{n}$.

$\boldsymbol{Tw_i}$ and $\boldsymbol{J_i}$ are the trustworthiness and judgment values of the node $\boldsymbol{i}$.

The net trustworthiness is a combination of direct and indirect trust values:

$$Tw = \alpha_{DT} \times DT + \alpha_{IT} \times IT \ .$$

where $\boldsymbol{\alpha_{IT}}$ is the indirect trust coefficient given by:

$$\alpha_{IT} = \frac{TS_{self}}{TS_{self} + \Sigma \frac{TS_i}{n_{recomm}}} \times \frac{\Sigma J_i}{n_{tot}} \ .$$

and $\boldsymbol{\alpha_{DT}}$ the direct trust coefficient is given by: $\alpha_{DT} = 1 - \alpha_{IT}$.

$\boldsymbol{TS_{self}}$ refers to the timestamp of the trust value of the node itself, while $\boldsymbol{TS_i}$ denotes the timestamp of the trust value of the node $\boldsymbol{i}$.

$\boldsymbol{n_{tot}}$ is the total number of nodes in the network, whereas $\boldsymbol{n_{recomm}}$ is the number of nodes that responded with recommendations.

3.2 Judgement

Judgment is one of the new features introduced that aims to imitate the human behavior in a technical approach. The judgment ability is represented by the overall

experience of dealing with the node in question. That experience includes both the total number of control messages exchanged and the total number of actions whether positive or negative. The two judgment values related to the number of actions (J_A) and messages (J_M) exchanged are given below:

$$J_A = \frac{\Sigma A_i}{Maximum\ \ A} \qquad J_M = \frac{\Sigma\ messages_i}{Maximum\ \ messages}$$

At last, the overall judgment value is:

$$J = J_A \times J_M$$

4 User Behavior and Capability Based Control Access

We have proposed a new User Behavior and Capability based Access Control Model [16]. The proposed model has the following components: Users (*U*), Services(*S*), Devices (*D*), Environment (*Env*) and permission (*P*). Each entity is described with a set of attributes:

Entity = {att$_1$, att$_2$, …., att$_n$}.

Policy: <(U, S, D, Env), P>

where *P={permit, deny, obligation or recommendation}.*

Authorization decision is assigned according to the combination of all the entities.

We provide and construct an intelligent security policy specification following the main four steps:

1°)Behavior tracking: to collect the data about the person, the environment and the activities.

2°)Profile capability identification: According to the collected data, we define some discriminate factors to distinguish between the different behavior patterns. The next task consists to authenticate the users then to analyze the contextual data for attributing to each user included in behavior classes the right decision.

3°)Access control policy modeling and reasoning: It consists to represent data on standard format by using ontologies to ensure the interoperability, the sharing and the reuse of security policy. The current captured data and the inference rules are stored in the database to deduce a new knowledge and to check the consistency of the ontology.

4°) Evolving: A learning process is a continuous monitoring data provided over the time from different sources in order to update the behavior classes.

The design of our proposed access control model is an ontology-learning and evolving security policy for predicting the future actions of dependent people. This is reached by reasoning about historical data, contextual data and user behavior according to the access rules that are used in the inference engine to provide the right service according to the user's needs.

Our ontology model was built using three case studies: deaf person, blind person, Alzheimer person. We have shown the efficiency of an adaptive access control and

the role of tracking the behavior, profile capability in such adaptive access control system. The access control is ensured according to the assignment of the users to behavior and capability groups then we check the valid time, location, device, service and environment to assign the “permit” or “deny” decision.

5 Conclusion

The proposed trust model has been implemented using Java language and Eclipse IDE platform. A server in our architecture is the device that provides the service to other nodes. It can be a computer, an RFID reader, or even a sensor. Our model will be tested on Android mobile phones using Android SDK tools in Java. A real evaluation will takes place in a residence dedicated to physically impaired people.

The proposed access control model is based on the semantic web technologies (OWL language, SWRL for rule specification and SPARQL to query the ontology). The ongoing work is aiming to deeply explore the behavior clustering and classification tools and to improve our sensing data base. We are planning to deploy our model in Tele-monitoring health care platform to provide automatic assistance for dependent and frail people living alone.

References

1. Furnell, S.M., Dowland, P.S., Illingworth, H.M., Reynolds, P.L.: Authentication and Supervision: A survey of User Attitudes. J. Computers & Security 19(6), 529–539 (2000)
2. Helkala, K.: Disabilities and Authentication Methods: Usability and Security. In: 7th International Conference on Availability, Reliability and Security, pp. 327–334 (2012)
3. Rodwell, P.M., Furnell, S.M., Reynolds, P.L.: A Non-Intrusive Biometric Authentication Mechanism Utilizing Physiological Characteristics of the Human Head. J. Computers & Security 26, 468–478 (2007)
4. Al-Khazzar, A., Savage, N.: A2BeST: Graphical Authentication Based on User Behaviour. In: International Conference on (2010)
5. Rocha, C.C., Lima, J.C.D., Dantas, M.A.R., Augustin, I.: A2BeST: An Adaptive Authentication Service Based on Mobile User’s Behavior and Spatio-Temporal Context. In: The International Conference on, pp. 771–774. Springer, Heidelberg (2011)
6. Lima, J.C.D., Rocha, C.C., Augustin, I., Dantas, M.A.R.: A Context Aware Recommendation System to Behavioral Based Authentication in Mobile and Pervasive Environments. In: 9th International Conference on Embedded and Ubiquitous Computing, pp. 312–319 (2011)
7. Brosso, I., La Neve, A.: A Continuous Authentication System Based On User Behavior Analysis. In: The International Conference on Availability, Reliability and Security, pp. 380–385 (2010)
8. Ahamed, S.I., Haque, M.M., Hoque, E., Rahman, F., Talukder, N.: Design, Analysis and deployment of omnipresent Formal Trust Model (FTM) with trust bootstrapping for pervasive environments. J. of Systems and Software 83(2), 253–270 (2010)
9. Boukerche, A., Yonglin, R.: A secure mo bile healthcare system using trust-based multicast scheme. J. of IEEE on Selected Areas in Communications 27(4), 387–399 (2009)

10. Zia, T., Islam, M.Z.: Communal Reputation and Individual Trust (CRIT) in Wireless Sensor Networks. In: International Conference on Availability, Reliability and Security, pp. 347–352 (2010)
11. El Husseini, A., M'hamed, A., El-Hassan, B., Mokhtari, M.: Trust-based Authentication Scheme with User Rating for Low-ressource Devices in Smart Environments. J. Personal and Ubiquitous Computing 10(1), 21–27 (2012)
12. Asmidar, A., Roslan, I., Jamilin, J.: A Review on Extended Role Based Access Control (E-RBAC) Model in Pervasive Computing Environment. In: IEEE International Conference on Intelligent Pervasive Computing, pp. 533–535 (2009)
13. Sadat, E.S., Amini, M., Zokaei, S.: A Context-Aware Access Control Model for Pervasive Computing Environments. In: IEEE International Conference on Intelligent Pervasive Computing, pp. 51–56 (2007)
14. Yao, H., Hu, H., Huang, B., Li, R.: Dynamic Role and Context Based Access Control for Grid Applications. In: The 6th International Conference on Parallel and Distributed Computing, Applications and Technology, pp. 404–406 (2005)
15. Filho, J.B., Martin, H.: A generalized context-based access control model for pervasive environments. In: The 2nd International Workshop on Security and Privacy in GIS and LBS, pp. 12–21 (2009)
16. Zerkouk, M., M'hamed, A., Messabih, B.: A User Profile Based Access Control Model and Architecture. I. J. Computer Networks & Communications 5(1), 171–181 (2013)