Context-Based Security (and Safety) Meta-Policies for Pervasive Computing Environments: The Case of Smart Homes

Pravin Shetty and Seng Loke

School of Computer Science and Software Engineering, Monash University, Australia
{Pravin.Shetty@csse.monash.edu.au, swloke@csse.monash.edu.au}

Abstract. Context-based security is an approach for modeling adaptive security solutions based on the situation of use of the system. Security policies in this approach are not static as it used to be in traditional systems. The security actions to be taken are based on the knowledge of the combination of various factors such as the location of the user, the surroundings, time, temperature etc making the security policies more adaptive. The aim of this paper is to present security meta-policies based on an existing approach known as Contextual Graphs and the multilevel access model, which we presented in our previous paper. These meta-policies determine within what contexts actions in other policies should be taken – it is in this sense that we have the notion of other policies "embedded" within the meta-policy. Our approach can be easily used in various smart environments, even for context-aware safety meta-policies. The paper presents their use in a smart home scenario.

1 Introduction

Computers have become more pervasive and their functionality more *transparently* integrated into homes and communities. As a result, new applications have emerged making everyday living easier for people. Context based security is an emerging approach for more flexible security solutions. It aims at coping with the security problems resulting from the high heterogeneity and dynamicity of ubiquitous environments. It provides a convenient way for modeling security requirements in complex systems.

The paper presents context-based security policies for a smart home scenario using contextual graphs developed by [12] augmented with details about specific security actions which relate to other security policies. Hence, we can think of the contextual graph policy as a meta-policy. The contextual graph approach towards security policies facilitates ease of understanding and flexibility in defining security policies.

The remainder of the paper is organized as follows. Section 2 presents the concept of context-based security. Section 3 discusses the need for context-based security in a smart home environment. Section 4 describes a brief presentation of contextual graphs that will be used to model context based security. Section 5 gives an overview of basic security policies referred to from our meta-policy contextual graph. Section 6

develops a context based security meta-policy for a smart home. In section 7, related work done is discussed. Section 8 concludes the paper.

2 Context Based Security

In traditional security systems, protected resources such as documents, hardware devices and software applications follow an On/Off access policy [13]. On, allows to grant access and off for denying access [13]. This access policy is static and based on user's identity. Due to the high mobility of the pervasive systems and the heterogeneity of devices used, security policies must become more flexible in order to respond to these highly dynamic computing environments [14]. Thus, the security structure should be sensitive to the varying contexts. The figure shown below gives the idea behind context based security:

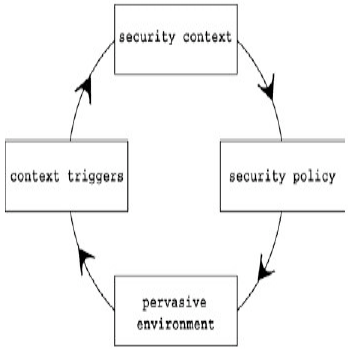

Fig.1. Context based security [5, 3]

As shown in the figure the pervasive environment is initially controlled by some security policy depending upon the initial context at that time [5, 3]. Context triggers denote the dynamic changes that occur in the environment in the course of time. These changes ultimately result in the change of the context leading to a new context. Security context denotes this new context that has to be considered while deploying new security actions as a result of the change. A security policy indicates the rules and regulations that govern who has the access and who doesn't in each type of situation. Thus, the security policy should be flexible enough to accommodate changing contexts.

2.1 Security Context

Kouadri and Brézillon [12] described the security context as: *"A set of information collected from the user's environment and the application environment and that is relevant to the security infrastructure of both the user and the application*." Thus, a security context can be thought of a combination of information at an instant of time based on which the security policies take appropriate security actions to decide the access control rights.

2.2 Context Based Security Policies

The role of a security policy is to recognize valuable system assets and clarify security responsibilities [3]. It imposes a set of requirements about the security infrastructure and defines which kind of security mechanisms need to be implemented in the form of security actions. Context-based security policies [15] aim at considering context explicitly as a guide to deduce which mechanisms to enforce in a particular situation.

3 Need For Context Based Security In Context Aware Environment Like Smart Homes

Smart home is an upcoming example of ubiquitous computing. A communication infrastructure is installed that allows the various systems and devices in the home to communicate with each other [16]. In early stages of security, the user needed to carry smart cards for authenticating himself. But with the introduction of advanced biometrics with automatic sensing capabilities there is no burden of carrying these smart cards. As each person's retina, thumbprint or voice is unique, these features are used to check the authenticity of the users.

The design of a smart home needs to take into account not only the form of the house itself but also the requirements, both generic and specific, of the people who may live in and visit the house. The security system in smart homes must be adaptive to the changing situations. The user should be given the right to formulate the security actions based on the changing context and store it in the database. Thus, the use of context-based security in smart homes is very important. It gives the security policy the flexibility to adjust its security actions according to the situational information. This prevents any unauthorized access to the devices at home. A policy can restrict access to information or resources based on several factors, including attributes pertaining to the subject, the resource or the environment [16]. For example, subjects can be classified into roles such as "resident" or "guest." Access rights can depend on the subject's classification (i.e resident), as well as on his or her actual identity (i.e parent, child etc.). Access also may be restricted based on the subject's location, or based on environmental factors such as the temperature or the time of day. The sensors sense the combination of all these factors present and the security policy generates the security action based on the rules stored in the database by the users.

4 Basic Security Policies

Mobile Ambients first proposed by Cardelli and Gordon [8] and then further extended by Bugleisi [7] and Braghin [2] are very efficient to model multilevel security issues. These three notions are very effective in providing a full proof security solution in the any computing scenario by stating various security steps to be taken in the corresponding scenario. On this basis we have in all five cases that form the basic security policies in this paper. The paper uses them in appropriate scenarios

depending on the context. Thus, the combined use of these five policies and a contextual graph representing the contexts of use of these policies provides a context based security solution in pervasive environments. This section briefly describes the five policies using ambient (representing a boundary of security restrictions) notions.

Policy1: Authenticate returning mobile agent

When a privileged process (agent or person) leaves the parent ambient (e.g., a host institution) to execute some external independent activities, it relinquishes its local privileges and authority within its bounding parent ambient and ambient community. It exits the parent and might later return to the parent ambient. At this point an ***Authentication mechanism*** is needed to check the authenticity of the returning original process. **Cardelli** and **Gordon** [8, 9] suggest that these high-level privileges must not be automatically restored to the returning agents/processes without first verifying their identity. This is to preserve the security and integrity of the ambient as well as the services and resource contained within it.

Policy2: Fire Wall Access

So if any agent/process has to enter an ambient, it has to know the name of the ambient and also posses the capability to enter in it. The functionality of firewall is achieved with the help of restriction primitives and with the help of anonymity of the ambient name. Thus without knowing the ambient name, no process or agent can go out or enter in the parent ambient. This helps in achieving protection of the resources from unwanted agents. The ambient name could be interpreted as a secret password.

Policy3: Encryption using shared keys to secure the data while communication

Cardelli and Gordon also put forth the encryption primitives to communicate between two ambients or between an ambient and a remote agent. These primitives helped in maintaining the **Confidentiality** of the message or data. Consider a Plaintext message **M**. The encryption of the plaintext message is done with the help of the encryption key **k**. The Ciphertext produced is indicated as $\mathbf{M}_{\mathbf{k}}$ [9]. A name can represent a shared key, as long as it is kept secret and shared only by certain parties. A shared key can be reused multiple times, e.g., to encrypt a stream of messages. A message encrypted under a key ***k*** can be represented as a folder that contains the message and whose label is ***k***. It is represented via the ambient **k[<M>]** [10]**.**

Policy4: Security Multi-Levels

In general, an enclosed ambient environment would typically contain numerous subambients as well as active processes, agents and information resources. These groups of subambients within an ambient may be arbitrarily nested and organised in a hierarchical structure. Ambients and processes which are at the higher level of the nested structure are responsible for managing resources which are more vital and important than those which are at lower level. In such kind of multilevel environments, it is necessary to restrict the access to the flow of information depending upon the need and the security levels. Information can only flow from lower levels of security to higher levels and not conversely. A policy for this assigns levels to users and restricts information flow among the users.

Policy5: Movement of data and entities through different communities

The multilevel security policy mandatory access control security in the boxed ambients provided restricted access to information based on the various security levels in the hierarchical levels. The access is defined by the level at which the agents are which are predetermined based on their needs. But Braghin [2] was of the view that the implementation of mandatory access control security is complex as agents and processes may move from one security level to another. The agents themselves may be confidential or may be carrying secure/confidential information. Thus there is no way of ensuring the agents that they will not be illegally attacked, accessed or executed by untrustworthy entities at the lower security levels.

The **Security Boundary** [2] concept put forth by Braghin guarantees absence of information leakage. According to this concept every high-level data or process should be encapsulated into a boundary ambient. A boundary ambient can be opened only when it is nested into another boundary ambient. A policy for this states that the protected information cannot be read without being contained within some safety boundary (e.g., physically, an item cannot be viewed in the absence of a bodyguard).

5 Contextual Graphs

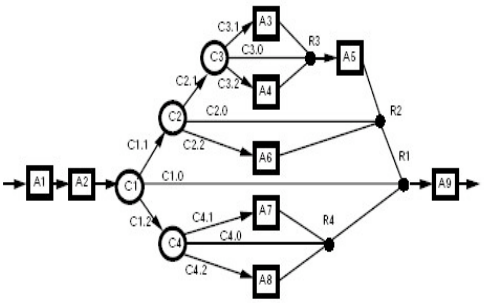

Fig.2. Contextual graph [4]

A contextual graph (CxG) allows a context-based representation of a given problem solving for operational processes by taking into account the working environment [3]. A contextual graph treats security actions to be taken in context based security as a problem solving process that allows only safe actions to be taken by the user as long as s/he interacts with the devices. Unlike decision tree, contextual graph have no decision nodes. They have "chance" nodes where a contextual element is analyzed to select the corresponding path. Also, there are no probabilities [5]. Contextual graphs are a promising approach for the modeling of context-based policies. They give a better understanding of the security actions to be taken in each situation. Contextual graphs support incremental knowledge acquisition [5]. The security administrator may easily add/modify secure paths based on new detected breaches. Thus, security policy has the capacity of evolving by accommodation and assimilation of practices [5]. Minimum number of elements has to be added to the context graph whenever a new policy is inculcated.

6 A Meta Policy Approach For Context Based Security Policies

The approach of context graph defined in the above section can be effectively used to model the security policies defined in section 4. Each of the contextual node of the context graph accounts for existence or non-existence of a single valid context. Depending upon that, various security actions that act as authentication mechanisms are taken. The combination of such existence or non-existence of a valid context along with the various security actions taken manifests the security policies, which in turn decide the access to the aspired resources. Only paths that result in the access of the resources are indicated in our approach. The unsuccessful ones depending on the policies are omitted. This paper will explain the use of such a combination in Smart Homes. In smart homes there should be two levels of access. First the user has to get access into the house and then to the various smart devices. This approach will talk about both these issues. This section is divided into three subsections. The first section defines the security policy along with its related terms. In the second section we will talk about how access is granted into the house based on different contextual information. The third subsection talks about the access the devices from home as well as from a remote area in a different community.

2.1 Policy Definition

This section gives the various types of users associated with the smart home. It also specifies the various types of contextual information that is going to be used for implementing the security meta-policy. Finally the various security actions to be taken depending upon the information received are also stated. All the users need to know the secret code of the home network to get access to the network.

Roles: Owner, Child, Other members, Guests, Maintenance staff.

Contextual information considered: Role, Location, Time.

The five policies above are integrated into a contextual graph in that security actions taken in the graph are those with respect to these policies. The approach gives safe access to the devices. So anything which is not specified is considered as unsafe and is denied and hence not shown.

The Secret code S in the diagram can be considered as a secret name of the smart home network, which has to be known by each and every person who, wants to enter the house. In case of guests, the owner is responsible for producing it. This secret code is similar to the secret name of the ambient in case of ambient terms.

Security actions: These are the various techniques, which are used for authorizing the user at the various security points. The security actions are taken in conjunction with the security policies specified.

1. **SAo:** This security action is taken by the security policy when a user departs from the home network temporarily, curbing all her/his rights. The system gives a secret password to each user so that his identity can be checked when s/he would come back again. This security action although not given in the two figures below is mandatory for all local entities. When they arrive back then they have to revoke their rights by presenting their identity.

2. **SAi:** This security action is taken by the system when a user who had temporarily departed needs the access to the network. If the location is just outside the house at the door then the retina and the thumb print scanner checks the identity and this is enough to validate the local user. If the access place is remote then the user has to first enter the secret code of the smart home network, which is mandatory for any user and then the secret password is given to him/her at the time of departure.

3. **SAf1:** This security action is required in case of access for some foreign agent into the network. It prompts the user for her/his password to authenticate her/him-self to the system. It can either be a normal identification by the scanners when the access point is the door or a normal password if the access point is at remote location.

4. **SAf2:** This security action is required in case of some foreign agent entry into the network. It helps the user to get into the network. It can be the administrator authentication in case of door access to ensure that s/he is with the foreign user or can be one more level of password authentication if the location is remote.

5. **SAe:** This security action ensures that the data/information is carried in an encrypted format. It is taken when the access point is a remote location.

6. **SAr:** This security action prompts the users to enter their respective roles. This is used while accessing the devices inside the house.

7. **SAb:** In this security action the transfer of information between remote high level entities is carried through one more high level entity in order to prevent accidental leakage of data to the low level entities or unauthorised users.

8. **SAsi:** The security action SAi which when taken with the help of biometric identification tools. These tools are used for user authentication in order to have authorized access to the valuable resources. We have many devices such as Thumb Print scanner, Voice recognition, palm prints, hand/wrist vein patterns, retinal/iris eye scans, hand geometry/topography, keystroke dynamics or typing rhythms, and signature verification. In case of thumb print scanner the user presses his or her finger against an input device for verification in order to gain access. Within seconds, access is either granted or rejected, based upon stored fingerprints. In case of the Voice recognition, the users voice is recorded and matched with the one stored before in the database. The same methods apply in retina scanning but with the help of retina properties of the users.

9. **SAso:** The security action SAo which when taken with the help of biometrics (Retina scan or Voice recognition) as described above.

10. **SAsr:** The security action SAr which when taken with the help of biometrics (Retina scan or Voice recognition) as described above.

6.2 Getting Access to the Home Network

Getting access to the home network is the first step in accessing the devices. The contextual graph shown in Figure 3 gives the various scenarios in which a user is given access to the home network. The access is given only when a particular user satisfies the various criteria decided by the security policy. The secret password has to be known by each and every user and is a mandatory condition if he wants the access.

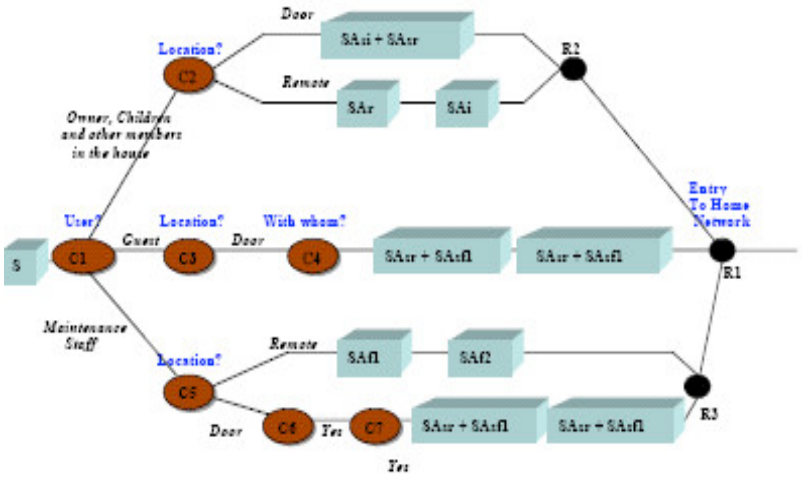

Fig.3. Part 1 of security meta-policy (Getting access to the home network)

1. When the owner of the house wants the access to the house, s/he has to first enter the secret code of the home network with the help of some wireless device. If s/he is not having the device then because s/he being the administrator of the network is given access to the network. But for others, carrying a device is a must. If the access point is the door then the owner is authenticated with the help of retina scanner, which in this case serves to satisfy the requirement of the security actions, **SAr** and **SAi** together. If s/he wants to access the network from a remote location such as his/her office then s/he has to enter the secret code of the network, her/his role, and the secret password that validates that s/he is a local (occupants of the home) entity. As s/he is at the top security level s/he is not asked for more identification. S/he gets access to the home straight away. Such kind of authentication is part of a multilevel access security model. The retina scanner in this case makes sure that only the authenticated person from the home community is given access. Once the owner is in the house he can access the devices according to the policy in Figure 4.

2. Children are given access to the home similar to the owner, as they are also the local entities of the home community. Once they are inside the house they are given access to the devices depending upon the devices and also on the presence or absence of the owner of the house as in Figure 4. The only difference is that in their case they are not allowed to access the devices from a distant location.

3. The remaining members from the house like spouse, parents, grandparents who are staying in the house also have to face similar kinds of authentication while entering the home. Once inside the network they are given access according to their predefined security level, which is needed by the security action **SAr**.

4. Guests are treated in a different manner. They are given access to the home network after passing through an authentication procedure in a multilevel access model. They are given access only when their location is at the door of the house.

Further as per case 2 they have to pass two authentication levels necessitated by the security actions **SAf1** and **SAf2**. For SAf1, they have to first validate themselves with the help of retina scan. For SAf2, they are given access only if they are with the owner of the house. The retina scanner first validates them and then the owner. Thus, the validation of owner helps in getting the guest in the home network. If this is not satisfied then the guest is not given the access. Once inside the owner need not be with them all the time, and can access the devices in the home based on their predefined security levels as dictated by Figure 4.

5. The maintenance staff is the one from which the security package is purchased from. They are required to monitor the performance of the smart devices. They can (but need not) come every weekend at a particular time to have an overall check up. They are also considered as foreign entities like guests. The retina scanner first validates them and then they have to enter a password given to them, which will help them to enter the home network. But a situation might also happen when there is an emergency. Emergency can be when an unauthorized person is trying to access a particular device in the house. In such situations, the staff might have to enter the house not necessarily at the specified time. They can get access to the network in such cases from any location. They can enter the home network after validating twice: first by entering the password given to them, and then using an emergency code that they are also given that will get them into the network. The difference from the owner in such access is that it just allows them to disconnect all the smart home facilities. In such cases, the owner is contacted and then the necessary actions are taken based on the owners' consent.

6.3 Accessing the devices

The following section indicates how the security policy provides controlled access to the devices in the home network. The following approach when used in conjunction with the approach in the previous section can be effectively used to implement stern security policies

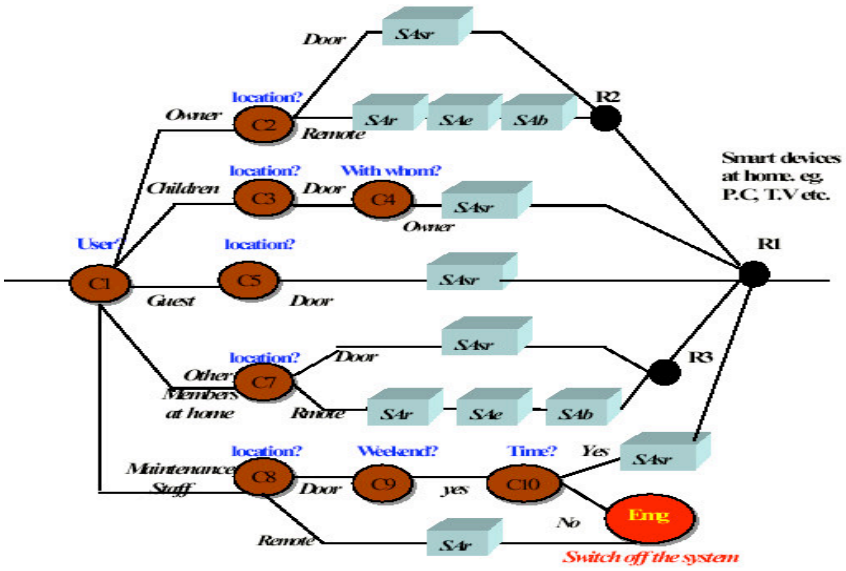

Fig. 4. Part 2 of Security meta-policy (Access to the device)

The above approach shows how Context based security is implemented in smart homes. The following subsection describes the various security actions taken by the security policy in appropriate situations. Let's have a look at the various valid scenarios in which the smart devices in the home can be accessed after passing through various authentication levels.

Scenario 1. There are two different contexts in this scenario.

Context 1: Role= User, location= home; Context 2: Role= User, location= outside.

If the user is the owner of the house, s/he is considered at the topmost security level. If s/he is in the house s/he can access the device by just entering his/her role in case of manual authentication. If the process is automatic then either the thumb print scanner or retina scanner authenticates him.

If the owner is not at home and wants to communicate with his/her PC then s/he has to go through the three authentication levels that depict the security actions deployed by the model as shown in Figure 4. Once s/he gets in the network s/he has to enter his/her role, which will prove that s/he is the administrator. After this the most important security action taken by the policy is encryption of the further information, which is communicated between the device and the user.

Further, in order to prevent the accidental leakage of data to high-level or unauthorised entities, the messages are first sent to the server which is kept at the

security company which checks whether the communicating entities are at the same level or not. The security action **SAb** accounts for this checking.

Scenario 2. There is just one valid context in this case. Valid context is that in which the access to the device is granted.

Context: Role= Children, location= home & with parent

If the users are the children in the house, they are given access to the devices only when the owner is with them. Further the access is granted only when they are at home and is based on their security levels.

Scenario 3. In this case also there is just one valid context.

Context: Role= Guest, *location= home*

Guests in this model are the owner's friends, relatives or colleagues. If the guests want to access the devices they have to first get inside the house using the part of the policy defined in the first contextual graph. They can only do that when the owner of the house is with them. After getting in they can access the devices as per their predefined security levels by either entering their usernames/passwords which will decide their security level based on the predefined one's or by normal biometrics in case of an advanced scenario.

Scenario 4. There are two different valid contexts in this scenario.

Context 1: Role= other members of the house, location= house.

Context 2: Role= other members of the house, location= outside.

Other members are spouse, parents of the owner. The security policy behaves in a similar fashion as in the case of the owner. If the members of the house other than the owner want to access the devices then they are given access after performing two different sequences of security actions in two different contexts. If they are within the house then they are given access based on their security level as predefined. The biometrics devices sense their role. The security action **SAsr** takes care of that. When the access point is a remote location they have to first get in the home network with the help of the first policy (Figure 3). Then they can access the resources based on their role/security level by manually entering their username/role through some remote devices. Beyond this as the information transfer is between two remote devices the communication has to be secured. Our security policy prompts the necessary security action (**SAe**) to be taken to account for that. This is Policy3, which provides an encrypted communication between the remote place and the local devices. SAb assures that there is no leakage of data in the process of communication.

Scenario 5. The maintenance staffs are allowed to access the devices only at weekends and at a particular time. If they arrive at the specific time then they can access the particular device according to their predefined security levels, which is sensed by the sensor at each of the devices. This is done in the security action denoted by **SAsr**. If not approved, then they are not allowed to access any devices. They are limited in what they do with the system – they can only turn off the working of all the devices and then take the necessary steps depending upon the cause of the

unauthorized access. A red node in the figure 4 denotes this. This special denotation is used to make things clear in emergency situations and is very much in lines with the definition of the context graph in respect of the number of outputs.

In this way the security meta-policy proposed would take appropriate security actions based on the context at that moment and will give controlled access to the resources. The contextual graphs shown above can be expanded to include more possibilities as and when the need arises.

7 Related Work

This section briefly highlights the existing projects and technologies that have influenced my work in using ambient calculus in context based security and how my model is different than those existing ones. Although the concept of contextual graph was first explored by Mostefaoui *et al.* (2004) [12], there have been few more people who tried their hands on context based security solutions using other methods. Al-Muhtadi *et al.* (2000) [1] talked about security is smart homes. They invented a component called Tiny SESAME that can be easily ported to any distributed computing devices that adapts to the environment with changing resources. The combination of Tiny SESAME and Jini can be used to create a dynamic, secure environment of distributed computing devices. Covington *et al.* [10] focused on the design of security services that incorporate the use of security-relevant "context" to provide flexible access control and policy enforcement. Based on their security policy they provided a generalized role based access control model that provided more flexible access control and a security subsystem that can adapt itself based on current conditions in the environment. Mostefaoui *et al.* (2004) [12] put forth the concept of contextual graph for modeling security in context aware environments. They present a new model for policy specification based on the new approach. The security policy based on such an approach depends on the contextual information of the user and the environment. Contextual graph proved to be very effective approach in modeling a complex situation. Brezillon *et al.* (2004) [3] also talks about how contextual graphs are used to model security in a context aware environments. In their paper they gave an example of how context based security is used in a hospital scenario. This paper also extends the work of Mostefaoui *et al.* [12] by using contextual graphs for modeling security meta-policies in context aware application like smart home. A difference between their work and ours lies in the use of various security actions grounded in other policies, i.e. we refer to other policies from within our (meta-)policy. Also a contribution of our work is the exploration of policies for a smart home.

7 Conclusion

Due to ubiquitous nature of the today's computing world security is of utmost important. The traditional static authentication techniques are no longer valid and

justified. This situation is due to the lack of consideration for context in existing security systems. Context based security helps the security policy to adapt to the new threats as it comes. It aims at providing flexible security models for distributed infrastructures, where the user's and application environments are continually changing. In this paper, we have presented an approach that helps in context based security for a smart home. The type and nature of the authentications that are demanded by the security policy depend on the information that is collected from the environment. Further, contextual graph approach helps to add/modify secure paths based on the newly detected contexts that need to be inculcated for security. The model presented although explained in a smart home environment is a generalised model, which can be used, in any context aware environment or enterprise, from the office to factories. There is a fine line between *context-aware security* to *context-aware safety* (e.g., children cannot operate the stove unless in the company of an adult – as determined by location sensors), and one can transition from one to another with an analysis as exemplified in this paper.

References

1. Al- Muhtadi, J., Anand, M., Mickunas, D., Campbell, R., "Secure Smart Homes using Jini and UIUC SESAME", September 2000.
2. Braghin, C., Cortesi, A., Focardi, R. (2002), "Security Boundaries in Mobile Ambients", Computer Languages, 28(1):101-127, November.
3. Brezillon, P., Mostefaoui, G.K., (2004) "Context-based security policies: a new modelling approach"**,** Pervasive Computing and Communications Workshops, Proceedings of the Second IEEE Annual Conference on, 14-17 March 2004, pp. 154 – 158.
4. Brezillon, P., (2003)," Context Dynamic and Explanation in Contextual Graphs", Springer-Verlag Berlin Heidelberg, pp 94-116. http://www-sysdef.lip6.fr/~brezil/Pages2/Publications/26800094PB.pdf
5. Brézillon, P., "Using context for Supporting Users Efficiently", (2003), Proceedings of the 36th Hawaii International Conference on Systems Sciences, HICSS-36, Track "Emerging Technologies", R.H. Sprague (Ed.), Los Alamitos: IEEE, CD-Rom (2003a)
6. Brézillon, P., "Task-realization models in context graphs", (2005), CNRS & University Paris 6, France).
7. Bugliesi, M., Castagna, G., Crafa, S. (2001), "Boxed ambients", Proceedings TACS 2001, LNCS 2215:38-63, Springer-Verlag.
8. Cardelli, L. and Gordon, A. D. (1998), "Mobile Ambients", Proceedings FOSSACS'98, volume 1378 of Lecture Notes in Computer Science, pp. 140-155, Springer-Verlag.
9. Cardelli, L. "Abstraction for Mobile Ambients" (1999), Microsoft Research, April.
10. Covingtony, M., J., Fogla, P., Zhan, Z., Ahamad, M., "A Context-Aware Security Architecture for Emerging Applications", College of Computing, Georgia Institute of Technology.
11. Dulay, N., "Adaptive Context Aware Security", Department of Computing, May 2004.
12. Mostefaoui, G.K., Brezillon, P., (2004), **"**Modeling context-based security policies with contextual graphs", Pervasive Computing and Communications Workshops, Proceedings of the Second IEEE Annual Conference on , 14-17 March 2004, pp. 28 – 32.
13. Mostefaoui, G.K., Brezillon, P., (2003), "A Generic Framework for Context-Based Distributed Authorizations", in proc. 4th International and Interdisciplinary Conference on

Modeling and Using Context (Context'03), LNAI 2680, Springer Verlag, Stanford, CA, June. 2003, pp. 204-217.
14. Mostéfaoui, K., (2003), "Security in Pervasive Environments, What's Next?" in the proceedings of the 2003 International Conference on Security and Management (SAM'03), Las Vegas, Nevada, USA, June 2003, pp. 93-96.
15. Mostéfaoui, G.K., Pasquier, J., (2003), "Deterministic Context-Based Security Policies: An Object-Oriented Approach" in the proceedings of the ACIS 4th International Conference on Software Engineering Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD'03), Lübeck, Germany, October 2003, pp. 160-165
16. Smart homes
http://www.jrf.org.uk/housingandcare/smarthomes/default.asp
17. Tripathi, A., Ahmed, T., Kulkarni, D., Kumar, R., Kashiramka, K., "Context-Based Secure Resource Access in Pervasive Computing Environments", Department of Computer Science, University of Minnesota.