ISSN: 2321-7782 (Online)
Volume 2, Issue 3, March 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Multilevel Security in Pervasive Computing Environments by using UUID

P. Murugavel[1]
Computer Science & Engineering
RVS Educational Trust's Group of Institutions
Dindigul – India

V. Aravinda Raja[2]
Computer Science & Engineering
RVS Educational Trust's Group of Institutions
Dindigul – India

K. Vimal[3]
Assistant Professor
Dept. of Computer Science & Engineering
RVS Educational Trust's Group of Institutions
Dindigul – India

S. Abirami[4]
Assistant Professor
Dept. of Computer Science & Engineering
RVS Educational Trust's Group of Institutions
Dindigul – India

Abstract: ***The security is the most important thing in the pervasive environments. The personal information's are identified by the malicious user. Some of the drawbacks are involved in the UPnP architecture. They are user authentication, and service access control. These are all not suitable in the pervasive environments. And also the integrated heterogeneity of the pervasive environments provides the different security and pervasive environments depending upon the services and the environment provided. In our proposed concept we not only provide the multilevel user authentication but also providing the flexible security approach that adapt to the network. For security purpose we use the multi level negotiation protocol. In our proposed concept first the user registered into the network for the securely accessing the network. Because in our proposed concept the only authorized person can access the networks. After that the registration process the key will be send through their mobile. With the help of the password we can enter into the site. In this stage the authentication and authorization process is performed. We can access the system in secure manner. In our concept we can control the system via the mobile phones in secure manner because the authorized person can only access the system.***

Keywords: UPnP, SOAP, UUID, Authentication, Integrity.

I. INTRODUCTION

Mobile computing is a very broad term which can be used to define any means of using a computer while outside of the corporate office. This could include working from home or on the road at an airport or hotel. The means to perform mobile computing could include kiosks used to remotely connect to the corporate office, home computers, laptops, tablets or smart phones. Specialized or integrated devices could also be considered as mobile computing devices. Lasco is a worm that initially infects a remote device using the SIS file format. SIS file format (Software Installation Script) is a script file that can be executed by the system without user interaction. The smartphone thus believes the file to come from a trusted source and downloads it, infecting the machine.

1.1 Existing System

In our existing concept, one patent for authentication and authorization proposes a secure handshake service based on digital signatures to provide authentication for devices. Such devices allow control points to access a given service whenever the control point features match the requirements of the service, including device model, supported media formats, and so forth. Another patent offers a dedicated solution for user authentication and authorization in UPnP networks. A device must provide a hierarchy of authentication folders configured in a control directory server. The user's Personal Identification Number (PIN) is used for authentication and for providing data access control according to the authentication level. However, data access control

by itself is not enough in pervasive environments, since the proliferation of services is available all the time. Besides, services access control also plays an important role in pervasive systems.

In the case of the UPnP Forum's proposed solution, devices enforce their own access control through the UPnP Device Security and Security Console specifications. Device Security provides services for authentication, authorization, replay prevention and privacy of SOAP actions. In order to establish and maintain the access control policies, a special control point, called Security Console, manages all security aware devices that implement the Security Device specification and is available in the entire network.

1.2 Disadvantages

1) User information is not defined or available during the handshake process.

2) They are protected by law and require fees when used in third-party applications.

3) In spite of being a standard UPnP specification, no user-related information is required during the authentication and authorization Sessions to provide access control.

1.3 Proposed System

To overcome the problems presented in our existing concept, in our proposed concept introduces an UPnP extension called UPnP User Profile (UPnP-UP), which enables user authentication and authorization for devices and applications altogether. The user authentication process is based on a multilevel security architecture that breaks security concerns into three different layers, providing a flexible and a transparent way of selecting security properties for a given pervasive environment. In addition, the security properties are negotiated among UPnP appliances during the execution of discovery and control protocols. The focus is on three different scenarios, namely, i) residential environments, ii) shared, but well controlled environments like offices and laboratories and iii) shared, but entrusted environments such as airports.

In addition we use the UPnP-up server for authorization purposes. In our proposed concept both the authentication and then the authorization are provided for more security. Current UPnP standard and specifications are based on a reactive behavior, which means that UPnP control points must invoke an UPnP service, or actions, in order to consume it. The user is first register and then login into the system. After that discovers their required devices. Finally we are accessing the devices.

1.4 Advantages

1) Our proposed concept provides the high or multi level security when compared to the existing system.

2) This system provides efficient result.

3) The authentication and the authorization are performed in efficient manner.

II. JAVA CONTROL FLOW STATEMENTS

Web browser that can run applets is an implementation of the Java VM. Java byte codes help make "write once, run anywhere" possible. You can compile your program into byte codes on any platform that has a java compiler. The byte codes can then be run on any implementation of the java vm. That means that as long as a computer has a java vm, the same program written in the java programming language can run on windows 2000, a Solaris workstation, or on an imac.

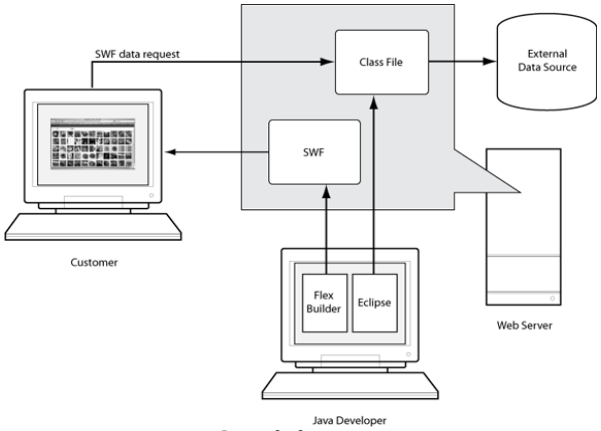

Fig.1Control Flow statements

2.1 Modules

- ✓ User Registration
- ✓ Authentication and Authorization
- ✓ Device Discovery
- ✓ Service Accessing

2.2 Modules Description

2.2.1 User Registration

User registration is the first phase. In this stage first the user gives the username and then password into the web services for registration purpose. In this stage the request and response are considered as an SOAP request and response. In our proposed concept we achieve a multilevel security for this reason first we register into the system after that we can login into the system. These are all the process is performed in the user registration stage.

2.2.2 Authentication Authorization

After the registration process is completed then we are login into the system with the help of the same username and then the password. After the registration processes the key which means that the secret code is passed through the mobile. With the help of the key only we can access the system. In this stage the authorization and then the authentication process are performed. Authentication means we allow the authorized person. Authorization means the actual operation that is check or validate whether the accessed person is valid user or not.

2.2.3 Device Discovery

If the registration and the authorization process is completed, next we search the devices or discover the devices for accessing the services. The authorized person can only enter into the system for accessing purpose. We discover all the devices present in the system. In this stage we achieve the multi level security in the system. In our concept we use the mobile as a control and the systems are the client.

2.2.4 Service Accessing

The service accessing is the final stage. In the device discovery stage we discover what are all the nearest peripherals are available here. In this accessing stage we access the selected nearest peripherals. Say for example, if we access the refrigerator or printer means, we can accesses these through our proposed concept. These are all the processes are performed in the service accessing stage.

III. UML DIAGRAM (UML STANDS FOR UNIFIED MODELING LANGUAGE)

UML stands for Unified Modeling Language. This object-oriented system of notation has evolved from the work of Grady Booch, James Rumbaugh, Ivar Jacobson, and the Rational Software Corporation. These renowned computer scientists fused their respective technologies into a single, standardized model. Today, UML is accepted by the Object Management Group (OMG) as the standard for modeling object oriented programs.

IV. USECASE DIAGRAM

Use case diagrams model the functionality of a system using actors and use cases. Use cases are services or functions provided by the system to its users. The purpose of use case diagram is to capture the dynamic aspect of a system. But this definition is too generic to describe the purpose. Because other four diagrams (activity, sequence, collaboration and State chart) are also having the same purpose. So we will look into some specific purpose which will distinguish it from other four diagrams.

V. CLASS DIAGRAM

The class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing and documenting different aspects of a system but also for constructing executable code of the software application. The class diagram describes the attributes and operations of a class and also the constraints imposed on the system. The class diagrams are widely used in the modeling of object oriented systems because they are the only UML diagrams which can be mapped directly with object oriented languages. The class diagram shows a collection of classes, interfaces, associations, collaborations and constraints. It is also known as a structural diagram.

VI. ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control. Activity diagram is another important diagram in UML to describe dynamic aspects of the system. Activity diagram is basically a flow chart to represent the flow form one activity to another activity. The activity can be described as an operation of the system. So the control flow is drawn from one operation to another. This flow can be sequential, branched or concurrent. Activity diagrams deals with all type of flow control by using different elements like fork, join etc.

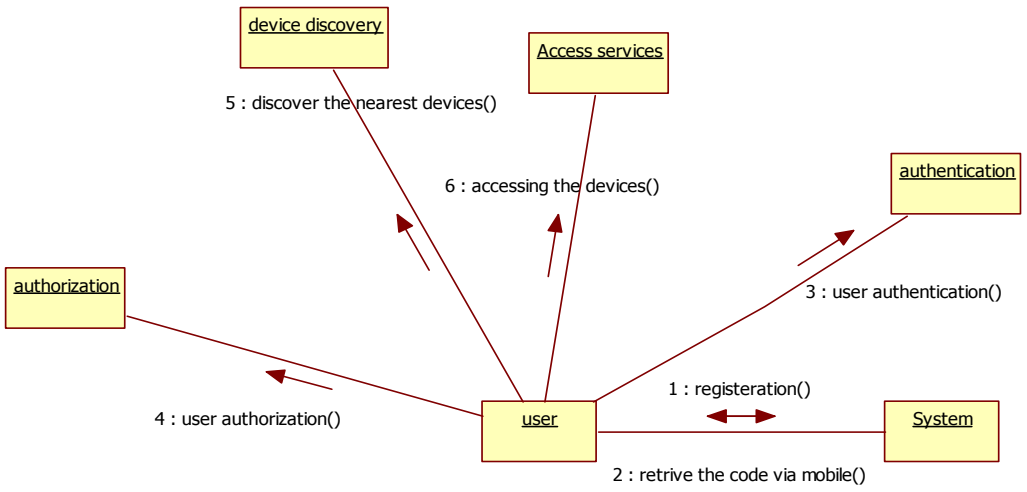

Fig.2 Collaboration Diagram

VII. System Testing

Testing is the one step in the Software Engineering process that could be viewed as destructive rather than constructive. Software testing is a critical element of software quality assurance and represents the ultimate reviews of specification, design and coding. Testing is representing an interesting anomaly for the software.

VIII. Feasibility Study

8.1 Authentication and Authorization

After the registration process is completed then we are login into the system with the help of the same username and then the password. After the registration processes the key which means that the secret code is passed through the mobile. With the help of the key only we can access the system. In this stage the authorization and then the authentication process are performed. Authentication means we allow the authorized person. Authorization means the actual operation that is check or validate whether the accessed person is valid user or not.

IX. Conclusion

Our proposed concept is mainly focused on the authorization and authentication. In our concept the systems are controlled through the mobile phones. First we register into the site; during the registration process we give the valid phone number. Because the secret code is send through the give mobile number. After that we can login into the system with the help of the secret code. The Valid user can only access the system. In this stage, we achieve a authorization and authentication process. Then we can discover what are the nearest peripherals are available. IF we find the devices then access these nearest devices. Say for example, we can access the nearest printers or any other peripherals through the mobile.

References

1. H. Park, “Interoperability model for devices over heterogeneous home networks”, IEEE Trans. Consumer Electronics, vol. 55, no. 3, pp. 1185- 1191, Aug., 2009.
2. J. Weast, “Advanced Universal Plug and Play Technology Topics”, IEEE Education & Learning, Jul., 2009.
3. V. Lortz, M. Saaranen, “Device Protection Service: 1”, Standardized DCP (SDCP), Version 1.0. UPnP Forum Committee, February, 2011.
4. L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea, “Lessons learned from the deployment of a smartphone-based access-control system”, Proc. of the 3rd Symposium on Usable Privacy and Security, SOUPS ’07. New York, NY, USA: ACM, 2007, pp. 64–75.
5. J. Kim, Z. Kim, and K. Kim, “A lightweight privacy preserving authentication and access control scheme for ubiquitous computing environment”, Proc. of The 10th International Conference on Information Security and Cryptology, Berlin, Heidelberg: Springer- Verlag, 2007, pp. 37–48.
6. J. Yves Tigli, S. Lavirotte, G. Rey, V. Hourdin, and M. Riveill, “Context-aware authorization in highly dynamic environments”, IJCSI International Journal of Computer Science Issues, vol 4, no. 1, pp. 1694-0784, Nov., 2009.
7. H. Nakashima, H. Aghajan, and J. C. Augusto, Handbook of Ambient Intelligence and Smart Environments, 1st ed. Springer Publishing Company, Incorporated, 2009.
8. J. Karl, Upnp CDS USER PROFILE, Rancho Santa Margarita, CA. U.S. Patent 8 185 949, 2012.
9. H. Miao; S. Park, "A semantic metadata infrastructure for UPnP AV to maximize quality of user experience", Proc. of IEEE Consumer Communications and Networking Conference (CCNC), pp.223-227, January, 2011.
10. A.L.V. Guedes, D.F.S. Santos, J.L. Nascimento, L.M. Sales, A. Perkusich, H.O. Almeida, "BRisa UPnP A/V Framework," Proc. Of International Conference on Consumer Electronics, ICCE Digest of Technical Papers, pp.1-2, January, 2008.

Author(s) Profile

P.MURUGAVEL is doing final year Bachelor of Engineering Degree in Computer Science and Engineering from RVS Educational Trust’s Group of Institutions, Anna University, Chennai, Tamilnadu, India

V.ARAVINDA RAJA is doing final year Bachelor of Engineering Degree in Computer Science and Engineering from RVS Educational Trust's Group of Institutions, Anna University, Chennai, Tamilnadu, India

K.VIMAL Presently he is working as Assistant Professor in Computer Science and Technology at RVS Educational Trust's Group of Institutions Dindigul, TamilNadu, India. Already he has worked as Assistant Professor in National Engineering College, KovilPatti past 7 years.

S.ABIRAMI Presently she is working as Assistant Assistant Professor in Computer Science and Technology at RVS Educational Trust's Group of Institutions Dindigul, TamilNadu, India. She had experience in quality assurance in Indian Space Research Organization, Bangalore, India for 3 years.