Security and Privacy Preservation over Interconnected Networks

J. Augustin Jebakumar[1], N. Gowdham[2], G. Josephine Kirubha[3], M. Navaneetha Krishnan[4]

[1, 2]PG Student, [3, 4]Assistant Professor
Department of Computer Science
St. Joseph College of Engineering
Sriperumbudur, India.
augustinjebakumar777@gmail.com, gowdhamn@gmail.com, josephinekirubha@gmail.com, mnksjce@gmail.com

Abstract- Security is a key concern in a wide spread network. Preserving private information is to be given due importance by all communication devices and search engines, since there is a threat of unauthorized users accessing secure information by trapping the network devices. Existing wide spread network of computers, mobile and other electronic devices does not define proper protocols neither based on user's location nor based on the end user's requirements in connecting to the network. Our proposed solution provides the most better and promising solution for a good network of plug and play Networks along with high level of authentication and authorization solutions. The proposal uses Flexi-Negotiable Security solutions that takes into account the cost and crude for such implementations along with best interoperability among the connected devices. Set of authorization policies are generated by a network manager using XACML based on the based on the available resources and the number of connected devices thus proving a reliable and secure network of devices.In this project, we are trying to incorporate a control point which will take care of controlling the devices access points. Each individual user needs to get authentication and authorization to access the resources in the network. Control point will take care of validating the request by the users. Once the users holds the authentication/authorization to access the resource in the network. They are permitted or else, no option to access the resources and they will be restricted. The authentication will be verified by the control points through a secure SOAP based web services. Our proposed system involves the above said techniques and it's associated with attribute based authentication. So that, higher designated people will be provided with more access options.

Index Terms: *-Mobile Computing Security, Authentication, Authorization, Universal Plug and Play.*

*****

1. INTRODUCTION

UPnP technology defines architecture for pervasive peer-to-peer network connectivity of intelligent appliances, wireless devices, and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to enable seamless proximity networking in addition to control and data transfer among networked devices. The UPnP Device Architecture (UDA) is more than just a simple extension of the plug and play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors. This means a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. Finally, a device can leave a network smoothly and automatically without leaving any unwanted state behind.

The technologies leveraged in the UPnP architecture include Internet protocols such as IP, TCP, UDP, HTTP, and XML. Like the Internet, contracts are based on wire protocols that are declarative, expressed in XML, and communicated via HTTP. Using Internet protocols is a strong choice for UDA because of its proven ability to span different physical media, to enable real world multiple-vendor interoperation, and to achieve synergy with the Internet and many home and office intranets. The UPnP to ad-hoc or unmanaged networks whether in the home, in a small business, public spaces, or attached to the Internet.

UPnP technology provides a distributed, open networking architecture that leverages TCP/IP and Web technologies

architecture has been explicitly designed to accommodate these environments.

Further, via bridging, UDA accommodates media running non-IP protocols when cost, technology, or legacy prevents the media or devices attached to it from running IP. What is "universal" about UPnP technology? No device drivers; common protocols are used instead. UPnP networking is media independent.

UPnP devices can be implemented using any programming language, and on any operating system. The UPnP architecture does not specify or constrain the design of an API for applications; OS vendors may create APIs that suit their customers' needs.

2. LITERATURE REVIEW

This section covers the details regarding the UPnP Device Connectivity and Architecture as well as the Audio/Video User Authentication. Let D the set of available devices in a local network, SD the set of available devices that expose UPnP services, called UPnP Devices, and CP the set of available devices that consume UPnP services from SD, called UPnP Control Points, such that SD = D - CP and CP = D - SD.

The UPnP connectivity model is defined as a set of different steps described as follows. In Step 1, a control point CPi (i = 1...n) searches for available UPnP devices during the discovery phase, namely SDj (j = 1... m). The control point CPi learns about each SDj device capabilities in Step 2 by parsing a shared SDj's XML file device description, and the control point CPi executes SDj's UPnP services through SOAP (Simple Object Access Protocol) in Step 3. In Step 4, the event phase allows the control point CPi to keep listening to state changes of each SDj device, while updating the graphical user interface accordingly in the presentation phase, or Step 5.

The UPnP A/V specification for audio and video [14] is shown in Fig. 1. The control point browses multimedia items from a UPnP Media Server device (Step 3) and these items can be rendered in the UPnP Media Renderer (Steps 5 and 6). This specification is focused on the UPnP technology dedicated to distributing and executing digital content such as music, videos, and images through the network. BRisa [15] is a worth example of the UPnP A/V specification, as a wide variety of TV, games, and consolesDespite offering zero configuration and a flexible connectivity, no user authentication and authorization mechanisms are provided. These requirements enable the customization of UPnP applications by collecting user preferences and information from the environment. For instance, it is not possible to build an application for recommending multimedia contents based on user preferences, such as music genres rock and blues in a UPnP A/V scenario.

Besides, considering that the basic idea is to support an open networking architecture, UPnP services do not cope with the user properties when accessing them. In this context, it is not possible to grant or deny access to a service based on user attributes and information from the environment. For instance, any user, without prior authentication or authorization, can request the UPnP service CreateJob from a UPnP Printer just with direct access to a control point in the current UPnP specification.

Due to the heterogeneity of devices, services and users in pervasive environments, security plays an important role for controlling access to information and customized services. Although the UPnP solutions for security only deal with device information, they are still not enough to acquire user information, or require static user information such as username and password, limiting the usability in pervasive computing environments, since each user would have to register him- or herself in each UPnP local network. Recent advances in pervasive computing have brought new solutions that use UPnP as the technology for discovering devices and services [17]-[19]. Nevertheless, many of those use non-standard mechanisms for device and user authentication and authorization process in pervasive environments. To sum up, it should be important to provide an authentication and authorization specification that extends the UPnP standard by allowing a seamless device-to-device interoperability in a scalable networked environment.

3. PROPOSED METHODOLOGY

The system mainly focus to give the entire control to a common point called “Critical Control Point” which emphasis to discover the devices and list the devices. It has its entire access dependencies on a Profile Server, which will provide the UUID (Universal Unique Identifier) for accessing the network Data. The user is provided with a media for requesting the data from a Server. In-turn on receiving the request the server will contact the Critical Control.

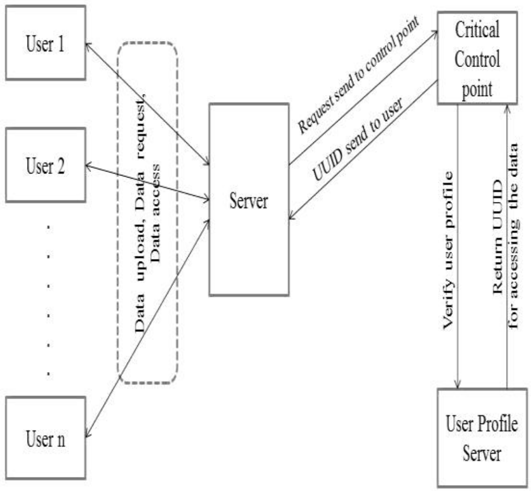
User 1
User 2
User n
Data upload, Data request, Data access
Server
Request send to control point
UUID send to user
Critical Control point
Verify user profile
Return UUID for accessing the data
User Profile Server

Fig 2: Architecture Diagram

With the purpose of offering the secured and accurate data to the User. Here, we use MD5 and AES algorithm in all the levels, from User via Server and Critical Control Point to User Profile Server.

A)Data Requisition Module

Data’s are fixed to eradicate the requisition with initial process checking of the requisition when creating assigned of the task. Predetermined the problem with duplicate sever configuration. Showing the critical point constrain for the page for the referenced request to the device.

B)Device/Request Discovery Phase

Requests device status and WNS connection status in the notification response.Defines the notification type in the specifies the time to live (TTL).The device specifies the same access token can be used on subsequent notification requests until it expires.

C)Device/Request Validation Module

In this case, all dispatch routines must be careful to check each device request of validating the object that they receive. Otherwise, the device might crash when trying to use device extension information.Device creates overall control device objects in validating the access paradigm . After validation, the device authenticates and creates another set of device objects in its routine.

D) Request Approval Module

To apply for a request provider device approval, the complete establishment is provided for ensuring the data set. Applications may be for a one- or two-year term but after processing the request, the approval is validated. Assigns a provider so that the authorized persons identified in the agreement can use for other device request in critical point control.This request for approving the provider must not be used as a reference number for individual device activities.

E) Request Process Module

The Process Request method is called by an Http Application object when it wants the handler to process. The current HTTP request and to generate a response for the device was implemented in this module.The is a re-useable property to access the module request for the device in order determine the valid user handler for replicated critical device access.

F) Security Evaluation Module

The Security Target determines the scope of the evaluation in this module depiction.It includes a claimed level of Assurance that determines how rigorous the evaluation is in providing device access control.They define several degrees of rigor security for the testing and the levels of assurance that each confers. They also define the formal requirements needed for a product or system to meet each Assurance level.

4. RELATED WORK

In order to protect UPnP environments from illegal accessand a variety of other threats, researchers have proposed manyframeworks and architectures that can be used in pervasive

applications [20]-[23]. However, these solutions provide nonstandardtechnologies, which bring challenges to achieveinteroperability with others. For this reason, the architecturaldecisions on any UPnP-based technology should take intoaccount its general protocols to not only be easily integratedwith UPnP networks, but also safely deploy UPnP servicesand appliances based on user profiles.There are many relevant works proposed in the context ofthis research. One patent for authentication and authorizationproposes a secure handshake service based on digitalsignatures to provide authentication for devices [11]. Suchdevices allow control points to access a given servicewhenever the control point features match the requirements ofthe service, including device model, supported media formats,and so forth. Nonetheless, user information is not defined oravailable during the handshake process.

Another patent offers a dedicated solution for userauthentication and authorization in UPnP networks [12]. Adevice must provide a hierarchy of authentication foldersconfigured in a control directory server. The user's PersonalIdentification Number (PIN) is used for authentication and forproviding data access control according to the authenticationlevel. However, data access control by itself is not enough inpervasive environments, since the proliferation of services isavailable all the time. Besides, services access control alsoplays an important role in pervasive systems. Therefore, theyrepresent a major drawback for those solutions because theyare protected by law and require fees when used in third-partyapplications.

In the case of the UPnP Forum's proposed solution, devicesenforce their own access control through the UPnP DeviceSecurity and Security Console specifications [3]. DeviceSecurity provides services for authentication, authorization,replay prevention and privacy of SOAP actions. In order toestablish and maintain the access control policies, a specialcontrol point, called Security Console, manages all securityawaredevices that implement the Security Devicespecification and is available in the entire network. In spite ofbeing a standard UPnP specification, no user-relatedinformation is required during the authentication andauthorization sessions to provide access control.The UPnP Forum committee has proposed another securitymodel for UPnP devices and applications called UPnP DeviceProtection Service [4]. This security model is based on theX.509 certification architecture and requires username andpassword for user authentication and access control. The trustmechanism requires proximity between user and UPnP device,through PIN or the Near Field Communication (NFC)authentication process. In contrast, despite a peer-to-peerauthentication and authorization approach, there are a lot ofobstacles when considering pervasive environments. First, theuser's credential as a combination of username and password requires previous users sign-on process, as well as previousknowledge of the existence of the device. Last, but not least,all users need to be nearby of the target devices in order toaccess UPnP services in a protection-enabled device, thusreducing flexibility. To sum up, these aforementionedintricacies make the UPnP Device Protection Serviceunsuitable for pervasive computing environments.

5. CONCLUSION

The system mainly focuses on giving the entire control to a common point called "Critical Control Point" which emphasis to discover the devices and list the devices. It has its entire access dependencies on a Profile Server, which will provide the UUID (Universal Unique Identifier) for accessing the network Data.

6. REFERENCES

[1] Thiago M. Sales, Leandro M. Sales, Hyggo O. Almeida, Angelo Perkusich, "Multilevel Security in UPnP Networks for Pervasive Environments" Consumer Electronics, Vol. 59, No. 1, February 2013.

[2] M. Jeronimo, J. Weast, UPnP Design by Example, Intel Press, Boston, 2003.

[3] V. Lortz, M. Saaranen, "DeviceProtection Service: 1", Standardized DCP (SDCP), Version 1.0. UPnP Forum Committee, February, 2011.

[4] L. Kagal, T. Finin, and A. Joshi, "Trust-based security in pervasive computing environments", Computer, vol. 34, pp. 154–157, Dec., 2001.

[5] 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.

[6] 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.

[7] 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.

[8] M. L. Damiani and C. Silvestri, “Towards movement-aware accesscontrol”, Proc. of the ACM GIS International Workshop on Security and Privacy in GIS and LBS, New York, NY, USA: ACM, 2008, pp. 39–45.

[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.

[11] Q. Ni and M. Sloman, “An ontology-enabled service oriented architecture for pervasive computing”, Proc. of Int. Conf. on Information Technology: Coding and Computing, vol. 2, pp. 797 – 798, April, 2005.

[12] U. Hengartner and P. Steenkiste, “Protecting Access to People Location Information”, Lecture Notes in Computer Science, Springer Berlin, 2004, vol. 2802, pp. 222–231.

[13] P. Robinson and M. Beigl, “Trust Context Spaces: An Infrastructure for Pervasive Security in Context-Aware Environments”, Lecture Notes in Computer Science, Springer Berlin, 2004, vol. 2802, pp. 119–129.

[14] S. Creese, M. Goldsmith, B. Roscoe, and I. Zakiuddin1, “Authentication for Pervasive Computing”, Lecture Notes in Computer Science, Springer Berlin, 2004, vol. 2802/2004, pp. 439–488.