ISSN 1512-1232

A SIMULATION BASED EVALUATION OF HOME NETWORKED APPLIANCES SECURITY SCHEME

Mazhar Ul Hassan

School of Computer and Mathematical Sciences
Liverpool John Moores University, Byrom Street, Liverpool L3 3AF, UK
Email: M.ul-hassan@2006.ljmu.ac.uk

Abstract

The term peer-to-peer refers to the concept that in a network of equals (peers) using appropriate information and communication systems, two or more individuals are able to spontaneously collaborate without necessarily needing central coordination. A Network Appliance is defined as a dedicated function consumer device with an embedded processor and a network connection. Security for such devices in distributed network environments presents many challenges, and remains a largely unresolved issue. Considering security, various schemes have been proposed, however research shows various weaknesses within the reported solutions. We propose a novel scheme called the Home Networked Appliances Security Scheme (HNASS) to secure communication among peers utilizing services of home networked appliances. The key feature of this scheme is still utilizing a simple architecture to protect peers both within and outside the network. We believe this scheme could yield such a solution which can be evolved into a more generalized and well protected standard for such networks.

I. INTRODUCTION

Peer-to-peer (P2P) has become one of the most widely discussed terms in information technology in recent years. The term peer-to-peer refers to the concept that in a network of equals (peers) using appropriate information and communication systems, two or more individuals are able to spontaneously collaborate without necessarily needing central coordination [1].

In a P2P network, peers can join or leave the system without any intervention from a centralized server, which facilitates seamless integration of any number of new nodes (peers) to existing systems. Understandably, the decentralized nature of P2P networks facilitates scalability. P2P systems, beginning with KaZaA [2], Napster [3], Gnutella [4], and several other related systems, have become immensely popular in the past few years, primarily because they offered a way for people to get music without paying for it [5]. For example, in the case of KaZaA, which is used mainly for music file sharing, users can search for particular song and after searching users could download without knowing the location of the host peer. P2P networks are interesting in their own right, but in this paper we consider them as a means to facilitate the deployment of networked appliances within the home. The characteristics of P2P networks make them ideal for this task, and to explain this we must consider the concept of Networked Appliances as they relate to P2P networks further.

It is known that the same level of efficiency is required both for the specialist and the home user to address increased complexity associated with the network appliances configuration. Networked appliances are manually connected therefore, special purpose hardware is needed to provide pre-determined hardware interfaces. These interfaces are needed to allow the devices we own to be interconnected. Research initiatives have tried to standardize how devices are interconnected by describing and discovering services using attribute-based techniques which are known *a priori* [6]. These standards are known as inflexible and do-not provide any mechanisms to describe and discover services in a generic way.

A Networked Appliance is defined as "a dedicated function consumer device with an embedded processor and a network connection" [7]. Security is not just about keeping people out of your network. Security within Networked Appliances is an important aspect to be seen. Especially in situation when there are more than one receptive of the services provided by Networked Appliances. Security also provides access into your network in the way you want to provide, allowing different network appliances to work together. The tighter your security controls are, the greater the level of access that you can safely provide to trusted external networked appliances. Clearly security is an important issue, therefore we have proposed a novel scheme known as the Home Networked Appliances Security Scheme (HNASS). This scheme has been designed to secure all service requests besides taking measures to protect against any intruders posing threats to the peers utilizing one of the provided services.

The rest of this paper is organized as follows. In the reported literature there are a variety of schemes that have been proposed for the implementation of networked appliances, but research shows there are weaknesses within these schemes. All such schemes are discussed in Section 2. In Section 3 HNASS is proposed and explained as a solution to the problem of P2P networked appliance security. In section 4, evaluation details are covered. Conclusions and future work are covered in Section 5.

II. RELATED WORK

Research initiatives such as UPnP, OSGi, Home Electronic System (HES), Home Audio and Video Interoperability (HAVi) and Digital Home Working Group (DHWG), have tried to standardise how devices are interconnected. They achieve this by describing and discovering services using attribute-based techniques which are known *a priori*. However, it is known that for various reasons, these standards do not full-fill the criteria of a secure solution. This makes security an important and difficult challenge. The above mentioned standards address a number of challenges, but they are inflexible and do not provide any mechanisms to describe and discover services in a generic way.

We consider a number of these research initiatives in particular: ePerSpace, UPnP, OSGI and NASUF. A brief introduction to each of these standards is as follows.

ePerSpace: ePerSpace is a project under the EU 6th Framework program for the development of personalized communication services within home networks [8]. The ePerSpace framework provides Global Network Integration and Interoperability which allows interconnecting audio and video to exchange its content between distributed services in a secure manner.

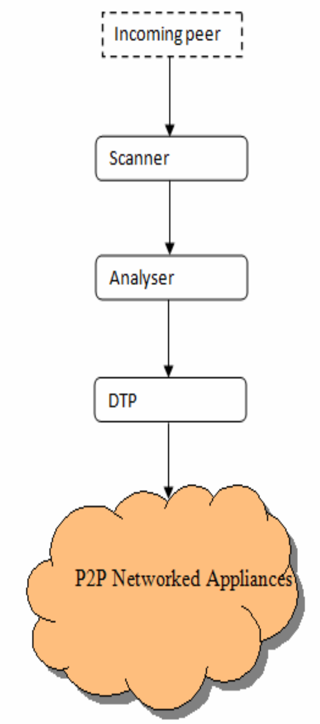
Universal Plug and Play (UPnP): UPnP is a technology framework for simplifying the connection of networked devices. Devices are connected to the computer, at which point they instantly starts working, *i.e.* they are automatically detected by the operating system. UPnP does not require any particular type of network connection; it works with Ethernet, Wi-Fi, Bluetooth and other physical media. UPnP is also designed to work with many different types of networked devices and operating systems. Many home network routes offer UPnP support [9, 10].

Open Services Gateway Initiative (OSGi): The Open Services Gateway Initiative (OSGI) [11] was founded in March 1999. It was specifically designed for the delivery of a wide range of services to end users. OSGI deploys services over wide area networks to local networks and devices. This is achieved using a complete end-to-end solution architecture from the service provider, who actually operates the service through the local networks and devices that deliver it to the end user. This scenario is also applicable to residential gateways, in-vehicles, and in mobile phone environments, among many others. Various services run on the OSGi framework. The framework is a service-oriented architecture, and responsible for the management of various services it contains. OSGi works using the JVM and is programmed in the Java language. Because of the characteristics of Java, application programs are limited to the Java run-time environment and are not allowed to access other parts of operating system, so Java has better security than many other languages. The characteristics of Java can protect the home area network from various types of malicious attack and probing. OSGi consists of a gateway between the Internet and the home network, which is accessed remotely by providers managing services and smart appliances in the home. This solution is centralized and the user is still involved in local configuration of devices even if the gateway itself needs no configuration.

Networked Appliance Service Utilization Framework (NASUF): Networked Appliance Service Utilization Framework (NASUF) utilizes the concept of services. In a service enabled network, appliances offer their services to other appliances when needed. These services are dynamically discovered and composed within a P2P network without any centralization [12]. In a P2P home network each device with its own services will have NASUF as well as application specific services that disperse the functions devices provide as independent services within the network. For example a network-enabled TV could have three application specific peer services; a visual service; an audio service; and a terrestrial TV receiver service.

III. HOME NETWORKED APPLIANCES SECURITY SCHEME (HNASS)

The Home Networked Appliances Security Scheme (HNASS) follows an intermediate approach between the existing schemes and some of the new concepts which have been proposed as a part of this scheme. In HNASS all peers outside of our P2P networked appliances network can freely use services but will go through certain steps before joining the network. There are three components of HNASS: namely a scanner, analyzer and a Decision Taking Peer (DTP), which work with the other P2P networked appliances in order to provide security. HNASS defines various operations to perform its set task. These operations within implementation aid each other in their routine work. Therefore in some cases it is essential for one function to perform in association with some of the main and sub function. Details of each of these functions are also included in the following specification of this scheme.



Peer to Peer Network with HNASS

In the above figure a scanner scans all incoming peers and views their UIDs, its connection with other peers and its properties, forwarding the results on to the analyzer. The analyzer needs the above three classes of information from the scanner. Using this information the analyzer decides whether to allow or deny the incoming peer. In fact, the analyzer cannot take any action except making decisions about incoming peers. If there is any problem with a peer, for instance, it is connected with any malicious or non trusted peers, the analyser reports a connection error to the incoming peer. The peer is then sent to the DTP (Decision Taking Peer) which will either allow or deny a peer based on the analyzer's decision.

A. Scanner

A scanner has two functions *i.e.* UIDs and properties, on the basis of which a scanner scans all incoming peers and then forward them to the analyzer if verified otherwise peers will be sent back to the sender in case of non verified peers.

Check UID Function

User Identification (CUIDF) is a function that will be called by a scanner to check identification of an incoming peer.

Forward Check UID Function (FCUIDF) is a function that will be called by the scanner after UID of the incoming peer is checked and verified by the CUID function. After UID verification the FCUIDF will forward a peer to the next step.

Reverse Check UID Function (RCUIDF) is a function that will be called by a scanner if UID of incoming peer is checked but not verified by the CUID function. If the UID of a peer is not verified the RCUIDF will discard the peer and send it back the sender.

Check Properties Function

Check Properties Function (CPF) is a function that is called by the scanner to check different properties of all incoming peers. For example it will check whether the incoming peer is a trusted peer or not, whether it is infected by any viruses or whether the peer is using any encryption method.

Forward Check Properties Function (FCPF): As this is the last scanning function of the scanner, here this function will allow a peer if all the properties of incoming peer have been verified by a function CPF. After verification a peer will be forwarded to the analyzer which is the next process after scanning.

Reverse Check Properties Function (RCPF): If there is any problem with one of a property of incoming peer, RCPF will be called by a scanner in order to discard the peer and send it back to the sender.

B. Analyzer

To analyze incoming peer, the analyzer needs three types of information from the scanner *i.e.* the name of a peer i.e UID’s, its connection with other peers and finally its properties. On the basis of this information the analyzer will make a decision whether to allow or deny the incoming peer. In fact analyzer cannot take but only make a decision about the incoming peer; therefore for the decision *taking* process a peer will be sent to the Decision Taking Peer (DTP) if verified/accepted otherwise it will be sent back to the sender.

Check Analyser Function (CAF)

To make a decision about incoming peer, Check Analyzer Function (CAF) will be called by the analyzer. The CAF will analyze a peer and make a decision based on the analysis.

Forward Check Analyser Function (FCAF) is a function that will be called by the analyzer once name of a peer i.e UID’s, its connection with other peers and its properties have been verified by the Check Analyzer Function (CAF). Here the FCAF will forward a peer to the Decision Taking Peer (DTP), where it will enact the decision made by the analyzer.

Reverse Check Analyser Function (RCAF) is a function that will be called by the analyzer if information regarding a peer's name i.e. UID's, properties and its connections with other peers are not verified by the CAF. In this case the RCAF will be called by the analyzer. Peer will then be discarded and sent back to the sender.

C. Decision Taking Peer (DTP)

The DTP (Decision Taking Peer) receives all of the information about the incoming peer from the analyzer. As mentioned earlier analyzer makes a decision whether to allow or deny a peer, whereas the DTP takes a decision and will allow/deny the incoming peer based on a decision made by the analyzer.

Allow Decision Taking Peer Function (ADTPF): To take a final decision about the incoming peer and allow it to our P2P networked appliance network to use/offer services, a function Allow Decision Taking Peer Function (ADTPF) will be called by the DTP. This will be done only if the peer is allowed by the analyzer.

Deny Decision Taking Peer Function (DDTPF): If a peer is not verified and the analyzer makes a decision to discard it, the DDTPF will be called to deny the peer and send it back to the sender.

IV. EVALUATION

Evaluation could be seen as one of the important aspect of this research. Although proposed scheme is fully capable of making p2p communications more secure but we understand that evaluation result could give us direction about both the upper level of efficiency and the possible future work. We have created scenarios which can fit and reflect the working of HNASS. There could be many situations which could be used to major performance of this scheme; however scenarios described within this section were carefully selected to obtain the concrete observations.

i. Evaluation with a Basic p2p Network

This experiment could be seen as one of the essential and basic experiment. The purpose of this experiment is to monitor the modified form of NASUF to make sure that all the functions of HNASS are fully integrated and operable. Since it was not possible to carry out any further experiment without being implemented functions validated. Each of the written function has been placed in different locations of NASUF therefore there was a need to re-compile NASUF framework which have been done. That given us complete messages that the functions have been integrated successfully with the existing structure and NASUF have been further modified with the integration of the proposed and developed scheme i.e. HNASS. It could be noted that this experiment should be seen as a technical validation and not a formal validation of HNASS. As formal validation has already been verified and tested with the successful re-compilation of NASUF package in a Java environment. We have evaluated the final and modified structure with a simple network of four peers. All the peers have been noted communicating normally and we have observed a usual behavior of communication as it was expected. As according to the specification of HNASS all the functions excluding those parts which dealt with the suspicious peer were found working exactly as defined by the proposed scheme. In the concluding remarks we can write here that the scheme has been successfully integrated and performed well in accordance with a description of each individual specified and integrated methods of HNASS. This also proved that the proposed scheme and its implemented form has highly adoptable and interoperable feature. Based on this evaluation experiment we are confident that the scheme could also be extended and could well suit with other frameworks designed to create similar environment. Screen shots of this and the remaining experiments describe below could be seen inside index of this dissertation.

ii. Evaluation in the Presence of Intruder

This is an interesting experiment as it is designed and planned to monitor effectiveness of HNASS which is designed and developed to make p2p communication more secure within a home appliances network. It is extremely important for a scheme to have special mechanism which can block any intruder peer attempt to access the services or the other peer participating in the network. Likewise it was necessary to consider the scenario where an intruder peer access the network for service utilization. Under this situation there are two scenarios that can be taken into accountability. In our first scenario, if a peer is already using services from our P2P Networked Appliances. In the mean time an external peer also wants to access same services. Unless peer uses services and don't release, external peer won't be able to use services at the same time. Access will be denied. In any case, a function must be called to check encryption, as well as nature of the data even if a peer is not encrypted.

In the second scenario once external peer founds that peer is already using those services which it needs, it will access peer and will request for releasing those services. If external peer is not using any encryption of data then after releasing services from Peer, that external peer will access them. But if external peer uses encrypted data then Peer will call CEF to identify nature of the data of that external request. CEF will forward that request to DF where it will decrypt data. If data is safe then Peer will release services and external peer may use its required services, but if external peer is a threat then Peer won't release services it uses. We have evaluated both scenarios and have found out that the Encryption Decryption function are found working at a satisfactory level and attempt to access network under conditions described above were unsuccessful. It was a crucial experiment to reveal how HNASS tackles a genuine threat to the home appliances network.

iii. Evaluation with large number of peers

This experiment dealt with a situation where large numbers of peers are part of a home appliances network. With no doubt when we have large number of peers, we would expect to see a higher message activities, thus it puts the whole network at the risk of security attack. Therefore it was very crucial to monitor the performance of HNASS. We have observed an active response to various requests in the network using the proposed and the developed scheme and have not seen any sign of threat with respect to stealing information etc. However overall reaction of the network and response to several requests were slower than the above two evaluation experiments. This might be due to so many requests both for joining the network and the network services. One important aspect lies in the fact that even in such situation HNASS behaves normally without creating any type of exceptional errors. This also verified and validated both implementation and operational efficiency of the scheme in a different environment

V. CONCLUSION AND FUTURE WORK

In this paper we have presented a novel scheme to secure home networked appliances within a peer to peer network. HNASS utilizes a combination of three components to provide secure communication between various peers. In addition HNASS introduces measures to protect any attack by an intruder to any of the peers associated with the established network. HNASS scheme has been implemented and evaluated. Evaluation experiments have shown impressive results. In future we will be conducting further research experiments to monitor our proposed scheme for performance in a diverse range of environments. We aim to share our research findings with the ongoing research in this area.

References

1. D. Schoder, K. Fischbach, and C. Schmitt, "Core Concepts in Peer-to-Peer Networking," in *Peer-to-Peer Computing: The Evolution of a Distruptive Technology*: IGI Global, 2005, pp. 308.
2. P. Sanderson, "Identifying an existing file via KaZaA artefacts," *Digital Investigation,* vol. 3, pp. 174-180, 2006.
3. E. Palomar, J. M. Estevez-Tapiador, J. C. Hernandez-Castro, and A. Ribagorda, "Security in P2P networks: survey and research directions," Seoul, South Korea, 2006.
4. Gnutella, "The Gnutella Protocol Specification v0.4," vol. 2009, 2009.
5. D. S. Wallach, "A survey of peer-to-peer security issues," Berlin, Germany, 2003.
6. M. Merabti, "Networked appliances in home entertainment," vol. 223, pp. 288 - 293, 2006.
7. S. Moyer, D. Marples, S. Tsang, and A. Ghosh, "Service portability of networked appliances," Piscataway, NJ, USA, 2001.
8. ePerSpace, "Towards the era of personal services at home and everywhere," vol. 2005: ePerSpace, 2005.
9. B. A. Miller, T. Nixon, C. Tai, and M. D. Wood, "Home networking with Universal Plug and Play," *IEEE Communications Magazine*, vol. 39, pp. 104-109, 2001.
10. Microsoft, "Understanding Universal Plug and Play," vol. 2008: Microsoft, 2004.
11. D. Marples and P. Kriens, "The open services gateway initiative: An introductory overview," *IEEE Communications Magazine,* vol. 39, pp. 110-114, 2001.
12. P. Fergus, A.Taleb-Bandiab., A.Mingkhwan., M. Merabti, and M. Hanneghan, "A semantic Framework for self-adaptive networked appliances," presented at IEEE Consumer Communications and Networking Conference(CCNC'05), Las Vegas, Nevada, USA, 2005

Article received: 2010-10-12