Secure Personal Pervasive Active Space

Jalal al-Muhtadi † and Khaloud Zainalabdeen ††

†Assistant Professor at the College of Computer and Information Sciences, King Saud University, Riyadh, KSA
††Faculty of Computer and Information Science, King Abdul-Aziz University, Jeddah, KSA

Summary
Securing Pervasive Active Space is an important issue to achieve the privacy and safety of the person's information exchanged. Thus, because this type of networks has many features such as flexibility and dynamic nature that raises the risks of illegitimate access and steal the sensitive information. In recent years, there are a lot of considerations and works about securing the information exchanged inside these types of networks. Notice that, much research done in this field was either a suggestion of solutions without an implementation or an implementation of some of the security aspect while other concepts are missing. In this paper, we provide a new security protocol for Personal Pervasive Active Spaces especially the networks that have similar design to the Mobile Gaia. This security protocol will take in consideration the different security aspects such as authentication, data confidentiality, and integrity and access control. In addition, we will evaluate the performance of the protocol by simulating the system.

Key words:
Pervasive and ubiquitous computing. Security. Mutual authentication. Cryptography.

1. Introduction

Pervasive computing is a great technology that simplifies the use of information and communication and it is integrates the physical and digital components to presents many interested applications such as smart homes. As computing grows to be more pervasive, people expect to access services and information at anytime and anywhere. Therefore, the direction in the future is to develop more ubiquitous/pervasive computing spaces that called "active" where there is an interaction between digital and physical devices in order to benefit from the available resources effectively. Moreover, pervasive network means focusing on a new type of networks where there is no infrastructure. Rather, the devices are joined for a special purpose. As an example: the devices owned by one user joined to share resources or to indicate the location. This development increases the concerns about the security challenges facing the networks because of the potential attackers that has the capability to collect sensitive data, retrieve information from databases and, modify the environment without any permission. The problem of using pervasive computing is the ability to collect or use personal data without permission or without the knowledge of the person. For this reason, the security for distributed environment and pervasive computing is an important requirement to achieve a good level of privacy and safety.
Nowadays, there is much discussion about the rules or requirements needed to protect such these systems while their usefulness is still present. In this paper, we set up a new security protocol for the Personal Pervasive Active Space that has the similar architecture to Mobile Gaia. This security protocol will consider the connection between devices in a secure and authenticated manner and will provide Access control. In Mobile Gaia architecture, each space must have a coordinator, for coordinating and maintaining the various devices in the space. Choosing the device with best memory and CPU to be the coordinator to manage the space. Other devices in the space will act as clients or service providers.

2. Related Work

As observed in searching for the related works in the concept of distributed, wireless system we can divide these systems into three categories: system concerns and implement some aspect of security, system suggest solution but not implemented yet, and system didn't concern the security. Talking about the systems that implement some aspect of security, we have JINI system, CORBA, an extended chaotic maps and Multi-lateral localization. First, JINI system [3] is a Java based dynamic distributed system developed by Sun Microsystems. It uses the features of access control list and the lease to define the rights for devices to use several services. However, there are some missing security concepts such as the mutual authentication, integrity, non-repudiation and encryption. We can cover these concepts using some technologies of Java such as Java Remote Method Invocation (Java RMI) but in this way, the programmer needs to consider how to integrate it or use it. Second, CORBA system [1], [10] that is belongs to the Object Management Group. It is implement to handle the security issues for an object-oriented distributed system. In addition, it provides a predefined access rights but it is not suitable for all the applications. Thus, the implementers need to consider its required access rights. Another problem, non-repudiation security issue is incomplete since it depends on a framework that has no prototype or implementation called ISO non-repudiation framework.

Manuscript received June 5, 2016
Manuscript revised June 20, 2016

Finally, it needs to deal with other security issues in its design like encryption to protect the resources, integrity. Third, an extended chaotic map scheme [11] that is focuses in the remote authentication of the user and the denial-of-service (DoS) attacks. In the proposed authentication scheme, a security analysis was present to shows it can cover 11 security requirements including the mutual authentication, user anonymity and key session agreement. But there is no mention about the implementation of the system. Furthermore, they did not simulate the system to shows its usefulness and its performance.

Fourth, multi-lateral localization privacy in pervasive environment. In that protocol, they focus on the problem of collecting location information that can shows some of personal habit without the permission of the person. Also, they protect any side information that can gives any hint about the location. It developed a three-layer privacy protocol by combining the information hiding and homomorphic encryption called Paillier cryptosystem. It is not necessary to use all the security levels. However, any user can choose the level of security he wants especially in a resource-constrained mobile computing environment. It calculates the target location by minimizing the mean squared error (MMSE) between the measured distances and the calculated distances. This protocol does not deal with other security issues such as secure communication between nodes and active attack.

On the other hand, the systems that suggest solution but not implemented are Mobile Gaia Middleware, Trust Management Architecture for Pervasive Computing Systems. First, the Mobile Gaia [5], [7] is a middleware used in an ad-hoc pervasive space where the devices are belongs to one person for the purpose of communication and share resources. This group of devices have named a personal active space that is manage by the user through a common interface. The proposed security solution in Mobile Gaia is to focus into how to authenticate devices before it is connect to the personal space and how to control the access to the shared resources and information. But there are other concepts must be considered for securing the personal active space such as message integrity and non-repudiation. Therefore, the implementation of the security solution is essential with the thinking about some missing security concepts such as the encryption.

Second, the Trust Management Architecture paper that proposed by University of Maryland Baltimore County [9]. It suggests solution to secure the system by distributes the responsibilities of security between some devices. In addition, it uses the simplified PKI [4], Centaurus model and, Centaurus Capability Markup Language (CCML) [6] for the user interface (messaging). Still, this solution has no implementation. Third, the trust metric based on soft security [12], the focus of this paper was to discover the trust parameter for systems that depends its security on trust metric. Because the strong think about trust parameter, will affect the strength of security. Furthermore, they works hard to give a measure for the Anti-Attack metric.

Finally, the systems that does not concern the security are Universal Plug and Play, MANET, WISE, and Easy Living. In the Universal Plug and Play system, problems encountered some security. First, it enables the attacker to access the system with no restriction in access right. Another problem is the unlimited permits to get information from remote devices. In this case, the system will be subject to the denial of service (DoS) attacks. Furthermore, the devices can access the networks without any authentication. So, there is no mention of any consideration of security inside the design of UPNP. Mobile ad hoc Networks (MANET) is another example of the systems that does not concern the security. This system's design has some problems such as the problem of mobile nodes that are not part of any organization made the security upon predefined trusts impossible. Another problem is the advantage of no infrastructure to build this network made some security mechanism not suitable to use such as Key Server. Finally, securing ad hoc networks needs to be consider.

Another work is the Wireless Intelligent Sensors (WISE) that is a new architecture for monitoring patient in a tele-medical environment [2]. In this medical system, the risks of illegitimate access increase by wearing devices that makes sensitive information available. So, it needs special consideration to secure information such as encryption, access control, integrity and, repudiation which is not available right now. Finally, the EASYLIVING system that proposed by Microsoft research department [8] aimed to build an intelligent environment which makes the interaction easier. It allows a person in his home to make a call by just speaking to the target person from anywhere inside the home. This system's design does not consider any security issues related to gathering information such as the person location that reduce privacy and increases risks. The system needs to improve security and make the system more private.

3. System Design

As seen before, in defining a security protocol we have to consider some concepts: authorization, non-repudiation, integrity, access control, and encryption. Initially the design will start using Gaia Mobile initial specification and then extend as necessary.

First, there is some abbreviations required to use in describing the security protocol/interaction:

KS_{Pub}	S public key
KS_{Priv}	S private key
$E(r, KS_{Pub})$	r is encrypted using S public key

$D(c, KS_{Priv})$	c is a cipher text decrypt using S private key
S(c, KSpriv)	c is signed using S private key
$V(c, KS_{pub})$	verification of sender sign using S public key

First, the coordinator of the space is the device who is responsible to manage the work of the cluster. The coordinator will set the name for the space let say the space name is (S). Then, it uses a key pair for this coordinator (KSPub, KSPriv). In addition, the coordinator will store an access control list (ACL) including each device with its access right to the services available. Access control list must distributed to the principles for updating the space information, or if coordinator crash or disconnected. For the integrity, the information stored in the list will hashed before distributed for prevent it from alteration by illegitimate users. Also, all client devices must store a list of all spaces that has permit to access. Adding each space name with its certificate name.

The discussion will divided into two main phases:

1. First Phase: Setting up a space:

In this phase, the mutual authentication concept is applied when the device register at the first time. Notice that, the client will initiate all the calls and the action will do inside the coordinator. In addition, the process of retrieving public\private key will be using the digital certificate of the entity. After the coordinator of the space (S) discovers a device (B) nearby, it will invite the device to join the space (S). The system will start the process of authentication as follow:

a. Device (B) will check if the space name (S) is exists in the list of permitted spaces.
b. If the space (S) exists in the list, device (B) will call the remote function inside the coordinator to encrypt a random number (r) using coordinator space public key (S) to authenticate the coordinator identity then call the signature remote function to sign the encrypted message using device (B) private key. Notice that, we need to apply the signature for the purpose of non-repudiation, and ensure that device (B) owns the public key.
c. Then, device (B) will call the remote function inside the coordinator to verify the signature using (B) public key then it calls the remote function to decrypt the message and return the random number to the device (B).
d. After that, the device (B) will call the encryption remote function to encrypt new random number using the device public key (B) to achieve mutual authentication then call the signature remote function to sign the encrypted message with coordinator private key (S).
e. The device (B) will call the remote function to verify the signature using coordinator public key (S) then it call the decryption remote function to decrypt the message and return back the random number.

2. The interaction with services:

The coordinator has an important role in distributing the rights of which device can use such service which is stored in access control list (ACL). The access control list defines each device with its access right to which services can access. However, this distribution must be in a way that no one can alter its content by adding service or removing other. This can be accomplish using the hash function. As we know, hash function or digest function is use heavily for ensuring the integrity of the data, which has the best performance comparing with shared key and public/private key

.

a. The device (B) requests a service from Coordinator (C).
b. The device (B) will call the remote function at the coordinator to check the rights in ACL to ensure that it has the authority to use this service. If the device (B) has the access right to use this service then the authentication phase will start.
c. The device (B) will call the encryption remote function to encrypt the shared key (SK) with device (B) public key and call the signature remote function to sign the encrypted shared key by coordinator (C) private key.
d. After, the device (B) will call the remote function to verify the signature by using (C) public key then call the decryption remote function to decrypt the message by its private key. Now, device (B) has the shared key and can use it for this session.
e. The device (B) will call the encryption remote function to encrypt the random number with shared key (SK) and call the signature remote function to sign the message by device (B) private key to achieve mutual authentication and non-repudiation.
f. Device (B) will call the remote function to verify the signature using (B) public key in the certificate then it call the decryption remote function to decrypt the message using shared key (SK) and return the random number to (B).

3. Also, we achieve a secure communication channel using data envelop concept.

Notice that, the client can request any service reside at other client. Then, the target client will check its access rights in the ACL list. If it has, the authentication process using data envelop will be applied with the help of the space coordinator.

4. System Implementation

The implementation process is using Microsoft Visual Studio .Net with the use of .Net Remoting feature to achieve the communication between different applications. Therefore, we need to build an abstract class that is inherit from the "*MarshalByRefObject*" in order to achieve the remote calls from other applications to the coordinator. Another application needed is the server or coordinator application that used to listen to the remote object requests. Also, the client application is needed to initiate the requests of the remote object. For the cryptography, we use both symmetric and asymmetric cryptography. The asymmetric cryptography is used to set up the space and to exchange the symmetric shared key for the purpose of authentication. The selected asymmetric key algorithm was the *RSA (Rivest, Shamir and Adleman)*. On the other hand, the symmetric cryptography used was *Rijndael or Advanced Encryption Standard (AES).* Also, we used the hashing algorithm *Message Digest algorithm 5 (MD5)* for the data integrity. In this project, *(MD5)* used to check that ACL list does not change. The certificate used in the project was x.509 certificate.

5. System Evaluation

In order to evaluate the system, it is important to measure the performance of the security protocol. As we know, we can measure the performance of the system by measuring the communication time and, the cryptography speed. The communication time means the time needed to send a message and get the respond from the remote application. When talking about the communication time, there are some factors affect in measuring it such as processor speed and memory capacity. In addition, the network distribution will affect the speed because when all the parties communicate inside one computer it will be faster than communicating over multiple computers. Another issue is the technology used in the communication such as Wifi or, over internet.
First, the performance of communication in the case of simulating the system inside one computer will be smaller in comparing with the use of multiple computers.
Second, the cryptography speed means the time needed to get the key from the certificate and apply it on the message. Third, it depends on the algorithm used, key length and, key retrieval way.
In asymmetric cryptography, we chose the RSA algorithm with 1024 bits key length. However, in the symmetric key the Rijndael or Advanced Encryption Standard (AES) block cipher algorithm is used. Also, in talking about the hashing algorithm used in hashing the ACL list the MD5 is chosen.

Here, is the evaluation of time in milliseconds needed to complete the security protocol. We use five client applications to communicate with the Coordinator in order to evaluate the performance. Notice that, these information is collected using the simulated system where all the applications reside on one computer rather than multiple computer using .Net Remoting features inside the Microsoft Visual Studio .Net. This evaluation on a PC computer that has the following properties:

table 1:computer property used in systme simulation

Processor	Intel Core 2 Duo 2.10 GHz
Memory (RAM)	2.00GB
System type	32-bit operating system
Windows edition	Windows Vista Home Basic

The evaluation of performance to do the complete security protocol:

table 2: shows the evaluation of performance of the complete secruity protocols

Process	Time to complete the process
Retrieve public key from certificate + RSA encryption (1024bits)	09.25 milliseconds
Retrieve private key from certificate + RSA decryption (1024bits)	12.99 milliseconds
Retrieve private key from certificate + sign the message (RSA+MD5)	15.46 milliseconds
Retrieve public key from certificate + verify signature (RSA+MD5)	11.01 milliseconds
Generate random number	0.00 milliseconds
Rijndael encryption (symmetric 256bits)	0.011 milliseconds
Rijndael decryption (symmetric 256bits)	0.033 milliseconds
The time needs to complete security protocol	48.754 milliseconds
Communication time	01.2 milliseconds
MD5 hashing (for ACL distribution)	05.63 milliseconds

6. Conclusion

In this paper, we discuss a new security protocol for Personal Pervasive Active Space that has similar design to Mobile Gaia. We focused on the issue of authentication after discovering devices and secure communication among devices. We talked about the design of the system to show the interaction between devices. Also, we simulate the system using .Net Remoting feature to handle the communication between different applications. Finally, we made an evaluation of the system performance to show its practicality.

7. Future Work

Modern world with advanced internet technologies dealing with millions of transactions every day; people always concern with their privacy and security of data and personal information. This paper presented a protocol in order to provide different security aspects such as authentication, data integration and authorized control of users. Therefore, in validating the protocol we used a system for proposed protocol simulation purpose. The idea need to be improved in future by applying on different systems with more features and attributes related with different kind of users, which can cover other security issue related with people. Further, it can be enhanced through providing more measurement techniques and dimensions, which can effect on user's data confidentiality.

References

[1] A. Alireza, U. L. (2000). The Challenges of CORBA Security. Springer-Verlag .
[2] Emil Jovanov, D. R. Networks, Patient Monitoring Using Personal Area Networks of Wireless Intelligent Sensors. Huntsville: University of Alabama in Huntsville.
[3] ERONEN, P. (2001). Security in the JINI Networking Technology: A Decentralized Trust Management Approach. Master's Thesis.
[4] IETF. (n.d.). Simple Public Key Infrastructure (spki) Charter. Retrieved from http://www.ietf.org/html.charters/spkicharter.html
[5] James Bresler, J. A.-M. Gaia Mobility: Extending Active Space Boundaries to Everyday Devices. Urbana-Champaign: University of Illinois at Urbana-Champaign.
[6] Lalana Kagal, V. K. A Highly Adaptable Infrastructure for Service Discovery and Management in Ubiquitous Computing. Baltimore: University of Maryland Baltimore County.
[7] Shiva Chetan, J. A.-M. Mobile Gaia: A Middleware for Ad-hoc Pervasive Computing. Urbana-Champaign: University of Illinois at Urbana-Champaign.
[8] Steve Shafer, J. K. (1998). The New EasyLiving Project at Microsoft Research. Microsoft Corporation.
[9] Tim Finin, A. J. A Security Architecture Based on Trust Management for Pervasive Computing. Baltimore: University of Maryland Baltimore County.
[10] Zhou Xingshe, L. X. (2000). Design and Implementation of CORBA Security Service. IEEE , pp. 140-145.
[11] Chun-Ta Li · Cheng-Chi Lee · Chi-YaoWeng.(2013).An Extended Chaotic Map based on user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments. Springer Science.
[12] Madhu Sharma Gaur, Dr. Bhaskar Pant. (2014).Trust Metric based Soft Security in Mobile Pervasive Environment. Modern Education & Computer Science Publisher.
[13] Tao shu, Yingying Chen, and Jie Yang, Member, IEEE. (2015). Protecting Multi-Lateral Localization Privacy in pervasive environment. IEEE.

Jalal Al-Muhtdi received the M.S. and PH.D degrees in Computer Science from University of Illinois at Urbana-Champaign in 1999 and 2005 respectively. He worked as Assistant Professor at King Saud University (2005-present). Also, he worked as a Director of Center of Excellence in Information Assurance (COEIA) at King Saud University, (2013-2016)

Khaloud Zainalabdeen received the B.S. and M.S. degrees in Computer and Information System from King Saud University in 2007 and 2010, respectively. She worked at King Abdul-Aziz University as a lecturer.