Demonstration of Security in Service Discovery and Access for Ubiquitous Networks

Juan Vera del Campo Josep Pegueroles Miguel Soriano

Department of Telematic Engineering,
Polytechnic University of Catalonia, Spain
Email: {juanvi, josep, msoriano}@entel.upc.es

Abstract

Nowadays, networked electronic devices allow users to access services wherever they are. In ubiquitous networks, clients notice the network to be everywhere and hence also ask networked services to be accessible everywhere. In such scenario, announcement and discovering of services are crucial. Current service discovery protocols exist are limited to a concrete network technology and do not fit mobility and security requirements for a global and ubiquitous solution. In this demonstrator the authors introduce a Multiprotocol Service Discovery solution for heterogeneous networks and describe their work for including security as a main design goal of the proposal.

1. Introduction

Ubiquitous networks and pervasive computing make services available everywhere and from multiple kind of devices. However, the lack of interoperability for different service discovery and access protocols and the limited interconnectivity between networks bring new challenges for such scenario. To overcome these drawbacks, FP6 UBISEC [5] project proposed a middleware [4] that manages the dynamic composition of the networks, integrates existing protocols, and provides a generic service to clients for performing service discovery and access. The above mentioned solution included security as one of the design parameters to take into account. In the described scenario, security mostly concern the theft of the identity of some user when it is forged in order to take advantage of his privileges and the theft of the brand of a server used by another server to attract potential customers. Moreover, information attached to service descriptions, especially user profiles, should be protected from unauthorized third parties wishing to collect private data from clients.

Our demonstrator will in particular demonstrate the secure service discovery across multiple discovery domains, and the secure access to services that are not IP reachable. Security services will comprise: Reachability and Availability of data; Data Integrity and Authenticity of the Communication circumstances; Data Confidentiality; Privacy; Non repudiation; Untraceability and Liability.

2. The Middleware Platform

The Middleware platform proposed in [4] was called Multiprotocol Service Discovery Framework (MSD). It is intended to be a middleware platform that lets applications to discover and use services in heterogeneous, mobile and insecure network environments.

The system architecture is structured in five modules: the cache, the network, the security, the group management and the proxies for other protocols. The cache and network modules form the core system and on their own let the registering, discovering and using of services including bridging between different networks and roaming. The rest of the modules are pluggable in those virtual machines with more features. See Fig. 1.

The MSD-aware applications are intended to run in a peer to peer fashion, without the need of a central repository. When a centralized server is needed (for instance for compatibility reasons with concrete Service Discovery Plugins as SLP) an algorithm will result in the election of an MSD manager performing all the centralized functions. This algorithm is executed with the participation of all MSD entities with the whole functionalities.

The network module sets an abstract layer between the MSD and the actual network interface. There is no need of a common address space or even a common network configuration. The MSD sends and receives packeted units called Messages. These messages can be unicasted, multicasted or multiplexed inside Connections. The MSDs identify each

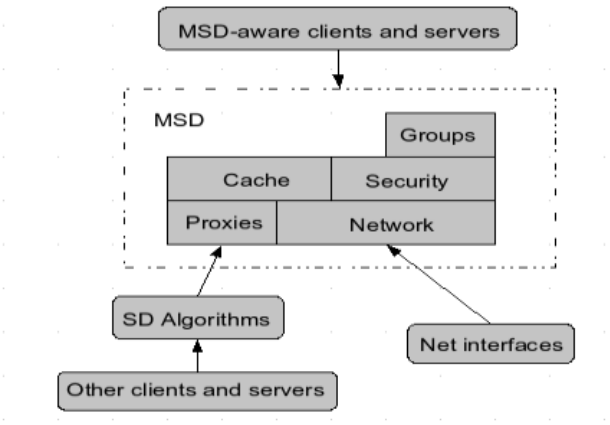

Figure 1. Modules of the MSD

other by means of a Universal Unique Identifier (UUID). There can be MSDs in any network acting as bridges and routing messages between the network interfaces they have got.

3. Security in the platform

Following the security services mentioned in the introduction, our platform assures that a service is always reachable within the area it is announced (reachability) and gives a mechanism for re-establishing availability against DoS attack (availability). Moreover, messages exchanged within the platform add a signed checksum allowing data integrity and authenticity check, both of service data and communication circumstances. Data Confidentiality is achieved by means of the ciphering of sensitive data. We define privacy as the confidentiality of the control plane, so its mechanisms are the same as for confidentiality. Finally, authentication methods in combination with signature functionalities provide non repudiation.

Security is integrated into the four main phases of the MSD platform: discovering other MSDs, joining of new members, service search and service access. PKI Credentials, trust relationships, leader election, group rekeying, encryption of data and signing of messages are some of the techniques used.

Leader election Some features of the platform, as plugins and groups, need a centralized management. Every MSD participates in the election and sends its PKI Credential and some pieces of information, as mobility, remaining battery and processing power. Then, the leader is chosen in a decentralized way among those with best attributes [2]. In dynamic environments, leaders may leave the network, so a new election process takes place when this event is detected.

PKI Credentials and trust relationships During the joining phase, new MSDs present their credentials to the group leader. Since the Certification Authority that signed the credential may be offline, leaders have to be able to assign a trust level to new MSD based on past history [1]. Only MSDs with a higher trust level than the configured one are allowed to join to the group.

Group rekeing After the joining or leaving processes, leaders must change the group key. The distribution of this key among the members of the group is secured with the mechanism in [3]. After the rekeing process, every MSD in the group and only MSDs in the group share the same secret key.

Encryption and Signing During the searching phase, the shared key and the personal private key of the MSD are used to encrypt and sign every message. Confidentiality of the group communications and Integrity of the data are assured by these mechanisms.

Service Access For those services that do not offer security at application level, the group key can be used to provide group confidentiality, and an SSL connection between client and server at MSD level can be established for those services that require further security.

4. Demonstrator

We developed a testbed supporting two different scenarios: one showing the deployment of the MSD without security, and the other including the security services.

4.1. Insecure Scenario: Remote printing service

User A is holding a mobile phone with Bluetooth networking and a camera. A takes a photograph on the fly and wants to print it on a printer connected to an Ethernet network. The Ethernet network has a WiFi Access Point. Some devices in the WiFi network also have Bluetooth interfaces. These can act as bridges. See Fig. 2.

User B publishes its printing service using SLP and the MSD platform detects and registers this service. Then, A takes a photograph and joins to the MSD network looking for available printers. The printing service in B is detected through the bridge M. Finally, A sends its photograph to B and it gets printed.

Notice that this scenario does not face security: malicious printers can be registered and the data is sent in clear, so anyone is able to eavesdrop the photograph taken by A.

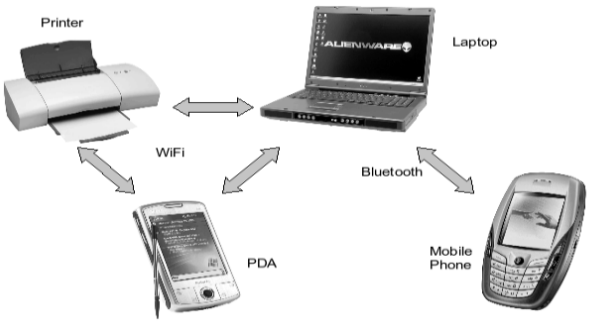

Figure 2. The insecure scenario

4.2. Secure Scenario: University Campus File Sharing

Teacher A holding a PDA with a Bluetooth network interface wants to get an exam E from the distributed exams database. He does not know where the file actually is, but his PDA can search for the desired resources. The network in the campus works in a decentralized fashion with many laptops offering bridging to the Internet. One specific laptop (M) offers an Internet gateway to Bluetooth devices. This bridge is managed by students. Teacher A should be able to get the exam E using his Bluetooth PDA connection without noticing the students he is accessing an exam. See Fig. 3.

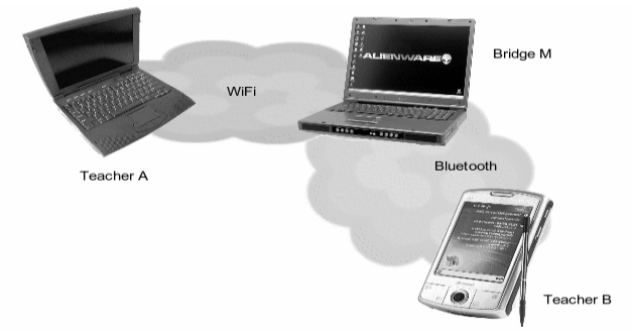

Figure 3. The secure scenario

The first step in the demonstration is the setting of the Teachers group. Then, only authorized members of this group will be able to access exams. It is possible to use the internal capabilities of the MSD to perform the grouping. Teachers join the group and a teacher leader is set to manage a server for the LKH rekeying [3] .

The next step is the publishing of the exam E for the Teachers group. Any description of the file-sharing service must be encrypted with the shared key K, so no student will be able to recognize that an exam is being published. When A searches for an exam he will notice the existence of E since A is an authorized member of the group named Teachers. Every message exchanged during the search must be secured with the key K. Once discovered, A downloads E from its actual location. To ensure confidentiality, A and B create an encrypted tunnel between them.

By means of the initial grouping, students cannot steal the identity of a teacher. Although pupils control the bridge M, the use of the common key prevents the eavesdrop of the communications between A and B. These points are demonstrated viewing the messages logged in A, B and M.

The security services provided by the platform are:

Confidentiality since students cannot read the exam E by sniffing the communication. This is achieved by means of encrypting the messages with TripleDES using the shared key of the group Teachers.

Integrity and No Repudiation because exchanged messages are signed with a private key. Every message includes a HMAC-RSA signed with the private key of the sender.

Privacy since students cannot discover that exam E has just being published. Searching messages are encrypted with TripleDES using the shared key of the Teacher's group. No user outside the group is able to process messages searching for exams.

Authority and Authentication Students cannot steal the identity of a teacher. By means of X509 Certificates, Teachers identify themselves against the Teacher's group leader, and they are not accepted into the group without a valid certificate.

5. Acknowledgement

This work has been partially funded by UBISEC project under grant FP6 IST-2002-506926 and SECCONET project under grant CICYT - TSI2005-07293-C02-01.

References

[1] F. Almenez, A. Marin, C. Campo, and C. G. R. A Pervasive Trust Management Model for Dynamic Open Environments. In *First Workshop on Pervasive Security and Trust at MobiQuitous 2004, Boston, USA.*, 2004.

[2] J. Hernadez-Serrano, J. Pegueroles, and M. Soriano. GKM over large MANET. In *IEEE International Workshop on Self Assembling Wireless Networks*, 2005.

[3] Pegueroles, Wang-Bin, Soriano, and Rico-Novella. Group Rekeying Algorithm using Pseudo-Random Functions and Modular Reduction. *Lecture Notes in Computer Science*, 3032:875 – 882, 2004.

[4] P.-G. Raverdy, V. Issarny, R. Chibout, and A. de La Chapelle. A Multi-Protocol Approach to Service Discovery and Access in Pervasive Environments. In *Middleware'2005 CD*, 2005.

[5] www.ubisec.org. Main page of ubisec project, 2006.