Security in a Wireless Mobile Health Care System

Ramon Martí
Jaime Delgado
Universitat Pompeu Fabra (UPF)
Passeig de Circumval·lació 8
E-08003, Barcelona
Spain
E-mail: {ramon.marti, jaime.delgado}@tecn.upf.es

***Abstract*- The paper describes the requirements and implementation of security mechanisms for a Wireless Mobile Health Care system. All the security work in this paper has been analyzed and developed in the context of the MobiHealth project [1], co-funded by the European Commission (IST-2001-36006).**

I. INTRODUCTION

This paper describes the requirements and implementation of the security mechanisms for a Wireless Mobile Health Care system, MobiHealth, co-funded by the European Commission (IST-2001-36006). The following topics of security in the MobiHealth system are presented:

- MobiHealth System Overview: Overview of the project objectives, the different scenarios , the system architecture and the system components and communications.
- Security Solutions for MobiHealth: Description of the different possible solutions that have been considered for providing security to the MobiHealth system.
- MobiHealth Security Requirements: Description of the security requirements for the MobiHealth system, both general requirements as well as requirements related to the use of dynamic IP in some of the components of the system.
- MobiHealth Security Implementation: Description of the security options implemented in the MobiHealth system, from the description of the implementation issues related to the security in the different communication stack levels, the issues related to the use of dynamic IP, to the description of the security of the whole MobiHealth system as well as the security in the components, in the network and in the data communication level.
- Conclusions: Conclusions about implementation of security in the MobiHealth wireless mobile health care system.

It must be noted that the MobiHealth project started in May 2002 and it is expected to be finished in October 2003, so the trials to be started soon may lead to some changes in the final implementation.

II. MOBIHEALTH SYSTEM OVERVIEW

Before describing the security issues of the MobiHealth system, it is important to know a little bit more about this project, describing its objectives, the testing scenarios that have been defined and the system architecture.

A. MobiHealth Objectives

MobiHealth is a mobile healthcare project funded by the European Commission. MobiHealth aims at developing and trialing new mobile value-added services in the area of healthcare, thus bringing healthcare to the patient.

The MobiHealth system allows patients to be fully mobile whilst undergoing health monitoring. The patient wears a lightweight monitoring system – the MobiHealth BAN (Body Area Network) – which is customized to their individual health needs. Physical measurements such as blood pressure or ECG are measured by the MobiHealth BAN and transmitted wirelessly from the BAN to their doctor, the hospital or their health call centre.

Therefore, a patient who requires monitoring for short or long periods of time doesn't have to stay in hospital for monitoring but with their MobiHealth BAN can be free to pursue daily life activities.

The MobiHealth consortium unites 14 partners from five European countries and represents all the relevant disciplines. Partners include: hospitals and medical service providers, universities, mobile network operators, mobile application service providers and mobile infrastructure and hardware suppliers.

B. MobiHealth Scenarios

For implementing and testing the MobiHealth system, the following scenarios have been defined by the hospitals and medical service providers partners:

- Telemonitoring of patients with ventricular arrhythmia
- The lighthouse alarm and locator trial
- Physical activity and impediments for activity in women with Rheumatoid Arthritis
- Monitoring of vital parameters in patients with respiratory insufficiency
- Home care and remote consultation for recently-released patients in a rural area
- Support of home-based healthcare services
- Outdoors patient's rehabilitation
- Tele trauma team
- Integrated homecare in women with high-risk pregnancies

C. MobiHealth System Architecture

The MobiHealth system is composed of a set of different sensors connected to a PDA or mobile phone that transmits, in a secure way, all the patient data to a central server in the hospital. The authorized doctors can access these medical information from their computers (inside the hospital or even outside) both at real time as well as afterwards, and can even interact with the PDA.

The system, that is a BAN (Body Area Network), has been developed in a way that it is easily configurable, so different medical trials have been defined and are being done throughout all Europe.

Figure 1 describes the main components of the MobiHealth system and the interactions between them.

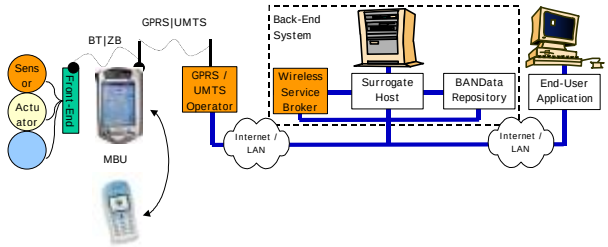

Fig. 1: MobiHealth system architecture

D. MobiHealth Components

The following are the different components that are defined in the MobiHealth system and their functionality:

- Sensor: A device, such as a photoelectric cell, that receives and responds to a signal or stimulus.
- Actuator: A device responsible for actuating a mechanical device, like one connected to a computer by a sensor link.
- Front-End: Hub for all the sensors and actuators in the BAN. It records all the data from all the sensors and actuators, and can send them to the MBU.
- Mobile Base Unit (MBU): PDA or Mobile Phone.
- GPRS/UMTS Operator: Network operator providing GPRS/UMTS access to Internet.
- Back-End System (BEsys): System composed of a Wireless Service Broker, a Surrogate Host and a BANData Repository. The BEsys has been installed in some of the GPRS/UMTS service providers, as well as in some of the Hospital / Health care centers.
- Wireless Service Broker (WSB): Authenticates and authorizes the MBUs.
- Surrogate Host (SH): Main server, where wireless sensor and actuator objects are "surrogated" inside the wired Internet, and where medical data is received.
- BANData Repository (BDR): A process that acts as a client to the Surrogate Host (i.e. it is a Jini service user of the MBU service provider). In addition, the BDR writes the medical data (i.e. measurements) to persistent storage.
- End-User Application (EUA): Computers in the Hospital / Health care centre, used to access the information from the Sensors and Actuators and to send new configuration parameters to the BAN, through the access to the BESys. They can be either a server in the Hospital / Health care centre, that accesses the data from the Surrogate Host or the BANData Repository and stores it in the already existing patients database, or user computers of the authorized employees, that access the information from the BANData Repository, from inside the hospital but also from outside.

E. MobiHealth Communication

Different communication interactions exist between the components of the MobiHealth system. These communications can be done in two ways: from the MBU/Sensors to the End-User Application, but also from the End-User Application to the MBU/Sensors:

- Sensor - Front-End: Wired communication (or wireless through Bluetooth or Zigbee).
- Actuator - Front-End: Wired communication (or wireless through Bluetooth or Zigbee).
- Front-End - Mobile Base Unit: Wireless communication through Bluetooth or Zigbee.
- Mobile Base Unit - GPRS/UMTS Operator: W-TCP|TCP|UDP/IP communication through GPRS/UMTS [with HTTP/HTTPS application layer protocol, and HTML data from MBU - Surrogate Host communication]*.
- GPRS/UMTS Operator - Wireless Service Broker: W-TCP|TCP|UDP/IP communication [with HTTP/HTTPS application layer protocol, and HTML data from MBU - Surrogate Host communication]. This communication is done through local LAN, when the WSB is installed in the same location as the GPRS/UMTS Operator, or through Internet when it is in a different location.
- Mobile Base Unit - Wireless Service Broker: HTTP/HTTPS application layer protocol, and HTML data [through different communication hops].
- Wireless Service Broker - Surrogate Host: Local (WSB in the same system as the Surrogate Host) or TCP/IP (in a LAN) communication, with HTTP/HTTPS application layer protocol, and HTML data.
- Surrogate Host - BANData Repository: Java Jini and RMI (Remote Method Invocation) access to remote sensor objects in the Surrogate Host. This communication is usually Local (BDR in the same system as the Surrogate Host) or through TCP/IP LAN communication.
- Surrogate Host - End-User Application: Java Jini and RMI (Remote Method Invocation) access to remote sensor objects in the Surrogate Host. This communication is done through TCP/IP Internet communication.
- BANData Repository - End-User Application: Remote access of the client to the data in the BANData Repository. TCP/IP-based communication internal to the hospital. The access is done through HTTP/HTTPS application layer protocol, and HTML data, and the communication through TCP/IP in Internet or LAN.

* In square brackets are displayed communications that pass through that communication path, but are generated in another one.

III. Security and Communication Solutions for MobiHealth

For the development of the security in MobiHealth, different existing security and communication technologies have been considered. This clause gives and overview of all of them.

A. IPSec

IPSec (IP Security) [2] is a protocol that provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets. IPsec consists of several separate protocols. Standard keying data exchange is actually optional, since the security mechanisms and the secret keys can be agreed beforehand and configured manually.

B. SSL/TLS - Secure Sockets Layer / Transport Layer Security

Secure Sockets Layer (SSL) [4] is a protocol that provides secure communications on the Internet. Transport Layer Security (TLS) [5] is the successor to the SSL, based on SSL 3.0 protocol. SSL/TLS provide data encryption, message integrity, server authentication, and optional client authentication for a TCP/IP connection. They run above TCP/IP and below higher-level protocols.

C. HTTPS

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) [6] is a Web protocol developed by Netscape that encrypts and decrypts user page requests and the pages returned by the Web server. HTTPS is just the use of Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layer. (HTTPS uses port 443 instead of HTTP port 80). HTTPS and SSL support the use of X.509 digital certificates from the server so, if necessary, a user can authenticate the sender. HTTPS is not to be confused with S-HTTP, a security-enhanced version of HTTP developed and proposed as a standard by EIT. [3]

D. JINI

Jini is a new idea that Sun Microsystems calls "spontaneous networking." Using the Jini architecture, users can plug any kind of device directly into a network and every other computer, device, and user on the network will know that the new device has been added and is available. Each pluggable device defines itself immediately to a network device registry. When someone wants to use or access the resource, their computer is able to download the necessary programming from it, to communicate with it. No longer device driver needs to be present in an operating system, sinceit knows about all accessible devices through the network registry. [3]

E. RMI (Remote Method Invocation)

RMI (Remote Method Invocation) is a way that a programmer, using Java, can write object-oriented programming in which objects on different computers can interact in a distributed network. RMI is the Java version of the remote procedure calls (RPC), but with the ability to pass one or more objects along with the request. The object can include information that will change the service that is performed in the remote computer. Sun Microsystems, inventors of Java, calls this "moving behavior." RMI is supplied as part of Sun Microsystem's Java Development Kit (JDK). [3]

IV. MOBIHEALTH SECURITY REQUIREMENTS

For the development of the security aspects of the MobiHealth system, general security requirements, as well as requirements related to the fact that dynamic IP is used in some parts of the system, had to be taken into account. These requirements are described in the following subclauses.

A. General Security Requirements

Different security requirements have to be taken into account when developing a mobile health care system. These include access security in all the hardware devices in the system (from the PDA to the hospital server and through all the computers in the communication way), security in data transmission (in all the transmission path from the PDA to the hospital server), and data storage security, mainly in the hospital server.

The security requirements in the MobiHealth system can be summarized as follows:

- Data sent from the MBU and to the MBU must be secured with encryption and user and server authentication in the communication path to the Surrogate Host.
- Access to data in the Surrogate Host from a computer different from where the Surrogate Host runs must be secured with encryption and user and server authentication.
- No data storage in the "disk", but some data storage for buffering, for the Front-End, MBU, GPRS/UMTS Operator, WSB and End-User Application (for Hospital employees computers).
- Secure data storage for the BANData Repository and End-User Application (for Hospital server with patients DB).

B. Dynamic IP Security Requirements

Apart from the requirements for the MobiHealth security, some requirements related to Dynamic IP of some of the components of the system have to be considered and taken into account for implementation of security in the MobiHealth.

Dynamic IP MobiHealth Components

Two components of the MobiHealth system may have dynamic IP:

Mobile Base Unit:

- The Address of the MBU is provided dynamically by the GPRS/UMTS operator.

End-User Application:

- If the End-User Application is the Hospital server, it probably has static IP.
- If the End-User Application is an Hospital employee accessing from inside the hospital it may have a static IP or dynamic IP, depending on the Hospital address distribution policy.
- If the End-User Application is an Hospital employee accessing from outside the hospital, it is probably connected through some ISP and it has a dynamic IP address.

Dynamic IP Protocol Issues

The use of dynamic IP in some of the components of the system has some implications in the security protocols, that have also to be taken into account in the specification of the security for the MobiHealth system.

Bluetooth

- Bluetooth is independent from the dynamic IP address that the system it is connected to is using to connect to Internet.

GPRS

- GPRS uses dynamic addresses, so client address may change.
- In GPRS address is not changed during a connection. Address can only change during a connection failure.

IPsec

- IPsec communication depends on node addresses: Client address and server address.
- IPsec is network layer security. It is based on node-to- node, so it is based on node addresses.
- IPsec is based on node-to-node security, so it can be used for end-to-end, end-to-node and node-to-node security.
- IPsec SPD (Security Policy Database) in a node (server/client/router) IPsec, filters packets depending on remote host (client/server) address.
- IPsec allows to grant access to data to more than one host. IPsec is independent from the user connected to that host).

HTTPS

- HTTPS communication depends on the server address.

HTTPS communication is independent from client address.

- HTTPS security depends on server (and client) certificates.

SSL/TLS

- SSL communication depends on server/responder address, and it is independent from client/initiator address.
- SSL security depends on server/responder certificates.
- In GPRS, dynamic address is changed, only when there is no connection. Using SSL, the client may reconnect to the server even with a different IP address.
- SSL can authenticate the server and the client hosts through X.509 certificates. SSL authentication is independent from the host addresses.
- SSL using X.509 certificates allows to grant access to data to more than one user.

V. MOBIHEALTH SECURITY IMPLEMENTATION

Different technologies have been analyzed to provide all the security required by the system, and the best solutions have been developed, taking into account the different technical (e.g. PDA computing power) and human restrictions (e.g. some users that may use the system may be old or disabled). It must be noted that the communications can be in the two ways: from the MBU/Sensors to the End-User Application, but also in the inverse way.

A. Security of Communications in MobiHealth

The different security protocols that have been considered for the MobiHealth system belong to different communication stack layers, and for this reason they provide different security features, that are described in this clause:

- Data link layer: Bluetooth, Zigbee, GPRS/UMTS, ...
- Network layer: IPsec, ...
- Transport layer: SSL/TLS, ...
- Application layer: Data encryption

Data Link Layer Security

Security in the Data Link Layer provides Hop-to-hop protection (encryption and authentication), with no user or application authentication. Security provided by Bluetooth, Zigbee or GPRS/UMTS, are examples of Data Link Layer protection.

Network Layer Security

Security in the Network Layer provides node-to-node protection (encryption and authentication), with no user or application authentication. The node-to-node protection in the network layer can be hop-to-hop protection or end-to-end protection. For the Network Layer protection, IPsec is an example, that can be used between systems using static IP.

Transport Layer Security

Security in the Transport Layer provides a end-to-end protection. Security in the Transport Layer provides application-to-application protection, and it can also include some user authentication. SSL/TLS or HTTPS are two examples of Transport Layer security.

Application Layer Security

Security in the Application Layer provides application-to-application and application_user-to-application_user protection, including user authentication. Application Layer security is provided through the encryption or/and signature of the data sent through the communications stack. SMIME or user-invoked cryptographic functions (e.g. OpenSSL) are example of tools that can be used to encrypt and sign data for the Application Layer security.

B. Dynamic IP Security

From the dynamic IP security requirement described previously, the implementation of the security in the MobiHealth has been restricted to the consideration of the following points:

- IPsec provides communications security, data encryption and node authentication, based on node addresses.
- IPsec is not suitable for providing communications security from the MBU, since it has dynamic IP, or from the EUA, since it may also have dynamic IP. Then, IPsec is not suitable to provide security to MBU - WSB, MBU - Surrogate Host, BDR - EUA or SH - EUA security.
- IPsec is suitable for providing communication security between hosts with static IP. Then, IPsec is suitable for providing security to GPRS/UMTS Operator - WSB, WSB - Surrogate Host and GPRS/UMTS Operator - Surrogate Host, Surrogate Host - BANData Repository, etc.
- SSL and HTTPS provide data transport-level security to communications requiring data encryption and user authentication, based on server node address.
- SSL and HTTPS are suitable for providing communications security from the MBU and the EUA. Then, it is suitable to provide security to MBU - WSB or MBU - SH, BDR - EUA or SH - EUA security.
- GPRS and Bluetooth are suitable for communications requiring data encryption and terminal authentication

C. MobiHealth System Security

Taking into account the different issues related to the security and to the MobiHealth requirements and architecture, the following security mechanisms have been selected for the MobiHealth system:

- Bluetooth | Zigbee security for encrypted and authenticated data transmission between the Front-End and the MBU.
- HTTPS for encrypted and authenticated data transmission between the MBU and the Wireless Service Broker.
- HTTPS for encrypted and authenticated data transmission between the Wireless Service Broker and the Surrogate Host, if both run on different computers.
- RMI security (SSL | IPsec) for the BANData Repository access to the Surrogate Host data, when both are in different systems.
- RMI security (SSL) for the End-User Application access to the Surrogate Host data, when both are in different systems.
- RMI or HTTPS security for the End-User Application access to the BANData Repository data.
- No data storage in the “disk”, except for buffering, for the Front-End, MBU, GPRS/UMTS Operator, WSB and End-User Application (Hospital employees computers).
- Secure data storage, with confidentiality and user access authentication, for the BANData Repository and End-User Application (for Hospital Workstation with patients DB).

Figure 2 shows implementation of the security in the MobiHealth system, described in the next subclauses. It includes the communication and security options implemented in MobiHealth:

- Network communication mechanism and security
- Data transfer protocol/mechanism and security

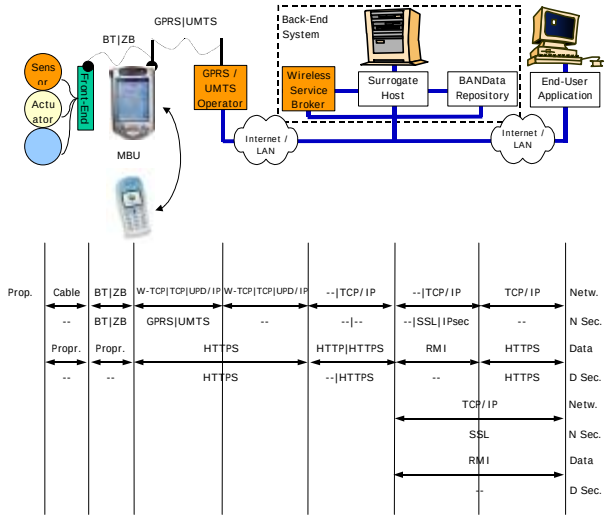

Figure 2: Security implementation in the MobiHealth System

D. MobiHealth Components Security

The different components of the MobiHealth system required different security levels and options.

- Sensor: No data must be stored in the sensor.
- Actuator: No data must be stored in the actuator.
- Front-End: No data must be stored in the "disk". Data can be stored in memory only for buffering and temporary disconnection recovery purposes.
- MBU (Mobile Base Unit): No data must be stored in the "disk". Data can be stored in memory only for buffering and temporary disconnection recovery purposes. MBU must act as an HTTPS client, supporting user and server authentication. An X.509 user certificate and private key must be stored in the MBU.
- GPRS/UMTS Operator: No data must be stored in the GPRS/UMTS Operator system.
- WSB (Wireless Service Broker): No data must be stored in the disk. Data can be stored in memory only for buffering and temporary disconnection recovery purposes.
- Surrogate Host: No data must be stored in the disk. Data can be stored in memory only for buffering and temporary disconnection recovery purposes. Surrogate Host must act as an HTTPS server, supporting user and server authentication.
- BANData Repository: Data is stored in a secure way. The system uses data encryption with an "internal" BANData Repository key, together with a secure data access.
- End-User Application: When corresponding to authorized employees from the Hospital / Health care centre, no data can be stored in the disk; data can be stored in memory only for buffering and temporary disconnection recovery purposes. When corresponding to the system with the Hospital patients DB, data must be stored in a secure way.

E. MobiHealth Network and Data Communication Security

Different network protocols and related security options have been selected for the MobiHealth system, as well as different data communication protocol-format and related security. Following is the detailed description of the network protocols / network protocols security implemented in MobiHealth, followed by the data communication protocol-format / data communication protocol-format security for each communication path in the system:

- Sensor - Front-End: wired / No security; Proprietary data communication protocol / No data communication security.
- Actuator - Front-End: wired / No security; Proprietary data communication protocol / No data communication security.
- Front-End - MBU: Bluetooth | Zigbee / Bluetooth | Zigbee security; Proprietary data format / No data communication security.
- MBU - GPRS/UMTS Operator: W-TCP|TCP|UDP/IP / GPRS/UMTS security; No direct data communication / --.
- GPRS/UMTS Operator - Wireless Service Broker: W-TCP|TCP|UDP/IP / No network level security; No direct data communication / --.
- MBU - Wireless Service Broker: No direct network communication / --; HTTPS / HTTPS encryption and user and server authentication.
- Wireless Service Broker - Surrogate Host: Local | TCP/IP (LAN) / No network level security; HTTP | HTTPS / No data security, but user authentication in HTTP | HTTPS encryption and user and server authentication.
- Surrogate Host - BANData Repository: Local | TCP/IP (LAN) / No network level security | SSL | IPsec security; RMI / No data security.
- Surrogate Host - End-User Application: TCP/IP / SSL security; RMI / No data security.
- BANData Repository - End-User Application: TCP/IP / No network level security; HTTPS / HTTPS encryption and user and server authentication.

VI. CONCLUSIONS

All the work presented in this paper can be summarized saying that using existing technologies has been fully feasible the development of a mobile health care system and the integration of security in it, both in the communications as well as in the data.

Additionally, the security options included in the MobiHealth system have the following features and advantages:

- Use of standard user-oriented security mechanisms.
- No use of IPsec host-oriented security.
- All communications and data from the MBU to the Surrogate Host are secured through authentication and encryption, independently from the underlying network.

ACKNOWLEDGMENT

All the work presented in this paper has been done in the context of the MobiHealth project, co-funded by the European Commission (IST-2001-36006).

REFERENCES

[1] MobiHealth web site (http://www.mobihealth.org)
[2] RFC 2401, "Security Architecture for the Internet Protocol" S. Kent, R. Atkinson, November 1998.
[3] Whatis.com (http://www.whatis.com)
[4] SSL3, "The SSL 3.0 Protocol", A. Frier, P. Karlton, P. Kocher, Netscape Communications Corp., November 18, 1996.
[5] RFC2246, "The TLS Protocol Version 1.0". T. Dierks, C. Allen. January 1999.
[6] RFC 2818, "HTTP Over TLS", Rescorla, E., May 2000.