EIB remote control through a secure channel via Internet: Domoware©

C. Fernández-Valdivielso, I.R. Matías, A.J. Mardones and F.J. Arregui
M. Jiménez*, J.A. Vera* and J. Roca*

Dept. Ingeniería Eléctrica y Electrónica
Universidad Pública de Navarra

31006-Pamplona (Spain)
carlos.fernandez@unavarra.es
Tel: 34 948 169 841
Fax: 34 948 169 720

** Dept Tecnología Electrónica*
Universidad Politécnica de Cartagena
30202 Cartagena (Spain)
jose.vera@upct.es

Abstract.

A new software tool implemented to achieve a remote control of any home automation system is presented: Domoware©. It has been designed in order to guarantee a secure channel of communication through Internet. The developed software tool follows the client/server architecture, therefore, it must be installed in two places (both of them with Internet access): a PC connected directly to the EIB installation (through the serial port) and a PC from where the remote control is going to be implemented. In short, Domoware© allows programming any EIB installation in a remote way; making easier and secure the maintenance and future reprogramming of the building.

1.- Introduction

The Universidad Pública de Navarra has been busy in the domain of Home Automation for many years. Home Automation Systems are taught as one of the subjects within the last year in the degree of the Telecommunication Engineer. Also, a laboratory with several Home Automation Systems is set up for use in education and research at the university [1]. Besides, a set of software tools for home automation systems is developed at the university [2]. Nowadays, as remote control via Internet is a hot topic, the convergence between EIB and Internet is being developed very fast. Nevertheless, the security of the messages is one of most important concerns in this field. In fact, Internet has important lacks of data, not only for the transmitted information but also for the running_software. In order to guarantee the privacy in the remote control of domotic installations, the Universidad Pública de Navarra in collaboration with the Universidad Politécnica de Cartagena have developed a new software tool named Domoware©. It allows the remote control of an EIB installation via Internet through a secure channel.

First of all, before trying to establish the communication channel, any remote control software must control the communication between the home automation system and the computer. Most of the building control systems (including EIB) use the serial port and the EIA232 communication protocol as interface between the installation and the user [3], and besides, this port is also used to load the application programs. Domoware© has been created to be applied in all those systems that use the EIA 232 and the serial port. So, once the communication between the computer and the home automation system is under control, the remote communication can be initiated. In this point is where Domoware© has special significance: it guarantees a secure channel to establish the communication between the installation and the remote control.

2.- Domoware© characteristics.

The main objective of Domoware© is guaranteeing the security while a remote control above any home automation system is being executed. Remote control of any home automation system includes not only communication with on/off actuators but also programming of the whole installation, testing or interrogating about the state of each device.

In order to establish the remote control, two computers are needed; one must be connected to the home automation system for local control, and the other one is located remotely. The communication between both computers is via Internet, as is the most universal channel and everybody can have access to it. Other communication channels have been also studied, such as direct connection trough a dedicated line or a telnet, but all of them have been rejected due to economic or security factors. Thus, dedicated lines are more expensive due to its maintenance and hire, and a telnet is not a very secure communication channel, so Internet is the best solution.

Domoware© has been created using the programming language Visual C++ v.6.0 [4]. This language was chosen because it is an oriented objets language, it supports interruptions and it can control the computer ports.

As Domoware© must be installed in two computers (the installation and the remote control station) a client/server architecture has been designed. In this point, there are two different cases:

1.- The client has got a problem and is looking for the solution.
2.- The client wants to control his own installation.

In the first case, the client requests the connection to a post-sale company or a maintenance company. His installation does not work as the user wants, and is looking for a fast solution. This is the case where the client is located at the computer that is directly connected to the home automation system, and the server is the computer that gives the technical support in order to program and maintenance the home automation systems in a remote way. This solution is faster and cheaper than traditional solutions.

The second case takes place when the user or the company wants to monitor their building anytime and from anywhere. Then, the server is the computer that is directly connected to the home automation system, and it will be waiting for the client's request, in order to receive instructions either to modify the program or to check the installation. The client is the computer from where the user wants to monitor his own building, from this computer, the user requests the connection to the server via Internet.

The main important feature of Domoware© is security. Domoware© uses public key cryptography for the authentication of both sides in the communication and private key cryptography for the transmission of the information.

3.- Domoware© security.

The main objective of security in Internet is protecting the information. This is because the communication channel can be tapped by modifying, listening or even intercepting the information travelling through it. So security in Internet is used in order to defend the information against external attacks [5].

There are two main methods to protect the communication in Internet:

1.- Firewalls: the system controls the incoming information and restricts it.
2.- Cryptography: the system uses coding methods to send the information.

Cryptography has been the chosen method used in Domoware©. The firewalls method was rejected as it is a limited method for software tools and because a hacker can "trick" the computer identifying itself with an allowed address. Once cryptography is chosen as the security method used in Domoware©, the security is based on four aspects:

- **Privacy**: the possible intruders can obtain nothing by listening the information.
- **Authenticity**: both sides of the communication are completely sure that the other computer is the right one.
- **Economy**: the information sent is just only the needed information.
- **Verifiability**: the message is the authentic one.

In order to keep all the objectives, Domoware© uses different cryptography methods:

3.1.- Symmetric cryptography:

This cryptographic method is also known as private key cryptography because the reliability of this method depends on the intruders' ignorance about the key. The coding and decoding of the information is done with the same key, so the transmitter and the receiver must know it. This cryptography method allows Domoware© to send information through a not secure channel and authenticate both sides of the channel. In order to define the private key several steps must be done (see figure 1):

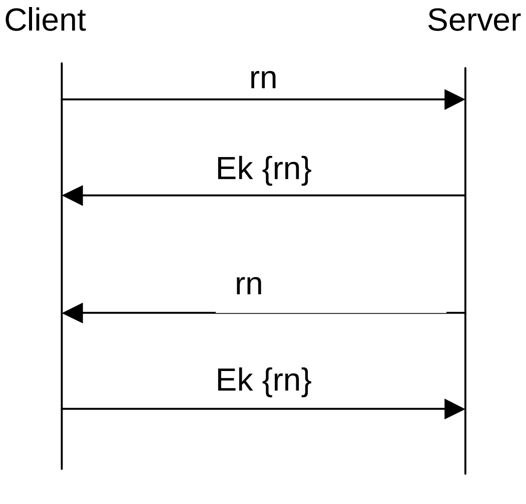


Figure 1.- Authentication using symmetric cryptography.

1.- The transmitter computer (client) sends a random number to the receiver computer (server).
2.- The server answers with the same random number (rn) but coded with K key.
3.- The client decodes the message and check that the random number is the same. In this point, the client is completely confidence about the server.
4.- The process is repeated from the server to the client.

Domoware© uses this cryptographic method during the communication between both computers.

3.2.- Public key cryptography:

This cryptographic method is safer but slower than the symmetric one (requires more computation). Due to this reason, both methods are usually combined in order to send information in a not secure channel. Thus, in this method there is a pair of keys (a public key and a private key) associated with an entity that needs to authenticate its identity electronically or to sign encrypt data. So, the public key is used to encrypt the information and the private key is necessary to decode the information.

Domoware© uses this cryptographic method in order to establish the secure channel between both computers.

3.3.- Hash algorithms:

The hash algorithms give summary of the message, that is transform a message in a shorter one applying an algorithm, that result is called ‘hash’. This method has got some properties:

- One message always presents the same hash whenever it is submitted to the same algorithm.
- This method is used to condense an arbitrary length message to a fixed size.
- The probability that two different messages had the same hash is 10^{-50}.
- Any change to a message in transit will, with very high probability, result in a different hash.

Domoware© uses these algorithms in order to establish the secure channel between both computers at the beginning of the communication.

3.4.- Two way authentication:

This is a kind of cryptographic protocol. It is used in order to verify the identity of both sides in the communication channel. In order to authenticate both computers, they have to send each other several parameters, and the protocol has got two steps (see figure 2):

1.- The client sends its information to the server:
IP address.
A random number.
The hash of its own private key.
An encrypted session key using the public key of the other computer.
2.- The server answers with the same parameters.

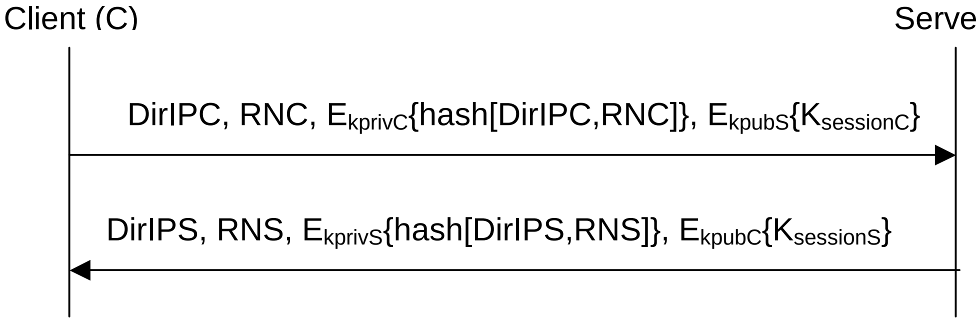

Client (C)
Server (S)
DirIPC, RNC, E_{kprivC}\{hash[DirIPC,RNC]\}, E_{kpubS}\{$K_{sessionC}$\}
DirIPS, RNS, E_{kprivS}\{hash[DirIPS,RNS]\}, E_{kpubC}\{$K_{sessionS}$\}

Figure 2.- Two way Authentication protocol.

Using this protocol, Domoware© achieves:

- Verify the client identity.
- Guarantee that the information from the client is only sent to the server.
- Verify the integrity of the information from the client.
- Verify the server identity.
- Guarantee that the information from the server is only sent to the client.
- Verify the integrity of the information from the server.
- The probability that two different messages have got the same hash is 10^{-50}.

Domoware© uses these algorithms in order to establish the secure channel between both computers at the beginning of the communication.

3.5.- Interlock protocol:

If the computers do not know the public key, they have to send their public keys to each other. Just in that moment, an intruder can intercept the communication and send its own public keys giving a wrong information to both computers and confusing them. This phenomenon is called "man in the middle attack". In order to try to solve this problem the "Interlock protocol" has been designed. It consists in sending only one half of the message and wait for the answer, if there is an intruder, it can not answer to half of the message and both computers can discover it and cancel the communication. This protocol does not solve the problem, but at least, it discovers the intruder stopping all the communications.

Domoware© uses this protocol in order to prevent the "man in the middle attack" just while both computers are establishing the secure channel between them at the beginning of the communication. Besides, in order to prevent the keys, Domoware© creates new public and private keys for each session in both sides of the communication channel.

4.- Domoware© server

As Domoware© can operate in two different configurations, there are two versions of Domoware© server: one if the user requests the service and the other in case of the client wants to monitor his installation. In both cases, the software tool is based on windows95 and all its functions are available as easy as push a button. In the next paragraphs, all the different versions of Domoware© server are briefly presented.

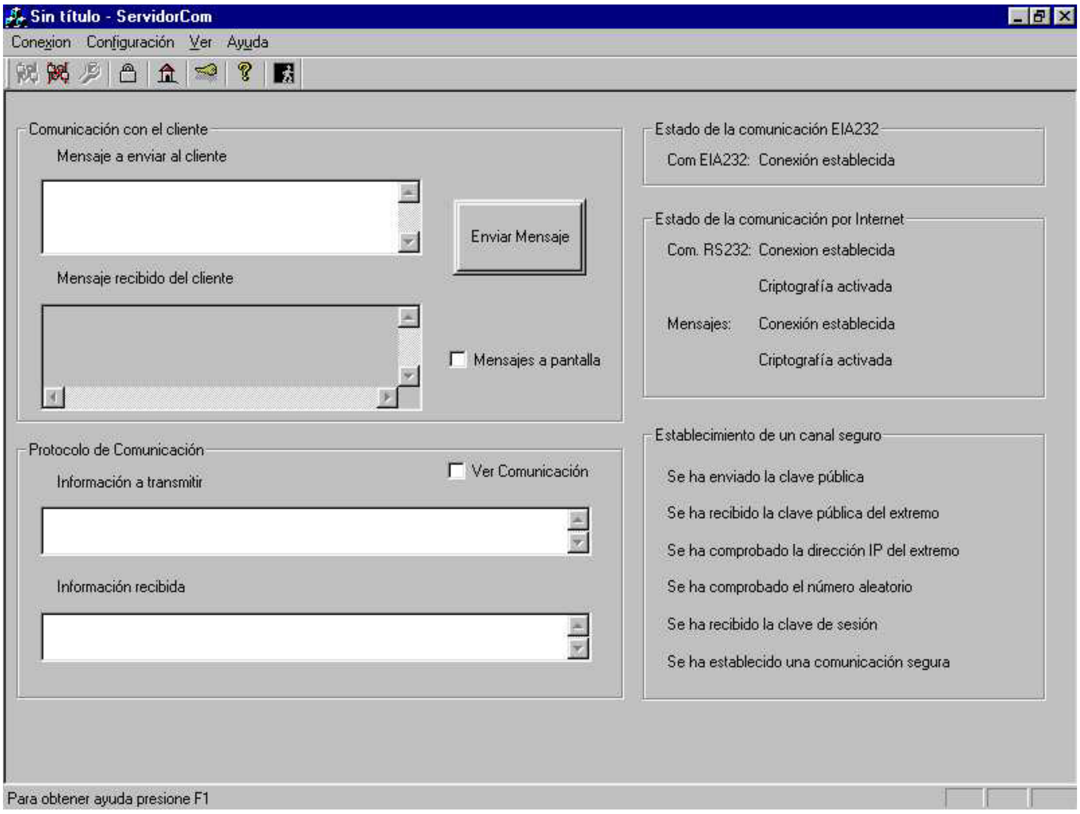
4.1.- Case 1: The user requests the service: Domoware© server.

In this case the server is the computer installed in a remote place without any direct connection to the installation, and a maintenance company probably supports it. In this version, the next options are available:

1. Establish the connection: with this order, the server waits for the client's request. Once the request has been accepted, the communication is opened, and the connection completed.
2. Change the EIA232 communication parameters: in this menu, six different parameters can be modified (this parameters change depending on the home automation system installed):
    - Serial port used.
    - Baud Rate.
    - Flow control.
    - Parity.
    - Number of data bits.
    - Number of stop bits.
3. Finish the communication: this order closes all the opened channel with the server and the EIA232 communication.
4. Run the software (installed in the remote home automation system): with this order, the installed home automation system can be managed.
5. Change the security state: this order only can be executed with an opened connection. It allows deactivating or activating the cryptography.
6. Change the password: this order allows changing the password, once it has been introduced.
7. Tool bar: this order allows viewing or hiding the tool bar buttons with al the other options).
8. State bar: this order allows viewing or hiding the state bar (where all the messages between computers are displayed).

Besides, Domoware© server presents four other sections in its main window (see figure 3):

1. Communication with client: here the server can send and receive messages to/from the client.
2. Communication protocol: in this section, the program shows the information to send and the received information.
3. Communication state: in this section, Domoware© shows information about the state of the connection.
4. Secure channel: in this section, the program shows information about the security of the channel.



Sin título - ServidorCom
Conexion Configuración Ver Ayuda
Comunicación con el cliente
Mensaje a enviar al cliente
Mensaje recibido del cliente
Enviar Mensaje
□ Mensajes a pantalla
Protocolo de Comunicación
□ Ver Comunicación
Información a transmitir
Información recibida
Estado de la comunicación EIA232
Estado de la comunicación por Internet
Establecimiento de un canal seguro

Com EIA232: Conexión establecida

Com. RS232: Conexion establecida

Criptografía activada

Mensajes: Conexión establecida

Criptografía activada

Se ha enviado la clave pública

Se ha recibido la clave pública del extremo

Se ha comprobado la dirección IP del extremo

Se ha comprobado el número aleatorio

Se ha recibido la clave de sesión

Se ha establecido una comunicación segura

Para obtener ayuda presione F1

Figure 3.- Main window of Domware©.

4.2.- Case 2: The user wants to control his installation in a remote way: Domoware© server.

In this case the server is the computer located at the installation directly connected to the home automation system, and the client is located in a remote place. The available options in this version are the same that in case 1 except "run software", as the client will run the software, not the server. Regard to the other sections, nothing changes.

5.- Domoware© client.

As in the case of Domoware© server, Domoware© client has two different versions, one for each option. In both cases, the software tool is based on windows95 and all its functions are available as easy as push a button. In the next paragraphs, Both versions of Domoware© client are briefly presented.

5.1.- Case 1: The user requests the service: Domoware© client.

In this case the client is the computer of the installation and it is directly connected to the home automation system. In this version, the available options are the next ones:

1. Establish the connection: with this order, the client opens the EIA232 connection and sends a request to the server in order to establish the secure channel. Once the request has been accepted, the communication is opened, and the connection completed. When the client finishes, the communication to the server will end.

2. Change the EIA232 communication parameters: in this menu, seven different parameters can be modified:
   - Serial port used.
   - Baud Rate.
   - Flow control.
   - Parity.
   - Number of data bits.
   - Number of stop bits.
   - Chose the server to establish the connection (if there are more than one available server).
3. Finish the communication: this order closes both the opened channel with the server and the EIA232 communication.
4. Change the security state: this order only can be executed with an opened connection. It allows deactivating or activating the cryptography.
5. Change the password: this order allows changing the password, once it has been introduced.
6. Tool bar: this order allows viewing or hiding the tool bar buttons with al the other options).
7. State bar: this order allows viewing or hiding the state bar (where all the messages between computers are displayed).

Besides, Domoware© client presents the same four boxes in its main window as Domoware© server. These sections have the same tasks as in Domoware© server.

5.2.- Case 2: The user wants to control his installation in a remote way: Domoware© client.

In this case the client is the computer from where the user wants to establish the remote control, so it is located in a remote place. The available options in this version are the same that in case 1 plus the option “run software”. As in the case of the Domoware© server, this option is used to run the software of the home automation system in the remote computer, not in the local computer directly connected the installation. Regard to the other sections, nothing changes.

6.- Domoware© operation.

In an ordinary installation, the EIB system sends the information to a computer directly connected through the serial port (EIA232). With Domoware©, the starting operation is the same: the EIB installation must be connected to a computer (the server or the client depending on the situation, as it has been shown before), and establish the communication. Once this communication is opened, Domoware© can operate in its normal way.

The first step is establishing the communication between the client and the server. For that propose, the client sends the request for a connection to the server, once the server has accepted this request, the “two way authentication” protocol with public key cryptography is launched. This protocol is implemented to authenticate both sides (the client and the server). This is one of the most important part of Domoware© operation, in this step, both computers send each other the next parameters:

The IP address.

A random number.

The signed hash with a private key related with the IP address and the random number.

A session key (encrypted with the public key of the other computer).

With all these parameters, Domoware© establishes a secure session between both computers. Besides, in order to avoid the "Man in the middle attack" Domoware© uses the "Interlock protocol" as it has been shown before. From this point, the remote control can be executed using a secure channel. And the home automation system software (ETS2) can be run in the remote computer with no problem.

Once the secure communication channel is established, the next step is transmitting the information in both directions: from the server to the client and from the client to the server. For this proposes, Domoware© uses symmetric key cryptography, besides, while the communication between both computers is taking place, Domoware© sends the encrypted information using IP packages and TCP protocol [6]. Figure 4 illustrates all the steps to establish the secure channel of communication.

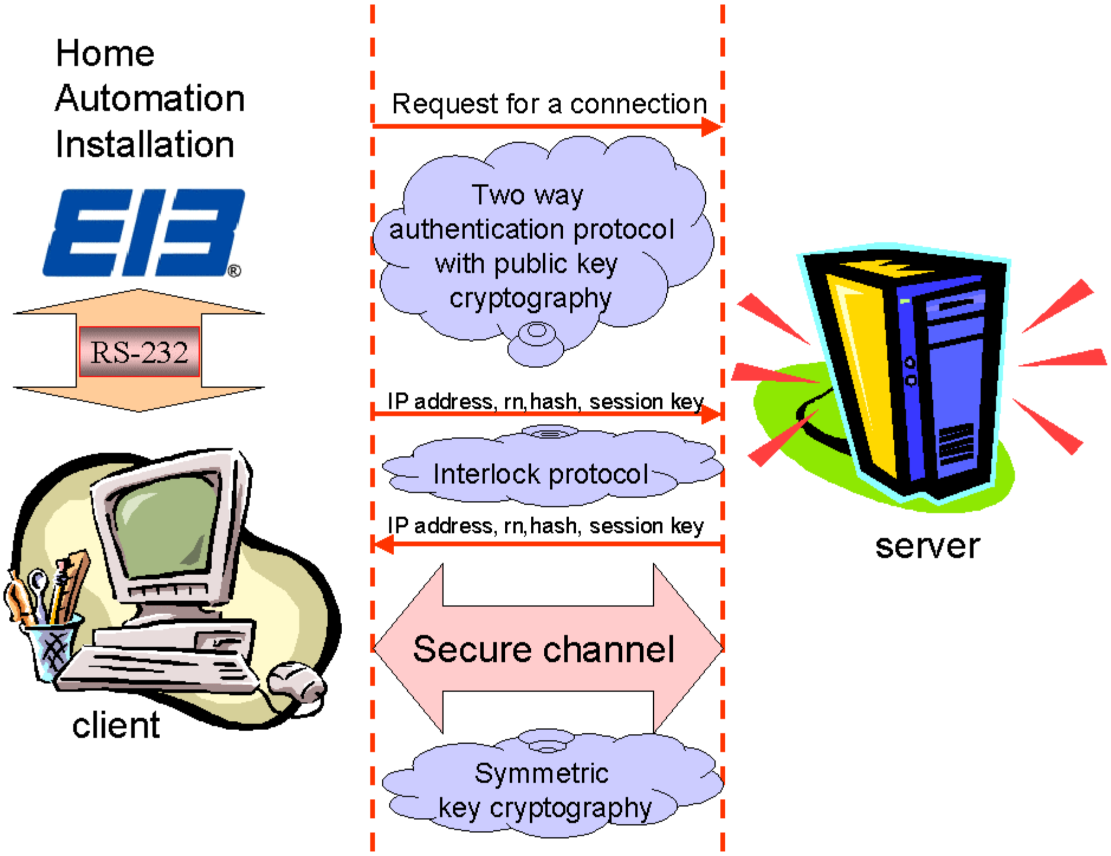

Home Automation Installation
EIB
RS-232
client
Request for a connection
Two way authentication protocol with public key cryptography
IP address, rn,hash, session key
Interlock protocol
IP address, rn,hash, session key
Secure channel
Symmetric key cryptography
server

Figure 4.- Two way Authentication protocol.

7.- Conclusion.

A new software tool called Domoware© has been designed and tested at the Universidad Pública de Navarra. This program has been implemented in order to guarantee a secure communication channel between two computers with the final propose of establishing a remote control of a home automation system. Domoware© operates under two different cases: when the user has got a problem and wants a fast solution with the minimum problems, and when a company or a particular user wants to monitor their installation from everywhere with a high level of security. Both cases have been presented with their own versions of Domoware©, and they have been successfully tested.

At this moment, the research group is still working in this software tool by improving the Domoware© characteristics as the transmission speed through Internet, the updating of the cryptography methods (faster and more secure), etc. Besides, a new English version is under development.

Acknowledgments.

This work has been supported by CICYT research grant TIC98-0397-C03-01 and by Gobierno de Navarra.

Bibliography

[1]: C. Fernández-Valdivielso, M.A. Galdeano, Prof. Ignacio R. Matías and M. López-Amo: “Design, Implementation and Set Up Laboratory of EIB System in the Telecommunication Degree”; **pp**.71-78, I Scientific EIB Conference, EIB Proceedings. Contributions part2/1999.

[2]: C. Fernández-Valdivielso, E. Daems, A. Pomares and I.R. Matías “EIB remote control through applets and mobile phones”, *EIB Event 2000 III Scientific Conference*..

[3]: J. Campbell: “Serial communications, reference guide for the C programmer”; Ediciones Anaya Multimedia, 1987.

[4]: J. Bates and T. Tomkins: “Microsoft Visual C++ 6”; Prentice Hall, 1999.

[5]: B. Schneider: “Applied Cryptography: protocols, algorithms and source code in C”; Wiley & Sons Inc., 1994.

[6]: D.E. Comer: “Internetworking with TCP/IP. Volume I Principles, Protocols and Architecture”; Prentice Hall, 1995.