9th IFAC Workshop on Programmable Devices and Embedded Systems
Roznov pod Radhostem, Czech Republic, February 10-12, 2009

Real-time control systems secured communication

Petr Czekaj*, Ondřej Krejcar**

**Technical University of Ostrava, Department of measurement and control, Ostrava, Czech Republic (petr.czekaj@ vsb.cz)*
*** Technical University of Ostrava, Department of measurement and control, Ostrava, Czech Republic (ondrej.krejcar@ vsb.cz)*

Abstract: As demands on privacy, personal data and in general secure and responsible dealing with confidential personal information are growing, the need for their protection grows as well. When confidential data are being transported, there is a high risk of their stole and misuse or complete loss. That's why a question of secure communication is one of the most actual topics of a present day. It's not just information technologies problem, but since embedded and automation devices are more and more sophisticated, able to use for example internet technologies, this question also concerns the area of automation and control systems. Especially in complex distributed control and measurement systems that supports remote control, internet visualization, wireless transfers or remote data acquisition, it is the primary goal to ensure the most secure and reliable communication. This work deals with securing the communication of embedded systems connected over public networks and internet. To fulfill that, PKI technologies are used. Benefits of secured communication are employed in Guardian system, patient monitoring platform developed at Technical University of Ostrava.

Keywords: PKI, PLC, Embedded, Authentication, Secure communication, Encryption.

1. SECURE COMMUNICATION

Secure communication can be defined by following statements:

- Secure communication is the communication where both communication subject, based on mutual authentication, believe that they are communicating with the announced subject and that they received the message from authenticated source.
- Transferred information cannot be intercepted because confidentiality is ensured
- Transferred information cannot be changed because integrity is ensured.
- Communication is permitted only to the authorised side because access control is realised.
- Communication cannot be repudiated because non-repudiation of sending and receiving messages is provided.

1.1. Digital signature for ensuring of the non-repudiation

Digital signature is a mechanism that provides proof of the data non-repudiation (authenticity of documents). Digital signature is created in two steps, Fig. 1:

1. Hash is counted from the document.
2. Hash is encrypted with user's private key that created the signature. Hash of the message encrypted by private key is called digital signature of the message.

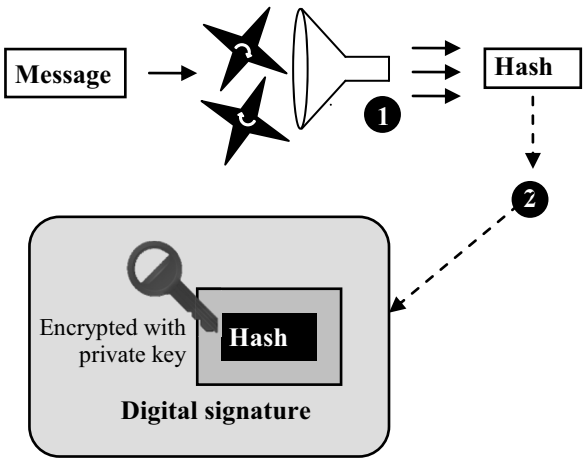

Fig. 1. Digital signature

Verification of the digital signature is made in three steps:

1. Recipient counts a hash from received message.
2. Recipient decrypts received digital signature using received sender's public key.
3. Recipient compares result from step 1 with the result from step 2. If both results are the same, digital

signature could have been created only by the one owning sender's private key… accordingly the sender. This fact also proves that message has not been changed during the transfer, thus ensures integrity of the message as well.

1.2. Authentication based on asymmetric cryptography

Digital signature can be also used as a tool for authentication, based on proving the ownership of the private key. User proves his identity demonstrating the ownership of the private key and ability of using it.

Principle of authentication based on asymmetric cryptography is simple. Side A (recipient) generates long enough random number. This number is sent to side B. Side B signs the number using its private key. Signed number is sent back to side A which verifies the signature.

In case there is a need of using cryptography instead of digital signature, recipient simply holds back the random number and sends it to the sender encrypted using sender's public key. Sender decrypts the numbed using its private key and returns it back to the recipient. Recipient checks if received number is the same as the one he encrypted.

2. SECURE DATA TRANSFER IN REAL-TIME SYSTEMS

Actual secure data transfer in real-time system using PKI capabilities presumes a device that enables to implement its own secure web server or other digital signature verify capable mechanisms. Secured communication can work in systems based on client-server model but and is able to work also in P2P systems for instance as well.

Considering client-server model, there is an embedded device providing secure web server. In general it can provide any other web or database services. This device realises its own certificate authority (CA). It is able to issue digital certificates which contain a public key and the identity of all other devices authorised to secure communication. It also provides all other services for certificate management (verifies certificates, revoke certificates, etc.). It protects the access to the database and any other resources. At any client attempt for communication, server verifies client certificate, thus it verifies the identity and ensures client's authenticity and non-repudiation. Server can be any embedded device, microcontroller or PLC that is able to realise secured web server. It ensures secure communication in direction client >> server.

Server itself presents its identity with its own certificate to every client that has requested the communication. Server certificate is issued based on unique IP address or server name. Server can use a self-signed certificate or can let any public certificate authority sign its certificate. This server certificate is verified by client before beginning of any communication. Client side can be made by any other embedded device, PLC, PDA, mobile phone, laptop, personal computer or any other device that can communicate over TCP/IP and support technologies like Java or .NET that provides necessary software capabilities for secure communication. This ensures authentication and non-deputation of server side and guarantees secure communication in direction server >> client.

Message integrity can be provided by existing methods of symmetric or asymmetric cryptography or using its own private cryptographic mechanisms.

Communication is illustrated very briefly in Fig. 2:

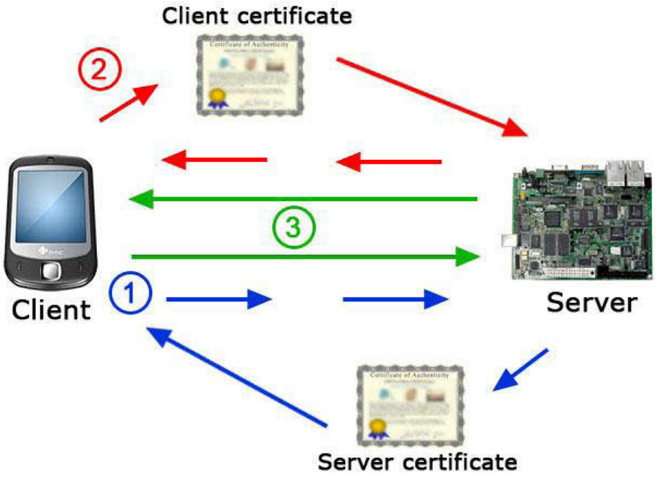

Fig. 2. Secure client-server communication

1. In the beginning of each communication client requests server's certificate and verifies its authenticity. After successful authentication client can be sure that it asks services from trusted subject.
2. In the next step, client presents its own certificate. Server verifies client's certificate and then is the client successfully authenticated, server enables him requested services and sources.
3. Client and server can communicate securely.

3. DEPLOYMENT

Possible use of secured communication is in GUARDIAN system, patient monitoring platform developed at Technical University of Ostrava.

Basic idea of this platform is to create a system that controls important information about the state of a wheelchair-bound person (monitoring of ECG and pulse in early phases, then other optional values like temperature or oxidation of blood...), his situation in time and place (GPS) and an axis tilt of his body or wheelchair (2axis accelerometer).

3.1. System architecture

Guardian system consists of several interconnected parts that can communicate among themselves, so they can approach their function. These parts are: measuring sensor, PDA or embedded device, and server for data processing and evaluation. Beside these, the most important parts that are

worth mentioning are various kinds of accessories, such as GPRS, WiFi, GSM, Bluetooth or GPS modules used for communication. Data acquisition and data transmission are the most important parts of the system.

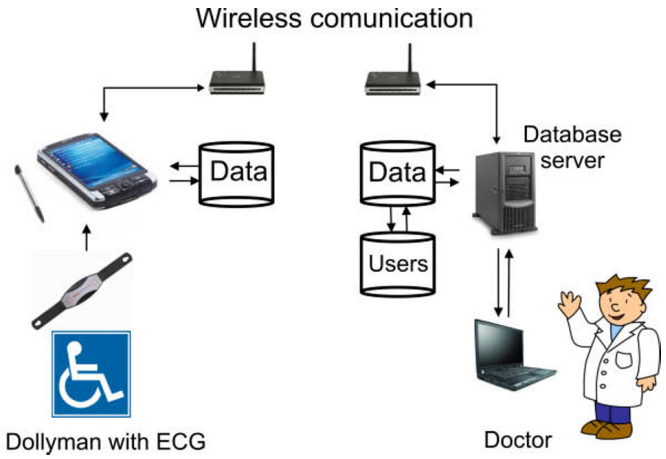

Fig. 3 Communication in Guardian system

System can display saved data from a database file. Doctor can configure or set a neural network. This change is shown in the XML file enshrining, where the neurone network setting of the patient is kept. Doctor receives information about worsening of patient's status. In case of doctor's reaction, he sends for an expert assistance, such as a helicopter or an ambulance. In case of false alarm, he can configure a neural network or leave it unchanged if that was a sporadic incorrect interpretation. Patient can browse data concerning his health status. Measured data is sent to server by WEB service.

Client's data are not only received but also pre-processed (data checking, risk elimination etc.). Measured data is saved. Then it is possible to analyze data using an artificial neural network. If the analysis shows that the measured data from ECG is critical, warning is sent. That notifies the doctor of incoming data.

3.2. Mobile part

Main part of whole system is an Embedded or PDA device. The difference between use of embedded or PDA device is in the possibility of visualizing measured data in both real-time charts and historical trend charts.

PDA is much better choice for Personal Healthcare where patient is already healthy and needs to review his condition or for multiple person usage. Embedded devices can be designed for one user, with the option to use an external display used for settings or with the possibility of usage in extreme conditions.

Application is communicating with an ECG Measurement Unit (Corbelt or BlueECG) through a virtual serial port using wireless Bluetooth technology. Then, after pushing a button, all necessary parameters are set and communication may begin. Measured data is stored on a SD Memory Card in a database in MS SQL Server 2005 Mobile Edition.

3.3. Server part

In order to run a server, an operating system supporting IIS is needed. IIS is an Internet Information Server application allowing users to connect to the web server by the well-known HTTP protocol. Web service transfers data between the server and PDA/Embedded devices. It reads the data, sends acknowledgments, stores the data in the database and reads it from there. Service is built upon ASP.NET 2.0 technology. SOAP protocol is used for data transfer that is in XML format. That is an advantage since it allows communication of multiple different technologies and platforms.

Following data transfers are performed:

- receiving measured data
- receiving patient data
- deleting a patient
- patient data sending

3.4. Securing Guardian system

Since patients medical data are considered to be strictly personal it is inadmissible to expose those data to potential misuse. Thus the most critical part of whole measuring chain regarding security is the wireless data transfer between embedded/PDA device and the database server. This part can be secured using means of PKI technologies, digital signatures and certificates in a way mentioned earlier. Communication between server and other client devices such laptops or hospital visualisation PCs can be considered dangerous as well. This is secured by means of hospital secure policy. On the other hand it can be involved in the Guardian system and protected our way as well.

Since a lot of widely used wireless secure network algorithms supported by embedded devices in general such as WEP, WEP2, WPA, etc. are considered to be not secure or are already deprecated, our secure solution offers great opportunity to create a secured system eliminating by its nature any intruders attempts for intercepting and misusing personal data. Not mentioning great amount of devices focussed preferably on closed control systems that does not support any secured data transfers at all.

This part is still in a phase of development and testing.

4. CONCLUSIONS

This secure communication allows not only to access the control systems from the internet, remote visualisations etc., but also in local networks of distributed embedded or PLC based control systems where it is essential to guarantee the correctness and legitimacy of transferred data or where the confidentiality of the data is a basic condition. Primary areas

of use are soft real-time systems, but it is not the condition. Only limit of use constitutes HW and SW equipment used in secured communication.

Using these technologies enables replacing of variety of security seals, stamps, watermarks or mechanical locks and obstructions and other forms of security which are nowadays overpowered in many ways bud still in use in a lot of present systems.

REFERENCES

DCCT – Diabetes Control and Complications Trial - http://diabetes.niddk.nih.gov/dm/pubs/control/ (10.04.2008)

Dostálek L, Vohnoutova (2006), *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 528, Computer Press, a.s., Brno

Janckulik, D., Krejcar, O., Martinovic, J.: Personal Telemetric System – Guardian, In Biodevices 2008, pp. 170-173, Insticc Setubal, Funchal,,Portugal, (2008).

Krejcar, O., Fojcik, P.: Biotelemetric system architecture for patients and physicians – solutions not only for homecare, In Portable 2008, 2nd IEEE International Interdisciplinary Conference on Portable Information Devices, Ga-Pa, Germany, (2008)

Krejcar, O.: Database Prebuffering as a Way to Create a Mobile Control and Information System with Better Response Time. In Lecture Notes in Computer Science, Computational Science – ICCS 2008, Volume 5101/2008, The International Conference on Computational Science 2008, pp. 489-498, Cracow, Poland, (2008).

Krejcar, O.: Prebuffering as a way to exceed the data transfer speed limits in mobile control systems, In Icinco 2008, 5th International Conference on Informatics in Control, Automation and Robotics, pp. 111-114, Insticc Press, Funchal, Portugal (2008).

Krejcar, O.: User Localization for Intelligent Crisis Management. In AIAI 2006, 3rd IFIP Conference on Artificial Intelligence Applications and Innovation, pp. 221-227, Athens, Greece, (2006).

Paulo Reis, Conferencia Telemedicina Onde Estamos e para onde vamos, Ericsson – (04.12.2006)