SOFTWARE MODULES AND APPLICATION LAYER'S SECURITY STRUCTURE OF RSMAD

Slawomir Gajewski, Malgorzata Gajewska, Marcin Sokol and Michal Brewka
Department or Radiocommunication Systems and Networks, Faculty of Electronics, Telecommunications and Informatics
Gdansk University of Technology, Gdańsk, Poland

Keywords: AES, RSA, RSMAD, VPN.

Abstract: The paper discusses the software modules of Radio System for Monitoring and Acquisition of Data from Traffic Enforcement Cameras (in short RSMAD). The structure of the application layer of the system has also been analysed in details, including: purpose, structure and principles of operation of software modules constituting this system. In addition, the paper presents and discusses the structure of security of application layer in the RSMAD system. What is more the paper highlights the advantages and disadvantages of the modular construction of ICT systems basing on the example of the RSMAD system.

1 INTRODUCTION

Radio System for Monitoring and Acquisition of Data from Traffic Enforcement Cameras (in short RSMAD) allows automatic transmission of image data (recorded by a traffic enforcement camera), storage and processing them for the purposes of proceedings against traffic offenders. RSMAD specificity means that the image data stream is generated, transmitted and stored in the system continuously.

RSMAD use appropriate technology solutions, ensuring the safety of data transmitted and stored within the system. A description of designs and procedures is presented later in this paper.

2 MODULAR STRUCTURE OF RSMAD

The basic assumptions made at the design stage of the RSMAD system were:

- Mobility of the solution and openness to different techniques and technologies of wireless data transmission,
- Independence on the used transmission technology, encryption, authentication and verification of the integrity algorithms,
- High scalability of the solution achieved by using a modular architecture,
- Secure transmission over the Internet by subtracting the VPN *(Virtual Private Network)* subnet which type and parameters have been chosen as the result of simulation,
- Centralized management of cryptographic parameters of the selected software modules, providing increased security and flexibility of the system.

Both the physical and application layers of the RSMAD system have a modular structure. The application layer consists of a group of functionally advanced and co-operating applications. Technical and functional parameters of these solutions, both hardware and software, are designed to handle very large amounts of data. Modular architecture of RSMAD is shown in Figure 1. The rest of this article will discuss the advantages and disadvantages of using this approach (Anderson, 2008).

2.1 Modules Description

RSMAD consists of five main modules. Three of them are directly involved in data transmission. These are RCM, RDM, RUM (Figure 1). Other modules: RLM and RKMM support the work of the whole system (KSSR DT 07.100 v. 1.0.1, 2009).

2.1.1 RSMAD's Licence Module (RLM)

RLM module is used for license management. The appropriate license code is generated for each unit

Gajewski S., Gajewska M., Sokol M. and Brewka M..
SOFTWARE MODULES AND APPLICATION LAYER'S SECURITY STRUCTURE OF RSMAD.
DOI: 10.5220/0003454000890093
In *Proceedings of the International Conference on Data Communication Networking and Optical Communication System* (DCNET-2011), pages 89-93
ISBN: 978-989-8425-69-0

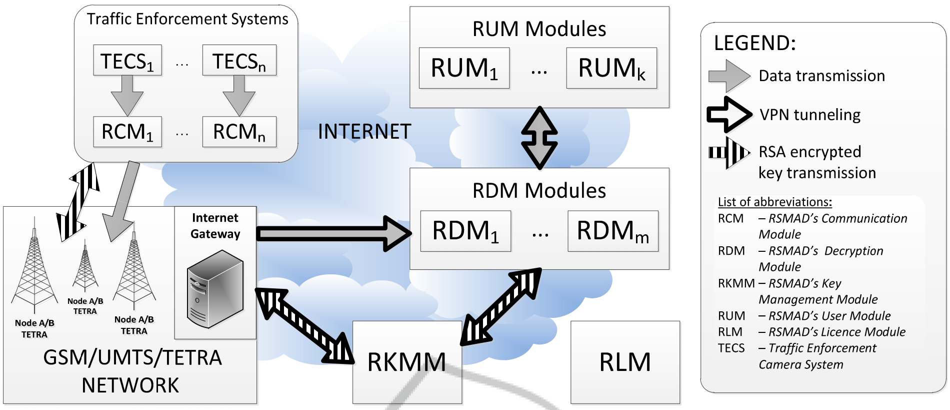
Traffic Enforcement Systems
TECS1 ... TECSn
RCM1 ... RCMn
INTERNET
RUM Modules
RUM1 ... RUMk
RDM Modules
RDM1 ... RDMm
Internet Gateway
Node A/B TETRA
Node A/B TETRA
Node A/B TETRA
GSM/UMTS/TETRA NETWORK
RKMM
RLM
LEGEND:
Data transmission
VPN tunneling
RSA encrypted key transmission
List of abbreviations:
RCM – RSMAD's Communication Module
RDM – RSMAD's Decryption Module
RKMM – RSMAD's Key Management Module
RUM – RSMAD's User Module
RLM – RSMAD's Licence Module
TECS – Traffic Enforcement Camera System

Figure 1: Modular architecture of the RSMAD system.

and stored in the database along with details of the owner of the traffic enforcement camera, the characteristic parameters of the device and its identifier. During saving of this data the license application creates a personal FTP (File Transfer Protocol) account and the appropriate folder structure on a network drive connected to the database server. The folder names correspond to unique identifiers which are set according to specific rules for each camera.

2.1.2 RSMAD's Key Management Module (RKMM)

One of the major modules of the RSMAD system is RKMM. It is responsible for distribution and management of cryptographic parameters. These parameters are needed to control encryption procedure by the individual RCM. **RKMM** assigns an individual vector of cryptographic parameters to each RCM. Elements of this **vector define: the type of encryption algorithm, its parameters and the encryption key with a validity period**. These parameters are generated and stored by the RKMM, in accordance to current security policies. This solution enables the selection of an encryption algorithm corresponding to the capacity of each terminal and compliant with current security policy.

Database, which co-operates with RKMM, stores all the generated cryptographic vectors which are unambiguously associated with the appropriate traffic enforcement cameras (Lam and LeBlanc and Smith, 2004).

2.1.3 RSMAD's Communication Module (RCM)

The role of the **RCM** module is proper preparing of a transport block which includes: a file in the *JPEG (Joint Photographic Experts Group)* format, additional information about the infraction obtained automatically from the traffic enforcement camera and a set of data entered by the user. Each block contains also the *GPS (Global Positioning System)* position which sets out unambiguously the location of the incident. All information except the JPEG file is saved to XML *(Extensible Markup Language)* file, to facilitate its further processing.

The next activity of the RCM module is the encryption and creation of abridged messages archive containing the JPEG and XML files. This operation is performed in order to prepare the transport block. Input parameters of the encryption process are determined basing on the vector of cryptographic parameters. After encrypting a transport block, the RCM application connects to an FTP server, using a personalized account (created by the RLM application). Thereby it obtains access to the assigned folder on the network drive of the regional data centre. RCM has the authorization only to record data (Postel,1985).

2.1.4 RSMAD's Decryption Module (RDM)

Most demanding in terms of complexity and CPU power module is RDM. This application is responsible for the decryption of transport blocks and saving them into database.

The realisation of the RDM module's tasks starts with the creation of a list of new transport blocks stored on an FTP server. In the next step, this module sends a request, to define a set of encryption vectors for all received transport blocks, to the RKMM server. A successful decryption procedure and verification of digital signature results in separation of a pair of JPEG and XML files.

The final stage of the algorithm implemented by the RDM module is the archiving of JPEG and XML files on a network drive and making an entry into database cooperating with the module. This entry contains, among others, the actual location of the JPEG file and all the additional data obtained from an XML file.

2.1.5 RSMAD's User Module (RUM)

Users's RUM module is responsible for communicating with the database and other IT systems participating in the procedure of issuance of a penal ticket. It allows the system operator to download photos and additional information stored in the database of the system. The extensive functionality of the application allows automatic filling in the penal documentation.

2.2 Security of RSMAD

When designing a RSMAD, it was decided to use a VPN solution, implemented in both the network and application layers. In turn, in the process of distribution of cryptographic vectors, it was decided to use the proven RSA algorithm ensuring secure, asymmetric encryption which protects it from eavesdropping in the channel (KSSR RT02.901v.1.1.0, 2009). The RSMAD system's security structure is multilayered and very complex, therefore in the rest of the work only some aspects of security architecture of the system will be discussed (Pieprzyk and Hardjono and Seberry, 2003).

2.2.1 VPN Tunnelling

VPN networks have been used to secure the transmission realized over the Internet. For this purpose, the private subnet from which the communication takes place via VPN tunnels has been isolated in the infrastructure of the mobile network operator.

Tunnels between the server and client parts of the RUM application are implemented basing on the L2TP *(Layer Two Tunnelling Protocol).* It results from the fact that there are many more RUM modules than the RDM modules, and they are supported by those who are responsible for preparing penal documentation. Using the tunnel in the connection, which is realized by software, is much easier to implement, and it provides much more scalable solution (Townsley and Valencia and Rubens and Pall and Zorn and Palter, 1999).

2.2.2 Structure of a Modified RSA Algorithm

A modified structure of the RSA algorithm which was decided to be used in the RSMAD system, is shown in Fig. 2. It is the typical RSA algorithm, enriched by an additional procedure of password verification. The verification is designed to filter out unwanted connections which would have to offload server performance with further steps of the RSA algorithm.

The procedure for determining an encrypted connection using the RSA algorithm is to generate public and private key on each side of the transmission. Only public keys are transmitted in the channel. After an exchange of these keys the encrypted transmission may begin.

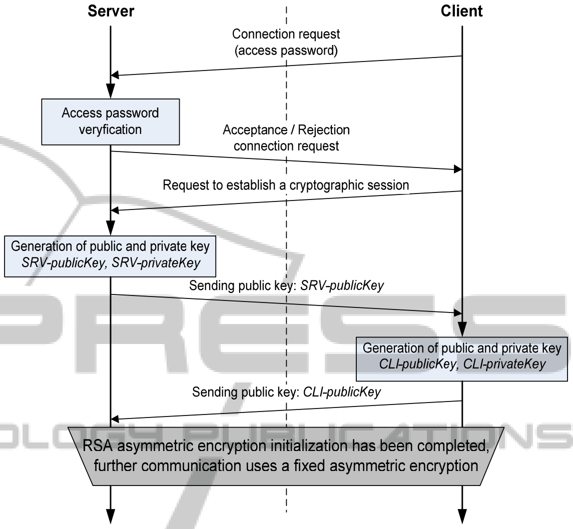
Server
Client
Connection request
(access password)
Access password
veryfication
Acceptance / Rejection
connection request
Request to establish a cryptographic session
Generation of public and private key
SRV-publicKey, SRV-privateKey
Sending public key: SRV-publicKey
Generation of public and private key
CLI-publicKey, CLI-privateKey
Sending public key: CLI-publicKey
RSA asymmetric encryption initialization has been completed,
further communication uses a fixed asymmetric encryption

Figure 2: RSA algorithm adopted for RSMAD.

The principle of the RSA algorithm performance is very simple – the sent public key allows encrypting messages. On the other hand, the complementary (generated by the same side) private key is necessary for decryption. Since the private key has not been sent within the channel, it is impossible (without a thorough analysis) for a third party to read the message secured in this way.

The main reason why RSA is used is the need to secure the transmission of the symmetric key used for encryption a transport block. The implemented solution allows the operation of the RCM and the RDM modules independently from each other, by using an FTP server. This means that despite the disruption in RDM application performance (e.g. due to an upgrade) it is not necessary to suspend the transfer of transport blocks by the RCM modules. This is a very important solution because it allows a temporary exemption (partial or total) of one module without affecting the whole system.

Because of the relatively short validity (for the current connection) of the set RSA key, a potential intruder does not have enough data to make an attempt of breaking a message encrypted this way. This means that the distribution of cryptographic parameters vectors, through the central RKMM module which is secured by RSA algorithm, can be considered safe (Wobst, 2002).

2.2.3 Encrypted Data

Data sent by the RCM module is first transmitted over the radio channel and then via GSM / UMTS / TETRA links to their networks' connection to the Internet. Between the operator's network and the Data Acquisition Center (in short DAC) VPN tunnels that protect data transmitted over the Internet have been compiled.

In addition, regardless of the security offered by the technology used for data transmission, it was decided to use the additional data encryption. Encryption algorithms supported by the RCM module are: AES-128; AES-192; AES-256; Triple-DES. These are algorithms approved by the National Institute of Standards and Technology and their safety is estimated to at least 2030 (NIST, 2003-2007). There is also an opportunity of easy migration to other solutions.

RKMM is equipped with mechanisms to improve the security of the system. It provides, inter alia, easy change of the data encryption algorithm in a situation of violation of any of the used algorithms.

2.3 Modular Architecture of RSMAD System as a Form of Securing and Increasing the System Reliability

This section will show the benefits of the modular system structure and policies of limited confidence in the RSMAD system. These benefits could be presented on examples of various types of interference in the system: acquisition of one of the RCM modules, acquisition of one of the RUM modules, eavesdropping of transmission in a wireless network, eavesdropping of transmission in the Internet. Those are the most probable attempts to intervene in the RSMAD system. However, there is also some probability of attempts of unauthorized physical access to servers on which RKMM, RLM, and RDM applications run. Physical security of the RSMAD system's servers unfortunately exceeds the scope of this paper.

A hypothetical situation can be imagined that the intruder steals a unit with an installed RCM module, for its thorough analysis and to gain unauthorized access to the RSMAD system.

The only data that can theoretically bring any benefit to an intruder are: license number of the RCM and IP addresses of the RKMM and the RDM modules. Trying to use the license would not bring any benefit, because each one is verified on-line during its input. Address of RDM module allows only access to the FTP server, with write-only permissions. RKMM IP address is useless, because this module verifies the password which is implemented in code of the software. Even if it would be overheard, in response to a query, the RCM module can only get an encryption parameters vector containing the information on encryption key with which the messages are protected, but not the pictures stored on this device.

In summary, the RCM module has been designed so that a failure or attack on one traffic enforcement camera does not endanger the safety of the entire RSMAD system.

3 CONCLUSIONS

Solutions used in the RSMAD system, and especially its modular architecture are its major asset. Security policy, developed specifically for the system, provides a very high level of data security. It should be noted that the maintenance of the RSMAD system in continuous operation is crucial because with the large number of supported devices, even a brief failure could result in very large losses. Thus, the system lets users to perform a software update on individual devices without interrupting the operation of the whole system. Flexibility that characterizes this system allows its easy and sustainable development and ensures low maintenance costs.

ACKNOWLEDGEMENTS

The project of RSMAD is realized under the research - development grant R02 N 0034 06 in years 2009-2012 in the Department of Radiocommunication Systems and Networks, Faculty of Electronics, Telecommunications and Informatics at Gdansk University of Technology in Poland. It's funded entirely by the National Centre for Research and Development.

REFERENCES

KSSR DT 07.100 v. 1.0.1, 2009. *General concept of*

RSMAD’s DAC (in Polish), Gdansk University of Technology, Poland.

Anderson, R., 2008. Security Engineering: A Guide to Building Dependable Distributed Systems.

Lam, K., LeBlanc, D., Smith, B., 2004. Assessing Network Security.

J. Postel,1985. *RFC959: File Transfer Protocol (FTP)*.

KSSR RT 02.901 v. 1.1.0, 2009. *Security architecture of the RSMAD system (in Polish)*, Gdansk University of Technology, Poland.

Pieprzyk, J., Hardjono, T., Seberry, J., 2003. Fundamentals of Computer Security.

Townsley W., Valencia A., Rubens A., Pall G, Zorn G., Palter B., 1999. *RFC2661: Layer Two Tunneling Protocol "L2TP"*. The Internet Society.

Wobst, R., 2002. Abenteuer Kryptologie

NIST, 03-2007. Special Publication 800-57 *Recommendation for Key Management – Part 1: General (Revised)*.