Security and Performance Analysis of IPsec-based VPNs in RSMAD

Marcin Sokol, Slawomir Gajewski, Malgorzata Gajewska, Leszek Staszkiewicz
Faculty of Electronics, Telecommunications and Informatics
Gdansk University of Technology
11/12 G. Narutowicza Str., PL-80-233 Gdansk, Poland
e-mail: {marcin.sokol, slawomir.gajewski, malgorzata.gajewska, leszek.staszkiewicz}@eti.pg.gda.pl

***Abstract*—The paper discusses the security architecture of the Radio System for Monitoring and Acquisition of Data from Traffic Enforcement Cameras with particular emphasis on the structure of the security of network layer of the system. The security of this layer of RSMAD is provided mainly basing on Virtual Private Networks. To implement a VPNs in RSMAD IPsec Encapsulation Security Payload in tunnel mode have been used. Data protection mechanisms and the type and parameters of the VPNs used in RSMAD have been selected on the basis of simulation results presented in the paper. Analysis of results shows also that the ESP protocol is a bit less efficient than Authentication Header protocol, which is obviously related to the fact that the ESP protocol supports data encryption. The paper also discusses some advanced solutions for communications and computation used in the RSMAD system.**

Keywords-AH; ESP; IPsec; RSMAD; VPN

I. INTRODUCTION

Radio System for Monitoring and Acquisition of Data from Traffic Enforcement Cameras (in short RSMAD) is an integrated (in terms of its functions) ICT system which uses for data transmission the radio technologies available on the market.

RSMAD is primarily used for transmission, archiving, analysis and processing of data of traffic infractions from traffic enforcement cameras (in short TEC). The purpose of the construction of this system is mainly to improve road safety by reducing the number of offences and their victims. RSMAD will significantly improve the work of the police and other departments responsible for traffic control. In this context, the system belongs to the class of the most substantive and technological advanced systems dedicated for the services dealing with TECs. In general, the performance of the RSMAD system is focused on transmission of violations recorded by the TECs to Data Acquisition Center (in short DAC). In RSMAD the data is being transmitted as cryptographically secured data blocks (data is encrypted and signed digitally). Currently the data transmission is performed via public mobile GSM systems *(Global system for Mobile Communications)*, UMTS *(Universal Mobile Telecommunications System)*, police trunked networks TETRA *(TErrestrial Trunked Radio)* as well as the Internet. In the future the use of networks based on LTE *(Long Term Evolution)* or LTE-Advanced will be possible [1]. RSMAD belongs to a group of systems with distributed structure. Equipment used in the system use dedicated software, allowing sharing system's resources. Unfortunately, in distributed systems additionally using public networks for transmission of data, the data security is a serious problem. This is because such networks are significantly exposed to the activity of intruders. Secure communication based on Virtual Private Networks (in short VPN) constitutes one of the key elements of RSMAD. For the implementation of VPNs developers of the system used mainly IPsec *(Internet Protocol Security)*, which is widely regarded to be the safest way to create VPN, which has been clearly confirmed by the authors' simulation studies.

II. RSMAD'S ARCHITECTURE

Data security in the RSMAD system will be ensured through the use of advanced security mechanisms such as: confidentiality, availability and integrity. **Already at the conceptual stage, the following, crucial for the future architecture of RSMAD assumptions has been made:**

- Security of information in RSMAD is a primarily consideration in relation to performance.
- Communication is only allowed with network devices which comply with strict security policies adopted.
- Due to the nature of data transmitted and processed in RSMAD, there is a real risk of loss of confidentiality.
- Implementing data protection mechanisms in RSMAD can not impede the work of its users.

A simplified architecture of the RSMAD system's security including VPN tunnels are shown in Fig. 1 (detailed architecture of the RSMAD system is presented in [2][3]). The concept of RSMAD is to use public telecommunications networks (in particular cellular) for data transmission. Public telecommunications networks are inherently far more vulnerable to all kinds of risks than other networks. The basic threats to the RSMAD system should include: *sniffing*, *spoofing* as well as *session hijacking*. Therefore, the use of effective and reliable data protection mechanisms in the system is particularly important.

Each of systems used for data transmission (GPRS, EDGE, UMTS, HSPA TETRA), uses different security mechanisms eliminating or reducing various risks in varying degrees. Therefore, it has been decided that the RSMAD system will be equipped with additional, independent form data transmission technology, mechanisms protecting from the threats associated with data transmission via public cellular networks.

 ISBN: 978-1-61208-161-8

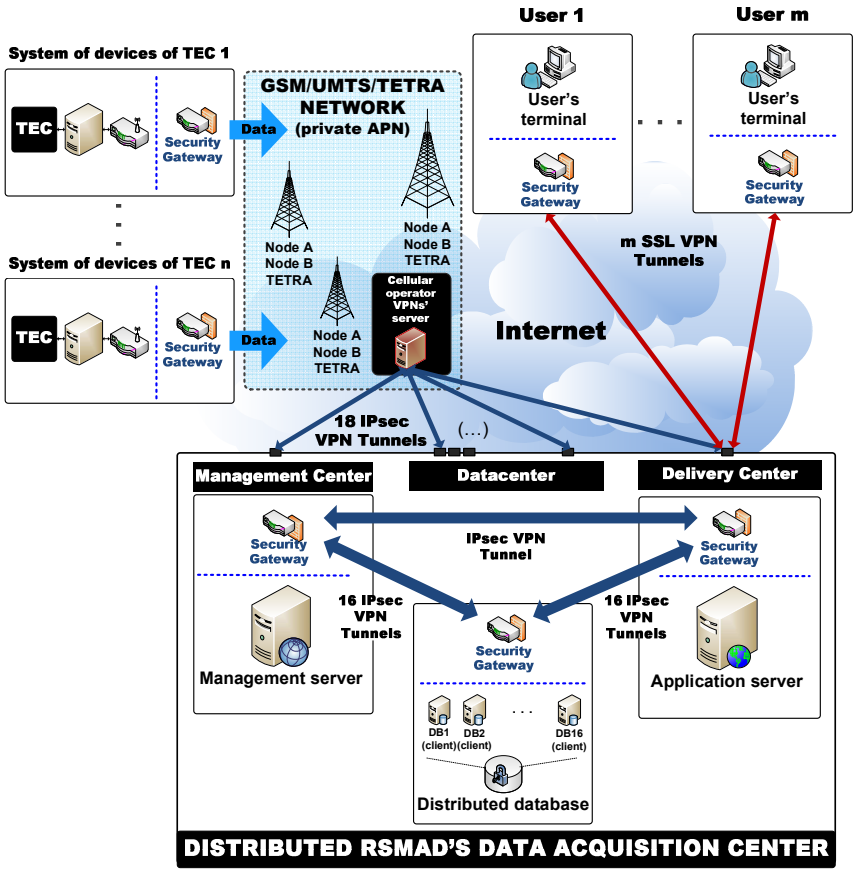

Figure 1. Simplified security architecture of RSMAD.

Thus, data protection in the RSMAD system is achieved through:

- Creating logical tunnels between the GGSN node *(Gateway GPRS Support Node)* and DAC, in a private APN subnet *(Access Point Network)* separated in the infrastructure of the GSM/UMTS operator.
- Setting data transfer limits on SIM/USIM cards *((Universal) Subscriber Identity Module)* in each location.
- Use of packets filtering and virus protection mechanisms as well as intrusion detection and prevention systems.
- Use of encryption and verification of data integrity mechanisms which are independent from the operator.

In a basic variant data will be encrypted using the *AES-128 (Advanced Encryption Standard)* algorithm and digitally signed using the *SHA-1 (Secure Hash Algorithm 1)* hash function. However, it should be noted that the security of data transmitted via public networks requires efficient performance of all securing mechanisms.

III. IP SECURITY: ARCHITECTURE AND BASIC COMPONENTS

IPsec protocol has been created through the efforts of the IPsec Protocol Working Group, being part of the IETF *(Internet Engineering Task Force)*. The primary purpose for which the group has begun work on the IPsec protocol was the supplementing the functionality of IP mechanisms to ensure the security of data transmitted using the same protocol. At the moment, the support for IPsec is one of the requirements of IPv6. In IPv4, the extension of the functionality offered by IPsec is optional. Cryptographic techniques used in IPsec, provide security to transmitted data at the level of the third layer of the ISO/OSI reference model.

IPsec protocol, by using different algorithms and cryptographic protocols provides three basic aspects of information security:

- Confidentiality.
- Integrity.
- Authentication.

There are two separate protocols in the IPsec protocols group, namely: AH *(Authentication Header)* and ESP *(Encapsulation Security Payload)*. AH protocol provides authentication using a string datagram message

 ISBN: 978-1-61208-161-8

authentication MAC *(Message Authentication Code)*. IPsec AH protocol does not ensure the confidentiality of data (data is not encrypted). ESP provides protecting the integrity and authentication of datagrams and, in addition, their encryption. It should be noted, however, that in ESP protocol authentication and encryption services are optional.

After testing of performance of AH and ESP protocols, RSMAD has been equipped with ESP protocol, despite the fact that its efficiency was slightly lower than the AH (on average about 15%), which is shown by the results of simulation presented in Table I and Table II. Following the recommendations of [4] and [5] AH protocol provides integrity of transmitted data, by calculating and adding checksum to each datagram. In case of AH the checksum value is calculated for the entire package (including IP header). AH protocol provides also effective protection against so-called „attacks by repetition". Protection against such attacks is achieved by attaching to each datagram, the next number (the serial number of the datagram).

Recommendations [4] and [6] and its subsequent recommendations [5] and [7] describe two possible modes of operation of AH and ESP protocols: transport and tunnel. In transport mode IPsec header (AH or ESP) is placed in the IP datagram directly before the header of transport layer protocol (e.g. TCP). In turn, in tunnel mode the IP datagram (IP header with data) is firstly placed in the encrypted portion of the data, and only then followed by the addition of IPsec header (AH or ESP) and the new IP header. It should also be noted that the datagrams transmitted using the ESP have a much more complicated structure than the AH datagrams. This complexity is primarily due to the fact that the ESP protocol provides confidentiality of transmitted data by using encryption. Recommendations [6] and [7] provide for such the use of block ciphers.

Parallel use of encryption algorithms and hash function is recommended, the more that the latter characterize with only marginal use on the processor, which has been clearly confirmed by the study conducted within the RSMAD project.

It has been decided to use in RSMAD the IA *(Integrated Architecture)* implementations of IPsec protocol also called an implementation of the IPsec protocol in TCP/IP stack. It is used both in hosts and gateways. It allows to ensure the end-to-end safety. In this case, IPsec is implemented, along with the IP protocol at the level of internet layer. The use of IPsec in this implementation does not require modification of the application but interference in the IP protocol itself. The advantage of this solution is undoubtedly the fact that it supports all IPsec modes.

IV. PERFORMANCE AND SECURITY ANALYSIS OF IPSEC PROTOCOL IN RSMAD

A. Introduction

The aim of this study was to evaluate the performance of IPsec protocol on various configuration parameters of the channel used for secure transmission of packets via private network. For all tests, the key exchange parameters of the channel, through which data associated with the authentication and encryption (keys) are transmitted, have remained constant. Fig. 2 shows a pictorial diagram of the laboratory station.

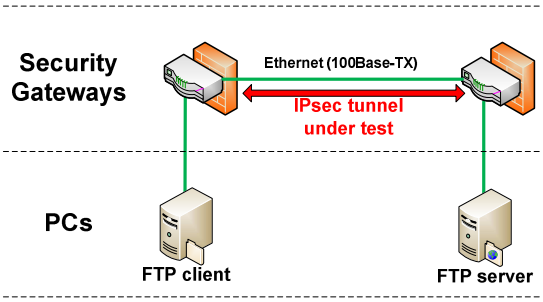

Figure 2. Simplified structure of laboratory station.

IPsec VPN tunnel was compiled between the security gateways ZyXEL ZyWALL 2 Plus. To exchange files between computers FTP *(File Transfer Protocol)* has been used. Technical characteristics of test scenarios are presented below:

1) ***Phase 1 of IPsec (permanently set):***
   - Encryption algorithm: *DES*
   - Hash function: *SHA-1*
   - Keys' exchange protocol: *Diffie-Hellmann's*
2) ***Phase 2 of IPsec (test scenarios):***

   a) ***test I parameters:***
   - Number of transmitted files: *500**
   - Total size of files: *320[MB]*
   - Device under test: *ZyWALL 2 Plus***

   ** files coming from traffic enforcement camera saved in the JPG format*
   *** max. VPN performance of ZyWALL 2 Plus is 24[Mbps]*

   b) ***test II parameters:***
   - Number of transmitted files: *1*
   - Total size of files: *320[MB]*
   - Device under test: *ZyWALL 2 Plus***

Parameters of phase 2 (data exchange) has been shown in Table I and Table II (columns 2 and 3).

B. Simulation Results

Results of simulation studies have been shown in Table I and Table II (columns 4 and 5).

The results of the studies show that the most efficient implementation of the IPsec protocol is implementation using the *DES* encryption algorithm and the *SHA-1* function for data integrity verification. As for the encryption algorithms, the least efficient algorithm is *AES-256*, although the differences in transmission are not very clear and are only about a few percent. Therefore, it seems that the selection of a set of cryptographic parameters VPN tunnels should be decided mainly for security reasons.

 ISBN: 978-1-61208-161-8

TABLE I. PERFORMANCE OF IPSEC PROTOCOL IN TUNNEL MODE

Type of IPsec	Type of hash algorithm	Type of cipher	Average data transfer rate in [Mbps]	
			Test I	Test II
ESP	SHA-1	**DES**	*18,80*	*21,44*
		3DES	*17,12*	*19,36*
		AES-128	*18,48*	*20,64*
		AES-256	*18,00*	*20,32*
	MD5	**DES**	*18,56*	*21,36*
		3DES	*16,64*	*19,60*
		AES-128	*18,08*	*20,88*
		AES-256	*17,92*	*20,24*
AH	SHA1	-	*21,28*	*22,48*
	MD5	-	*21,04*	*22,08*

TABLE II. PERFORMANCE OF IPSEC PROTOCOL IN TRANSPORT MODE

Type of IPsec	Type of hash algorithm	Type of cipher	Average data transfer rate in [Mbps]	
			Test I	Test II
ESP	SHA-1	**DES**	*19,24*	*21,93*
		3DES	*17,98*	*19,89*
		AES-128	*18,99*	*21,12*
		AES-256	*18,49*	*20,89*
	MD5	**DES**	*19,01*	*21,86*
		3DES	*17,03*	*20,20*
		AES-128	*18,60*	*21,34*
		AES-256	*18,49*	*20,74*
AH	SHA1	-	*21,88*	*22,99*
	MD5	-	*21,60*	*22,68*

As for encryption algorithms, the least efficient is *Triple-DES*, although differences in achieved transmission rates are not very clear and are only about a few percent. Therefore, it seems that the choice of a set of cryptographic parameters of VPN tunnels should be decided mainly by objective safety considerations which militate strongly in favor of the *AES* algorithm. Analysis of results shows also that the ESP protocol is slightly less efficient than the AH protocol, which is obviously related to the fact that the ESP protocol supports data encryption. Regularity can be noticed, that transmission of large files runs more efficiently (test I and test II scenarios). It results from restrictions of the FTP protocol used in the experiment. Research has also shown that introduction of additional (except VPN) mechanisms for data protection in a security gateway will cause additional (over 10 percent) reduction in the efficiency of the VPN network.

V. CONCLUSION AND FUTURE WORKS

IPsec can be undoubtedly considered as a very solid mechanism that allows the removal the imperfections and drawbacks of the IP protocol in the aspect of security. IPsec is currently agreeably recognized by most experts as the best mechanism to implement VPN in terms of security.

Without any doubt, the fact that the IPsec implementations exist for virtually all operating systems also speaks in favor of IPsec protocol. Definitely the most popular of these is FreeSWAN, designed for family of Linux operating systems.

In conclusion, we can acknowledge that IPsec is now the safest way to create a VPN network. Decreasing interest in this protocol, observed recently, is primarily due to the fact that SSL VPNs are much simpler to implement. Probably the role of SSL in telecommunications will consistently grow. However, despite a few flaws IPsec makes the impression of the best proposal, being far ahead of competitive solutions in terms of scalability and security.

Studies conducted in the RSMAD project have shown that the IPsec protocol is probably the best security protocol currently available. Similar analysis concerning other designed for similar purposes have shown that none of them was perfect. On one hand, IPsec is much better than any of the IP security protocols developed in recent years. On the other hand it seems to us that it will never lead to the creation of a fully secure system. The use of *AES* algorithm in IPsec protocol brings very tangible benefits: on the one hand it increases the security of transmission, on the other hand, the network provides a satisfactory efficiency. Therefore, it is worth noting that manufacturers of devices using IPsec protocol and *AES* need not incur any licensing costs. This affects very positively the dissemination of the *AES* algorithm, because it does not lead to an increase in prices of such devices and applications.

Until the appearing the IPsec implementations supporting *SHA-2* algorithms, we should we decide to use the implementations supporting *SHA-1* functions. Using the *MD5* function could realistically threaten the integrity of data transmitted via IPsec. In favor of *MD5* speaks only a significantly higher performance compared to the function of the SHA family (what is interesting, including *SHA-2*).

In view of the results of studies and security requirements for RSMAD, it was decided to use the IPsec ESP version (*AES-128*, *SHA-1*), in tunnel mode and implementation of the IA.

ACKNOWLEDGMENT

This research work is carried out under research and development grant No. N R02 0034 06 in 2009-2012, in the Department of Radiocommunication Systems and Networks, Faculty of Electronics, Telecommunications and Informatics in Gdansk University of Technology. The work is financed by the National Centre for Research and Development.

REFERENCES

[1] KSSR DT 07.100 v. 1.0.1, General concept of RSMAD's DAC (in Polish), Gdansk University of Technology, Poland 2009.

[2] KSSR RT 02.902 v. 1.1.0, Technical architecture for cryptographic security of RSMAD (in Polish), Gdansk University of Technology, Poland 2009.

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

[4] R. Atkinson, RFC 1826: IP Authentication Header, 1995.

 ISBN: 978-1-61208-161-8

[5] S. Kent and R. Atkinson, RFC 2402: IP Authentication Header, 1998.

[6] R. Atkinson, RFC 1827: IP Encapsulating Security Payload (ESP), 1995.

[7] S. Kent and R. Atkinson, RFC 2406: IP Encapsulating Security Payload (ESP), 1998.

 ISBN: 978-1-61208-161-8