Marcin Sokół, Małgorzata Gajewska, Sławomir Gajewski, Andrzej Marczak
Gdansk University of Technology

SECURE ACCESS CONTROL AND INFORMATION PROTECTION MECHANISMS IN RADIO SYSTEM FOR MONITORING AND ACQUISITION OF DATA FROM TRAFFIC ENFORCEMENT CAMERAS

Abstract: The study presents the architecture of the Radio System for Monitoring and Acquisition of Data from Traffic Enforcement Cameras (in short: RSMAD), particularly concerning access control and protection of confidential data. RSMAD security structure will be discussed in relation to network security issues. Additionally, the paper presents the results of the work associated with the modelling of potential threats to system security.
Keywords: AES, RSMAD, VPN

1. INTRODUCTION

Radio System for Monitoring and Acquisition of Data (RSMAD) from Traffic Enforcement Cameras (TEC) will be a highly integrated and distributed data communication system dedicated to the automatic acquisition and processing of static image data from traffic enforcement cameras. The key features of the RSMAD system, such as its modularity and scalability of the applied solutions, will provide the system with the flexibility to adapt its functionalities to the changing requirements of a system administrator. The implementation of the RSMAD system will improve the work of public institutions (including the police), the area of using traffic enforcement cameras and issuing fines.

The image data concerning traffic offences will be transmitted in the form of encrypted transport blocks to Data Acquisition Center (DAC), which will constitute the central point of the system. Data transmission will be carried out, using public cellular networks and the global Internet network. The structure of the DAC is to be distributed. It will also retain all the features of transparency. The DAC will include: Management Center (MC), Services Delivery Center (SDC) and Data Center (DC). The system will also enable a safe two-way communication with the Central Database of Vehicles and Drivers (CDVaD), in Polish: CEPiK.

The essential feature of the RSMAD will be its openness, which is known to be one of the biggest advantages of distributed systems. The openness of the RSMAD will enable sharing data resources by many users of the system. However, in terms of security, it is a very problematic feature of such systems. For this reason, the RSMAD can be far more exposed to attacks of intruders, than other electronic systems, functioning locally.

2. RSMAD SYSTEM RESOURCES ACCESS CONTROL METHODS

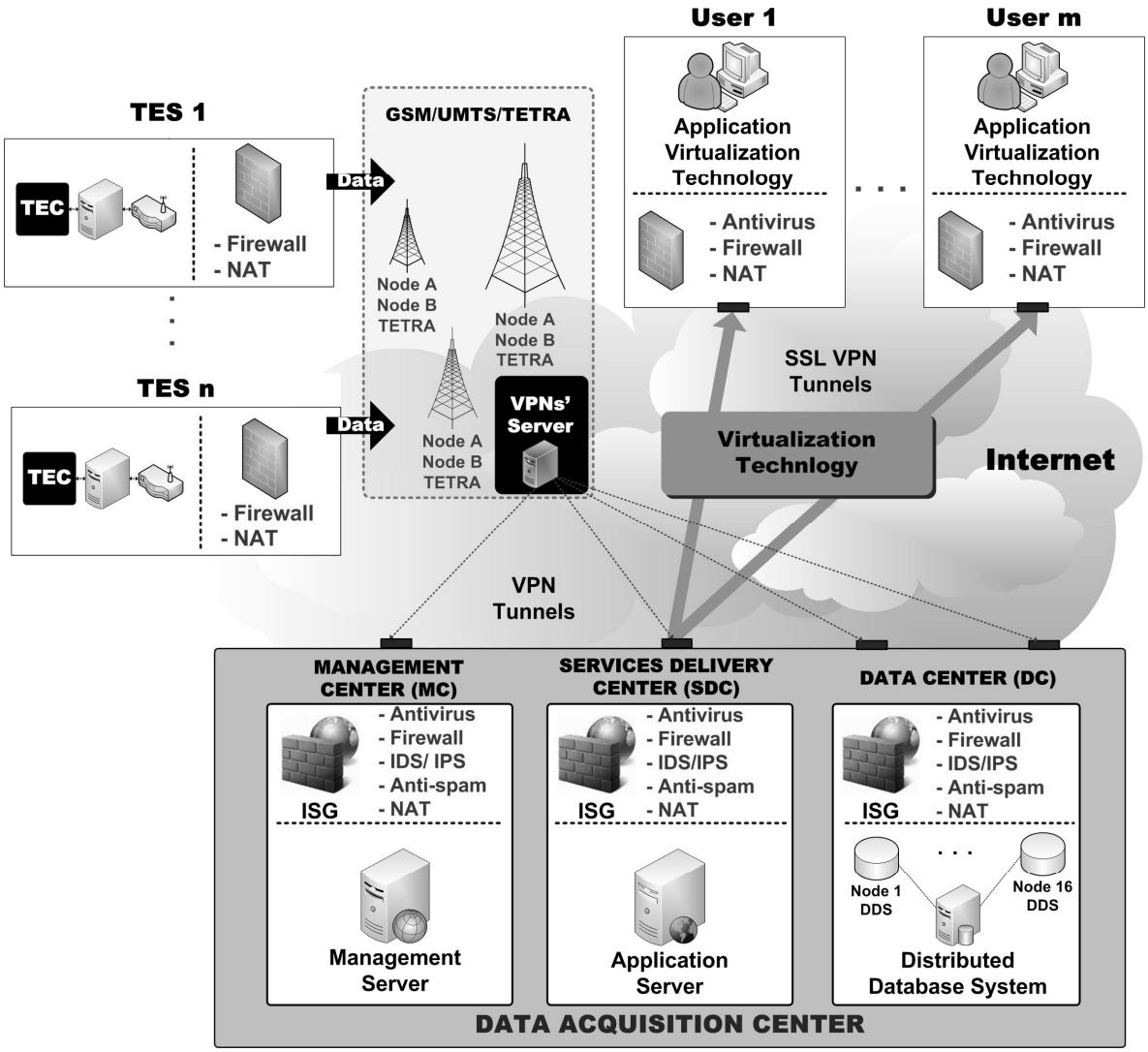
In practice, there are no telecommunication systems that are absolutely safe and provide "perfect forward secrecy" (**PFS**). The RSMAD system was chosen to use a model of safety based on the so-called computational security. It is one of the most practical indicators of the security level of information systems of all kinds. Computational security of the algorithm or protocol is defined generally as the amount of computational effort required by the best known methods of attack (at a certain moment). The algorithm/protocol is said to be secure, if the realistic level of computation required to break it (using the best known attack) considerably exceeds the computing resources of a hypothetical intruder. In this context, the RSMAD system will by equipped with cryptoalgorithms and protocols, which are characterized by the undisputed computational security.

The access control to the RSMAD system resources will be extremely important, because it directly determines the efficiency, flexibility and accessibility of the system. The RSMAD system uses the following rules of access control to system resources [6, 7]:

- **the control of user's access to system resources will be mandatory; the so called MAC principle *(Mandatory Access Control)*,**
- **access rights are to be assigned to users according to the rule of minimum rights** – this means that users who want to gain access to the resources of the system, will by default receive the lowest possible set of permissions, enough to perform their duties,
- **open access control will be used in RSMAD system –** the system will perform verification of every single access request generated by the user, which are to be granted by the control system, if not explicitly prohibited,
- **the granulation of access control will operate –** every user will have a precisely defined basic range of rights. It is assumed that if the user has higher access rights to a certain resource, lower rights to this resource will also be granted.

The structure of the security of the RSMAD system will be comprised of a several cooperating, complementary security modules [3]. The modular structure of the RSMAD security system will provide the opportunity to introduce efficient and easy changes in the network, application and service environments, as well as in the access methods, both in terms of quality (e.g. protocols, links etc.) and quantity (e.g. number of simultaneous connections) [7].

Fig. 1 presents the architecture of the RSMAD system, including the chosen information protection mechanisms [3].



List of abbreviations:

Anti-spam	-	anti-spam protection mechanism,
Antivirus	-	mechanism designed to detect and remove computer viruses,
IDS	-	*Intrusion Detection System,*
IPS	-	*Intrusion Prevention System,*
NAT	-	*Network Address Translation,*
SSL	-	*(Secure Socket Layer)* protocol securing transmission of encrypted data,
VPN	-	*Virtual Private Network,*
ISG	-	Integrated Security Gateway,

Fig. 1. Security architecture of the RSMAD system

It should also be noted that the RSMAD security system components are to be administrated from the level of the Management Center, which is to be located in a comprehensively secured area of the network (the so called controlled access area). The access to the resources of each area of the DAC will be secured, using advanced security gateways, which will also be protected. Firewalls will be used for this purpose, which will verify all the data that comes in and out of the gateway[1].

[1] In practice, the firewall functionality is implemented in the security gateways, by default.

3. CRYPTOGRAPHIC DATA PROTECTION METHODS IN THE RSMAD

It is a fact that a great number of successful intruders' attacks on ICT systems, which were said to be secured, were caused by protocols errors. Due to the characteristics of the data stored and processed in the RSMAD system, the owner of that system will be obliged to maintain comprehensive data security, through the application of both technical and organizational issues[2]. Therefore, it was decided to use publicly available algorithms and security protocols, in the RSMAD system. In accordance to the Kerckhoffs' principle, such approach provides the highest level of security. **In the basic version, it was decided to use the AES/Rijndael cryptoalgorithm *(Advanced Encryption Standard)*. The security protocols to be applied in the RSMAD are: IPsec *(IP Security)* and SSL *(Secure Socket Layer)*, which is closely related to the application virtualization technology**. The authors [4] correctly note that most attacks against the AES/Rijndael algorithm do not disclose its weaknesses and all the research conducted in the recent years have all the more confirmed the strength of this security algorithm and justified the opinion of the AES/Rijndael as being one of the best algorithms concealing data. This algorithm is characterized by a number of advantages, including:

- high performance of the software and hardware implementations (particularly important in the RSMAD system),
- development, in accordance with the Kerckhoffs' principle,
- lack of unambiguous publications on its shortcomings and weaknesses,
- lack of any patenting restrictions, concerning the algorithm.

The communication between the traffic enforcement devices and the CAD will be carried out via IPsec VPN protocol and the APN private subnet *(Access Point Network)* – fig. 1. In the RSMAD system, IPsec protocol will be used in the IPsec mode, known as the ESP *(Encapsulating Security Payload)*, operating in the tunnel mode. All the information transmitted to the DAC will be secured, using the IPsec protocol, irrespective of their nature. In order to ensure the confidentiality and integrity of the data transmitted via the protocol, certain algorithms will be used, AES/Rijndael-128 algorithm, respectively.
It should also be mentioned that the RSMAD system will be equipped with the ability to provide an easy migration to other solutions, in the future [3].

4. SAFETY AND PROTECTION OF DATA CONFIDENTIALITY IN THE RSMAD SYSTEM DATABASE

The mechanisms related to the security of the RSMAD database system can be divided into primary functional groups:

- organizational measures,

[2] Organizational measures of data protection go beyond the scope of this paper. More details on this subject can be found in [3].

- physical security, connected with the security of the physical layer,
- local security, including in particular: the use of a local IDS *(Intrusion Detection System)*, firewall and antivirus software.

The problem of efficiency and optimization of a distributed database of the system will be particularly important in the RSMAD. Even the effective security mechanisms are ignored, if they can cause a clear decrease of efficiency. For the protection of vital security system components, in particular: the maintenance and diagnostics server, application server and each of the nodes of the distributed database, IDS systems will be used (fig. 1).

The database system used in the RSMAD will be protected against all popular types of attacks on this type of systems, in particular:

- **attacks through direct connection to the Internet**[3],
- **so called *"weak passwords"* of the system administrator** - the use of "weak passwords" is one of the easiest methods of attack,
- **attacks on the browser service of database server** - the server browser service returns names and instance ports of the server to the client who sent the query, so if the client constantly sends a very large number of requests, the server is blocked for other queries; therefore it is an example of the DDoS/DoS *((Distributed) Denial of Service)* attack.

The attacks of *"SQL Injection"* [4] type are a particularly serious threat to the security of most systems. The RSMAD system, as early as at the stage of initial assumptions, was designed in compliance with all requirements needed to minimize the possibility of a successful attack of the *"SQL Injection"* type.

The TDE *(Transparent Data Encryption)* mechanism, which is the mechanism for the encryption of the data stored in the RSMAD database will apply to all data stored in the database system, in particular: database files, transaction log files, database backup and *"*snapshot copies*"* of the database. The tables in the RSMAD database system will be configured, using appropriate access controls, so that only authorized users can perform queries of the database.

4. CONCLUSION

In order to ensure the highest safety standards, the security measures in the RSMAD system will be applied in all the most critical areas, in terms of vulnerability to hacking. The RSMAD security structure will be based, in particular, on:

- verifying of user's identity,

[3] Although the problem does not appear to be serious, it is method of intrusion into the server, often and readily used by hackers.

[4] Attacks of the *"SQL Injection"* type is a security gap of Internet applications, which is caused by an inadequate filtering and the subsequent selecting and later executing of the commands sent as the SQL requests to the database.

- establishing and functioning of security domains,
- using of secure VPN connections,
- monitoring of safety,
- rational managing of security rules.

The possibility of the future easy migration to other solutions is to be retained. All the applied algorithms and security protocols will be unclassified.

The project is being carried out under the R02 N 0034 06 research-development grant, in the years 2009-2012, in the Department of Radiocommunication Systems and Networks, Faculty of Electronics, Telecommunications and Informatics at Gdansk University of Technology, and is funded entirely by the National Center for Research and Development.

References

1. Gajewski S.: *Future-Oriented Directions of Research on New Generation Cellular Technologies and System Application Solutions* (in Polish). Przeglad Telekomunikacyjny i Wiadomosci Telekomunikacyjne, no. 2-3/2010, Poland, **2010.**
2. KSSR RT 05.900 v. 1.0.0: *Architecture and technology stack of application layer of RSMAD system* (in Polish), Gdansk University of Technology, Poland, **2009.**
3. KSSR RT 02.901 v. 1.1.0: *Security architecture of RSMD* system (in Polish), Gdansk University of Technology, Poland, **2009.**
4. Rutkowski D., Sokół M., *Data security in IPsec VPN network based on AES-Rijndael cipher* (in Polish), Krajowa Konferencja Automatyzacji i Eksploatacji Systemów Sterownia i Łączności, Jurata **2009**.
5. Sokół M., *Security of All-IP core network in the UMTS cellular system* (in Polish), IV Krakowska Konferencja Młodych Uczonych, Kraków **2009**.
6. Pieprzyk J., et al., Fundamentals of Computer Security, Springer-Verlang Berlin Heidelberg, **2003**.
7. Microsoft Corp., *Assessing Network Security*, Microsoft Press, **2005**.
8. Menezes A.J., Oorschot P.C., et al., *Handbook of applied cryptgraphy*, CRC Press LLC, **1997**.
9. Mendrala D., Potasiński P., et al., *Serwer SQL 2008 – Administracja i programowanie*, Helion, **2009**.
10. Anderson R.J., *Security engineering: a guide to building dependable distributed system*, John Wiley and Sons Inc., **2001**.
11. Sokół M., *Security analysis of IPsec protocol in UMTS cellular system* (in Polish), Gdansk University of Technology, **2007**.

BEZPIECZNE METODY DOSTĘPU I MECHANIZMY OCHRONY INFORMACJI W RADIOWYM SYSTEMIE MONITOROWANIA I AKWIZYCJI DANYCH Z URZĄDZEŃ FOTORADAROWYCH

Streszczenie: W pracy omówiono architekturę Radiowego Systemu Monitorowania i Akwizycji Danych z Urządzeń Fotoradarowych (w skrócie: RSMAD), ze szczególnym uwzględnieniem mechanizmów kontroli dostępu oraz ochrony poufnych danych. Struktura zabezpieczeń systemu RSMAD omówiona została głównie w kontekście problematyki bezpieczeństwa sieciowego. Przedstawiono ponadto wyniki prac związanych z modelowaniem potencjalnych zagrożeń dla bezpieczeństwa systemu.
Słowa kluczowe: AES, RSMAD, VPN