Proceedings of the First European Teletrffic Seminar, Editors: G. Danilewicz, M. Glabowski, P.J.Kuhn, M. Pioro,
February 14-16, Poznan 2011, pp.195-202. ISBN:978-83-925375-5-7

On QoP method for ensuring availability of the goal of cryptographic protocols in the real-time systems

Bogdan Ksiezopolski
Institute of Computer Science
Maria Curie-Sklodowska University
pl. M. Curie-Sklodowskiej 5
20-031 Lublin, Poland

Zbigniew Kotulski
Institute of Fundamental Technological
Research of PAS, Pawinskiego 5B
02-106 Warsaw, Poland and
Institute of Telecommunications of WUT
Nowowiejska 15/19, 00-665 Warsaw, Poland.

Pawel Szalachowski
Institute of Telecommunications of WUT
Nowowiejska 15/19
00-665 Warsaw, Poland.

***Abstract*—Cryptographic protocols are secure due to application of security services. The security services applied for their protection can be classified into the three groups: hard, soft and extended. Among the extended ones, we can point out to the availability of the goal of the security protocol, which guarantees that protocols aims are achieved. In the real-time protocols as the video conference, the goal is both secure data transmission and good signal quality. When one of the goals is not ensured, the availability of the goal of the protocol is not guaranteed and the cryptographic protocol can not be realized. In this article we present the methodology of obtaining the balance between the quality of the signal in real-time systems and accomplishment of the required security services. Finally, the case study of video conference secured by VPN connections, is presented.**

I. Introduction

Nowadays advanced teleinformatic technologies provide us with a wide range of possibilities for the development of industry institutions and public services. Emphasis is put on the development of well-available, mobile information services called, e-anything, like e-government, e-money, and e-banking. Implementation of these services refers to a choice of proper level of security information exchanged between parties of protocols [2]. The security services applied for their protection can be classified into three groups. The first one can be named *hard* security services and it contains: confidentiality, integrity, authenticity, non-repudiation, identification (authentication, authorization), access control or secure data storage. The hard security services are accomplished by cryptographic algorithms that are mathematically justified security tools, hard to break by an attacker. The second group contains *soft* security services, including among others: privileges (rights) management, accountability, public trust (authorities), trust and reputation, audit, reliability. Such security services are usually put into practice by registering events, collecting data about users' behaviour, organizing security infrastructure, and building the emergency infrastructure. They do not guarantee complete security of protocols but help avoiding threats and detecting abuses. The third group can be called the *extended* security services and it contains the availability services: availability (of data), availability (of a service, the access), availability (of the goal of the security protocol). The services of this group are essential for proper functioning of the whole security protocol: they guarantee that the protocol aims are achieved. Their purpose can be easily defined even in the most complicated cases. However, how to obtain such a purpose, is not an easy task.

One of the important problems is establishing an appropriate level of security information, represented by security services in a given protocol. Traditionally, the aim is to provide the strongest possible security. However, the use of strong mechanisms may deteriorate the performance of a device with limited resources and pave the way for new threats, such as, resource exhaustion. In the end, it decreases system efficiency, availability and introduces redundancy. Another effect of overestimated security mechanisms is increasing the system complexity, which later influences implementation of a given project and imposes restrictions that decrease their functionality. The adequate solution in such cases is the introduction of an adaptable (or scalable) security model for the protocols, which can change the security level depending on particular conditions that take place at a certain moment and in given external conditions.

For real-time services, like secure video conferences or secure VoIP, the situation is much more complicated. The goal of the protocol is, both secure transmission of the data packages and ensuring good quality of the voice delivered into the listener's ear. This involves a proper balance of the security level of the security services applied to obtain security and their performance.

In the literature the security adaptable models are introduced as the Quality of Protection (QoP) models [1], [4]–[7]. QoP models allow calculation for different versions of the protocol which protect the transmitted data on different security levels. S.Lindskog and E.Jonsson tried to extend security layers in a few Quality of Service (QoS) architectures [4]. Unfortunately, the descriptions of the methods are limited to the confidentiality of the data and are based on different configurations of the cryptographic modules. C.S. Ong et al. in [6] present QoP mechanisms, which define security levels depending on security parameters. These parameters are: a key length, the block length and contents of an encrypted block of data. P.Schneck and K.Schwan [5] proposed an adaptable protocol concentrating on the authentication. By

means of this protocol, one can change the version of the authentication protocol which finally changes the parameters of the asymmetric and symmetric ciphers. Y.Sun and A.Kumar [7] created QoP models based on the vulnerability analysis which is represented by the attack trees. The leaves of the trees are described by means of the special metrics of security. These metrics are used for describing individual characteristics of the attack. Unfortunately, the majority of the QoP models can be recognized only for the three main security services: confidentiality, integrity and authentication. In the article [1] B.Ksiezopolski and Z.Kotulski introduced mechanisms for adaptable security which can be used for all the security services. In Section 2 we briefly present the model, which B.Ksiezopolski and Z.Kotulski introduce in [1].

In this article we are going to propose the methodology which provides possibility to obtain balance between the accomplishment of security services and the quality of the cryptographic protocol, which realize the service. We focused on the service named availability of the goal of the security protocol. The accomplishment of this service is especially important in the real-time services where delays are not allowed. We prepared the analysis by means of the Security Protocol Optimization Tool (SPOT) [15], the application whose the main function is the management of the security level of the exchanged data in the cryptographic protocol. This tool used the adaptable model [1] which introduces the Quality of Protection for security services guaranteed in the cryptographic protocol. The SPOT can be realized in the "user mode" in which the application visualizes the adaptable model. In this mode the experts can analyze the cryptographic protocol and optimize its security according to the individual requirements. In the article, we analyzed the video conference secured by the VPN connection as the example of real-time service. Finally, we presented the case study of secured VPN video conference where we checked how the signal quality depends on the guaranteed protection level.

We have organized the paper as follows: Sections 2 and 3, presents briefly the adaptable model of the security [1] and the SPOT application [15]. In section 4 we used the methodology, briefly described in sections 2 and 3 which introduce the QoP for the secured video conference. In section 5 the case study of the secured video conference is presented. Finally, in section 6 we comment on the results and present the conclusions.

II. Model of adaptable security

In this section we are going to describe briefly the model of the adaptable security which is described in the following article [1]. The security level of an electronic process depends on several factors. This level can be modified by the choice of security elements applied in a protection system. In the adaptable model [1] analytical expression is proposed for calculating the security level; its numerical value is a function of the three primary parameters:

1) L - the protection level;
2) P - the probability of an incident occurrence;
3) ω - the impact of a successful attack.

In the following subsections we describe these elements. Every protocol is divided into subprotocols and, within these subprotocols, steps. The main parameters listed in this section are computed for each service in each step. The calculation is made by means of formula 6 introduced in Section 2.4.

A. The protection level (L)

Security services are accomplished by security mechanisms and every service can be accomplished in different ways. Security mechanisms have attribute L^{XY}, where X is the abbreviation of the security service and Y is the number of security mechanism. These are the protection levels, which are defined in percent and describe their contribution of the protection of a particular service to the global protection level. The global protection level for a specific service is estimated according to formula 1. In Table 1 the security services and the security mechanisms, with appropriate L^{XY} values, for the TLS Handshake protocol are presented.

$$L^X = \sum_{Y=1}^{Y=N} L^{XY} \tag{1}$$

where:
X is the abbreviation of the security service;
Y is the number of security mechanism;
N is the number of selected security mechanisms.

B. The probability of an incident occurrence (P)

The details about the used security mechanisms are represented by the graphs. In Fig. 1 we can see the components graph for the integrity service and in Fig. 2 for the confidentiality service. Selection of the leaves refers to the selection of the particular configuration of the security mechanisms which will be used in the protocol. **1** Integrity

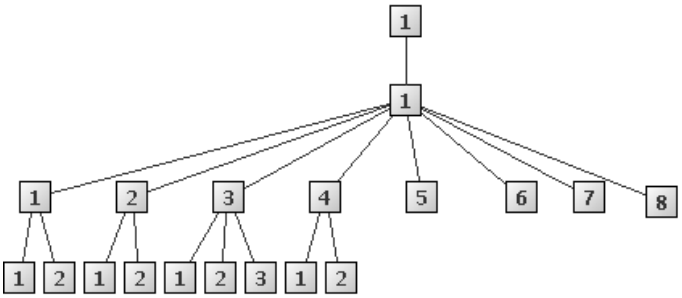

Fig. 1. The components graph for security service: integrity

1.1 Checkum MAC

1.1.1 Key management

1.1.1.1 Cryptographic modules (min. level 2) (LZ=80%, LK=70%, LP=80%, C=0.05, M=0.01)

1.1.1.2 Cryptographic modules (min. level 3) (LZ=80%, LK=80%, LP=90%, C=0.05, M=0.02)

1.1.2 Ports and interfaces of cryptographic modules

TABLE I
SECURITY SERVICES AND SECURITY ELEMENTS THAT REALIZE THEM IN TLS HANDSHAKE

	Security mechanisms					
		1	2	3	4	5
Security services	**Integrity of data (I)**	HMAC codes $L^{I1} = 60\%$	Advanced keys management $L^{I2} = 10\%$	Increase keys length $L^{I3} = 20\%$	Audit $L^{I4} = 10\%$	
	Confidentiality of data (C)	Encryption $L^{C1} = 60\%$	Advanced keys management $L^{C2} = 10\%$	Increase keys length $L^{C3} = 30\%$		
	Authentication of parties of protocol (Au)	Digital signatures $L^{Au1} = 50\%$	Advanced keys management $L^{Au2} = 10\%$	Advanced certificates management $L^{Au3} = 10\%$	Increase keys length $L^{Au4} = 25\%$	Audit $L^{Au5} = 5\%$

1.1.2.1 Cryptographic modules (min. level 2) (LZ=70%, LK=50%, LP=80%)
1.1.2.2 Cryptographic modules (min. level 3) (LZ=70%, LK=70%, LP=80%)
1.1.3 Specification of cryptographic modules
1.1.3.1 Cryptographic modules (min. level 2) (LZ=70%, LK=50%, LP=80%)
1.1.3.2 Cryptographic modules (min. level 3) (LZ=70%, LK=70%, LP=80%)
1.1.3.3 Increase digest lengths (LZ=10%, LK=60%, LP=40%)
1.1.4 Encryption mode supports integrity
1.1.4.1 Cryptographic modules (min. level 2) (LZ=80%, LK=70%, LP=80%)
1.1.4.2 Cryptographic modules (min. level 3) (LZ=80%, LK=80%, LP=90%, M=0.01)
1.1.5 Advanced keys distribution (LZ=80%, LK=50%, LP=80%, C=0.02)
1.1.6 Key usage (LZ=80%, LK=80%, LP=50%)
1.1.7 Compression method supports integrity (LZ=30%, LK=80%, LP=50%, C=0.01)
1.1.8 Audit (LZ=10%, LK=60%, LP=40%, C=0.01, M=0.03)

The leaves are described using the terms from [13].

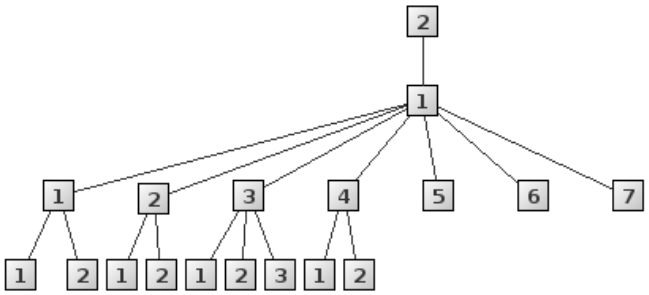

Fig. 2. The components graph for security service: confidentiality

2 Confidentiality
2.1 Encryption
2.1.1 Key management
2.1.1.1 Cryptographic modules (min. level 2) (LZ=80%, LK=70%, LP=80%, C=0.05, M=0.01)
2.1.1.2 Cryptographic modules (min. level 3) (LZ=80%, LK=80%, LP=90%, C=0.05, M=0.02)
2.1.2 Ports and interfaces of cryptographic modules
2.1.2.1 Cryptographic modules (min. level 2) (LZ=70%, LK=50%, LP=80%)
2.1.2.2 Cryptographic modules (min. level 3) (LZ=70%, LK=70%, LP=80%)
2.1.3 Specification of cryptographic modules
2.1.3.1 Cryptographic modules (min. level 2) (LZ=70%, LK=50%, LP=80%)
2.1.3.2 Cryptographic modules (min. level 3) (LZ=70%, LK=70%, LP=80%)
2.1.3.3 Increase key lengths (LZ=10%, LK=60%, LP=40%)
2.1.4 Key generation
2.1.4.1 Cryptographic modules (min. level 2) (LZ=80%, LK=70%, LP=80%)
2.1.4.2 Cryptographic modules (min. level 3) (LZ=80%, LK=80%, LP=90%, M=0.01)
2.1.5 Advanced keys distribution (LZ=80%, LK=50%, LP=80%, C=0.02)
2.1.6 Key usage (LZ=80%, LK=80%, LP=50%)
2.1.7 Audit (LZ=10%, LK=60%, LP=40%, C=0.01, M=0.03)

The leaves are described using the terms from [13].

Every leaf is described by the following parameters:

- LZ - the assets gained during successful attack on a given security element (100% = compromising the whole protocol);
- LK - the knowledge needed for an attack (100% = expert);
- LP - the costs needed for an attack (100% = the highest cost);
- C - the communication steps as an additional possibility of attack, $C \in$ [0/0.1] (0.1 = the highest threat);
- M - a practical implementation. The difficulty in implementation increases the probability of incorrect configuration. Error reports are an additional source of information, etc. $M \in$ [0/0.1] (0.1 = the highest threat).

Within service we define the additional security parameters:

- PP - the global assets possible to gain in a given process $PP \in$ [0/0.1] (0.1 = the highest threat);
- I - a kind of institution carrying out the information process. Some of the institutions are of high threat. $I \in$ [0/0.1] (0.1 = the highest threat);
- H - the potential risk for an attacker in the case of identification. The legal system and punishment of countries where the process is carried out. $H \in$ [0/0.1] (0.1 = a country with the lowest legal restrictions);

When we determine (by selection of leaves from the graph) the elements which we want to use for accomplishment of a given security service, we can compute probability of an incident occurrence: P. For every selected leaf we compute P, according to the formulae:

$$P_P = (1-(LK(1-\omega_{LK})+LP(1-\omega_{LP})))(LZ+(1-LZ)(C+M)); \quad (2)$$

$$P^{\delta} = P_P + [\delta(1-P_P)] \qquad \delta = (PP+I+H); \quad (3)$$

$$P = max(P^{\delta}); \quad (4)$$

where:
ω_{LK} - the weight defining potential attackers' lack of preparation in the domain of knowledge;
ω_{LP} - the weight defining potential attackers' lack of preparation in the domain of costs;
$\omega_{LK} + \omega_{LP} = 1$
P_P - the probability of a threat occurrence without considering the additional δ parameter
P^{δ} - the probability after taking into account the additional parameter δ
P - the probability of an incident occurrence for this service, within a given step.

After the calculation of probability of incident occurrence for all leaves we have to find the leaf which indicates the greatest probability (formula 4). This value will have the main contribution to the global probability of incident occurrence. The additional parameters are described in the article [1].

C. The impact of a successful attack (ω)

The impact of a successful attack is the second parameter (besides P) associated with risk. We calculate it, as previously, for each service in each step. We use for calculation the direct and indirect parameters presented below.
The direct parameters:
LZ - the assets gained during a successful attack on given security elements (100% is the compromise of the whole protocol);
F - the financial losses during a successful attack on given security elements (100% is the total financial loss).

The indirect parameters:
α - the necessary financial costs for repairing the damages done during a successful attack (100% is the maximal cost);
β - the losses of the value of the company shares or the company reputation (100% is the maximal market loss).

Impact of an attack is calculated by the formula:

$$\omega = \frac{LZ}{3}(F + \beta + \alpha). \quad (5)$$

D. Security level (F_S)

The global security level expresses the security of the whole cryptographic protocol. We calculate this factor according to the formula:

$$F_S = \frac{1}{a}\sum_{i=1}^{a}\frac{1}{b_i}\sum_{j=1}^{b_i}\frac{1}{c_{ij}}\sum_{x=1}^{c_{ij}}(L_{ij}^{x})^{Z}[(1-\omega_{ij}^{x})(1-P_{ij,ALL}^{x})] \quad (6)$$

where:
F_S is the security level accomplished by a given version of the cryptographic protocol, $F_S \in$ (0,1)
i is the number of the subprotocol in a given protocol,
$i = (1, ..., a)$;
j is the number of the step in a given subprotocol,
$j = (1, ..., b)$;
x is the number of the specific security service,
$x = (1, ..., c)$;
ω_{ij}^{x} is the weight describing an average cost of losses after a successful attack on a given service, $\omega \in$ (0,1);
L_{ij}^{x} is the value of a protection level for a given service, $L \in$ (0,1);
P_{ij}^{x} is the probability of an attack on a given service, $P \in$ (0,1);
Z is the scalability parameter for security elements, $Z \in$ (0,10).

III. Security Protocol Optimization Tool

In this section, we are going to describe briefly Security Protocol Optimization Tool (SPOT) [15] owing to which one can manage the security level of transmitted data by means of the cryptographic protocol. The SPOT was based on the adaptable model which was presented in the article [1]. The main aim of the adaptable model is calculating the versions of a given protocol which accomplished its functionality on different protection levels. The management system can switch between the calculated versions of the protocol.

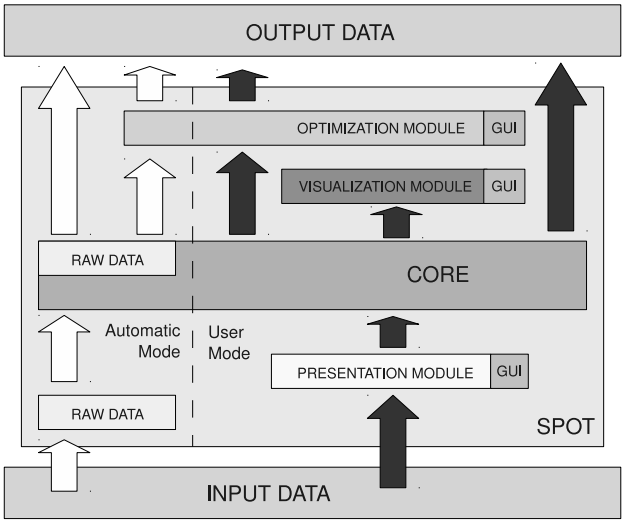

Fig. 3. The architecture of the SPOT

A. The architecture of the SPOT

The SPOT architecture is presented in Fig. 3. The architecture is based on the four main modules: the presentation module, core module, optimization module and visualization module. The SPOT can work in two modes the "automatic mode" and the "user mode". In Fig. 3 the automatic mode (white arrows) is separated from the user mode (black arrows) by the dashed line. In the automatic mode the SPOT is controlled by the configuration files where the details about the cryptographic protocol and required quality of protection

are defined. This mode is fully automatic and the results are generated without any interaction with the expert. The SPOT in this mode is the soft real-time system [11] so the SPOT response time is important but not critical for the system. In the user mode the SPOT can be configured by means of the graphic interface. This mode is not automatic and every operation must be defined manually by the expert. Details about the SPOT application can be found in the article [15]. In the next sections we will present the goals obtained by the SPOT and features of this application.

B. Goals obtained by the SPOT

1) Introducing the tool which will prepare the configuration of cryptographic protocol according to the specific requirements. The protocol configuration must be prepared in an automatic way when no user interaction is needed. This goal gives the possibility to introduce the quality of protection in the soft real time systems.
2) Visualize the adaptable model of security [1]. The tool allows the users to select interactively the data to be displayed in a friendly way. The adaptable model is complex so creating and analyzing the protocols without a friendly tool is difficult and time-consuming.
3) Parallel comparison (with all features given by the model) of the versions of the protocol.
4) The ability to analyze performance data in charts. It is very helpful to see how elements of the protocol behave in current configuration of the protocol.
5) Help to plan, review, maintain and understand logic structure of the protocol. We can study protocols and make changes easily in their configurations.
6) JAVA was used to implement the SPOT and we distribute this tool in one package, so it is platform-independent and very portable.

C. Features of the SPOT

1) Getting the results is very fast and simple.
2) The choice of actually having available graph nodes in the presentation module usage stage influences very much P_{ALL} and results in F_s. The prediction of the influence of the particular graph nodes is a difficult issue. In the presentation module we can easily get a list of all possible choices and parameters (P_{ALL},LZ) and the correlations between them.
3) SPOT provides visualization for the results. For each computation of F_s, SPOT automatically creates appropriate charts and imposes them on the previous charts. It can help see how changing the parameters affects the results. We can easily compare the versions of the protocol.
4) After creating the logic of protocol by an expert, he can write this to file. It is very useful because configuration can be loaded from file. A File's format is XML and this is a well known international standard. Owing to the usage of XML international standard, the output data can be easily used by other security application employed in a given architecture.

IV. Secure Streaming Video

In this article we would like to focus on applying the adaptable model [1] to the real-time systems which estimates the conditions providing the guarantees of achieving availability of the goal of the cryptographic protocol. We chose the streaming video as the service which must be accomplished in real time. Video conferences have different character and some of them can be made only if the appropriate security level is guaranteed. In these groups one can enumerate: military usage, management meetings from different branches or consultation during medical operation. These kinds of video conferences are mainly made as a tunnelling of VPN transmission. The usage of security mechanisms during secure VPN transmission influences the host efficiency which exchanges the data. The overestimation of security mechanisms can cause that the data processing will influence the quality of video signal. In many real-time systems, the loss of signal quality excludes its usage. In this situation on can reduce the protection level which will increase host efficiency and as a result it increases the signal quality. Unfortunately, we can imagine the situation when we can not decrease the data protection during video streaming and then the signal quality is not acceptable. In that situation the Video transmission must be stopped and then we can say that the quality of services called availability of the goal of the protocol is not guaranteed. In the article we would like to present the methodology of calculating different versions of the protocol which guarantees different protection levels. We assume that the required security level for VPN connection depends on security of informatics infrastructure from which the connection is made. We can imagine that the VPN connection is made from not trusted environment and then the security must be on a very high level. When the peers which take part in the video conference connect from different environments which have different levels of trust thus the highest requirements must be selected. We assume that three security requirement levels will be defined: *low*, *medium* and *high*. The first version, named *low*, is prepared for the scenario for the party that is trusted. The second version, named *medium*, transmits the data from the unknown party where one can not define the trust level. The third version, named *high*, is prepared for the scenario when connection is made with the set which has the status: no trust.

Among VPN technologies one can point to the TLS tunnelling as the p2p data transmission. In the article we study the video streaming as the real-time application which will be protected by the TLS tunnelling. The security mechanisms in the TLS protocol can be configured in different ways. During the transmission one can ensure confidentiality of the data by means of different symmetric ciphers, it could be [14]: 3des-cbc, blowfish-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr,cast128-cbc, arcfour, arcfour128, arcfour256, cast128-cbc. The connections integrity is accomplished by means of different hmac functions and it can

be [14]: hmac-md5, hmac-sha1, umac-64, hmac-ripemd160. The transmitted data can be protected by the TLS protocol with different combinations of symmetric cipher and hmac functions.

In the article we use adaptable model [1] to calculate different versions of the TLS protocol. We use SPOT applications owing to which we can easily prepare different versions of the protocol. The SPOT is used in the user mode so in the first step we apply the presentation module. In this module we define all parameters for the particular protocol.

A. Presentation module : configuration stage

In this step we prepare the table of security mechanism, graphs of security and steps of the protocol. The table of security mechanisms for the TLS protocol is presented in section 2.1, Table 1. After this operation we define the graphs of security. The TLS protocol guarantees three main security services: integrity of data, confidentiality of data and authentication of the parties of protocol. Two security graphs for the TLS protocol is presented in the section 2.2 (Figs. 1 and 2). These graphs refer to the integrity and confidentiality of the data.

In the last operation we define the steps of the optimized protocol. The data transmission is started by the TLS handshake protocol. The goals of the TLS Handshake Protocol are: authenticate the server to the client and the client to the server, set cryptographic keys and an encryption algorithm by negotiation. These actions are performed only once during video streaming tunnelled by TLS so its influence to the global efficiency is minimal. That is why during further study we would consider only one step in which the data is transmitted.

B. Presentation module : usage stage

In the first step of usage stage , we determine which security services are required for single steps of a given protocol. In the article we chose the security services which are presented in Table 2. “YES” in the table means that appropriate service is accomplished in a given step, and “NO” means that service is not made. As we mentioned above, during streaming video we simulate only one step, and in this step we require ensuring confidentiality and integrity of data.

Next we assign security mechanisms which are accomplished security services chosen before. In our case, security mechanisms possible to be selected are presented in Table 1. We present the selection of mechanisms which perform appropriate security service in Table 3. The numbers in this table identify the mechanisms according to Table 1.

In the next step, the value of other model parameters must be defined. The first one is the impact of successful attack. We can define these parameters when we assume the communication scenario. We assume that the most crucial data is exchanged and compromising the required security services can lead to the fundamental losses in the organization. We define three versions of the protocol, but we transmit the same type of data in each version. According to our communication scenario for the parameters F, α, β we set the values presented in Table 4.

TABLE II
SELECTED SECURITY SERVICES FOR THE STEPS OF THE PROTOCOL

		Steps of the subprotocol
		Step 1
Security services	**I**	YES
	C	YES
	Au	NO

TABLE III
SELECTED SECURITY MECHANISMS FOR THE SECURITY SERVICES

		Steps of the subprotocol
		Step 1 - Version 1 - low
Security services	**I**	1
	C	1
		Step 1 - Version 2 - medium
	I	1,3
	C	1
		Step 1 - Version 3 - high
	I	1,3
	C	1,3

Also, we set Z equal 1. The LZ parameter is taken from the graph.

TABLE IV
PARAMETERS FOR THE BASIC VERSION OF TLS PROTOCOL

	LZ	***F***	α	β
C	0.7	0.85	0.85	0.95
I	0.7	0.95	0.95	0.95

In the next step we determine the paths of the security graphs. The path estimation is crucial because in the model this choice determines the probability of incident occurrence. The selection will be different for three defined versions of the protocol. The main distinction relates to the selected security mechanisms because it determines the possible graph paths to choose. The choices for three versions of the protocol defined in the article are presented in Table 5.

The selection of specific graph path does not refer to any specific security mechanisms. The graph leavers are described by the notion introduced by the international standards as those created by the NIST or ISO/IEC organizations. In our example, the notion is taken from FIPS PUB140-2 [13] and this description refers to the group of security mechanisms which guarantees defined requirements. The specific security algorithms and security procedure must be defined manually by the security expert. After the analyses we assign the specific security parameters to the requirements defined in the security

TABLE V
SELECTED PATHS FOR THE SECURITY GRAPHS

		Steps of the subprotocol
		Step 1 - Version 1 - low
Paths of the security graphs	**I**	1.1.3.1
	C	2.1.3.1
		Step 1 - Version 2 - medium
	I	1.1.3.2, 1.1.3.3
	C	2.1.3.2
realize		**Step 1 - Version 3 - high**
	I	1.1.3.2, 1.1.3.3
	C	2.1.3.2, 2.1.3.3, 2.1.5

graph. The selection is presented in Table 6. In the first version we choose the RC2-CBC algorithm and MD5 hash function. In the second version we select the strongest symmetric algorithm (DEC-CBC) and hash function with the longest digest (SHA1). In the third version we select the symmetric algorithm with the key 3DES-CBC longer than that selected in the second version.

TABLE VI
SELECTION OF THE SPECIFIC SECURITY MECHANISMS

Ciphers
Version 1 - low
RC2-CBC + MD5
Version 2 - medium
DES-CBC + SHA1
Version 3 - high
3DES-CBC + SHA1

After the path selection from the security graph, we can compute the main parameters defined in the model and finally the global security level F_S. The results are presented in Table 7, where ω is the impact of successful attack, P is the probability of incident occurrence and L^Z is the protection level. During the analyses of Table 7 we can see that the global security level F_S increases in conjunction with modification of security algorithms. The adaptation of different versions of the same protocol can be the solution of changeable trust level of teleinformatics environment from which the peers make the VPN connections. Now is worth asking the question how the increase of security mechanisms level influences the peers efficiency which must process the data transferred by the VPN connection? In the next section we present the case study of VPN data transmission which will be accomplished by the security algorithms selected in this section and named as versions 1(low) , 2(medium) and 3(high). These results provide the answer to the question asked above.

V. CASE STUDY - VIDEO STREAMING

In this section, we would like to present the case study of audio/video streaming as the real-time service. This teleconference will be protected by the VPN data transmission which will be accomplished by the TLS tunneling. The VPN connection was made by the OpenVPN software and audio/video streaming was achieved by the VLC application. In the test we would like to check how the security mechanism influences the efficiency of the peers during the video teleconference. The host efficiency is the main factor which refers to the quality of the audio/video streaming. The video teleconference was made by two peers whose parameters are presented in Table 8. These hosts simulate the mobile devices which are connected to each other by the wireless network.

Other parameters which must be defined are the video streaming parameters. In Table 9 the requirements for the analyzed video conference are presented.

We checked the speed of transmitting the data in the video conference which was secured by the VPN connection. The results are presented in Table 10. The required quality of the video conference can be guaranteed only if we can transmit 240KB/s and simultaneously receive the same amount of data. The transfer the required level (480KB/s) is guaranteed by the first version of the protocol (low). For the second version (medium) it is equal to the required bit rate. The third version of the protocol, which accomplished the VPN connection on the high level, can not make the video conference of the required quality.

TABLE VII
THE FINAL RESULTS

	P	ω	L^Z
Version - low			
I	0.245	0.618	0.6
C	0.245	0.665	0.6
F_S	**0.1623**		
Version - medium			
I	0.150	0.618	0.8
C	0.175	0.665	0.6
F_S	**0.2127**		
Version - high			
I	0.150	0.618	0.8
C	0.150	0.665	0.9
F_S	**0.2580**		

TABLE VIII
THE HOST PARAMETERS

CPU	***RAM***	***network connection***
Host 1		
Intel Celeron 2GHz 128KB cache	512 MB	Wifi 11Mbit/s (IEEE 802.11b)
Host 2		
Intel Celeron M 1.46GHz 1MB cache	512 MB	Wifi 54Mbit/s (IEEE 802.11g)

TABLE IX
THE VIDEO CONFERENCE QUALITY REQUIREMENTS

video streaming (from one site)	
Cache size	320KB
Video resolution	640x352
Audio	4800 Hz, 2 channels, 128Kb/s
Video Bitrate	1792 Kb/s
Audio Bitrate	128 Kb/s
Global Bitrate	1920Kb/s (240KB/s)

TABLE X
THE BIT RATE OF VPN CONNECTIONS

Version 1 - low	
Bit rate	501KB/s
Version 2 - medium	
Bit rate	480KB/s
Version 3 - high	
Bit rate	453KB/s

VI. Conclusions

In the article we present the QoP methodology which estimates the version of the cryptographic protocol which ensures the availability of its goals. The secure video teleconference is analyzed as the example of real-time application. We show that overestimation of security mechanisms during data transmission leads to the decreasing efficiency of the devices from which the transmission is accomplished. In the article we apply the adaptable model [1] owing to which one can calculate different security versions of the same cryptographic protocol. Different versions of video teleconferences which are tunnelled by the VPN connection are presented. We created three versions of the TLS protocol which are designed for different environments with three levels of trust. Finally, we prepared the case study, in which we checked the performance of peers accomplishing the secure video conference by means of VPN connections tunnelled by the previously calculated TLS protocol. The results confirm that if we use strong algorithm, we may not be able to guarantee the quality of the transmitted signal and as a result we can not achieve the availability of goal of the cryptographic protocol. In such cases we have to balance between the quality of the signal and the guaranteed protection level. The methodology proposed in this paper makes it possible to obtain such a balance.

References

[1] B. Ksiezopolski, Z. Kotulski, Adaptable security mechanism for the dynamic environments, Computers & Security 26 (2007) 246-255

[2] M. Merabti, Q. Shi, R. Oppliger, Advanced security techniques for network protection, Computer Communications 23 (2000) 151-158

[3] C. Lambrinoudakis, S. Gritzalis, F. Dridi, G. Pernul, Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy Computers & Security 26 (2003) 1873-1883

[4] S. Lindskog, Modeling and Tuning Security from a Quality of Service Perspective. PhD dissertation, Department of Computer Science and Engineering, Chalmers University of Technology, Goteborg, Sweden (2005)

[5] P. Schneck, K. Schwan, Authenticast: An Adaptive Protocol for High-Performance, Secure Network Applications, Technical Report GIT-CC-97-22 (1997)

[6] C.S. Ong, K. Nahrstedt, W. Yuan, Quality of protection for mobile applications, IEEE International Conference on Multimedia & Expo (2003) 137-140

[7] Y. Sun, A.Kumar, Quality od Protection(QoP): A quantitative methodology to grade security services, 28th confrence on Distributed Computing Systems Workshop (2008) 394-399

[8] V. Blanco, P. Gonzalez, J.C. Cabaleiro, D.B. Heras, T.F. Pena, J.J. Pombo, F.F. Rivera, AVISPA: visualizing the performance prediction of parallel iterative solvers, Future Generation Computer Systems 19 (2003) 721-733

[9] L. Vigano, Automated Security Protocol Analysis With the AVISPA Tool, Electronic Notes in Theoretical Computer Science 115 (2006) 61-86

[10] B. Blanchet, A. Chaudhuri, Automated Formal Analysis of a Protocol for Secure File Sharing on Untrusted Storage, Proceedings of the 29th IEEE Symposium on Security and Privacy (2008) 417-431

[11] J.A. Stankovic, Real-Time Computing, University of Massachusetts, 1992

[12] P.Szalachowski, B. Ksiezopolski, Z.Kotulski, CMAC, CCM and GCM/GMAC: advanced modes of operation of symmetric block ciphers in the Wireless Sensor Networks, Elsevier: Information Processing Letters 110, pp.247-251, 2010

[13] FIPS 140-2: Security Requirements for Cryptographic Modules, 2001.

[14] T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, IETF, 2008.

[15] B. Ksiezopolski, P.Szalachowski, Z.Kotulski, SPOT: Optimization tool for network adaptable security, Springer: CCIS, Computer Networks, pp.269-279, 2010