On a Concept of Scalable Security: PKI-based Model using Additional Cryptographic Modules

Bogdan Księżopolski[1] and Zbigniew Kotulski[2]

[1] Faculty of mathematics, physics and computer science,
M. Curie-Skłodowska University,
Pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland,
bogdan@kft.umcs.lublin.pl
[2] Institute of Fundamental Technological Research of PAS,
Świętokrzyska 21, 00-049 Warsaw,
Poland and Institute of Telecommunications of WUT
Nowowiejska 15/19, 00-665 Warsaw, Poland
zkotulsk@ippt.gov.pl

Abstract. Public services called „e-anything" (e-government, e-banking, e-commerce, etc.) meet many different barriers, which reduce their efficient applicability. One of them is requirement of assurance of the information security when it is transmitted, transformed, and stored in the electronic service. It is possible to provide an appropriate level of security applying the present-day information technology. However, the level of the protection of information is often much higher than it is necessary to meet potential threats. Since the level of security strongly affects the performance of whole system, the excessive protection decreases the system's reliability and availability and, as a result, its global security. In this paper we present a model of scalable security for digital information transmission systems (being usually the crucial part of e-service). In our model the basic element of the security is the Public Key Infrastructure (PKI) enriched by specific cryptographic modules.

1 Introduction

Advanced teleinformatic technologies nowadays provide a wide range of possibilities of development of industry or institutions of public services. The high stress is put on the development of well-available information services called "e-anything", like e-government, e-money, and e-banking. These mentioned processes are fulfilled mainly in an electronic way, thanks to which one can increase their availability, cutting down the expenses at the same time.

Implementation of these services is connected with the choice of a proper level of security of information sent between parties of protocols [12, 14, 16]. Among teleinformatic technologies and cryptographic modules there are such, which assure different information security services e.g.: confidentiality, integrity, non-repudiation, and anonymity of data. The important problem seems to be the establishing an appropriate the level of information security fulfilled by services in a given protocol. Every use of any Internet service is connected with information exchange, which in the case of successful attack causes different threats to the whole process. This problem can be solved by estimating the security levels for each phase of the protocol [1]. Such an approach seems to be only a partial solution, because using a given specific service one can send information of different level of threats. A common practice is to use exaggerated means to ensure information security, which decreases efficiency, system availability and introduces redundancy. Another effect of exaggeration of security mechanisms is increasing the system complexity, which later influences implementation of a given project in practice, imposing restrictions that decrease their functionality.

The adequate solution such a case seems to be the introduction of scalable security model for the protocols, which can change security level depending on particular conditions that take place at a moment and in a given external conditions. In the paper we present a mechanism, which can modify the level of information security for each phase of protocol. The parameters, which influence modification of the security level, are: the risk of a successful attack, probability of a successful attack and independence of the security elements. The used security elements, which take care of the protection of information, are based mainly on PKI services and cryptographic modules.

2 Security services and supporting elements

In practice, realization of the electronic processes is connected with fulfilment of a number of legal and technical standards. While projecting the systems, we can take care of different security services [1, 2]. Among them we can enumerate: confidentiality of data, integrity of data, anonymity of the parties of protocols, non-repudiation of a sender and/or a receiver, authorization, secure data storage, management of privileges, public trust, and network and protocol/service accountability. Every security service has its own characteristics. A systematic presentation of the security services is given in Table 1.

Table 1. Characteristics of the security services

Group of services	Name of the service	Characteristics
Integrity	*Integrity of data*	Prevention against improper information modification or destruction
Non-repudiation	*Non-repudiation of action*	Non-repudiation of sending a message (the fact of communication)
	Non-repudiation of sender	Non-repudiation of sender's identity and the fact of sending a message by the sender
	Non-repudiation of receiver	Non-repudiation of receiver's identity and the fact of receiving a message by the receiver
Confidentiality	*Confidentiality of*	Guarantee of only authorized infor-

	data	mation access and disclosure
Authorization	*Authorization of parties of protocol*	Correct authorization of the parties of protocol is required to realize the steps of protocol
Privileges	*Management of privileges*	The function of a party in the protocol depends on his certain defined permission level
Anonymity	*Network anonymity*	Hiding the fact that there was a data exchange (hiding the information flow, hiding the network traffic)
	Anonymity of sender	Hiding the identity of message sender (without network anonymity)
	Anonymity of receiver	Hiding the identity of message receiver (without network anonymity)
Availability	*Availability of services*	Ensuring timely and reliable access to services and data and use of information
Public trust	*Trust between parties of protocol*	Possibility of public verification of action in protocol between parties of protocol
	TTP trust	Possibility of public verification of action in protocol with TTP usage
Secure storage	*Secure storage of data*	Confidential and permanent storage of information, available for legal users
Accountability	*Network accountability*	Events in network are registered to restore past threats
	Protocol/service accountability	Steps of protocols (access to services) are registered to restore past threats

The postulated system conditions, which are described by the security services, can be fulfilled with many different security elements. To achieve an appropriate level of security we can use different mechanisms [3, 4, 5, 6, 7]. In the article we will focus on two groups of solutions: services based on PKI [1, 3 4, 9, 10, 13, 15] and independent cryptographic modules [4]. The detailed descriptions of the used security mechanisms can be found in the literature, e.g., in the articles cited in the bibliography of this paper.

3 The concept of scalable security

The realization of electronic process is dependent of a proper level of security. During the projecting of mentioned process the security mechanisms are established. They are usually overestimated according to real risk. One can notice that there are differences connected with information sent in the same electronic process. They concern different threats, which in the case of successful attack will affect the parties of a protocol. In a case of small threat, there is a great possibility of decreasing redundant resources of information security, which in fact will improve efficiency of the protocol, system availability and, as a consequence, will increase its security

3.1 General requirements

Secure electronic processes are based on cryptographic protocols. Application of properly designed cryptographic protocol introduces many security services, which enable reliable realization of the electronic process. The protocols realize security services by means of various security elements: e.g. PKI-based services and cryptographic modules. The usage of these security elements is strictly defined in the steps of cryptographic protocols. As a result of that, any modification of their content is forbidden; otherwise it will ruin the whole concept of the protocols, what in fact negates an idea of scalable security.

Te solution of that contradiction is creating different protocols realizing the same service, applied on different level of security[1]. To precise a certain electronic service one constructs a protocol according to well-defined security requirements. Some security elements can be configured before the real process implementation, while the others introduced in a dynamic process of the system tuning. This can be done by using some unchangeable security elements whose change is critical for the processes.

3.2 Parameters of the scalable security

The security level of an electronic process can depend on several different factors. The security can be modified by means of their proper choice. In the presented model of the scalable security, the resultant protection of information is the following function of three primary parameters[2]:

[1] For simplicity, when we will change the element which is not important for the protocol's functionality, but important for its security, we will call it a new protocol.

[2] s is the security level, which is realized by a given version of cryptographic protocol;
i is a number of subprotocols in a given protocol;
j is a number of steps of parameters in a given subprotocol;
x is a concrete security service;
ω_{ij}^{x} is the weight describing an average cost of loses after successful attack for a given service;
$\omega \in (0,1)$
L_{ij}^{x} is a value of security elements for a given service; $L \in (0, 1)$
P_{ij}^{x} is the probability of attack on a given service; $P \in (0, 1)$
Z is a convergence exponent of the security elements. $Z \in (1, 25)$

$$F_S = \sum_{i}^{a} \sum_{j}^{b} \sum_{x}^{c} (L_{ij}^x)[\omega_{ij}^x (1 - P_{ij}^x)](\frac{\omega_{ij}^x L_{ij}^x}{\omega_{ij}^x})^Z \quad (1)$$

The three primary parameters in the equation (1) are:

1. *The protection level:* L_{ij}^x ;
2. *The risk of attack on a given service:* $[\omega_{ij}^x (1 - P_{ij}^x)]$;
3. *The dependence (coefficient) of security elements:* $(\frac{\omega_{ij}^x L_{ij}^x}{\omega_{ij}^x})^Z$;

Each of the above parameters in the formula (1) is calculated for all cryptographic protocols, all subprotocols of these protocols and all steps of the subprotocols.

Table 2. Security dependencies describing possible security services and security elements that realize them.

	1	2	3	4	5	6	7	8	9
Integrity of data (I)	Digital Signatures L_I1=50%	Key management L_I2=10%	Certificate management L_I3=10%	Directory services L_I4=5%	TTP to TTP interopera-bility L_I5=15%	PKG L_I6=10%			
Non-repudiation of action (NRM)	Digital Signatures L_NRM1= 30%	Time-stamping L_NRM2= 15%	Key management L_NRM3= 10%	Certificate management L_NRM4= 10%	Audit L_NRM5= 5%	Non-repudiation PKI L_NRM6= 10%	Directory services L_NRM7= 5%	Information repository L_NRM8= 5%	PKG L_NRM9= 10%
Non-repudiation of sender (NRS)	Digital Signatures L_NRS1= 30%	Time-stamping L_NRS2= 15%	Key management L_NRS3= 10%	Certificate management L_NRS4= 10%	Audit L_NRS5= 5%	Non-repudiation PKI L_NRS6= 10%	Directory services L_NRS7= 5%	Information repository L_NRS8= 5%	PKG L_NRS9= 10%
Non-repudiation of receiver (NRR)	Digital Signatures L_NRR1= 30%	Time-stamping L_NRR2= 15%	Key management L_NRR3= 10%	Certificate management L_NRR4= 10%	Audit L_NRR5= 5%	Non-repudiation PKI L_NRR6= 10%	Directory services L_NRR7= 5%	Information repository L_NRR8= 5%	PKG L_NRR9= 10%
Confidenti-ality of data (C)	Encryption L_C1=50%	Key management L_C2=10%	Certificate management L_C3=10%	SSS L_C4=15%	Directory services L_C5=5%	PKG L_C6=10%			
Authoriza-tion of parties of protocol (Au)	Registration L_Au1= 20%	Digital Signatures L_Au2= 20%	Key management L_Au3= 10%	Certificate management L_Au4= 10%	TTP to TTP interopera-bility L_Au5= 10%	Directory services L_Au6=5%	Authoriza-tion PKI L_Au7= 10%	AA L_Au8= 10%	
Manage-ment of privileges (MP)	Registration L_MP1= 50%	Authoriza-tion PKI L_MP2= 50%							
Network anonymity (AN)	Crowds L_AA1= 100%								
Anonymity of sender (AM)	Individual numbers L_AM1= 100%								
Anonymity of receiver (AR)	Broadcast-ing L_AR1= 100%								

Trust between parts of protocol (PTA)	Time-stamping L_PTA1= 30%	Information repository L_PTA2= 30%	Audit L_PTA3= 20%	TTP to TTP interoperability L_PTA4= 20%					
TTP trust (PTT)	Time-stamping L_PTT1= 30%	Information repository L_PTT2= 20%	Audit L_PTT3= 10%	TTP to TTP interoperability L_PTT4= 10%	Notary L_PTT5= 30%				
Secure storage of data (SS)	Encryption L_SS1=30%	Time-stamping L_SS2=10%	Key management L_SS3=10%	Certificate management L_SS4=10%	Non-repudiation PKI L_SS5=10%	Information repository L_SS6=15%	Directory services L_SS7=5%	Audit L_SS8=5%	PKG L_SS9=5%
Network account-ability (NA)	Logging L_NA1= 50%	Audit L_NA2= 20%	Encryption L_NA3= 10%	Digital Signatures L_NA4= 10%	Information repository L_NA5= 10%				
Proto-col/service account-ability (PA)	Logging L_PA1= 50%	Audit L_PA2= 20%	Encryption L_PA3= 10%	Digital Signatures L_PA4= 50%	Information repository L_PA5= 10%				

The first parameter defines the protection level for a given cryptographic service in a given step of subprotocol. This is a sum of chosen security elements, which guarantee security of a given service.

The second parameter shows a risk of attack on a given security service. This is a multiplication of average losses made by successful attack and probability of attack on a given security service.

The third parameter describes independence of security elements used to gain a proper protection level. The security elements are mutually connected; missing some protection of information mechanisms in one subprotocol (e.g., at the beginning of the protocol) strongly influences the security of other subprotocols. The level of convergence can also be changeable; it depends on, e.g., a number of subprotocols and the security level.

The security level of electronic processes mainly depends on the used elements of protection of information required by the security services. In this paper, the security elements are based on PKI services and cryptographic modules. In Table 2, dependences of security services and security mechanisms are presented. Every security service can be realized by different security mechanisms. Security level of a given protocol will depend, among other things, on an appropriate selection of the elements. For every security elements their contribution to the global protection of services is defined as L_{ij}^{x} . The individual contribution of particular services is defined in percent.

Security dependencies of the security elements (Table 2) are only an example. It can be created in a free way using different security mechanisms. The value of the parameter L is constant for particular security requirements. Creating the cryptographic protocol on a different level of protection, we do not modify this parameter.

3.3 Impact of successful attack

The parameters, which are set up during the risk calculation are the weights for particular services ω_{ij}^{x} . These weights indicate the average loses caused by a successful attack.

In the risk modelling, the impact is the result of an information security incident, caused by a threat, which affects assets. In the presented model of scalable security the resultant impact is obtained by combination of two kinds of impact, caused by direct and indirect reasons. Below we present the parameters used during the impact calculation:

The direct parameters:

LZ_{ij}^{x} are the assets gained during a successful attack on a given security elements (100% is the compromise of the whole protocol);

F_{ij}^{x} are the financial losses during a successful attack on given security elements (100% is the total financial loss);

The indirect parameters:

α_{ij}^{x} are the financial costs, which are necessary for repairing the damages gained during a successful attack (100% is the maximal cost);

β_{ij}^{x} are the losses of the value of the company shares or the company reputation (100% is the maximal market loss).

To calculate the impact of a successful attack (ω_{ij}^{x}) we use a combination of the parameters described above. Thus, the parameter LZ_{ij}^{x} describes the influence of potential harm of a given threat to compromise the whole process. The F_{ij}^{x} describes direct financial losses during the attack on the particular step of the protocol.

The next parameters are connected with an indirect impact of the successful attack. The first group of parameters (α_{ij}^{x}) is connected with the indirect financial losses, which must be taken after successful attack on the system. Those financial losses are due to damage and repairing of the information systems. The second group of parameters (β_{ij}^{x} .) describes the loss of the company securities or a company reputation.

By combination of all the mentioned parameters we obtain the impact of an attack in a particular process:

$$\omega_{ij}^{x} = (F_{ij}^{x} + \beta_{ij}^{x} + \alpha_{ij}^{x})\, LZ_{ij}^{x}$$

The impact parameter is a changeable part of the Equation (1) for a particular processes, because losses connected with a successful attack can be different for a concrete information process.

4 Usage of the scalable security model: e-auction

The concept of scalable security can be realized for different types of cryptographic protocols [8, 9]. In this paper we present an example, which implements the idea of scalable security for the electronic auction. The considered e-auction model is formulated as the cryptographic protocol [9].

4.1 The e-auction model

The analysed protocol of e-auction consists of four subprotocols: *certification, notification of auction, notification of the offer, and the choice of the offer*. In protocol take part *N* bidders (O_1, ... ,O_N), third trustworthy person that is GAP (central auction agency) as well as firm, which wants to announce the auction.

The first step of protocol is verification by GAP, the participants taking part in e-auction, that is the bidders O_N as well as firm F which wants to announce the auction (the *subprotocol of certification*). The next step is notification to GAP the auction by verified firm F. GAP publishes the conditions of notified auction, giving all requirements notified by F (*the subprotocol of notification of auction*). In the next step, person wanting to take part in auction, after the earlier verification, sends his offer to GAP (*the subprotocol of notification of the offer*). The last subprotocol is executed after elapsing of time for notification of offers, then the firm F as well as bidders O_N, send their parts of secret (needed to read offers) to GAP. After decoding them, they will be sent to firm F, where victorious offer will be chosen. In the same subprotocol, the firm F sends information about the victorious offer to GAP, and then it will be published to (be generally known) public message (*the subprotocol of choice of the offer*).

The communication between participants of the protocol is safe. We achieve it thanks to using public key cryptography, where every participant of the protocol possesses his private key (SK) as well as public key (PK). Those practical keys are not permanent; their validity ends with the validity of the registration number, which is achieved in the subprotocol of certification.

4.2 Security of a chosen sub-protocol

As we mentioned, we present usage of the scalable security for the subprotocol of notification of electronic auction. The protocol (see Fig.1) can be notified by any person, which obtained suitable authorizations in the subprotocol of certification.

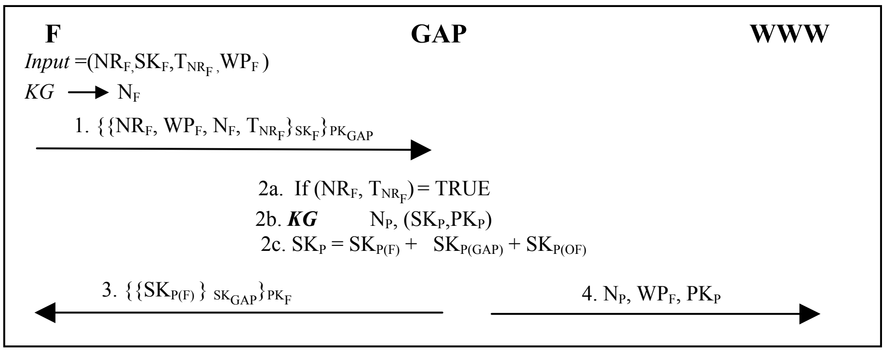

Fig. 1. A diagram of the subprotocol of the electronic auction notification

Such a person, called F, should possess the registration number NR_F, his time stamp T_{NR_F}, private key SK_F as well as conditions of notified auction WP_F . F generates with the help of the generator of random numbers (KG), his individual number N_F.

Step 1:
In the first step, F sends to GAP, signed digitally (SK_F) as well as coded (PK_{GAP}) the following information: his registration number (NR_F), his time stamp (T_{NRF}), the conditions of auction (WP_F), and his individual number (N_F).
Step 2:
The central auction agency (GAP) verifies the registration number of F, (NR_F) and validity of his timestamp. After positive authorization, GAP generates the individual number of auction (N_P) and the pair of keys for the concrete auction, (SK_P,PK_P). The private key of auction (SK_P) is divided into parts by using the threshold scheme of secret sharing. Secret is divided into three parts, designed for F($SK_{P(F)}$), for GAP ($SK_{P(GAP)}$) and for bidders in the auction ($SK_{P(OF)}$). Each part is necessary to reproduce the private key (SK_P).
Step 3:
GAP sends digitally signed (SK_{GAP}) and encrypted (PK_F), the part of the secret designed for F ($SK_{P(F)}$).
Step 4:
GAP publishes, for example on WWW site, the number of auction (N_P), conditions of it (WP_F) and the public key of the auction (PK_P).

4.3 Results

The Step 1, which must be executed, defines weights, which describe the risk „ ω_{ij}^{x} ” for particular security services in all the steps of subprotocol. In the described case the defined weights are constant for a given process. If any security service is not required in a given step, the weight of described risk is equal to zero. In Table 3 we present the values of weights for a given subprotocol.

Table 3. The values of weights for a given subprotocol

	Step 1	**Step 2**	**Step 3**	**Step 4**
ω^{I}	0.5	0.4	0.3	0.3
ω^{C}	0.7	0.7	0.5	0
ω^{NRS}	0.3	0	0.3	0.3
ω^{Au}	0	0.7	0	0
ω^{SS}	0	0.3	0	0
ω^{MP}	0	0.3	0	0

Table 4. Security elements for a given subprotocol.

	A						B						C					
	L^I	L^C	L^{NRS}	L^{Au}	L^{SS}	L^{MP}	L^I	L^C	L^{NRS}	L^{Au}	L^{SS}	L^{MP}	L^I	L^C	L^{NRS}	L^{Au}	L^{SS}	L^{MP}
Step 1	0.8	0.7	0.65	0	0	0	0.95	0.9	0.8	0	0	0	0.5	0.5	0.45	0	0	0
Step 2	0.35	0.85	0	0.95	0.65	0.5	0.5	0.9	0	1	1	1	0.3	0.35	0	0.5	0.45	0.5
Step 3	0.8	0.7	0.5	0	0	0	0.95	0.85	0.6	0	0	0	0.5	0.5	0.3	0	0	0
Step 4	0.5	0	0.4	0	0	0	0.8	0	0.55	0	0	0	0.5	0	0.3	0	0	0

During the Step 2, we define security elements, which realize chosen security elements (Table 4). This element is changeable for every version of described subprotocols. In the paper we describe three versions of the subprotocol, the first, basic ("A"), and others, with larger number of security elements ("B") and smaller number of security elements ("C").

During the Step 3, we set up probability of attack on a particular services in described steps of protocol. (Table 5). Those values are constant for a given process.

Table 5. The values of probability in a given subprotocol.

	Step 1	Step 2	Step 3	Step 4
P^I	0,8	0,3	0,3	0,7
P^C	0,7	0,9	0,8	0
P^{NRS}	0,4	0	0,2	0,6
P^{Au}	0	0,5	0	0
P^{SS}	0	0,3	0	0
P^{MP}	0	0,5	0	0

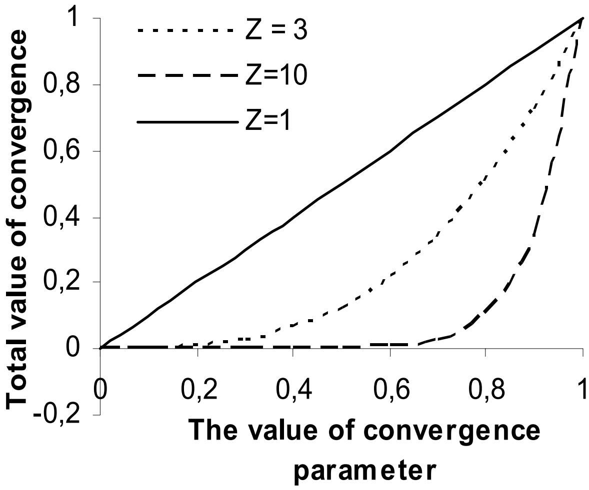

Fig. 2. Characteristic of the convergence parameter.

The last parameter is a parameter of function convergence whose characteristics are shown in Fig. 2. In the described subprotocol, the value of parameter Z = 3 was chosen.

In the last Step 4, checking the security level of the particular version of the subprotocol, we calculate the value of the function F, see Equation 1. The results of calculations are presented in Table 6.

Table 6. The values of security levels for particular steps and whole subprotocol

	Step1	*Step2*	*Step3*	*Step4*	*Total*
A	0.12351	0.37268	0.12502	0.00869	**0.62991581**
B	0.29296	0.77342	0.25435	0.04784	**1.36858231**
C	0.02675	0.04318	0.02131	0.00659	**0.09785187**

5 Conclusions

Analysis of this paper shows that we three versions of described subprotocol, each with different level of protection. The basic level (“A”) is much higher than the level with a few security elements (“C”). Thus, the level (“C”) could be used only in a case of transporting unimportant data. The version with the highest security level (“B”), guarantee the strongest protection of the subprotocol. This version is adequate for transmission of critical data between the parties of the protocol.

The prior setting up different security levels for all subprotocols in the whole e-auction protocol helps us to change particular versions of subprotocol, creating freely scalable with respect to the security level, final version of the protocol. Such a possibility can be useful in a case of modifying the security levels in particular phases of subprotocol [17], which can decrease system performance and, as a result, its security.

References

1. Lambrinoudakis, C., Gritzalis, S., Dridi, F., Pernul, G.: Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. Computer Communication 26. Elsevier (2003) 1873-1883
2. NIST: Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories (2004)
3. Patel, A., Gladychev, P., Katsikas, S., Gritzalis, S., Lekkas, D.: KEYSTONE project, Support for Legal Framework and Anonymity in the KEYSTONE Public Key Infrastructure Architecture (2000)
4. Kulesza, K., Kotulski, Z.: On Automatic Secret Generation and Sharing for Karin-Greene - Hellman Scheme. In: J. Sołdek, L. Drobiazgiewicz, (ed.): Artificial Intelligence and Security in Computing Systems, Kluwer (2003) 281-292
5. Groves, J.: Security for Application Service Providers. Network Security, Issue 1, January 1, (2001) 6-9
6. ISO/IEC 11770-3: Key management-Part 3: Mechanisms using asymmetric techniques (1999)
7. ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates (2002)
8. Barlow, L.: A Discussion of Cryptographic Protocols for Electronic Voting (2003)
9. Księżopolski, B., Kotulski, Z.: Cryptographic protocol for electronic auctions with extended requirements; Annales UMCS Informatica v.2 (2004)
10. Teoh, A., Ngo, D., Goh, A.: Personalised cryptographic key generation based on Face Hashing; Computer & Security 23. Elsevier (2004) 606-614
11. Saez, G.: Generation of key pre-distribution schemes using secret sharing schemes. Discrete Applied Mathematics 128. Elsevier (2003) 239-249
12. Groves, J.: Security Application Service Providers. Network Security, Issue 1. Elsevier (2001) 6-9
13. Reiter, M., Rubin, A.: Crowds: Anonymity for Web Transaction. ACM Transaction on Inf formation and System Security, Vol. 1, No. 1 (1998) 66-92
14. Merabti, M., Shi, Q., Oppliger, R.: Advanced security techniques for network protection. Computer Communications 23. Elsevier (2000) 151-158
15. Tzong-Sun, W., Chien-Lung, H.: Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks. Computer & Security 23. Elsevier (2004) 120-125
16. Patton, M.A., Josang, A.: Technologies for Trust in Electronic Commerce. Electronic Commerce Research, 4. Elsevier (2004) 9-21
17. Moitr, S., Konda, S.: An empirical investigation of network attacks on computer system. Computer & Security 23. Elsevier (2004) 43-51