ON PROBABILISTIC MODELING OF INCIDENT OCCURRENCE IN ELECTRONIC PROCESSES

Bogdan Księżopolski[1], Zbigniew Kotulski[2]
[1]Faculty of Mathematics, Physics and Computer Science
M. Curie-Skłodowska University,
Pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland
e-mail:bogdan@kft.umcs.lublin.pl
[2]Institute of Telecommunications of WUT
ul. Nowowiejska 15/19, 00-665 Warsaw, Poland
and Institute of Fundamental Technological Research of PAS
ul. Świętokrzyska 21, 00-049 Warsaw, Poland
e-mail:zkotulsk@ippt.gov.pl

ABSTRACT

Public services called „e-anything" (e-government, e-army, e-banking, e-commerce, e-logistic, 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 an electronic service. Creating proper information security systems is a complex process. Usually, it is preceded by risk analysis by means of which one can create system with a proper protection level. In a mentioned process, the important element is to calculate the probability of threat occurrence and then probability of incident occurrence as a combination of threats [8]. In the paper we present the model by means of which we can calculate the probabilities of incidents occurrence. As an example of application of the general procedure, we present the analysis for the model of a cryptographic protocol realizing e-auction [6].

1. INTRODUCTION

Advanced teleinformatic technologies, nowadays provide a wide range of possibilities of development of industry or the institutions of public services. The big stress is put on the development of well-available information services called "e-anything" like e-government, e-money, e-banking. These mentioned processes are fulfilled in 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 proper level of security of the information transmitted between the parties of protocols [12,13,14]. Among teleinformatic technologies and cryptographic modules there are such that protect different information security services, e.g.: confidentiality of data, integrity, non-repudiation, and anonymity of the parties. The choice of proper security mechanisms, which guarantee the adequate level of protection, [1] depends (among others) on the assumed security conception. This conception can be created by means of different methodologies [9,10] but, in fact, in each of them one should take into account a number of similar components, which influence the risk of a given process. Among them one can enumerate: assets taking part in the process, threats of the assets, vulnerabilities of the assets, the impact of successful attack, and safeguards. The setting up the mentioned components is connected with a number of numerical parameters characterizing quantitatively the process. One of the most important parameters is the probability of an incident occurrence. In this paper we propose a method of modeling the probability of incident occurrence and usage of this model for one of the electronic services: the electronic auction.

The e-auction process considered in this paper is based on the cryptographic protocol presented in [6].

2. SECURITY CONCEPTION

One of the elements, which are needed for creating information security systems, is

setting up the conception of security. As mentioned above, the components needed in the risk management process are complex, based on many information security items [8]. In our model we need the following elements.

Assets
The basic step in setting up security process is analyzing the organization assets. One has to establish the level of vulnerabilities of assets and on this base one will set up proper security elements.

Threats
Potential threats can cause harm on gathered assets by a given organization. The harms can be caused by attack on information taking part in process or on the system. The threats must use vulnerabilities in assets and then can cause some harm. Threats can be divided into human and environmental and next into deliberate and accidental. For setting up the threats one should define the level of such threat and calculate the probability of such incident occurrence.

Vulnerabilities
A weakness of an asset that can be exploited by one or more threats is known as Vulnerability. Vulnerabilities associated with assets include weaknesses in physical layout, organization, procedures, management, hardware, software, information etc. A vulnerabilities in itself does not cause harm but only in case of attack

Impact
Impact is the result of an information security incident, caused by a threat, which affects assets. The impact could be the destruction of certain assets, damage security system and compromise of confidentiality, integrity, availability, non-repudiation, authenticity, reliability etc. Possible indirect impact includes financial losses, company image etc.

Safeguards
Safeguards are practices, procedures or mechanisms that may protect against a threat, reduce vulnerability, and reduce the impact of an information security incident.

Risk
The risk is characterized by a combination of two factors, the probability of the incident occurring and its impact. Any change to assets, threats, vulnerabilities and safeguards may have significant effects on risk.

Scalable security
As an additional item in the risk management process one can attach the scalable security [11]. Every analysis of the information protection often shows new vulnerable structures in the system, which causes additional security elements. These protections are often over-established, which generally decrease efficiency, availability of the system, and excess redundancy. Thanks to scalable security one can change security level depending on given requirements of the electronic process.

All of the above mentioned elements are closely connected and their relationship is precisely presented by standards [3,4,5,8] and analyzed in articles [1,2,9,10,12,13,14]. Consideration on security of any system is a never-ending process. The risk analysis cannot be stopped, because the threats can never be eliminated for certain.

3. THE MODEL

The condition of making electronic services more widespread is to guarantee a proper level of information security. The first step in the process of creating security system is to establish security requirements, which guarantee a concrete service (Fig.1). Next, one sets up security elements, mechanisms that guarantee the security requirements. The chosen elements and the rules of their usage are described by means of protocol. The security elements used should protect against potential threats of the process. The result of a harm in a case of successful attack is defined by means of the additional parameter (Impact) and it depends on gained assets. The risk value of the concrete process is established after analyzing the mentioned items.

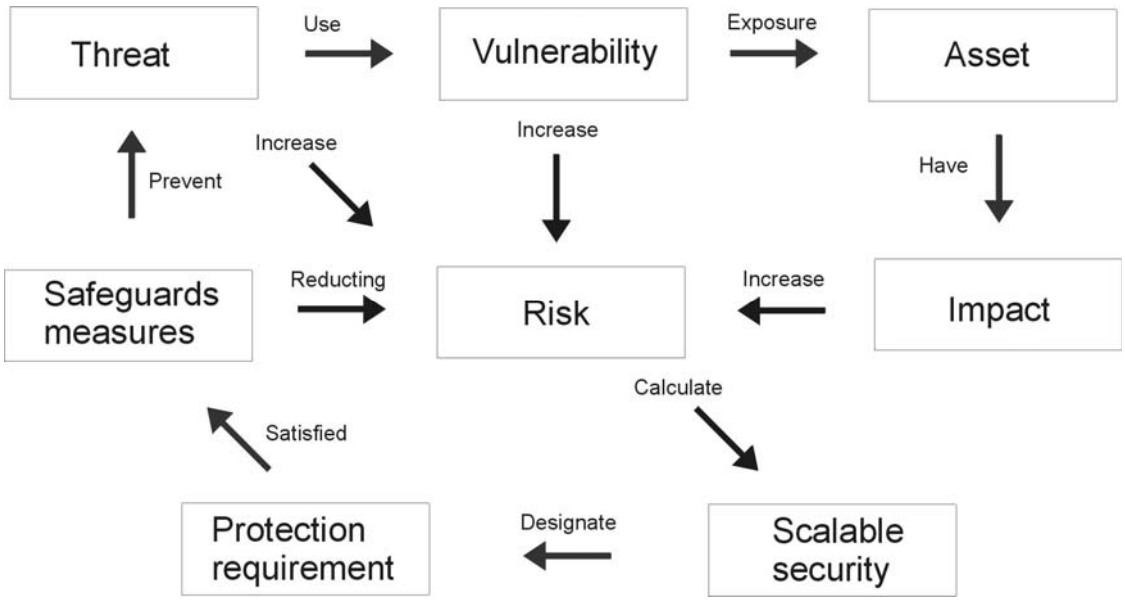

Figure 1: The cycle and relationship of security elements for risk management

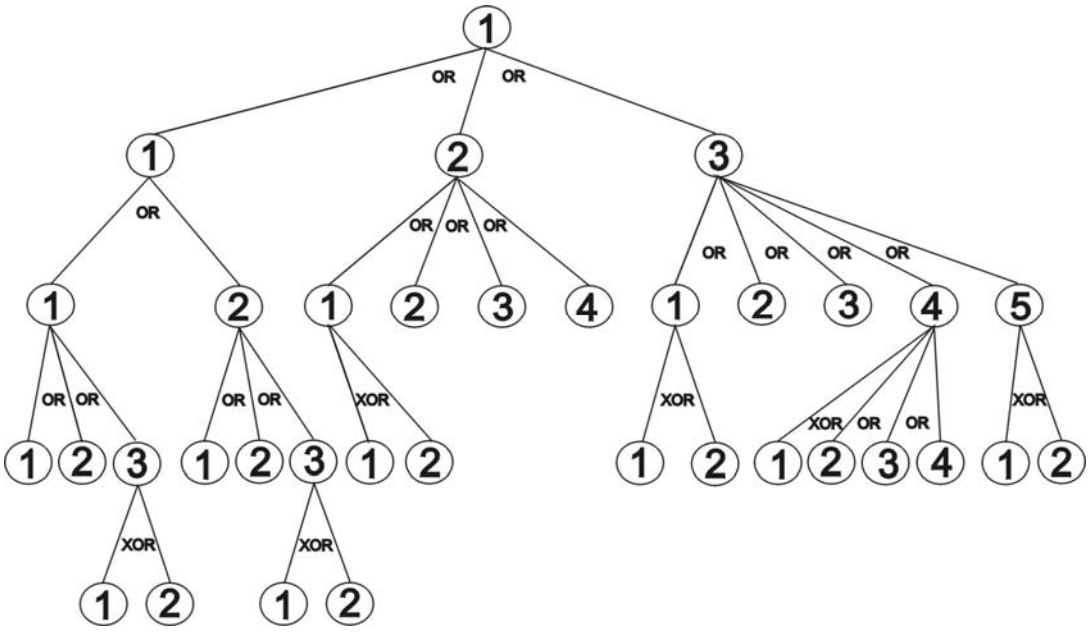

Figure 2: The graph for security service: integrity.

Additional security mechanism, which one can use in the process of risk defining, is the scalable security [11]. Every time, at the end of risk defining cycle, one can calculate the system protection level. As a result of particular risk analyses, which often influence on used security elements, one gains a number of possible versions of the protocol. During practical realization of a given process one can choose such a version of the protocol, which will realize a given service in an optimal way with sufficient security protection.

In the paper, we present a model, which can be used for calculating the probability of threat occurrence and the probability of incident occurrence as a function of a range of threats.

3.1 The graph of the security services

Security requirements for a given process can be defined by means of properly selected security services. Among them, we can take care of: confidentiality, integrity, non-repudiation, anonymity, availability of data and other security elements [1,2,14]. The

defined requirements on the system, expressed in terms of security services, we realize by means of security elements such as: digital signature, encryption, time-stamping, trustworthy third party services, secure secret sharing, etc.

At the beginning we create the combination of possible security elements, which can be used in the security model, and we present them by means of a graph. On the graph, we also define detailed security parameters whose choice influences the information security level. For every service, we create an individual graph (Fig.2). On Fig. 2 we present an example of the combination of security elements for the integrity security service. The choice of particular graph edge correspond to the choice of a concrete security element. Choosing concrete security elements, we join the numbers of graph nodes of particular graph edges, putting dotes between them. Below we preset graph description for the integrity security service (Fig.2). To simplify the graph, we use only the main security elements. The whole graph should be based on security mechanisms, which are described in international standards (see, e.g., ISO, IEC, IEEE, ETSI).

1. Integrity

1.1 Digital signature

(LZ,LK,LP = heritage)

1.1.1 Cryptographic key management
Cryptographic modules (min. level 2) [5] (LZ=80%, LK=70%, LP=80%, C=0.05;M=0.01)

1.1.1.1 Generating keys by using biometric method, PKG [7] (LZ=80%, LK=100%, LP=100%,M=1,02)(LK+5%,LP=+5%)

1.1.1.2 Audit (LZ=10%,LK=60%, LP=40%) (LK=+5%, LP=+5%, C=0.01;M=0.03)

1.1.1.3 Ports and interfaces of cryptographic module *(LZ,LK,LP = heritage)*

1.1.1.3.1 Cryptographic modules (min. level 2) [5] (LZ=70%, LK=50%, LP=80%)

1.1.1.3.2 Cryptographic modules (min. level 3) [5] (LZ=70%, LK=70%, LP=80%)

1.1.2 Cryptographic key management
Cryptographic modules (min. level 3) [5] (LZ=80%, LK=80%, LP=90%, C=0.05, M=0.02)

1.1.2.1 Generating keys by using biometric method, PKG [7] (LZ= 80%, LK=100%, LP=100%,M=0.02){LK+5%,LP=+5%)

1.1.2.2 Audit (LZ=10%, LK=60%, LP=40%) (LK=+5%,LP+5%, C=0.01, M=0.03)

1.1.2.3 Ports and interfaces of cryptographic module *(LZ,LK,LP = heritage)*

1.1.2.3.1 Cryptographic modules (min. level 2)[5] (LZ=70%,LK=50%,LP=80%,)

1.1.2.3.2 Cryptographic modules (min. level 3)[5](LZ=70%, LK=70%, LP=80%)

1.2 Key management

(LZ,LK,LP = heritage)

1.2.1 Key generation
(LZ,LK,LP = heritage)

1.2.1.1 Cryptographic modules (min. level 2) [3], Security techniques (min. EAL 3)[4] (LZ=80%, LK=70%, LP=80%)

1.2.1.2 Cryptographic modules (min. level 3) [3], Security techniques (min. EAL 4)[4], (LZ=80%, LK=80%, LP=90%, M=0.01)

1.2.2 Key distribution
(LZ=80%, LK=50%, LP=80%,C=0.02)

1.2.3 Key usage (LZ=80%, LK=80%, LP=50%)

1.2.4 The end of key life cycle (LZ=30%, LK=80%, LP=50%, C=0.01)

1.3 Certificate management

(LZ, LK,LP = heritage)

1.3.1 Subject registration
(LZ,LK,LP = heritage)

1.3.1.1 Detailed verification of subject *(*LZ=70%, LK=30%, LP=90%,C=0.02*)*

1.3.1.2 Standard verification of subject *(*LZ=70%,LK=20%,LP=70%,C=0.02 M=1,01*)*

1.3.2 Certification renewal *(*LZ=70%, LK=50%, LP=30%,C=0.02*)*

1.3.3 Certificate generation *(*LZ=70%, LK=80%, LP=80%,M=0.01*)*

1.3.4 Certificate dissemination
(LZ,LK,LP = heritage)

1.3.4.1 The certificate verification is available as specified in the CA Certification Practice Statement *(*LZ=30%, LK=60%, LP=30%, C=0.03, M=0.01*)*

1.3.4.2 The certificate verification is available 24 hours per day, 7 days per week *(*LZ=30%, LK=80%,LP=30%, C=0.03, M=0.02*)*

1.3.4.3 The certificate verification is additionally checked by another TTP. (LZ=30%, LK=80%, LP=70%,C=0.02; M=0.01*)* (LK+5%, LP+5%)

1.3.4.4 The certificate information is available depending on the permission level (LZ=15%, LK=50%, LP=30%*)* (LK+5%, LP+5%)

1.3.5 Certificate revocation and suspension
(LZ,LK,LP = heritage)

1.3.5.1 The maximum 72 hours delay between receipt of a revocation request or report and the change to revocation status information being available to all relying parties (LZ=30%, LK=60%, LP=40%, C=0.01*)*

1.3.5.2 The maximum 24 hours delay between receipt of a revocation request or report and the change to revocation status information being available to all relying parties *(*LZ=30%, LK=80%, LP=40%, C=0.01; M=0.01*)*

Particular graph edges join together by means of Boolean operations. Choosing a concrete edge, at the same time we create Boolean function of the particular security elements. In a given process we can choose a number of edges at he same time. The condition of correct choice is the result of created Boolean function, which equals 1.

Introducing additional security elements to the system, a part from getting additional information security we cause an extra threat for the assets. Therefore any change in the system protection influences the calculated probability.

Some security elements have such a feature that their choice modifies parameters of higher edges (e.g., 1.1.2.2 - LK=+10%, LP=+10%, C=0.01, M=0.03).

By means of the graph we present all steps of the protocol, which realize a given service.

3.2. Parameters of the probability of a threat occurrence

As we mentioned above, any threat for the concrete process is obtained by means of combination of two parameters: the probability of threat occurrence and its level. Particular security elements, which are presented in the graph description, are defined by means of these parameters.

The parameters presented on the graph belong to the main group of parameters, which are a part of the model. There is also an extra group of parameters, which make corrections to the model, but its choice is not necessary. These parameters are treated as a checklist. Below we present the parameters used in the model:

The main probability parameters (graph):

- **LZ** – Assets gained during a successful attack on a given security element (100% – compromising the whole protocol)
- **LK** – The knowledge needed for an attack (100% - expert)
- **LP** – Costs needed for an attack (100% - the highest cost)
- **C** – The communication steps as additional possibility of an attack ($C \in [0 \div 0.1]$ (0.1 – the highest threat)
- **M** – A practical implementation. Difficulties of implementation increase the probability of incorrect configuration. Error reports are additional source of information, etc. $M \in [0 \div 0.1]$ (0.1 – the highest threat)

The additional security parameters (checklist):

- **PP** – The global assets possible to gain in a given process $PP \in [0 \div 0.1]$ **(**0.1 – the highest threat)
- **I** – The kind of institution realizing a process. Some of them are of high threat. $I \in [0 \div 0.1]$ **(**0.1 – the highest threat)
- **H –** The potential risk for attacker in a case of finding out the incident. The lawmaking and punishment of the countries where the process is realized. $H \in [0 \div 0.1]$ (0.1- the country with minimal restrictions)

The additional term used in graph is "heritage". The nodes of parameters marked in that way take the values of parameters from the lower graph edges.

3.3. The mechanisms

The mechanisms by means of which we calculate the probability of partial threats and, what it follows, the probability of an incident is a combination of the mentioned parameters. The measure, which defines particular threats whether proper assets will be gained, are the parameters **LK,** as a required level of knowledge, and **LP** as required costs. Certainly, the calculation of these parameters is preceded by a detailed analysis of mentioned elements vulnerabilities. These parameters are modified by appropriate weights ω_{LK}^{P} and ω_{LP}^{P} **(** $\omega_{LK}^{P} + \omega_{LP}^{P} = 1$), which

define potential lack of attacker preparation as far as knowledge and costs. Apart from needed requirements for a successful attack one has to established potential profits which attacker can gain. It is defined by means of **LZ** parameter, which describes influence of potential harm for a given threat to compromise a whole process.

An additional parameter, which increases vulnerabilities of a given threat, and at the same time, the whole process, is the parameter **C,** as an extra communication step used in a given element.

The other mentioned parameter is **M**, which describes practical implementation of the security mechanisms. By adding the complex security elements one increases possibility of making mistakes in implementation whose exampled result could be error reports, which provide attacker with additional information. If the mentioned parameters (**C,M**), are not marked on a given graph edge, it means that values are standard and the parameters do not influence probability.

In the process of setting up the probability of an attack, one can use the parameters, which in a detailed way can characterize a given process described by means of the parameter A.

By combination of all the mentioned parameters we obtain the probability of a particular threat occurrence:

$$P_{ijz}^{K} = (1-(LK_{ijz}^{K}\omega_{LK}^{P}+LP_{ijz}^{K}\omega_{LP}^{P}))\times (LZ_{ijz}^{K}+(1-LZ_{ijz}^{K})(C_{ijz}^{K}+M_{ijz}^{K}))$$

$$^{A}P_{ijz}^{K} = P_{ijz}^{K}+[A\times(1-P_{ijz}^{K})],$$

$$A=(PP^{P}+I^{P}+H^{P}),$$

where:

i – Security services.

j – Security elements.

z – Parts of security elements.

K – Step of the protocol.

A – Additional security parameters.

P – The concrete process.

P_{ijz}^{K} – The probability of a threat occurrence without taking into consideration additional parameters A. This is the value of part z in the element j for the service i in step K for a given protocol.

$^{A}P_{ijz}^{K}$ – The probability after considering additional parameters A.

ω_{LK}^{P} – The weight defining potential attackers lack of preparation, as far as knowledge.

ω_{LP}^{P} – The weight defining potential attackers lack of preparation, as far as costs.

$$\omega_{LK}^{P} + \omega_{LP}^{P} = 1$$

We calculate all partial probabilities for every chosen graph edge.

The next step in the model is calculating probability of incident occurrence in a given step. First, we find the highest probability among calculated partial probabilities in a given step. This value will be the main factor of incident occurrence probability in a given step. It is caused by the fact that the security of information system is like a chain; the weakest knot affects its strength.

$$_{M}P_{i}^{K} = \max(P_{ijz}^{K}).$$

The probability of the incident occurrence in a given step depends not only on the highest threat but also on all other threats possible in a given step. Therefore we calculate correction to the total probability as a contribution of all partial probabilities. The number of partial probabilities can be defined by parameter "n".

Thus, we write the series of the partial probabilities.

$a_0^B = {}_{M}P_{i}^{K}$ – The base element of the series.

$a_0 = (1 - a_0^B)$ – The zero element of the series.

$a_1 = a_0 x_1$ – The first element of the series.

a_n – n-th element of the series,

$$a_n = [a_0 - \sum_{k=1}^{k=n-1} a_k]\, x_n \quad where\ n \geq 2 \quad .$$

x – The partial probability of all security elements (P_{ijz}^{K}).

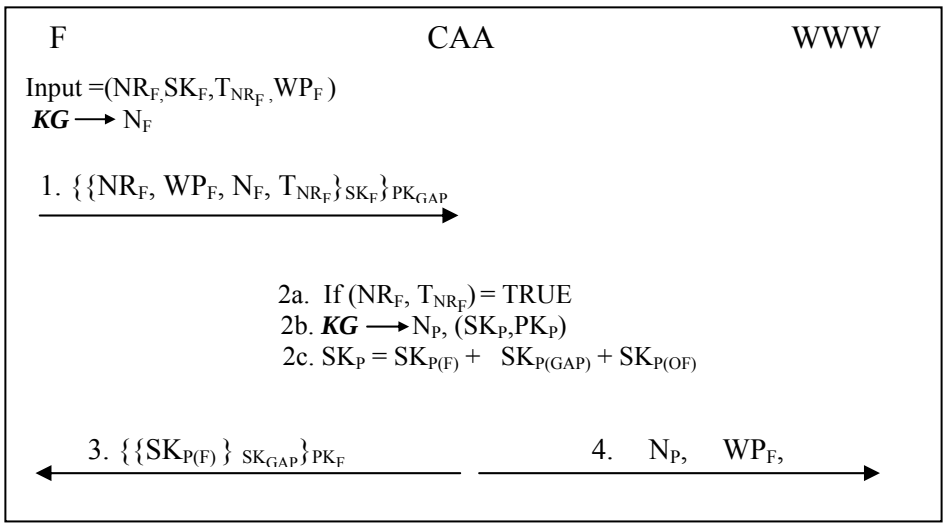

Figure 3: Graph to the e-auction notification subprotocol.

The total correction to incident probability occurrence is:

$$ {}_P P_{in}^K = a_0^B + \sum_{k=1}^{k=n} a_k $$

n – The number of elements in the series.
After calculating the mentioned parameters, we can obtain total probability of incident occurrence for a given service at a given step.

$$ P_{ALL} = {}_M P_i^K + {}_P P_i^K . $$

4. EXAMPLE

Above we present an exampled usage of described mechanism for electronic service, described by cryptographic protocol. We chose the protocol, which realize electronic auction [6].

The considered e-auction protocol consists of four subprotocols: *certification, notification of auction, notification of offer as well as choice of offer.* In protocol take part *N* bidders (O_1, ... ,O_N), third trustworthy person that is *CAA* (Main Auction Agency) as well as firm, which wants to announce the auction.

The first step of protocol is verification by CAA, 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 CAA the auction by verified firm F. CAA 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 earlier verification, sends his offer to CAA (*the subprotocol of notification of offer*).

The last subprotocol is executed after elapsing of time for notification of offers, then firm F as well as bidders O_N, send their parts of secret (needed to read offers) to CAA. 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 CAA, and then it will be published to (be generally known) public message (*the subprotocol of choice of offer*).

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

The chosen sample protocol

In the article we will present usage of mechanism for subprotocol of notification of electronic auction whose description we show below (Fig. 3).

The protocol can be notified by any person, which got earlier in subprotocol of certification suitable authorizations. Such a person, indicated as *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 NF.

Step1:
In the first step, F sends to CAA, signed digitally (SK_F) as well as coded (PK_{GAP}) following information: his registration number (NR_F), his time stamp (T_{NRF}), the conditions of auction (WP_F) as well as his individual number (N_F).

Step2:
The main auction agency (CAA) verifies the registration number F (NR_F) as well as validity of his gauge of time. After positive authorization CAA generates the individual number of auction (N_P) as well as a few keys for concrete auction (SK_P,PK_P). The private key of auction (SK_P) is divided by use of the threshold scheme of dividing secret. Secret is divided into three parts, designed for F ($SK_{P(F)}$), for CAA ($SK_{P(GAP)}$) as well as bidders in auction ($SK_{P(OF)}$). Each part is necessary to reproduce private key (SK_P).

Step3:
CAA sends digitally signed (SK_{GAP}) as well as coded (PK_F) - the part of secret designed for F ($SK_{P(F)}$).

Step4:
CAA publishes, for example on WWW site, the number of auction (N_P), conditions of it (WP_F) as well as its public key (PK_P).

Results

The first element established in an incident probability defining process in a given steps of the protocol is defining the mechanisms used. Below we present the Boolean function created from the graph elements based on the considered cryptographic protocol of e-auction. Due to our choice, the rests of graph elements are equal zero:

Step 1:
1.1.2.3.1 = 1.1.2 = 1.2.3 = 1.3.4.2 = 1.1.2.2 =1
F_{BOLL} = (1.1.2.3.1 ⊕ 1.1.2.3.2)∨(1.1.2.2) ∨ (1.2.2) ∨(1.2.3) ∨ (1.3.4.1 ⊕ 1.3.4.2)

Step 2:
1.2.1.2 = 1.2.2 = 1.3.1.2 = 1.3.3 = 1
F_{BOLL}= (1.2.1.2 ⊕ 1.2.1.1) ∨ (1.2.2)∨ (1.3.1.2 ⊕ 1.3.1.1) ∨ (1.3.3)

Step 3:
1.1.2.3.1 = 1.1.2 = 1.2.3 = 1.3.4.2 = 1.1.2.2=1
F_{BOLL} = (1.1.2.3.1 ⊕ 1.1.2.3.2)∨(1.1.2.2) ∨ (1.2.2) ∨ (1.2.3) ∨ (1.3.4.1 ⊕ 1.3.4.2)

Step 4:
1.3.4.2 = 1.3.4.3 = 1.3.4.4 = 1
F_{BOLL}=(1.3.4.1 ⊕ 1.3.4.2)∨(1.3.4.3) ∨ (1.3.4.4)

After establishing Boolean functions, one can check correctness of choice and potential collisions of security mechanisms. The next step is to choose additional security parameters. In described case we chose all additional parameters and their values are:
PP=0.05 (auction of higher importance)
I=0.03 (auction realized by universities)
H=0.03 (auctions take place in a country of a little strict lawmaking).
Next parameters to be established in the described protocol are ω_{LK}^{P} and ω_{LP}^{P}. They are assumed to be constant in the protocol. In our case, we assumed that ω_{LK}^{P} = 0.8 (attackers have a little knowledge) and ω_{LP}^{P}=0.2 (attackers have the large founds).

Having established parameters mentioned, we can calculate probability of an incident occurrence in a given step. Below we present the numerical results:

	${}_{M}P_i^K$	${}_{P}P_i^K$	P_{ALL}
Step 1	0.384	0.181	0.565
Step 2	0.551	0.190	0.741
Step 3	0.384	0.181	0.565
Step 4	0.182	0.140	0.322

Table 1: The calculated probabilities of an incident occurrence for the e-auction protocol.

5. CONCLUSIONS

In the paper we presented the model by means of which one can calculate the probability of incident occurrence in a given step of protocol. The proposed model can be used in a risk management process to establish particular threats and to calculate the risk in a

function of the probability of incident occurrence [8]. Another usage of the model can be the mechanism of the scalable security [11], by means of which we can modify security of a given process by defining the adequate protection level.

Moreover, in the paper we presented an example of application of the proposed procedure for analysis of a sample electronic service (in our case: the e-auction model). The obtained results show how the probability of a potential attack on the security service of integrity changes on each step of the protocol. The probability of a successful attack can be calculated by combing the value of a potential attack with parameters (probabilities) describing safeguards. The required items are usually defined during the risk management process (see .Fig. 1).

BIBLIOGRAPHY

[1] 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*, Computer Communication, Elsevier, 2003, v. 23, pp. 1873-1883.

[2] S. Gritzalis, S. Katsikas, D. Lekkas, K.Monstantinos, E. Polydorou: *Securing The Electronic Market: The KEYSTONE Public Key Infrastructure Architecture*, Computer & Security, Elsevier, 2000, v.19, pp. 731-746.

[3] FIBS PUB 140-2: *Security Requirements for Cryptographic Modules*.

[4] ISO/IEC 15408: *Information technology – Security techniques – Evaluation criteria for IT security*.

[5] ISO/IEC 19790: *Security techniques – Security requirements for cryptographic modules*.

[6] B. Księżopolski, Z. Kotulski: *Cryptographic protocol for electronic auctions with extended requirements*, Annales Informatica, UMCS, 2004, v.2, pp. 391-400.

[7] A. Teoh, D. Ngo, A. Goh: *Personalised cryptographic key generation based on Face Hashing*, Computer & Security, Elsevier, 2004, v. 23, pp. 606-614.

[8] ISO/IEC FDIS 13335-1: *Information technology – Security techniques – Concepts and models for managing and planning ICT security*.

[9] B. Madan, K. Goseva-Popstojanova, K.Vaidyanathan, K. Trivedi: *A method for modeling and quantifying the security attributes of intrusion tolerant systems*, Performance Evaluation, Elsevier, 2004, v.56, pp. 167-186.

[10] K. Farn, S. Lin A. Fung: *A study on information security management system evaluation- assets, threat and vulnerability*, Computer Standards & Interfaces, Elsevier, 2004, v.26, pp. 501-513.

[11] B. Księżopolski, Z. Kotulski: *On a concept of scalable security: PKI-based model with supporting cryptographic modules*, in: J.Wachowicz [ed], Electronic Commerce Theory and Applications, pp.73-83. ISBN 83-88617-42-7.

[12] J. Groves; *Security Application Service Providers*, Network Security, Elsevier, 2001, Issue 1, pp.6-9.

[13] M. Merabti, Q. Shi. R. Oppliger: *Advanced security techniques for network protection*, Computer Communications, Elsevier, 2000, v.23, pp. 151-158.

[14] M.A. Patton, A. Josang: *Technologies for Trust in Electronic Commerce*, Electronic Commerce Research, Kluwer, 2004, v. 4, pp. 9-21.