On the Modelling of the Computer Security Impact on the Reputation Systems

Bogdan Ksiezopolski, Adam Wierzbicki, Damian Rusinek

On the modelling of the computer security impact on the reputation systems

Bogdan Ksiezopolski[1,2] Adam Wierzbicki[2] Damian Rusinek[1]

[1] Institute of Computer Science, Maria Curie-Sklodowska University,
pl. M. Curie-Sklodowskiej 5, 20-031 Lublin, Poland.
[2] Polish-Japanese Institute of Information Technology
Koszykowa 86, 02-008 Warsaw, Poland.

Abstract. Reputation systems are an important factor for building trust in virtual communities. In the article we introduce reputation module for Quality of Protection Modelling Language which allows to represent the reputation system as a part of the protocol, where all operations and communication steps can be consistently modelled. Owing to the proposed approach the reputation systems can be formally specified and computer security impact can be considered as a factor of the metrics in the reputation systems. Finally, we model and analyse the case study of the eBay reputation system with modification which will refer to the computer security impact.

1 Introduction

Reputation systems are one of the most successful and important forms of trust management in open communities. Sophisticated algorithms and system designs can be applied in order to increase the resilience of reputation systems to various forms of attacks, such as coalition attacks, whitewashing, Sybil attacks and many others. Attacks against reputation systems depend on the capabilities of the attackers and defence mechanisms that protect reputation systems which significant part are based on technical measures [1]. The complete analysis of the computer security impact for the distributed reputation systems is a very difficult task, which should nevertheless be performed, because only then we can be sure that a reputation system has been properly tested. The completeness of analysis can be achieved by means of a formal approach, where reputation system can be represented as a part of the protocol, where all operations and communication steps can be consistently modelled. In the article [4] B.Ksiezopolski introduced the Quality of Protection Modelling Language (QoP-ML) which provides the modelling language for making abstraction of cryptographic protocols that put emphasis on the details concerning quality of protection. The intended use of QoP-ML is to represent the series of steps which are described as a cryptographic protocol. Additionally, in the QoP-ML the security economics analysis can be performed which is named adaptable security in literature [2, 3].

In this article we would like to present the syntax and semantics of a new structure for the QoP-ML which is required for analysing a reputation system.

A major contribution of this work is introducing the ability of formally specifying distributed reputation systems together with other protocols and functions of information security that support the reputation systems. Owing to the introduced reputation module the reputation systems can be analysed from the technical and information security perspectives. The reputation values of agents are calculated according to the defined algorithms which are abstracted as a process in the operating system which is realized by means of the host. This host is defined as a part of the whole IT architecture by means of which distributed communities can be abstracted. In this infrastructure one can model defence mechanisms and analyse their impact on the reputation system. The reputation module proposed in this paper, which is a part of the QoP-ML, is the first modelling language which allows abstracting and analysing reputation systems from the technical and information security perspectives in a formal way.

2 Reputation in QoP-ML

In this article we introduce the new reputation module owing to which the reputation analysis can be prepared simultaneously with standard quality of protection analysis of used security mechanisms. The reputation analysis will be will be performed simultaneously with the QoP evaluation according to the methodology presented in the article [4].

For reputation modelling in the QoP-ML one has to use two structures which were introduced in the QoP-ML: functions and security metrics. Additionally, we would like to introduce a new structure which will be used for reputation modelling, the *modules* structure. The semantics of all structures which are required during the reputation modelling in the QoP-ML is presented in the next sections.

2.1 Functions

The function modifies the states of the variables and pass the objects by communication channels. The function with the reputation qop parameters is declared as follows:

```
fun post(id)[Reputation: par1, par2, par3, par4, par5]
```

This function is named `post` and includes two types of factors. The functional parameters, which are written in round brackets, they are necessary for the execution of the function. The additional parameters, which are written in square brackets, influence the system reputation.

2.2 Security metrics

In the case of representing the reputation metrics, the structure `data*` will be used because the reputation can not be measured but can be modelled [4]. Below we present the example of the *metrics* structure used for reputation modelling.

```
metrics
{
  }
data*()
  {
    primhead[function][reputation:algorithm]
    primitive[post][alg1]
  }
}
```

The body of the `data*` structures contains two operators: `primhead` and `primitive`. The `primhead` operator defines the required parameters for agent actions which influence its reputation. In the presented example for `data*` the two parameters were defined, the first one is the function name which describes the operation influencing the modelled reputation. The second one defines the name of the additional module (*reputation*) for the previously defined function with the name of the algorithm which calculates the value of the reputation of this function. Then, the `primitive` operator is used which defines the details about previously defined functions. In our example the `data*` operator defines that the `post` function will be calculated according to the algorithm defined in the module *reputation* and the name of this algorithm is *alg1*.

2.3 Modules

In this article we introduce a new structure which will be used for defining details for different analysis modules according to the base QoP-ML analysis. This structure is named *modules*. In the presented approach, the structure for the reputation analysis will be presented. The security metrics structure in the QoP-ML approach is based only on static values which are defined as the *primitive* structure. One of the main features of the *modules* structure is enabling the representation of the results in the dynamic way. It means that the results defined in this structure can be estimated by means of the algorithms define mathematics operations.

In the next part of this section the exemplary declaration of this structure will be presented. Afterwards, this structure will be described.

```
modules {
  reputation {
  # rep=0
       alg1(par1, par2, par3, par4, par5){
        if(rep<=100){
           extra = (par4 * par5)/2;
           rep = rep + (par1 * par2 * par3) + extra;
                    }
        if(rep>100 || rep <200){
           extra = (par4 * par5)/2;
           rep = rep + par1 + par2 + par3 + extra;
                               }
        else{
          rep = rep + (par1 + par2 + par3 + par4 + par5)/5
            }
      }
   }
}
```

The *modules* structure is started by the operator `modules`. Inside the body of the *modules* structure one can define different types of modules. In the presented example the *reputation* module is described. In the specific modules, the initial values of variables can be defined, they are precoded by the # operator. After this, the algorithm which estimates the reputation value is defined `alg1(par1, par2, par3, par4, par5){}`. The name of the algorithm is not restricted and in the presented example it is *alg1*. In the round brackets the parameters of the algorithm are defined. The values of these parameters are defined during the QoP-ML protocol modelling in the specific function which are taken into consideration during reputation modelling. The body of the `alg1` algorithm includes the arithmetic operations which define the algorithm of reputation value calculation. In the *modules* structure one can use condition statements. In this example, three possible calculations can be prepared and they are changed depending on the current value of *rep* variable. When the *rep* variable will be lower or equal to 100 `(rep<=100)`, then the first conditional statement will be true and the relevant algorithm will be executed. When the *rep* variable will be higher than 100 and lower than 200 `(rep>100 || rep <200)`, then the second conditional statement will be true. In other cases the *else* structure will be executed. In the *modules* structure one can use other operators which are the same as in the language C.

3 Case Study - reputation in the eBay

In the article we would like to model the eBay reputation system [6] with modification which will refer to the computer security impact. In the QoP-ML one can model the reputation system where the mark will be modified depending on the security measures used. One can imagine the scenario where the rates of seller transaction will be modified by the attacker as the part of Men in the Middle Attack. That kind of attack can be easily performed when the rate will be submitted by means of non-encrypted channel. As the defence from this attack can be usage of TLS protocol, which first of all authenticates the eBay server and encrypts transmitted data. In this case study we would like to present the possibility of modelling the reputation systems with computer security impact and in the basic way the reputation of an agent (seller) a can be computed as:

$$r(a) = \sum_{m=1}^{n} (m \cdot s) \tag{1}$$

where:
$r(a)$ - the overall reputation value of the agent a;
m - the single rate for the transaction from the set $\{-1, 0, 1\}$;
s - the security impact value, $s \in R$;
n - the number of transactions.

In the case study we presented three scenarios which differ in the type of security technology used for rating the eBay transactions. We modelled the agents

reputation system based on formula 1. The security impact s will be equal to 1.3 when the transaction rating is sent by the security channel (with the TLS protocol) and will be equal to 0.7 when the the security channel is not used. It means that the transaction rate will be increased by 30% when the rate is secured against technical attacks and will be decreased by 30% when it is not secured.

For all scenarios we assume that agents (sellers) have 100 transactions and these transactions are rated by other agents (buyers or reviewers). We assume that all of these transactions are good and only honest buyers can asses the transactions. In the first scenario (version 1) the buyers will send 100 reviews by means of the secured channel (with the TLS protocol). In the second scenario (version 2) the buyers will send 100 reviews by means of not secured channel (without the TLS protocol). In the third scenario (version 3) the buyers will send 50 reviews by means of the secured channel (with the TLS protocol) and 50 reviews by means of the not secured channel (without the TLS protocol).

4 QoP and reputation evaluation

The QoP evaluation investigates the influences of the security mechanisms for the ensuring security attributes. That kind of evaluation can be found in the articles [4, 5]. In this article we would like to focus on the reputation evaluation which is a new type of evaluation introduced here. The QoP and reputation evaluation algorithms are implemented in the Automated Quality of Protection Analysis tool (AQoPA). The AQoPA tool can be downloaded from the web page of the QoP-ML Project [7]. In the QoP-ML models library (included in the AQoPA tool) one can find presented in this article eBay reputation model.

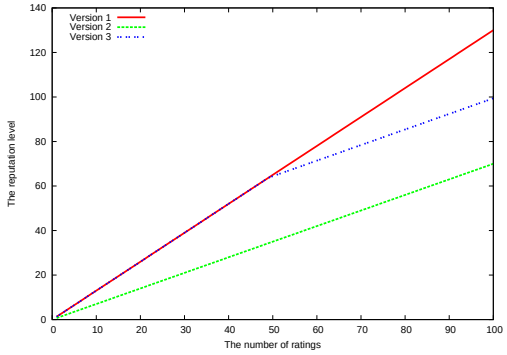

Fig. 1. The reputation evaluation for the modelled system

In the article we analysed a simple reputation algorithm based on the eBay reputation system where we added modification referring to the computer se-

curity impact. In Fig. 1 the results, which refer to the three analysed versions (scenarios) are presented. One can notice significant difference between the overall reputation level of the seller for versions 1 and 2. Version 1 refers to the rates, given by the secured channel, while in version 2 rates are not encrypted. The advantage of transaction rates which are submitted by secure channel is that we are sure that these rates were not modified as the results of one of technical attacks. In the second version we can not be sure that the transactions rates were not modified. This lower level of credibility of the submitted transactions reviews causes lower overall reputation level of the seller. The third version shows the combination of two earlier analysed behaviours of the transactions reviewer. In Fig. 1 one can notice that the last 50 rates submitted by means of not secure channel have less contribution to the overall reputation level of the seller.

5 Conclusions

The aim of this study was to present the new structure for the Quality of Protection Modelling Language (QoP-ML) which is required for analysing a reputation system. Owing to this module one can model and analyse the reputation systems from the technical and information security perspectives. In the article we modelled the case study in the QoP-ML where the eBay reputation systems were modified. In that system the transactions rates were modified depending on the fact of securing the transmission channel between the transaction reviewer and the eBay portal. We have shown that the reputation systems, taking into account factors related to information security, can provide protection against technical attacks on them.

Acknowledgements

This work is supported by Polish National Science Centre grant
2012/05/B/ST6/03364

References

1. Hoffman K, Zage D, Nita-Rotaru C, A survey of attack and defense techniques for reputation systems. Journal ACM Computing Surveys; 2009, 42(1).
2. Ksiezopolski B, Kotulski Z. Adaptable security mechanism for the dynamic environments. Computers & Security 2007; 26, pp.246-255.
3. Ksiezopolski B, Kotulski Z, Szalachowski P. Adaptive approach to network security. Communications in Computer and Information Science 2009; 158, pp.233-241.
4. Ksiezopolski B, QoP-ML: Quality of Protection modelling language for cryptographic protocols . Computers & Security 2012; 31(4), pp.569-596.
5. Ksiezopolski B., Rusinek D., Wierzbicki A.: On the efficiency modelling of cryptographic protocols by means of the Quality of Protection Modelling Language (QoP-ML). ICT-EurAsia 2013, LNCS, 7804, 2013, pp.261-270.
6. Schlosser A, Voss M, Brckner L. On the Simulation of Global Reputation Systems. Journal of Artificial Societies and Social Simulation 2006, 9(1).
7. The web page of QoP-ML project; link to the AQoPA tool: http://qopml.org/.