2009 International Conference on Machine Learning and Computing
IPCSIT vol.3 (2011) © (2011) IACSIT Press, Singapore

Performance Metrics for Information Security in Intelligent Grid

Razvan Bogdan [1+], Versavia Ancusa [1], Mircea Vladutiu [1]

[1] "Politehnica" University of Timisoara
Bd. V. Parvan nr. 2, 300223, Timisoara, Romania

Abstract. Qualitative methods are available for risk management, but better results would be obtained using quantitative risk management based on specific metrics and the expected loss. Intelligent grid is an architecture proposed as a solution to the problems of ambient intelligence based on intelligent agents. Measuring the improvement obtained by applying different security methods is of high importance.

Keywords: intelligent grid, metrics, quantitative measures, risk management, evaluation

1. Introduction

State-of-the-art ideas regarding artificial intelligence declare that a plethora of security techniques should be adopted in order to accurately identify those abusive behaviors that prevent the investments in computational intelligence to surpass human intelligence [5]. By surmounting such malicious activities, it is achieved what is called a reflective system, namely a system that can reference and modify their own behavior in the context of a system malfunctioning. In order to measure the obtained improvements towards the security and reliability of an intelligent system, different measuring techniques are expected to be presented. However, it has been demonstrated [4] that statistical data regarding the threats, the numbers of attacks, the consequences of such attacks and the action of threats, all these necessary to calculate values for security information metrics, are still not available. The effect is that the capacity to make use of security performance metrics has provided leisurely advancement.

Intelligent grid [1] is proposed as a solution based on intelligent agents for the existing problems of ambient intelligence [2], such as power consumption, portability, scalability, configurability and reliability.

This paper is organized as follows: Section 2 briefly presents the solution based on intelligent agents, named intelligent grid and also the methods proposed so far for attaining a secure and dependable system. Section 3 presents specific metrics for evaluation risk management in a given system. The improvement in security and reliability it's being targeted based on the metrics. The last section presents future work.

2. Solution based on intelligent agents

Ambient intelligence represents an electronic environment which is sensitive to the presence of human factor, especially aimed at being controlled by its user [1]. However, there are specific problems to be solved in such architecture, like computing power, power control, security and reliability. Intelligent grid is a solution based on the concept of ambient intelligence, but in this case are exploited the drawbacks of this architecture. For example, besides typical ambient intelligence devices, intelligent grid proposes to use the general computing systems, such as PCs. Therefore, intelligent grid includes not only multimedia and sensor networks, but also the required computation. In this architecture different levels can be identified: the device level incorporates all pieces of equipment, such as sensors, actuators, controllers, DSPs and PCs. The connection level is represented by the links between the elements of the device levels. And lastly, the

[+] Corresponding author. Tel.: + 40726651711; fax: (+40) - (0) - 256 - 403.214.
E-mail address: rbogdan@cs.upt.ro

collection level is defined by the networks and functionalities completed with the streaming data. In order to address this architecture it was chosen a middleware based on intelligent agents. By using agents, there is a raising of the abstraction level (Fig. 1), the physical aspect not being relevant any more.

It has been demonstrated [2, 4] that security and dependability are complex problems because of the distributed nature of such a collection of networks. Reliability is another main problem, because unreliability is inherent to the disappearing electronics concept. Therefore a design for reliability emphasizes as a method for attaining a secure non-traditional system [5] such as intelligent grid. In [2, 3] different techniques have been provided so as to improve the security and reliability of intelligent grid. The first step was to classify the threats on such networks and provide a threats model.

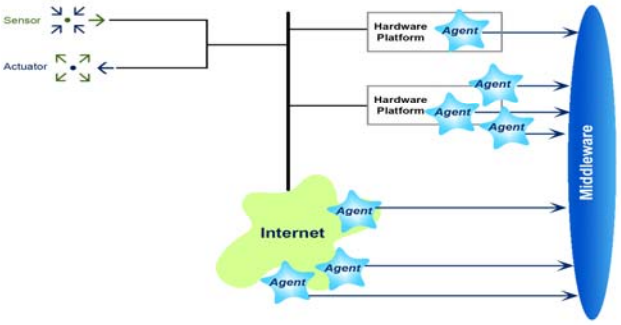


Fig.1: The intelligent grid with intelligent agents [1]

	Unenhanced sample	Enhanced sample	
Failure	x_1	x_2	M_1
Survival	$n_1 - x_1$	$n_2 – x_2$	M_2
	n_1	n_2	N

Fig.2: Risk matrix

In order to realize the authentication of the sender, a solution based on digital signatures has been adopted based on hash functions. In terms of owner-consumer paradigm, a possible attack can be one of impersonating the consumer. In this case, the execution of a malicious mobile agent can be realized after a previous transfer on the consumer container. A solution to such a case is to adopt a broker. In the case of intelligent grid this is represented by a distinctive agent targeted to guarding the data traffic on the network. Another technique for achieving fault tolerance in intelligent grid was to construct dedicated detection schemes for different intrusions. Such schemes aim at detecting those attacks that can be identified by a signature.

The following problem to be address in order to achieve a fault tolerant, reliable system is to measure in quantifiable terms, the improvement achieved by investing in the presented security methods. In other words, specific metrics should be employed to determine the effectiveness of security investments and strategies.

There are two categories of information security metrics, namely qualitative metrics and quantitative measures. The first category use subjective evaluations of risk, such as low, medium, high [4] and are useful for establishing a security project's progress. Even so, these metrics cannot be employed in order to make significant risk-management decisions. Risk analysis and risk management support themselves by means of quantitative performance metrics that provide cost-benefit analyses and return-on-investment (ROI) estimations. In other words such metrics can provide the degree of compliance with some security requirements. These requirements can be formulated as the number or percent of systems certified and also those that can measure the real effectiveness of security controls. Such quantitative metrics enable peculiar defensible and awareness management decisions concerning information security investments and strategies. In the same time, it is argued [6, 7] that it is essential to employ risk management approaches based on metrics in order to manage information security in a given system. The approach of failure-time analysis is first introduced in [4] and enhanced in this paper, by introducing additional required metrics to determine the relative risk. These metrics are applied to the non-traditional model based on intelligent agents, namely intelligent grid.

3. Information Assurance

A reliable program for information assurance can be measured in terms of the malicious attacks that can be avoided and in the same time by the implied losses of these attacks prevented of taking place. It is a question of establishing the effectiveness of investment in a program for information assurance. In [8] it is argued that expected loss offers a convenient metric in order to establish if it guarantees an investment in information security. The expected loss can be computed in terms of the security investment. The terms that are used are products of probabilities and consequences because are expectations of investments (in equation (1) noted I). Therefore the probability of a successful attack offers the loss implied by a successful attack. The expected loss before investment (E0) and expected loss after investment (EI) can be computed in terms of probabilities.

$$E_{IBnet} = E_0 – E_I – I = [p_0 \text{ x } v(t)] – [p_I \text{ x } v(t)] – I = (p_0 – p_I) \text{ x } v(t) – I \qquad (1)$$

In order to obtain a confident investment, the condition is that EIBnet > 0. In this set of equations p0 and pI are the probabilities of a successful attack [4] before and after a security investment. It is interesting to notice that v(t) is a function which measures a successful attack’s total economic consequences.

The following problem is to establish the probabilities from the last equation. In this regard, the medical communities of biostatisticians have proposed different techniques and methodologies which can be used in order to measure the effectiveness of security countermeasures. The basic feature of such methodologies is the study of different groups upon which different drugs have been administered. The biostatistics approaches can be channelized in a manner that can provide the possibility to measure countermeasures’ effectiveness and also to develop performance metrics. The methodology which presents the most promising results is failure-time analysis.

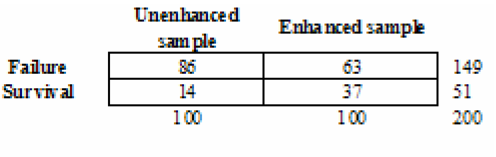
This method can be used to study a minimum of two groups of systems. One of these groups will have no security enhancements, while the other groups are invested with different proposed enhancements in information security. It represents a quantitative approach for establishing and investigating the relationships among security policies, methodologies, technologies and the losses that their use seek to avoid.

3.1. Relative Risk

For the case of intelligent grid architecture the main concerns appear from intentional malicious attacks. In this case, their actions are a threat to the reliability of the system. In the case of a thorough analysis, the attacks are expected to occur from individuals or different groups. A typical methodology for such a situation [4, 9] is to consider two substructures of the information infrastructure, which are differentiated by two distinct collections of security countermeasures. The probability of system failure of the first group is p0. The characteristic of this group is that it doesn’t have any security investment in new security technology, while the second group, which probability is pI, has such an investment. A specific design used to compare two collections with different characteristics is called the risk matrix [9]. The independent samples of systems are noted n1 and n2, representing the unenhanced systems and enhanced systems. A set from each of n1 and n2 represents the number of systems who have failed in each group. Let these two sets be x1 and x2.

Risk metric	Expression	Domain	Null Value
Risk difference (RD)	p_o-p_I	[-1,1]	0
Relative risk (RR)	p_0/p_I	(0, ∞)	1
log RR (L_{RR})	log(p_o)-log(p_I)	(- ∞ , ∞)	0
Odds ratio (OR)	$\frac{p_0 /(1 - p_0)}{p_I /(1 - p_I)}$	(0, ∞)	1
log OR (L_{OR})	$\log\frac{p_0}{1-p_0} - \log\frac{p_I}{1-p_I}$	(- ∞ , ∞)	0

Fig.3: Measures for Relative Risk



	Unenhanced sample	Enhanced sample	
Failure	86	63	149
Survival	14	37	51
	100	100	200

Fig.4: Risk matrix for general computing systems [4]

From this risk matrix, it can be concluded that x1 of n1 unenhanced systems fail and x2 of n2 enhanced systems also fail. The sum of the first row provides the total number of failures, while the sum of the values from the second row offers the total number of survivals ($M_1 = x_1 + x_2$, $M_2 = (n_1 - x_1) + (n_2 – x_2)$, $N = n_1 + n$).

3.2. Relative Risk’s Measures

In [4] is proposed that different measures of relative risk can be derived from failure-time data. Each measure is a function of the probabilities of the positive response in the two collections [9]. Each function will indicate a variance which takes place from the null hypothesis H0: p0 = pI. This variance occurs because it can be associated a link between the affiliation to a collection and the probability of system failure.

A first metric implied is the risk difference, RD, defined as the algebraic difference between the probabilities of system failure in the two groups, being equal with zero under the null hypothesis [9]. When calculating the difference in the sample proportions the risk difference is obtained. Each of the terms from the algebraic difference is the natural estimator for p0 and pI.

$$\hat{RD} = \hat{p}_0 - \hat{p}_1 \quad (3), \qquad \hat{p}_0 = \frac{x_0}{n_0} \quad \hat{p}_1 = \frac{x_1}{n_1} \quad (4)$$

The relative risk (risk ratio), RR, is the ratio of the two probabilities, RR = p0/pI, being equal with zero under the null hypothesis. The estimation of RR is done using the ratio of the sample proportions.

$$\hat{RR} = \frac{\hat{p}_0}{\hat{p}_1} \quad (5), \qquad \hat{OR} = \frac{\hat{p}_0 / (1 - \hat{p}_0)}{\hat{p}_1 / (1 - \hat{p}_1)} \quad (6)$$

Whenever the relative risk is higher than one, the failure is more likely in the first group and when is less than one, the failure is more likely in the second group. Similarly, if the relative risk is one, the risk of system failure is equal in both groups. Another metric, the odds ratio, OR, is the ratio of the odds of failure in the two collections. In order to estimate OR it is necessary to calculate equation (6). The estimation is given similar to RR with respect to value one. Following next, we propose to introduce different other metrics in order to obtain the entire domain as being the real line and also to provide a more precise granularity of the risk management and security improvement by enhancing a system with security techniques.

3.3. Risk distribution, Odds distribution

As it can be depicted from Fig.3, both the relative risk and odds ratio have a domain of the positive real line and one for the null value. Because the domains are not symmetric about their null values, it is useful to introduce two other metrics, let’s call them risk distribution and odds distribution, obtained by a log transformation. The result is that the domain becomes the real line.

$$\hat{L}_{RR} = \log \hat{RR} = \log \frac{x_0 n_1}{x_1 n_0} \quad (7), \qquad \hat{L}_{OR} = \log \hat{OR} = \log \frac{\hat{p}_0 / (1 - \hat{p}_0)}{\hat{p}_1 / (1 - \hat{p}_1)} = \log \frac{x_0 (n_1 - x_1)}{x_1 (n_0 - x_0)} \quad (8)$$

The importance of introducing these two metrics is that the confidence intervals are bounded with the domain of the parameters that are measured. A useful metric is named attributable risk fraction, being defined as it is presented in equation (9). The estimation of AR is based on equation (10).

$$AR = \frac{p_0 - p_I}{p_I} = RR - 1 \quad (9), \qquad \hat{AR} = \hat{RR} - 1 = \frac{x_0 n_1}{x_1 n_0} - 1 \quad (10), \qquad PAR = \frac{a_1 (RR - 1)}{1 + a_1 (RR - 1)} \quad (11)$$

In defining this metric, RR = p0/pI is the relative risk of failure among exposed versus non-exposed groups. Attributable risk fraction is a measure of the partial or fractional increase in the risk of failure when, for example, a given system is attacked by a certain type of threat. However such a metric as AR it doesn’t provide an account of the prevalence of the risk in group and is presenting partial results compared to a necessity of an overall perspective of a certain type of attack. In order to extend the results of AR, population attributable risk fraction can be employed. This metric is defined as the proportion of all cases of the failure in the group that are attributable to exposure to the risk factors, such as threats. In other words this measure addresses the question “What fraction of systems failures could be avoided if a certain risk (attack) could be completely eliminated in the group?” Practically this measure responds to the problem of estimating the impact of developing certain measurements of avoiding a peculiar attack. The methodology for this case is to consider a group of N systems such that the fraction exposed to a risk in the sample is expected to reflect the fraction exposed in the entire number of systems. In order to calculate PAR, in the general set of systems consider a1 = P(E) to be that fraction which is exposed to the risk factor. The population attributable risk is the proportion of all cases of the failure that would be prevented if the exposure to the risk factor (threat) were eliminated in the overall number of systems.

$$\hat{PAR} = \frac{\hat{a}_1 (\hat{RR} - 1)}{1 + \hat{a}_1 (\hat{RR} - 1)} \quad (12), \qquad \hat{a}_1 = \frac{n_1}{N} \quad (13), \qquad \hat{RR} = \frac{\hat{p}_0}{\hat{p}_1} \quad (14), \qquad \hat{PAR} = \frac{n_1^2 x_0 - x_1 n_0 n_1 N}{x_1 n_0 N + n_1^2 x_0 - x_1 n_0 n_1 N} \quad (15)$$

In order to estimate PAR is necessary to calculate equations from (12) to (14). The final form for estimating PAR is presented in equation (15).

4. Practical Results

Intelligent grid is an architecture where different devices such as sensors, DSPs, PCs etc. are interacting in order to create an area meant to be controlled. Different attacks can threat the reliability, security and dependability of such architecture. Therefore certain techniques are to be adopted [2, 3] in order to avoid the effects of these attacks. By implementing such security techniques, we talk about an enhanced system. One of the components that form the intelligent grid is the general computing systems. Without losing from generality we can calculate the improvement obtained by enhancing the general computing systems with the proposed techniques taking into consideration the benchmark results obtained in [4]. In this case, two groups of systems were observed in the conditions of one population being enhanced with security mechanisms, while the other one functioning with a minimum of security mechanisms. In others words, based on the proposed metrics we can determine the improvement obtained by using security techniques from the general computing systems point of view. In Fig.4 it can be observed that 86 of 100 unenhanced systems have failed during the test period, while adopting security measures, only 63 of 100 enhanced systems have failed. If we calculate the relative risk we can notice that is equal with 0.86/0.63 = 1.365 which demonstrates that the total number of safe systems increases by a percentage of 36.5. The attributable risk fraction is 0.365 which means that the proportionate risk increases by a percentage of 3.65 when exposed to a threat. Further on, if we consider that 60% of this population was attacked by a certain type of attackers which can be identified by their signatures [2], the population attributable risk is 0.95. This means that 95% of the malfunctioning of the general computing elements may be attributable to the specific types of attacks.

5. Conclusions and future work

This paper represents a rational continuity of the work previously presented. It applies specific metrics in order to establish the improvement obtained in an intelligent grid network after applying certain methods for enhancement the reliability and security of the architecture. Previous benchmark results are employed, but in the same time new metrics are introduced. Based on these different predictions towards the attacks have been presented. As future work, we intend to extend this methodology of evaluating the security enhancement to the other components of the intelligent grid so as to provide risk predictions for the entire complex network.

6. References

[1] V. Ancusa, R. Bogdan, Mircea Vladutiu, Redundancy at Link Level for Non-traditional Grids Implemented with Intelligent Agents, *Proc. of the 4th International Conference on Networked Computing and Advanced Information Management (NCM 2008),* South Korea, 2008.

[2] R. Bogdan, M. Vladutiu, Providing Security in Intelligent Agent-Based Grids by Means of Error Correction, *Proc. of the International Conference on Future Networks, Bangkok, Thailand, 2009.*

[3] R. Bogdan, M. Vladutiu, Intrusions Detection in Intelligent Agent-Based Non-traditional Grids, *Proc. of the International Conference on Education Technology and Computer, Singapore, 2009.*

[4] J.C.H. Ryan, D.J. Ryan, Performance Metrics for Information Security Risk Management, *IEEE Security & Privacy,* Vol. 6, Nr. 5, 2008.

[5] Carl E. Landwehr, Cybersecurity and Artificial Intelligence, *IEEE Security&Privacy,* Vol. 6, Nr. 4, 2008.

[6] Andrew Jaquith, Security Metrics: Replacing Fear, Uncertainly and Doubt, Addison-Wesley Professional, 2007.

[7] Debra S. Herrmann, Complete Guide to Security and Privacy Metrics, *Auerbach Publications,* 2007.

[8] L. A. Gordon, M.P. Loeb, The Economics of Information Security Investment, ACM Trans. *Information and System Security,* vol. 5, no. 4, Nov. 2002, pp. 438-457.

[9] J. M. Lachin, Biostatistical Methods: The Assessment of Relative Risks, *John Wiley & Sons,* 2000