17th Symposium IMEKO TC 4, 3rd Symposium IMEKO TC 19 and 15th IWADC Workshop
Instrumentation for the ICT Era
Sept. 8-10, 2010, Kosice, Slovakia

An Approach to Measure the Operational Security of Intrusion Tolerant Systems

Domenico Luca Carnì, Angelo Raffaele Cerra, Domenico Grimaldi

Department of Electronics, Computer and System Sciences,
University of Calabria, 87036 Rende - CS, Italy
Ph.: +39 0984 494712, fax: +39 0984 494713, {dlcarni, grimaldi}@deis.unical.it

Abstract **-** A new approach to evaluate the operational security of the Intrusion Tolerant System (ITS) is proposed. It is based on the mapping of the concept of the system security into that of system dependability. This approach permits to consider in the unified view all the security strategies and mechanisms to realize the defense system. Therefore the semi-Markov process is used to emulate the variability of the fault rate. Owing to the strong connection of the operational security of ITS with the attributes of system dependability (availability, integrity, confidentiality and reliability), the measurement procedure is pointed out to estimate the security parameters (availability, integrity, confidentiality), and the index for the operational security evaluation. This last is the Mean Time To Security Failure and is correlated to the attribute of system reliability. Indeed, it takes into consideration as long is immunity of the system to the attack. Numerical results of three case studies are shown to validate the measurement procedure.

I. Introduction

Internet security is become an important research topic to contrast the attacks from viruses, worms and hackers. The problem is that the software and hardware devices connected to the network are complex systems, and the relations among the variables that describe their behaviour are not simply enumerable or determinable [1]. Depending on this aspects, the network security is not simple to realize and a priori to evaluate.

In order to evaluate the security of the network, the fundamental strategies to point out the security mechanism must be taken into consideration. There are two basic strategies to implement network security mechanisms. The first uses preventive mechanism as the firewall to stop the unwonted access to the network. This mechanism is not absolute secure, and intrusion is possible. The second uses techniques [2] based on Intrusion Tolerant System (ITS). To the ITS is demanded the task to detect and tolerate the attack. The ITS tries to repair and remove any damage caused by the intrusion. ITS permits to the system to perform the normal functionality in despite of partially successful attack.

In the literature, the security evaluation is associated to the dependability concept. This is the capacity of the system to deliver service that can be justifiably considered trusted [3]. In order to perform the security evaluation, two different analysis techniques are used: qualitative or quantitative analysis.

As concerning with the qualitative analysis, the different approaches are based on: (i) verification of the correctness implementation of the ITS, and (ii) mathematic model to asses the strategies of security mechanisms [4]-[5].

As concerning with the quantitative analysis, the different approaches can be classified in four classes: (i) framework for the dependability and security estimation [6], [7], (ii) probabilistic estimation of the security system evolution [8], [9], (iii) game theory like technique [10], [11], (iv) vulnerability evaluation the of the system by the attackability metric taking into account the access method, and the contrast opposed by the data and the communication channel [12].

In the paper is proposed a new approach for the evaluation and the measurement of the ITS operational security. It is based on the semi-Markov process to emulate the variability of the fault rate. Based on this approach, the measurement procedure is pointed out to evaluate the security parameters (availability, integrity and confidentiality) from the corresponding attributes of the system dependability, and the security index. This is the Mean Time To Security Failure (MTTSF), and is correlated to the attribute of system reliability. It takes into account as long is immunity of the system to the attack. Therefore, it can be assumed as general parameter of the security measurement.

Feature of the proposed approach is to consider in the unified view all the security strategies and mechanisms to realize the defence system. Moreover, the proposed approach meets the idea proposed in [6] and [7] concerning with the relationship between security analysis and mechanism of dependability analysis. It is based on the analysis proposed in [8], but introduces as novelty the use of the semi-Markov chain to emulate the variability of the fault rate.

The paper is organized as follows. Initially, with the intent to well define the contest in which the proposed measurement procedure can operates, aspects concerning with the network security strategies are resumed. Successively, once the mapping of the concept of system security into that of the system dependability is established, the dynamic behaviour analysis of ITS state transition is discussed. The measurement procedure of the ITS operational security is presented. Finally, to validate both the proposed approach and the measurement procedure pointed out, the numerical results of three case studies are shown and analysed.

II. Network security strategies

The network security can be managed with two different strategies. In the first, the concept is to point out mechanisms to prevent the attack. In the second, the concept is to limit the damages of the attack, once the first strategy faults.

In order to implement the first strategy, the firewall is used. This last consists on a set of hardware and software components developed to manage and control the data traffic, among the network links, and in different TCP/IP stack levels. The design characteristics of the firewall require to satisfy some fundamental properties. These are: (i) all the informative units would to flow in a single connection, (ii) only that is defined in the security policy would to be authorized, and (iii) the device would to be immune to the attack.

The firewalls can be classified in two main categories. The first is desktop or personal firewall [13], that protects the single host from the unauthorized access by means of control techniques. This category is used in the Small Office Home Office scenario, where the security of the end users is generally guaranty. The second category [14] is the network firewall that permits the centralization of the security strategy and protects the network.

In order to implement the second strategy of network security, the ITS is used. It can detect and stop in real time the anomaly. By using this component, the input/output data are managed by the device that implements the ITS to permit at the system to operate in continuity when it is not in the good state. To reach this goal, the mechanisms included into the ITS are (i) intrusion detection, (ii) fragmentation, (iii) replication, (iv) migration, (v) masking, (vi) isolation, (vii) containment, and (viii) recovery. One of the most important components of the ITS is the Intrusion Detection System (IDS), that is devoted to detect the attack and to generate the intrusion triggers. Once detected the intrusion, the successive step is the minimization of the damage caused by the attack.

III. Dynamic behaviour analysis of ITS by state transition

The analysis of system security can be related to the mechanism of system dependability analysis. Indeed, strong connection is between the concept of system security and that of system dependability [15]. In particular, some concepts defined in the system dependability analysis can be mapped into the system security analysis. An example of the mapping is the following:

- *input space*, defined in the dependability field as the totality of the system input, can be mapped into the security field as the totality of the admissible input devoted to the normal functionality of the system or to malicious intent;
- *usage environment*, defined in the field of dependability as the mechanism selecting the inputs from the input space, can be mapped in the security field as the set of permitted or malicious user request;
- *system failure*, used to quantify the dependability of the system, can be mapped in the security field as *system breach*, that represents the evaluation of the probability of operative block toward the failure;
- *load*, defined in the dependability field as the stress in time unit of the system, can be mapped in the security field as the attacker effort to reach his goal.

On the basis of the relation among the system dependability concepts and the system security concepts, it is possible to use the mechanisms devoted to the dependability estimation to define and quantify the parameters to measure the system security.

As concerning with the ITS, it can be described by the direct state transition diagram (Fig. 1). The model proposed in [2] is modified by including different states to take into consideration the modality of the attack and the system redundancy.

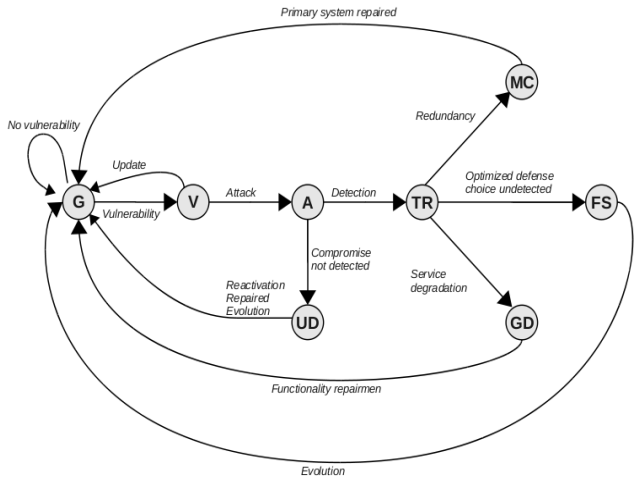

Figure 1 - State transition diagram describing the behaviour of the intrusion tolerant system.

Initially the system is in the Good state G, and no vulnerabilities are found. If the attack founds the vulnerability, the system state changes into the Vulnerability state V. During this time interval the attacker tries to compromise the system security. It is possible that the system administrator detects and resolves the attack, than the state of the system comes back to G. Otherwise the system state changes in attacked state A. In this state the Intrusion Detection System (IDS) can detect the anomaly by changing the system state in TRiage state TR, or, if the anomaly is not detected, the state is the Un-Detected state UD. In the TR state there are others two possibilities of evolution: (i) the state changes in Service Degradation state GD, and (ii) if the redundancy component is present, the state can change in Masquerade state MC. If the detection system doesn't recognize the attack typology, the ITS change the TR system state in the Fail-Secure state FS.

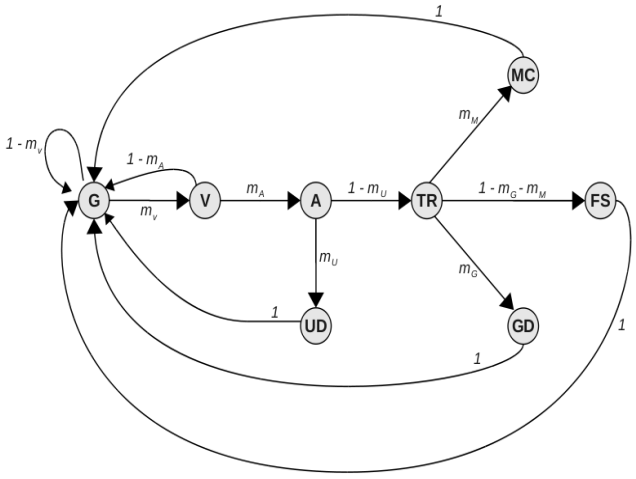

Figure 2 - Directed graph describing the Embedded Discrete Time Markov Chain.

IV. Measurement procedure of ITS operational security

The direct graph shown in Fig. 2 is used to evaluate the security parameters of availability, integrity and confidentiality.

In particular, it is taken into consideration that the failure rate has Weibull distribution. This distribution allows to represent the scenarios where the failure rate is increasing, decreasing, and constant [16].

The ITS evaluates the presence of illegal activity with the hypothesis of exponential distribution of the detection rate. If an anomaly is detected, the apparatus runs the defence procedure with the goal to came back in correct functionality state. With the assumption of non exponential distribution of the state transition, the stochastic process can be described by a continuous time semi-Markov chain.

By considering S the state set, and Ω the probability space, it is possible to define the following random variables:

$$\begin{aligned} X_n &: \Omega \to S \\ T_n &: \Omega \to N \end{aligned} \tag{1}$$

where X_n represents the occupied state of the transition n, and T_n the time instant in witch occurs the event. The pair (X, T) is a Semi-Markov Process (SMP), and each element $q_{ij}(t)$ of the kernel $Q(t) = [q_{ij}]$ is equal to:

$$q_{ij}(t) = \Pr[X_{n+1} = j, V_n \le t \mid X_0, \dots, X_n;\ T_o, \dots, T_n\ ] = \Pr[X_{n+1} = j, V_n \le t \mid X_n = i\ ] \tag{2}$$

where V_n is the residence time in a state equal to $(T_{n+1} - T_n)$. Defined m_{ij} the transition probability between the state *i-th* to *j-th*, in the steady state condition, it is [17]:

$$m_{ij} = \lim_{t \to +\infty} q_{ij}(t). \tag{3}$$

The transition matrix $M = [m_{ij}]$ describes the Embedded Discrete Time Markov Chain (EDTMC). The elements of this matrix are represented by the labeled directed graph shown in Fig. 2. The meaning associated to these elements is denoted by the parameters described in the Tab. 1.

The chain of Fig. 2 is ergodic and only one probability vector $(\pi_G, \pi_V, \pi_A, \pi_{UD}, \pi_{TR}, \pi_{GD}, \pi_{MC}, \pi_{FS})$ exists [19]. In particular, by using the results given in [18], the probability of each state of the EDTMC in steady state is:

Table 1 - Parameter description of Embedded Discrete Time Markov Chain.

Parameter	Description
m_V	Existing vulnerability
m_A	Exploit start
m_U	Attack not detected
m_G	Service degradation
m_M	Redundancy service active

$$\begin{aligned} \pi_G &= \frac{h_G}{\eta} & \pi_{TR} &= \frac{m_A m_V \tilde{m}_U h_{TR}}{\eta} \\ \pi_V &= \frac{m_V h_V}{\eta} & \pi_{GD} &= \frac{m_A m_G m_V \tilde{m}_U h_{GD}}{\eta} \\ \pi_A &= \frac{m_A m_V h_A}{\eta} & \pi_{MC} &= \frac{m_A m_M m_V \tilde{m}_U h_{MC}}{\eta} \\ \pi_{UD} &= \frac{m_A m_U m_V h_{UD}}{\eta} & \pi_{FS} &= \frac{m_A m_V \tilde{m}_{GM} \tilde{m}_U h_{FS}}{\eta} \end{aligned} \tag{4}$$

$$\begin{aligned} &\tilde{m}_V = (1 - m_V);\ \tilde{m}_A = (1 - m_A);\ \tilde{m}_U = (1 - m_U);\tilde{m}_{GM} = (1 - m_G - m_M) \\ &\eta = h_G + m_V\{h_V + m_A[h_A + m_U h_{UD} + \tilde{m}_U(h_{TR} + m_G h_{GD} + m_M h_{MC} + \tilde{m}_{GM} h_{FS})]\}. \end{aligned} \tag{5}$$

The elements of the vector

$$(h_G, h_V, h_A, h_{UD}, h_{TR}, h_{GD}, h_{MC}, h_{FS}) \tag{6}$$

represent the mean residence time in the state $(G, V, A, UD, TR, GD, MC, FS)$ respectively.

According to the transition state diagram in Fig. 2, the parameter evaluating the availability (A) of the system in the full service can be determined from (4). It is equal to:

$$A = 1 - (\pi_{UD} + \pi_{FS}). \tag{7}$$

Moreover, the parameter evaluating the integrity (I) of sensible data into the system can be determined as:

$$I = C = 1 - \pi_A. \tag{8}$$

Without information about the characteristics of the system, the parameter evaluating the integrity I can be assumed coincident with that evaluating the confidentiality C. The two attributes A and I can't be used with absolute certainty to characterise the security level if the typology of the system is unknown.

By considering the absorbing Markov chain shown in Fig. 3, the matrix M can be renumbered considering that the transient state came first, followed by the absorbing states. By taking into consideration this renumbering, the canonical form of the M matrix is:

$$M = \begin{bmatrix} T & R \\ 0 & I \end{bmatrix} \tag{9}$$

where, I is the identity matrix, T includes the transient state transition, and R includes the absorbing state transition [19].

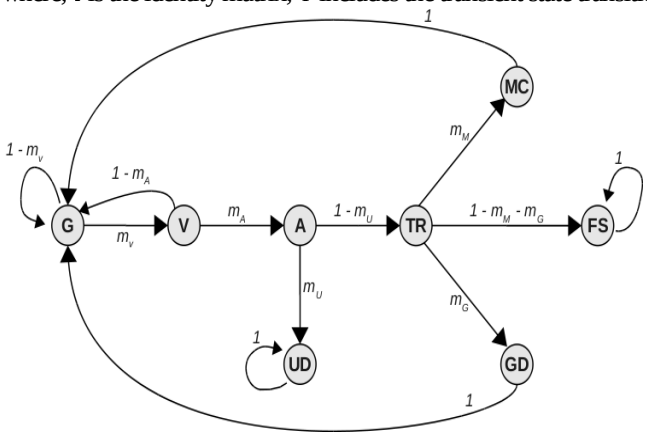

Figure 3 - Absorbing Embedded Discrete Time Markov Chain.

The dimension of T is $(N_{tr} \times N_{tr})$, with N_{tr} number of transient states, the dimension of R is $(N_{tr} \times N_{abs})$, with N_{abs} number of absorbing states. The dimension of I is $(N_{abs} \times N_{abs})$. Therefore, the dimension of the matrix M is $(N_{tr} + N_{abs}) \times (N_{tr} + N_{abs})$. From the matrix M is computed the fundamental matrix F that give the expected number of times that the process is in a transient state, starting from another transient state [19]. F is defined as:

$$F = (I - T)^{-1}. \tag{10}$$

In this paper, the start state taken into consideration is G, and the absorbing states are UD and FS. The other states are transient. With the calculation of F is possible to estimate the resilient time f_j into transient state before the state changes into the absorbing state.

Finally, on the basis of the strong connection between dependability and security, previous discussed, the first row of the matrix F multiplied by the vector (6) furnishes the formula for the evaluation of the parameter MTTSF [18]. It is:

$$MTTSF = \sum_{j \in S_{tr}} f_j h_j = \frac{h_G(m_A m_V)^{-1} + h_V m_A^{-1} + h_A + \tilde{m}_U(h_{TR} + m_G h_{GD} + m_M h_{MC})}{[1 - \tilde{m}_U(m_G + m_M)]}. \tag{11}$$

V. Numerical tests

The attack to the system security can be classified versus different aspects: (i) target, (ii) technique, and (iii) attacker typology. The Information Assurance Program (IAP) [20] gives the guidelines to classify the different threat toward the system security and provides the base to identify the different case studies.

In order to validate the proposed approach and the measurement procedure, three different case studies are chosen: (i) E1, high protection level, (ii) E2, medium protection level, and (iii) E3, low protection level. Tab. 2 and Tab. 3 show the correspondent values assumed for the transition probability, and the mean residence time, for each security test.

From (7) can be evaluated that the system can correctly operate for 98% of the time in the case E1, 89% of the time in the case E2, and 78% of the time in the case E3. From (8) can be evaluated that the integrity (I) of sensible data is 94% in the case (E1), 83% in the case (E2), and 74% in the case (E3).

According to the values of transition probability (Tab. 2) and the mean residence time (Tab. 3), the values obtained for MTTSF are shown in Tab.4. As expected, the value of MTTSF decreases as decreases the security level.

By taking into consideration the second scenario E2, Fig. 4 shows the trend of the MTTSF versus the mean residence time h_G evaluated in relative time unit and the attack probability m_A. As increases the attack probability the MTTSF decreases. Moreover, as decreases the residence time the MTTSF decreases.

Table 2 - Transition probability.

	m_V	m_A	m_U	m_G	m_M
E1	0.5	0.4	0.2	0.3	0.3
E2	0.7	0.6	0.5	0.2	0.2
E3	0.9	0.8	0.7	0.1	0.1

Table 3 - Mean residence time in relative time unit.

	h_G	h_V	h_A	h_{UD}	h_{TR}	h_{GD}	h_{MC}	h_{FS}
E1	60	40	30	20	50	40	40	20
E2	30	60	50	40	70	60	60	40
E3	10	90	80	70	90	80	80	70

Table 4 - MTTSF.

MTTSF
941
335
253

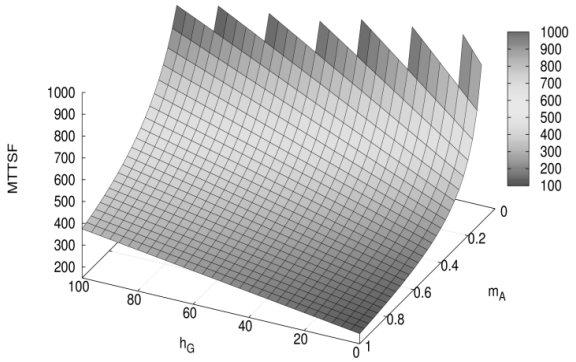

Figure 4 - MTTSF versus h_G and m_A.

VI. Conclusion

A new approach to measure the operational security of the Intrusion Tolerant System is proposed. It is based on the practical assumption that the system security analysis has strong connection with the system dependability analysis. Therefore, the attributes of the system dependability are taken into consideration to define the parameters of the system security.

Based on this approach, the measurement procedure is pointed out. In particular, the semi-Markov chain is used to emulate the variability of the fault rate and to evaluate the security parameters (availability, integrity and confidentiality), and the security index Mean Time To Security Failure. This last is correlated to the attribute of system reliability and is assumed as general parameter of the security measurement. Feature of this approach is that all the security strategies and mechanisms to realize the defence system are considered in the unified view. The validation of the proposed approach is performed by numerical tests. These tests are developed to highlight the correct relation between the estimated parameters and the different system security level chosen.

References

[1] Jun Lu, Yu Wang, Zhongwang Wu, Yu Lu, "Network behaviour description and behaviour base modeling method", Multiconference on Computational Engineering in Systems Applications, IMACS, pp. 1353-1356, February 2007.
[2] D. Wang, B. Madan, K. S. Trivedi, "Security analysis of SITAR intrusion tolerance system", Conference on Computer and Communication Security, 2003.
[3] A. Avižienis, J. C. Laprie, B. Randell, "Fundamental concepts of dependability", LAAS Report n. 01-145, 2001.
[4] "Information technology security evaluation criteria (ITSEC). Provisional harmonised criteria", www.ssi.gouv.fr/site_documents/ITSEC/ITSECuk.pdf
[5] "Trusted computer system evaluation criteria", http://csrc.nist.gov/publications/history/dod85.pdf.
[6] D. M. Nicol, W. H. Sanders, K. S. Trivedi, "Model-based evaluation: From dependability to security", IEEE Transactions on Dependable and Secure Computing, vol. 1, pp. 48–65, January-March 2004.
[7] E. Jonsson, L. Stromberg, S. Lindskog, "On the functional relation between security and dependability impairments", Proceedings of the New Security Paradigms Workshop 1999, Sep. 22–24 1999.
[8] R. Ortalo, Y. Deswarte, M. Kaaniche, "Experimenting with quantitative evaluation tools for monitoring operational security", IEEE Transactions on Software Engineering, vol. 25, no. 5, pp. 633–650, Sept/Oct 1999.
[9] S. Jha, O. Sheyner, J. Wing, "Minimization and reliability analysis of attack graphs", CMU Tech. Report, CMU-CS-2-109, May 2002.
[10] K. Lye, J. M. Wing, "Game strategies in network security", International Journal of Information Security, vol. 4, no. 1-2, pp. 71-86, 2005.
[11] P. Liu, W. Zang, "Incentive-based modeling and inference of attacker intent, objectives, and strategies", Proceedings of the 10th ACM conference on computer and communication security, pp. 179–189, 2003.
[12] P. Manadhata, J. M. Wing, "An attack surface metric", CMU-CS-05-155, July 2005.
[13] R. Chiong, S. Dhakal, "On the insecurity of Personal Firewall", Intern. Symposium on Information Technology, ITSim 2008, vol.4, pp. 1-10.
[14] E. Al-Shaer, H. Hamed, R. Boutaba, M.Hasan, "Conflict classification and analysis of distributed firewall policies", IEEE journal on selected areas in communications, vol. 23, N. 10, October 2005.
[15] B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, S. Page, D. Wright, "Towards operational measures of computer security", Journal of Computer Security, vol. 2, pp.211-229, 1993.
[16] T. A. De Long, D. T. Smith, B. W. Johnson, "Dependability metrics to assess safety-critical systems", IEEE Trans. on Reliability, vol. 54, n.3, pp. 498-505, Sept. 2005.
[17] B. R. HaverKort, I. G. Niemegeers, "Performability modelling tools and techniques", Perf. Ev., vol. 25, pp. 17-40, 1996.
[18] K. S. Trivedi, "Probability and statistics with reliability, queuing, and computer science applications", John Wiley&Sons, 2001.
[19] C. M. Grinstead, J. L. Snell, "Introduction to probability", AMS, 1997.
[20] J. Lowry, "An initial foray into understanding adversary planning and courses of action. DARPA", Information Survivability Conference and Exposition (DISCEX II), vol. 1, pp. 123-133, 2001.