A Model For Analyzing Security Parameters in Computing and Communication Infrastructures

V. Zorkadis[1] and D. A. Karras[2]
(1) Dept. of Computer Science, University of Ioannina, Ioannina, GREECE,

(2) Department of Business Administration, University of Piraeus, Rodu 2, Ano Iliupolis Athens, GREECE

Abstract: In this paper a model for studying the security related behavior of an information infrastructure is developed. The model allows the estimation of critical parameters of the infrastructure components. These parameters could support the risk analysis and assist the decision making process in resolving the trade-offs between security and quality characteristics of the services provided by the complex computing and communication system. *CSCC99 Proceedings,* pp.5761-5764
Key-Words: Security modeling, information infrastructure, security planning, security parameters, risk analysis, security threats

1. Introduction

The increasing role of computer systems and networks makes crucial the issue of ensuring their security attributes in terms of secrecy, integrity and availability. The security attacks in information systems may result in [1]: information disclosure, unauthorized modification of files and messages, masquerading or successful break-in, decreasing services availability, repudiation in sending and receiving messages or creating and modifying files, and the possibility of traffic analysis. These attacks may emanate from legitimate users, unauthorized users and processes, such as malicious software.

Security violations leave abnormal patterns of system usage and accounting [2,3]. To cope with intrusions or attempted break-ins, system monitoring techniques or intrusion-detection mechanisms and audit trails are used, that rely on the collection of audit data and their comparison with the usage and accounting profiles maintained by the system [4]. The conditional probability of detecting an intrusion given that the intrusion has occurred is called intrusion coverage and used as a measure of the effectiveness of the intrusion-detection mechanism. The number of normal and abnormal usage and accounting types (patterns) is extremely high and they can be differentiated only partially so that it is very difficult to have an intrusion coverage close to 1. An alarm is triggered if certain thresholds are reached. The detection sensitivity level and the false alarm rate depend on the thresholds set [5]. Increasing the detection sensitivity level leads to higher false alarm rates, i.e., better intrusion coverage appears to be in trade-off with false alarms.

Audit trails, i.e., data that allow tracing from users and transactions of related processes, records and reports and in the inverse direction, aim to detect or deter system intrusion and to help assess the damage caused by intrusions in the case of successful ones. Issues regarded in research efforts in the context of audit trails include the analysis and specification of auditable events and the quality improvement of the mechanisms related to efficiency, protection and the prevention of denial of service. They, also, include the association and analysis of related events and the automation of intrusion detection and damage assessment functions [4].

Intrusion detection mechanisms can be used in stand-alone or networked systems. They are based on the development of user and system or network resources usage profiles, and knowledge-oriented or statistically oriented methods. They have limitations, since the absence of rules for all possible intrusion scenarios or inaccurate statistical distributions do not lead to detection of intrusions or attempted break-ins. On the other hand, they may lead to false alarms, if unexpected user actions or resource usage patterns occur, which are not foreseen by the rules or the distributions used.

To study the behavior of security attacks or intrusion processes, models have to be developed and used, since it is quite impossible to directly analyze real computer systems and networks or information infrastructures to this respect.

In section 2, the model is described and the mathematical notations and the system equations are discussed. In section 3, we apply the model and discuss the various results obtained for a set of parameter values. Finally, section 4

summarizes this paper with conclusions and future directions.

2. Model Description and Analysis

In this paper we develop and use Markov models by considering the states of each system component of the information infrastructure, which reflect system functioning with respect to the above stated possible attacks. These states are explicitly associated with the security attributes of secrecy, integrity and availability. On the other hand, the existing dependencies between the component systems comprising the infrastructure are taken into account in the proposed models. While single system security models exist in the literature [4,6], the suggested models for analyzing security parameters in infrastructures is the first research effort for investigating the effects of multiple dependent systems operation in the infrastructure security planning.

We assume constant arrival rates of attacks and constant state transition rates, which allow the use of exponential or geometrical distributions, since there are no exact analytical solution methods for non-Markovian models. (Approximation techniques may be used in the case of non-constant rates.)

Model A

Figure 1 shows the model, which relates to a single system and consists of 7 states. The system is in state 0 when there are no security violations or attempted attacks. All security attributes are well maintained. With the first attempted attack, the system enters in state 1. The system remains in this state as long as it is under attack, the attacks are not detected and the system has not been penetrated. From this state, transition back to state 0 takes place if the attacks are detected or to state 2, if the attacker obtains authentication information and penetrates the system. The attacker remains in state 2 as long as he obtains (disclosures) confidential information and may move to state 3 if he starts to modify files, programs and messages or to state 4 if he chooses to hinder the access of authorized users to programs, hardware and data. When the attacker is detected, the system enters in the state 5, where it is reconfigured and transition back to state 0 occurs. Transition from state 0 to state 6 may take place if a false alarm is triggered. After the reconfiguration the inverse transition occurs. Transitions between states 2, 3 and 4 take place according to the actions of the attacker, which lead to unauthorized information disclosure, modification and access to system or network resources, respectively.

Notation and system of equations

In this paper we use the following notation, which is common in textbooks on stochastic processes, queueing theory and Markovian chains in particular [7].

$ë_{ij}$, is the transition rate from state i to state j, p_{ij}, is the transition probability from state i to state j and P_i, is the probability of the system or network or infrastructure to be in state i (steady state).

From the state-transition-rate diagram shown in Fig. 1, it is obvious that the Markov chain is irreducible and we accept the limit that $P_k = lim\ P_k(t)$ as $t \to ¥$. In the equilibrium case we are interested in that the flow must be conserved in the sense that the input flow must equal the output flow for any given state. By inspection we can establish the following equilibrium (steady-state) equations for the model A.

$$(l_{01}t_{01} + l_{06}t_{06})P_0 = l_{10}t_{10}P_1 + l_{50}t_{50}P_5 + l_{60}t_{60}P_6 \quad (1)$$

$$l_{10}t_{10}P_1 + l_{12}t_{12}P_1 = l_{01}t_{01}P_0 \quad (2)$$

$$(l_{23}t_{23} + l_{24}t_{24} + l_{25}t_{25})P_2 = l_{12}t_{12}P_1 + l_{32}t_{32}P_3 + l_{42}t_{42}P_4 \quad (3)$$

$$(l_{32}t_{32} + l_{34}t_{34} + l_{35}t_{35})P_3 = l_{23}t_{23}P_2 + l_{43}t_{43}P_4 \quad (4)$$

$$(l_{42}t_{42} + l_{43}t_{43} + l_{45}t_{45})P_4 = l_{24}t_{24}P_2 + l_{34}t_{34}P_3 \quad (5)$$

$$l_{50}t_{50}P_5 = l_{25}t_{25}P_2 + l_{35}t_{35}P_3 + l_{45}t_{45}P_4 \quad (6)$$

$$l_{60}t_{60}P_6 = l_{06}t_{06}P_0 \quad (7)$$

By means of this model we may analyze the systems comprising an information infrastructure separately. The security-related dependence between these systems can be taken into account if we adapt the probability transitions from state 1 to state 2 of the controlled system by adding to its initial value the equilibrium probability of the controlling system being in state 2. We assume successful attacks in the various systems are independent. However, if the controlling system is penetrated, the controlled system may be penetrated immediately or with higher probability than when it is attacked directly and not through the controlling system.

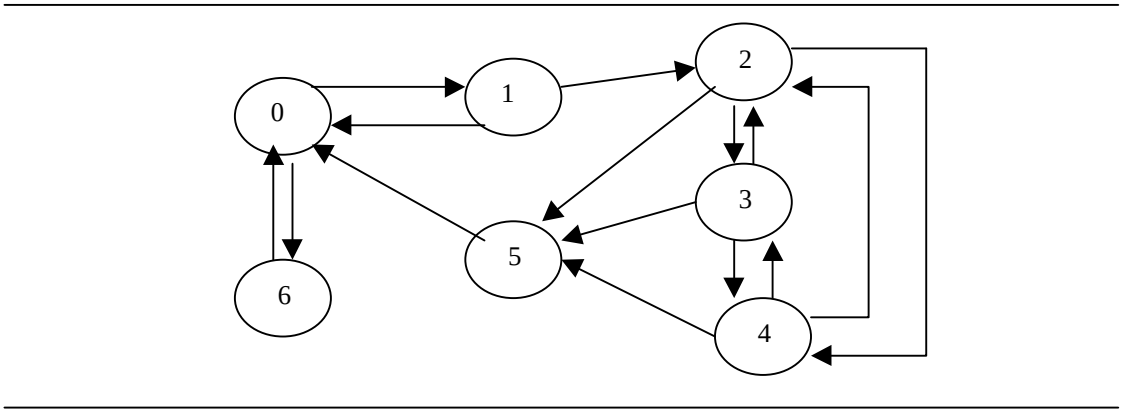


Fig. 1. State-transition-rate for the diagram of model A for a single system or network.

Model B

Figure 2 shows the model, which relates to two systems or networks comprising an information infrastructure and consists of 12 states. The systems are in state (0,0) when there are no security violations or attempted attacks. With the first attempted attack, the attacked systems enter in state (1,0) or (0,1) if it is the first or the second system attacked. From this state transition to state (1,1) may occur if both systems are under attack. Transition to state (2,0), (2,1) or (0,2), (1,2) takes place if the attempted intrusion leads to successful penetration of the first or the second system, respectively. If one of the systems is occupied then the second system is penetrated as well, (2,2). From this state transition to state (3,3) occurs when the penetration is detected. After the reconfiguration of the systems state (0,0) is entered. From state (0,0) transition may occur to state (4,0) or (0,4) if a false alarm of the first or the second system is flagged. After the false alarm is resolved current state becomes the (0,0). From Fig. 2 we obtain the following equilibrium equations by simplifying the numbering of the states: (0,0) – 0, (1,0) – 1, (0,1) – 2, (1,1) – 3, (2,0) – 4, (0,2) – 5, (2,1) – 6, (1,2) – 7, (2,2) – 8, (3,3) – 9, (4,0) – 10, (0,4) – 11.

$$\left(l_{01}t_{01} + l_{02}t_{02} + l_{10,0}t_{10,0} + l_{11,0}, t_{11,0}\right)P_0$$

$$= l_{10}t_{10}P_1 + l_{20}t_{20}P_2 + l_{30}t_{30}P_3 + l_{10,0}t_{10,0}P_{10} + l_{11,0}t_{11,0}P_{11} \quad (1)$$

$$(l_{13}t_{13} + l_{14}t_{14})P_1 = l_{01}t_{01}P_0 \quad (2)$$

$$(l_{23}t_{23} + l_{27}t_{27})P_2 = l_{02}t_{02}P_0 \quad (3)$$

$$(l_{35}t_{35} + l_{36}t_{36})P_3 = l_{13}t_{13}P_1 + l_{23}t_{23}P_2 \quad (4)$$

$$l_{48}t_{48}P_4 = l_{14}t_{14}P_1 \quad (5)$$

$$l_{58}t_{58}P_5 = l_{35}t_{35}P_3 \quad (6)$$

$$l_{68}t_{68}P_6 = l_{36}t_{36}P_3 \quad (7)$$

$$l_{78}t_{78}P_7 = l_{27}t_{27}P_2 \quad (8)$$

$$l_{89}t_{89}P_8 = l_{48}t_{48}P_4 + l_{58}t_{58}P_5 + l_{68}t_{68}P_6 + l_{78}t_{78}P_7 \quad (9)$$

$$l_{90}t_{90}P_9 = l_{89}t_{89}P_8 \quad (10)$$

$$l_{10,0}t_{10,0}P_{10} = l_{0,10}t_{0,10}P_0 \quad (11)$$

$$l_{11,0}t_{11,0}P_{11} = l_{0,11}t_{0,11}P_0 \quad (12)$$

We solve the above equations for steady-state probabilities. From these we may calculate the probabilities for each system.

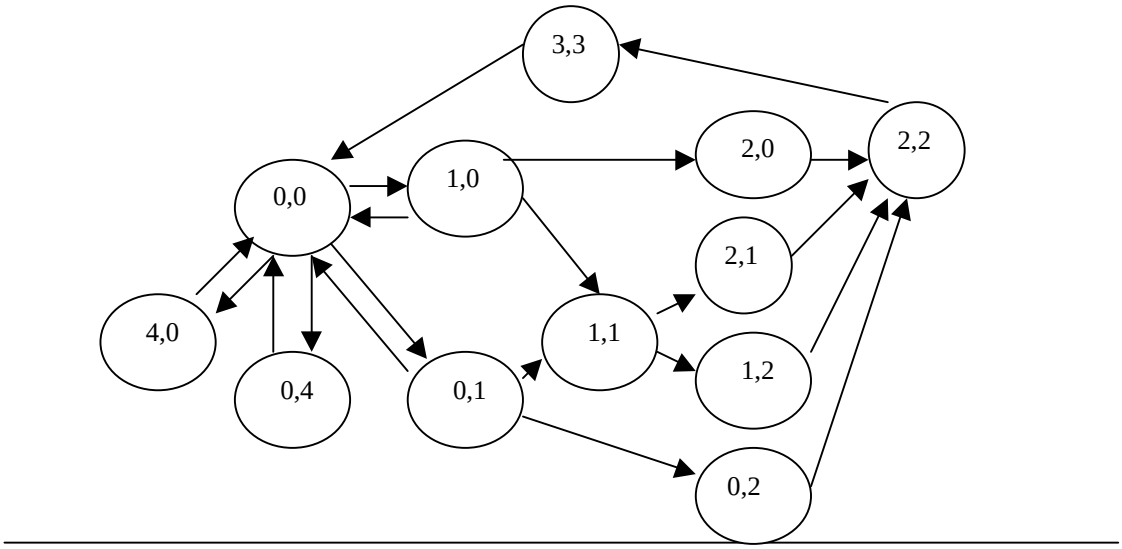
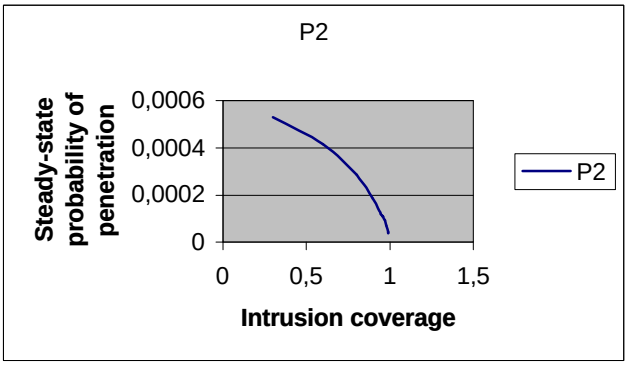


Fig. 2. State-transition-rate diagram of model B for two interconnected systems or networks.

3. Numerical Results

The selection of the parameter values is based on the tests and results of [4,5]. We assume transition rates equal to 1 per day from the states 0 and 1 and transition rates 20 from states 2, 3, 4, 5, and 6 to all others and the transition probabilities, $t_{01} = 1\text{-}t_{06}$, $t_{10} = 1\text{-}t = 0.1$, $t_{23}=t_{24}=t_{32}=t_{34}=t_{42}=t_{43}=(1\text{-}t)/2$, $t_{12}=t_{25}=t_{35}=t_{45}=t$, $t_{50}=t_{60}=1$, t=0.2,……,1.0 (intrusion coverage).

With these assumptions we have obtained results, shown in the next diagram, which validate our infrastructure modeling approach.



4. Summary

In this paper we presented two models for the analysis of security-related attack processes by means of Markovian chains. The first model is proposed for use in the analysis of single systems or networks, while the second in the analysis of two interconnected systems or networks. The models allow for the calculation of the expected probability of the systems to be in various states such as safe-state, under attack, penetrated and in false-alarm-state. Future work will aim to expand the models with respect to the number of systems comprising an information infrastructure, to the distributions used and the to case of multiple, independent intrusions. Also, future work will aim at the development of simulation models for the analysis of the security-related behavior of information infrastructures, and as a validation tool for the analytical ones. Furthermore, the involvement of neural networks for approximating the probability distributions in the analytical models, through using the simulation model in the training and test stage, will be investigated.

References:

[1] P. Helman and G. Liepins, "Statistical foundations of audit trail analysis for the detection of computer misuse", IEEE Trans. On Software Engineering, SE-19, 1993, pp. 886-901.

[2]D.E. Denning, 'An Intrusion-detection Model', IEEE Trans. On Software Engineering, SE-12, 1987, pp. 222-232.

[3]C. Stoll, 'Stalking the Wily Hacker', Communications of the ACM, 1988, pp. 484-497.

[4] B. C. Soh and T. S. Dillon, "Setting optimal intrusion-detection thresholds", Computers & Security, Vol. 14, 1995, pp. 621-631.

[5] G.E. Liepins and H.S. Vaccaro, 'Intrusion Detection: Its Role and Validation', Computers & Security, Vol. 11, 1992, pp. 347-355.

[6] B. C. Soh and T. S. Dillon, "System intrusion processes: a simulation model", Computers & Security, Vol. 16, 1997, pp. 71-79.

[7] L. Kleinrock. "Queueing Systems, Volume I: Theory, John Wiley and Sons, New York, 1975