Computer Communications 52 (2014) 47–59

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Mean privacy: A metric for security of computer systems ☆

Jaafar Almasizadeh, Mohammad Abdollahi Azgomi *

Trustworthy Computing Laboratory, School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran

ARTICLE INFO

Article history:
Received 13 March 2013
Received in revised form 13 April 2014
Accepted 27 June 2014
Available online 4 July 2014

Keywords:
Computer systems
Security
Privacy
Quantification
Information theory

ABSTRACT

In this paper, we propose a new approach for quantitative security analysis of computer systems. We intend to derive a metric of how much private information about a computer system can be disclosed to attackers. In fact, we want to introduce a methodology in order to be able to quantify our intuitive interpretation of how attackers act and how much they are predictable. This metric can be considered as an appropriate indicator for quantifying the security level of computer systems. We call the metric "Mean Privacy" and suggest a method for its quantification. It is quantified by using an information-theoretic model. For this purpose, we utilize a variant of attack tree that is able to systematically represent all feasible malicious attacks that are performed to violate the security of a system. The attack tree, as the underlying attack model, will be parameterized with some probability mass functions. The quantitative model will be used to express our intuition of the complexity of the attacks quantitatively. The usefulness of the proposed model lies in the context of security analysis. In fact, the analysis approach can be employed in some ways: Among several options for a system, we can indicate the most secure one using the metric as a comparative indicator. The security analysis of systems that operate under a variety of anticipated attack plans and different interaction environments can be carried out. Finally, new security policies, countermeasures and strategies can be applied to increase the security level of the systems.

1. Introduction

Ideally, we would like to have computer systems that are completely secure. Unfortunately, past and current experiences have shown that even the best attempts to build secure systems are not perfect. Generally speaking, the main sources of insecurity in computer systems are as follows. First, during the design and development phases, it would not be feasible to make a computer systems' software and hardware components completely free of vulnerabilities. These vulnerabilities would be suitably exploited to make the systems insecure. Second, the interaction environment of systems with users is very complex. Thus, the behavior of malicious attackers cannot be well understood. Third, with freely available attacking tools, conducting a large number of attacks against systems is a highly automated process. As a result, compared with the past situation, it requires a lower skill level and has a higher probability of success. Fourth, human-made errors leading to security holes and flaws frequently occur. Usually, such errors stem from the lack of sufficient experience and professional competence. These errors, due to their human nature, are always expected to be present, more or less.

In fact, the big advantage that attackers have is that they need to find only a single weakness of a system, while the system administrator must know and cover all weaknesses of the system to obtain perfect security. We need to analyze security from a relative point of view. As a practical matter, it is strongly accepted that an absolute system security level cannot be achieved. Therefore, it is recommended to consider security as a quality of service (QoS) attribute of systems (e.g., availability, reliability, delay, etc.) so as to be able to quantify how much their security level can be achieved. In other words, to validate the efforts made for securing systems, it is necessary to obtain a quantitative metric indicating their security level. Such a metric can characterize how good the security efforts are and how much they can be trusted.

Ideally, the process of quantitative security evaluation of a computer system can answer the following questions: With an initial design, is the system needed to be redesigned to meet its security requirements? With a default configuration, is the system needed to be reconfigured to meet the security requirements? Can the system provide a specified security level and meet the security requirements? By how much can the desirable security be achieved? What is the tolerance threshold of the system when

☆ This research was supported by the Research Institute for ICT of Iran.

* Corresponding author. Address: School of Computer Engineering, Iran University of Science and Technology, Hengam St., Resalat Sq., Tehran 16846-13114, Iran. Fax: +98 21 73225322.

E-mail address: azgomi@iust.ac.ir (M. Abdollahi Azgomi).

http://dx.doi.org/10.1016/j.comcom.2014.06.009
0140-3664/

confronted with attackers, that is, what the intensity level of malicious attacks can be handled and responded by the system security mechanisms? Answering such questions is a very useful task because it can provide more insights into security issues of a system under study. With the answers in hand, the security experts can make appropriate decisions of how to change existing security policies, services and mechanisms and define new ones.

To address such issues, we seek to find a way for the prediction of the complexity level of an attack process against a system. It is desirable to estimate how much attack scenarios are predictable. We define a new metric for the security analysis of computer systems that is appropriately consistent with our purposes. We propose the term "Mean Privacy" and a way for its quantitative evaluation. It is a predictive measure of the level of diversity and sophistication of attack scenarios. In fact, it is a good criterion that can be used to quantify the intuitive view of how attackers may behave. Clearly, in practice, we are not able to obtain exact values for security metrics. Indeed, in most situations, the computation of the exact values of the metrics is neither feasible nor necessary. The essential issue is to derive a reliable criterion so that it will be possible to quantitatively compare systems from the security standpoint.

For this purpose, we suggest a probabilistic model for describing an attack process and computing the respective metric. We employ some ideas from the field of information theory and apply them to our problem. The main idea behind this paper is to extend the concept of entropy to perform security analysis. In fact, this paper is our initial trends towards utilizing the fundamental concepts of information theory for developing a systematic method of security evaluation. In order to compute the quantitative metric, the proposed attack model needs to be parameterized using suitable data. The input parameters to the model are attack data and the output of the analysis process of the model is the desirable metric.

This paper is generally organized as follows. In Section 2, related works on security metrics are introduced. In Section 3, the details of the proposed modeling approach, step by step, are explained. In order to clarify the underlying concepts of the model and its applications, an illustrative example is given in Section 4. Finally, conclusions and future works are presented in Section 5.

2. Related work

The challenging area of quantitative security evaluation has been received much more attention in recent years. In this section, we want to provide a general overview of the most important methods worked out in this important area of security analysis. Due to the incomplete administrator's knowledge of the behavior, intent and skill level of attackers, the prediction of their behavior would be a very difficult task. That is, due to the uncertainty in the attack process, it cannot be completely captured. Thus, the use of probabilistic and stochastic models and concepts in the area of security evaluation can be an appropriate approach. As will be shown, stochastic and probabilistic modeling techniques used in the context of dependability evaluation, have been extended and also used to evaluate certain security metrics. In a number of publications, state-based stochastic models, like Markovian models or stochastic Petri nets, have been introduced as useful tools for quantitative security analysis. On the other hand, probabilistic models have also extensively been used to evaluate security metrics. For instance, some models such as attack graphs, Bayesian networks and model checking can probabilistically be defined and analyzed. In contrast to stochastic models, which are parameterized with continuous probability distributions, these types of models are primarily parameterized with discrete probability distributions.

Sallhammar et al. [1] suggest the use of game theory as a method for computing the probabilities of expected attacker behavior in a quantitative stochastic model of security. By viewing system states as elements in a stochastic game, they compute the probabilities of expected attacker behavior and model attacks as transitions between the system states. Having solved the game, the expected attacker behavior is reflected in the transitions between the states in the system model, by weighting the transition rates according to probability distributions. The proposed game model is based on a reward and cost concept and a detailed evaluation of how the reward- and cost parameter influence the expected attacker behavior is included. In the final step, continuous-time Markov chain (CTMC) is used to compute operational metrics of the system. In [2], Madan et al. used the state transition model of the scalable intrusion-tolerant architecture (SITAR) proposed in [3] and stochastic modeling techniques to capture the attacker behavior as well as the system's response to a security intrusion. The security quantification analysis is first carried out for steady-state behavior leading to metrics like steady-state availability. By transforming this model into a model with absorbing states, they computed a security metric called the mean time to security failure (MTTSF) and also the probabilities of security failure due to violations of different security attributes. Wang et al. [4] developed a stochastic reward net (SRN) model to capture attacker behavior as well as system response for the intrusion-tolerant system named SITAR. It was shown that the resulting analysis is useful in determining gains in security by reconfiguring such a system in terms of increase in redundancy under varying threat levels. Stevens et al. [5] described a probabilistic model for validating an intrusion-tolerant system that combines intrusion tolerance and security. The models were built with stochastic activity networks (SANs) formalism using the Möbius tool. This paper illustrates how probabilistic modeling can be used in an integrated validation procedure and successfully brings insight and feedback to a design. Also, Singh et al. [6] proposed an approach by using SANs to quantitatively validate an intrusion-tolerant replication management system. For this purpose, they characterized the intrusion tolerance provided by the system through several metrics defined on the model and studied the variations in these metrics in response to changes in system parameters to evaluate the relative merits of various design choices.

In [7], Kaâniche et al. presented some empirical analyses based on the data collected from the *Leurré.com* honeypot platforms deployed on the Internet. They provided some preliminary statistical modeling studies such as the analysis of the time evolution of the number of attacks taking into account the geographic location of the attacking machine, the characterization and statistical modeling of the times between attacks and the analysis of the propagation of attacks throughout the honeypot platforms in order to characterize attack processes. In [8], Jonsson et al. worked out a hypothesis on typical attacker behavior based on empirical data collected from intrusion experiments; attacking process can be split into three phases: the learning phase, the standard attack phase, and the innovative attack phase. The collected data indicated that the times between breaches during the standard attack phase are exponentially distributed. Oratalo et al. [9] provided the results of an experiment of security evaluation. The evaluation is based on a theoretical model called the privilege graph and transformed into a Markov model, which describes the system vulnerabilities that may offer opportunities to potential attackers to defeat some security objectives. They studied several modeling assumptions and discussed the validity of these assumptions based on an experimental study performed on a real system during more than a year.

McQueen et al. [10] proposed a new model for estimating the time to compromise of a system component that is visible to an attacker. The model provides an estimate of the expected value of the time-to-compromise as a function of known and visible