Security Modeling and Evaluation for the Mobile Code Paradigm

Anthony H.W. Chan and Michael R. Lyu

Department of Computer Science and Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong
{hwchan1, lyu}@cse.cuhk.edu.hk

There is no well-know model for mobile agent security. One of the few attempts so far is given by [1]. The model is, however, a qualitative model that does not have direct numerical measures. It would be great if there is a quantitative model that can give user an intuitive sense of "how secure an agent is".

Software reliability modeling is a successful attempt to give quantitative measures of software systems. In the broadest sense, security is one of the aspects of reliability. A system is likely to be more reliable if it is more secure. One of the pioneering efforts to integrate security and reliability is [2]. In this paper, these similarities between security and reliability were observed.

Security	**Reliability**
Vulnerabilities	Faults
Breach	Failure
Fail upon attack effort spent	Fail upon usage time elapsed

Fig. 1. Analogy between Reliability and Security

Thus, we have *security function*, *effort to next breach distribution*, and *security hazard rate* like the *reliability function*, *time to next failure distribution*, and *reliability hazard rate* respectively as in reliability theory. One of the works to fit system security into a mathematical model is [3], which presents an experiment to model the attacker behavior. The results show that during the "standard attack phase", assuming breaches are independent and stochastically identical, the period of working time of a single attacker between successive breaches is found to be exponentially distributed.

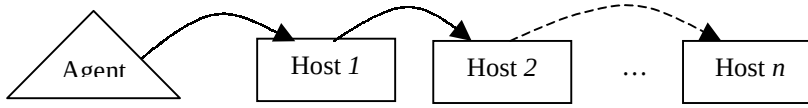

Fig. 2. A Mobile Agent Travelling on a Network

Now, let us consider a mobile agent travelling through *n* hosts on the network, as illustrated in Figure 2. Each host, and the agent itself, is modeled as an abstract machine as in [1]. We consider only the standard attack phase described in [3] by malicious hosts. On arrival at a malicious host, the mobile agent is subject to an attack effort from the host. Because the host is modeled as a machine, it is reasonable to estimate the attack effort by the number of instructions for the attack to carry out,

P.S. Thiagarajan, R. Yap (Eds.): ASIAN'99, LNCS 1742, pp. 371-372, 1999.

which would be linearly increasing with time. On arrival at a non-malicious host, the effort would be constant zero. Let the agent arrive at host i at time T_i, for $i = 1, 2, \ldots, n$. Then the effort of host i at total time t would be described by the *time-to-effort function*:

$$E_i(t) = k_i(t-T_i) \text{ , where k is a constant}$$

We may call the constant k the *coefficient of malice*. The larger the k_i, the more malicious host i is ($k_i = 0$ if host i is non-malicious). Furthermore, let the agent stay on host i for an amount of time t_i, then there would be breach to the agent if and only if the following breach condition holds:

$$\begin{aligned} & E_i(t_i+T_i) > \text{effort to next breach by host } i \\ \text{i.e.,} \quad & k_i t_i > \text{effort to next breach by host } i \end{aligned}$$

As seen from [32], it is reasonable to assume exponential distribution of the effort to next breach, so we have the *probability of breach at host i*,

$$\begin{aligned} \text{P(breach at host } i) &= \text{P(breach at time } t_i+T_i) \\ &= \text{P(breach at effort } k_i t_i) \\ &= 1 - exp(-vk_i t_i) \qquad ,v \text{ is a constant} \\ &= 1 - exp(-\lambda_i t_i) \qquad ,\lambda_i = vk_i \end{aligned}$$

We may call v the *coefficient of vulnerability* of the agent. The higher the v, the higher is the probability of breach to the agent. Therefore, the *agent security E* would be the probability of no breach at all hosts, i.e.,

$$E = \prod_{i=1}^{n} e^{-\lambda_i t_i} = e^{-\sum_{i=1}^{n} \lambda_i t_i}$$

Suppose that we can estimate the coefficients of malice k_i's for hosts based on trust records of hosts, and also estimate the coefficient of vulnerability v of the agent based on testing and experiments, then we can calculate the desired time limits T_i's to achieve a certain level of security E. Conversely, if users specify some task must be carried out on a particular host for a fixed period of time, we can calculate the agent security E for the users based on the coefficients of malice and vulnerability estimates.

References

1. Fritz Hohl. "A Model of Attacks of Malicious Hosts Against Mobile Agents". In *Fourth Workshop on Mobile Object Systems (MOS'98): Secure Internet Mobile Computation*, 1998.
2. Sarah Brocklehurst, Bev Littlewood, Tomas Olovsson and Erland Jonsson. "On Measurement of Operational Security". In Proceedings of the Ninth Conference on Computer Assurance (COMPASS'94): Safety, Reliability, Fault Tolerance and Real Time, Security, p.257-266.
3. Erland Jonsson. "A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior". In *IEEE Transactions on Software Engineering, Vol. 23, No. 4*. IEEE, April 1997.