Characterizing the Behavior of Cyber Adversaries: The Means, Motive, and Opportunity of Cyberattacks

Elizabeth Van Ruitenbeek, Ken Keefe, William H. Sanders
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
Urbana, IL, USA
Email: {evanrui2, kjkeefe, whs}@illinois.edu

Carol Muehrcke
Cyber Defense Agency
Wisconsin Rapids, WI, USA
Email: cmuehrcke@cyberdefenseagency.com

***Abstract*—To provide insight on system security and aid decision-makers, we propose a method to quantitatively evaluate the strength of a system's security. Our approach is to create an executable state-based security model of the system under attack. In this paper, we focus on the development of the adversary attack behavior model, which is one part of the overall security model. We show how three key aspects of an adversary's successful cyberattack—means, motive, and opportunity—translate into the notions of probability of success given attempt, probability of attempt, and precondition.**

***Keywords*-security quantification; state model; simulation; adversary attack behavior**

I. Quantitative Model-Based Security Metrics

Making sound security decisions when designing and maintaining a complex system is a challenging task. Analysts need to be able to understand and predict how different factors affect the overall system security.

To provide insight on system security and aid decision-makers, we propose a method to quantitatively evaluate a system's security. Our approach is to create an executable state-based security model of the system under attack. We run discrete-event simulations of the model and collect results on security metrics of interest. Figure 1 illustrates how this method generates answers to security decision questions by incorporating information about the system, its adversaries, and the security metrics.

An effective security model should contain information relevant to security analysis. In our proposed state-based security model, possible attack paths into a system are represented as a series of attack steps that incrementally change the state of the model. Each attack step, if successfully executed, can increase the adversary's access or knowledge of the system and move him or her closer to achieving attack goals, such as loss of confidentiality or integrity of specific data or loss of availability of specific services in the system.

One key component of our approach is the inclusion of adversary attack behavior models. We assert that meaningful measurements of system security cannot occur in a vacuum void of information about the system's adversaries. A sports team is considered "good" or "bad" depending on how its ability to compete compares to its opponents' abilities. Similarly, a system defense should be evaluated in the context of the opponents against which it will likely defend.

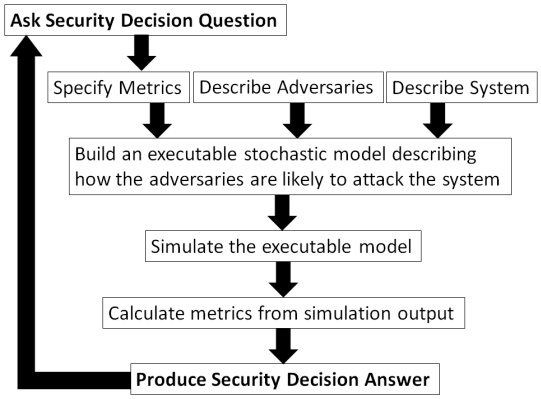

Figure 1. Method for Producing Quantitative Model-Based Metrics

Different systems face different adversaries. Government-owned systems are likely to attract attacks from nation-state adversaries. Corporate networks are likely to draw the attention of other types of attackers. To produce meaningful analysis results, security should be analyzed in the context of the specific adversaries likely to attack the system.

II. Means, Motive, and Opportunity for Cyberattacks

Examining the means, motive, and opportunity of a suspect or defendant is helpful in solving mysteries and establishing guilt in criminal cases. The concept of "means, motive, and opportunity" can also motivate the analysis of attacker behavior in the cyber realm.

When we construct a model to simulate an adversary (or set of adversaries) attacking a system, we speculate on how different factors drive attack behavior and determine attack attempt outcomes. An adversary may be faced with several potential attack step options. The adversary must first determine which attack steps are available options (i.e., where the adversary has the opportunity to attack) and then determine which available attack step option is most

attractive (i.e., where the adversary has the motive to attack). The success of an attempt is determined by the capability of the adversary to execute such an attack step (i.e., whether the adversary has the means to defeat the system defense). We now examine the three stages of an adversary's attack attempt.

A. Opportunity: Attack Step Precondition

An adversary in the cyberattack realm possesses the opportunity to execute an attack step when he or she possesses some minimum level of system access, system knowledge, and attack skill needed to attempt the attack. Within the security model, an attack step precondition formally states the minimum combination of access, knowledge, and skill needed, as perceived by the adversary. The attack step precondition is a necessary, but not sufficient, condition for an adversary to attempt an attack.

For example, when the attack step consists of an adversary gaining corporate network access from the Internet through the company's VPN, the precondition might specify that the attacker must possess Internet access and either knowledge of VPN account log-in information or VPN software exploit skill. An adversary who does not meet the precondition requirements will not attempt the attack step.

B. Motive: Probability of Attempt

The adversary possesses the motive to execute an attack when he is willing to attempt the attack given the opportunity. Within the security model, this willingness is quantified as the probability of the adversary attempting the attack step.

The probability estimate of an adversary possessing the motive to attempt a specific attack includes an implicit assumption of the time period. For some analyses, the time period may be as long as a decade; in other instances, the time period may be a few minutes.

The adversary's probability of attempting a particular attack step depends on the relative attractiveness of that attack compared with other attack step options. The adversary first considers all available attack step options, including the option to attempt no attack (the "do-nothing" attack step). The adversary then rates the attractiveness of each option using his or her personal attack goals and attack preferences. Attack goals include achievements such as crashing a web server or stealing credit card numbers from a database. Attack preferences describe the relative importance of four attractiveness measures.

The four attractiveness measures are (1) cost to the adversary in attempting the attack step, (2) payoff to the adversary for successfully executing the attack step, (3) probability of successfully completing the attack step, as perceived by the adversary, and (4) probability of being detected by the system during or after attempting the attack step.

Different adversaries may have different attack preference weights. A well-funded nation-state may care little about the cost of an attack but may tolerate only very low probability of detection in the attack steps it chooses to attempt. However, a resource-constrained lone hacker may try risker attack steps with a low probability of success and high probability of detection, but the cost to attempt must be low.

After the set of available attack step options have been rated with respect to attractiveness to a particular adversary, the adversary chooses one attack step to attempt. In certain circumstances, the "do-nothing" attack may be the most attractive option. Although the "do-nothing" attack step has no payoff, it also has zero cost, no probability of detection, and no probability of failing. In fact, when the "do-nothing" attack is consistently the most attractive attack step option for adversaries, this is a sign of a strong system defense. This situation means that the available attack options are too costly, with too little payoff, too high a probability of detection, and too low a probability of success, from the point of view of the attacker.

C. Means: Probability of Success Given Attempt

An adversary possesses the means to attack when he or she possesses the capabilities to successfully execute the attack step given that it is attempted. Within the security model, this capability is quantified as the probability of successfully executing the attack step given that it has been attempted. This probability is computed based on the balance of the attack skill of the adversary versus the defensive strength of the system. The defeat of strong system defenses requires more advanced attack skills.

These parameters taken together allow us to model the actions of an adversary with respect to a particular system.

III. Conclusions and Future Work

The adversary attack behavior model is a key part of a larger security model framework. This framework uses precise executable models to produce quantitative security assessments, as shown in Figure 1. A security analysis tool using this framework is currently under development.

Meaningful measurements of system security require information about the adversaries. To model attack behavior, we examine how the concepts of means, motive, and opportunity translate into probability of success given attempt, probability of attempt, and precondition in the model.

Future work on this project will include case studies and the development of security model validation methods.

Acknowledgments

The authors appreciate the valuable research contributions of Willard Unkenholz and Corky Parks. The work depicted here is performed, in part, with funding from the Department of Homeland Security under contract "FA8750-09-C-0039" with the Air Force Research Laboratory. We particularly wish to thank Douglas Maughan, Program Manager, Cyber Security R&D Center, Department of Homeland Security Science and Technology Directorate.