RRE: A Game-Theoretic Intrusion Response and Recovery Engine

ABSTRACT:

Preserving the availability and integrity of networked computing systems in the face of fast-spreading intrusions requires advances not only in detection algorithms, but also in automated response techniques. In this paper, we propose a new approach to automated response called the response and recovery engine (RRE). Our engine employs a game-theoretic response strategy against adversaries modeled as opponents in a two-player Stackelberg stochastic game. The RRE applies attack-response trees (ART) to analyze undesired system-level security events within host computers and their countermeasures using Boolean logic to combine lower level attack consequences. In addition, the RRE accounts for uncertainties in intrusion detection alert notifications. The RRE then chooses optimal response actions by solving a partially observable competitive Markov decision process that is automatically derived from attack-response trees. To support network-level multiobjective response selection and consider possibly conflicting network security properties, we employ fuzzy logic theory to calculate the network-level security metric values, i.e., security levels of the system’s current and potentially future states in each stage of the game. In particular, inputs to the network-level game-theoretic response selection engine, are first fed into the fuzzy system that is in charge of a
nonlinear inference and quantitative ranking of the possible actions using its previously defined fuzzy rule set. Consequently, the optimal network-level response actions are chosen through a game-theoretic optimization process. Experimental results show that the RRE, using Snort’s alerts, can protect large networks for which attack-response trees have more than 500 nodes.

EXISTING SYSTEM:

The severity and number of intrusions on computer networks are rapidly increasing. Generally, incident-handling techniques are categorized into three broad classes. First, there are intrusion prevention methods that take actions to prevent occurrence of attacks, for example, network flow encryption to prevent man-in-the-middle attacks. Second, there are intrusion detection systems (IDSes), such as Snort, which try to detect inappropriate, incorrect, or anomalous network activities, for example, perceiving CrashIIS attacks by detecting malformed packet payloads. Finally, There are intrusion response techniques that take responsive actions based on received IDS alerts to stop attacks before they can cause significant damage and to ensure safety of the computing environment. So far, most research has focused on improving techniques for intrusion prevention and detection, while intrusion response usually remains a manual process performed by network administrators who are notified by IDS alerts and respond to the intrusions. This manual response process inevitably introduces some delay between notification and response,
PROBLEM DEFINITION:

- Which could be easily exploited by the attacker to achieve his or her goal and significantly increase the damage.
- To reduce the severity of attack damage resulting from delayed response, an automated intrusion response is required that provides instantaneous response to intrusion.

PROPOSED SYSTEM:

In this paper, we present an automated cost-sensitive intrusion response system called the response and recovery engine (RRE) that models the security battle between itself and the attacker as a multistep, sequential, hierarchical, non zero sum, two-player stochastic game. In each step of the game, RRE leverages a new extended attack tree structure, called the attack-response tree (ART), and received IDS alerts to evaluate various security properties of the individual host systems within the network. ARTs provide a formal way to describe host system security based on possible intrusion and response scenarios for the attacker and response engine, respectively. More importantly, ARTs enable RRE to consider inherent uncertainties in alerts received from IDSes (i.e., false positive and false negative rates), when estimating the system’s security and deciding on response actions. Then, the RRE automatically converts the attack-response trees into partially observable competitive Markov decision processes that are solved to find the optimal response action against the attacker, in the
sense that the maximum discounted accumulative damage that the attacker can cause later in the game is minimized.

ADVANTAGES OF PROPOSED SYSTEM:

- Improves its scalability for large-scale computer networks, in which RRE is supposed to protect a large number of host computers against malicious attackers.

- Finally, separation of high- and low-level security issues significantly simplifies the accurate design of response engines.
IEEE Projects 100% WORKING CODE + DOCUMENTATION+ EXPLANATION – BEST PRICE
LOW PRICE GUARANTEED

SYSTEM ARCHITECTURE:

HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
IEEE Projects 100% WORKING CODE + DOCUMENTATION + EXPLANATION – BEST PRICE
LOW PRICE GUARANTEED

➢ Mouse : Logitech.
➢ Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

➢ Operating system : Windows XP/7.
➢ Coding Language : JAVA/J2EE
➢ IDE : Netbeans 7.4
➢ Database : MYSQL