ABSTRACT

Wu, Yu-Sung Ph.D., Purdue University, May 2009. Achieving High Survivability in Distributed Systems through Automated Response. Major Professor: Saurabh Bagchi.

Distributed systems typically have interactions among different services that create an avenue for propagation of attacks from one service to another. For critical applications, it is important that a cascading attack does not compromise all the services in the distributed system. Therefore, it is important to respond to an attack at runtime, by providing automated responses. The responses have the goals of containing the current attack and reconfiguring the system to make it more secure against future attacks. When choosing responses, one needs to consider the impact from using a response on the system (e.g. a firewall rule can cut off both the attack and the legitimate traffic). Also each response can have various degree of effectiveness on countering the attack. All these factors need to be considered beforehand.

We formalize the process of providing automated responses and the criterion for asserting global optimality of the selection of responses. We show that reaching the globally optimal solution is an NP-hard problem. Therefore we design a genetic algorithm framework for searching for good selections of responses in the runtime. For comparison, we present a baseline model to describe existing mainstream automated response systems. In real world, good response selection can change as the problem structure changes. Here the problem structure involves the protected target system and the attacks, both of which can change over time. The system constantly adapts itself to the changing environment based on short term history and also tracks the patterns of attacks in a long-term history.

Unknown security attacks, or zero-day attacks, exploit unknown or undisclosed vulnerabilities and can cause devastating damage. The escalation pattern, commonly

represented as an attack graph, is not known a priori for a zero-day attack. Hence, a typical response system provides ineffective or drastic responses. Our system "conceptualizes" nodes in an attack graph, whereby they are generalized based on the object-oriented hierarchy for components and alerts. This is done based on our insight that high level manifestations of unknown attacks may bear similarity with those of previously seen attacks. Thus, the response system may find similarities between an unknown attack and past attacks after they have been conceptualized to an appropriate level. This allows the use of history such as effectiveness of each response from past attacks to assist responses to the unknown attack.

We evaluate our system by injecting real multi-stage attack scenarios, not necessarily present in the system's knowledge base, and observe the survivability improvements from instantiating the proposed model.

This thesis lays down three distinct claims and validates them empirically. The claims are: (i) For automated response, consider a baseline mechanism that has a static mapping from the local detector symptom to a local response. This corresponds to the state-of-the-art in deployed response systems. Now consider our proposed model which takes into account global optimality from choosing a set of responses and also does a dynamic computation of the response combination from the set of detectors and other system parameters (inferences about the accuracy of the attack diagnosis, response effectiveness, etc.). The survivability of the application system with our proposed model is an upper bound of the survivability achievable through the baseline model. (ii) In some practical situations, the proposed model gives higher survivability than the baseline model. (iii) The survivability with our proposed model is improved when the system takes into account history from prior similar attacks. This kind of history is particularly important when the system deals with zero-day attacks.

Keywords: automated adaptive response, intrusion containment, e-commerce system, distributed system, survivability, attack graphs, attack variant, zero-day attack.