Active Defense Decision and Escalation Model

Sergio Caltagirone
University of Idaho
scaltagi@acm.org

Active defense is, as Sun Tzu in The Art of War, so eloquently phrased it, the "ability to defeat the enemy [by] taking the offensive." Some have interpreted this as indicating that the only way to permanently disable the enemy is to attack them. While this may not be an accurate reflection of Sun Tzu's meaning, modern system defenses are increasingly adding the capacity to defend to the capacity to detect. Some of these defensive actions may appear quite similar to a traditional "attack" on a computer system; however, active defense is not limited to only offensive actions, but to any action sequence performed, in an automated or non-automated fashion, to mitigate a threat against a particular asset.

Yet, executing any action that appears to be an "attack," even with the purpose of defense, is difficult to justify. There are a number of reasons for this, primarily the fear of legal liability, ethical responsibility, and the unknown consequences of the action loom greatest and prevent the adoption of active defense in any capacity. However, with a proper framework that maximizes benefit, minimizes cost, and takes into account important aspects of ethical, legal, and financial liability, it is possible to build a model that frees organizations to responsibly pursue active defense as a legitimate security tool.

The model proposed is designed to satisfy three primary criteria: (1) it should allow any organization to create an active defense policy and escalation ladder tailored to internal priorities as well as any required external criteria, (2) it provides organizations with a sense of confidence that they are free to actively protect themselves while not assuming unacceptable risk, and (3) it should lend itself to automated response. The model itself is divided into two phases, the active defense policy, and the escalation ladder. The first phase, the active defense policy, describes the assets to be protected by active defense, an evaluation of the threats (or classes of threats) that exist against those assets, and the value of the asset with respect to the consequences of a successful attack. Additionally, the policy describes the potential actions that can be taken to mitigate the risk of the threat, as well as the risks assumed by conducting an action. The most important step during the creation of the active defense policy is the scoring chart, which linearly scores assets, threats, and actions based on a number of categories such as financial, national security, ethical action, ethical consequences, and legal. The introduction of a scoring chart allows the direct comparison between threats and actions for the purpose of risk evaluation.

The second phase, the escalation ladder, describes the series of actions that an organization can consider to mitigate the threat against an asset taking into account internal priorities and external requirements. Each step is ordered according to some locally defined criteria – for instance, a company might identify risk of damaging external resources as the key element of these criteria. From the escalation ladder a graph representation for each threat is created where each node represents a potential action. Each node is then weighted by the formula: Risk_Score(Action) – Risk_Score(Threat) – Success_Order(Action). Where Success_Order returns the probability that an action will

be successful in mitigating a threat to the satisfaction of the policy and Risk_Score is a function that returns the total risk of the action or the threat.

At this point the model has created a feed-forward graph with weighted vertices. It is then a simple matter of traversing the graph using the well-defined shortest path algorithm. After the graph traversal, an ordered set of actions is produced which minimizes risk while maximizing benefit, making sure that the risk created by executing the action does not exceed the risk of losing the asset to the threat. However, if an action cannot be executed for some reason, then a contingency plan is formed, where the algorithm finds the next shortest path without that action.

Using the information provided by the organization in the active defense policy, the model has described the set of actions, ordered by internal priorities and external requirements, necessary to mitigate the threat against the particular asset. Most importantly, the set of actions can be shown to minimize risk while maximizing the potential success of the actions, thereby justifying the necessity and appropriateness of the actions taken. Using this model, organizations are free to explore active defense as a security tool while feeling confident that they will not expose themselves to undue risk.

The current work on the model is focusing on including a number of necessary but missing elements; such as, providing for unknown consequences (e.g. attacking the wrong machine), using the model as a legal justification for self-defense, and including confidence values with respect to the data provided by other security tools (e.g. intrusion detection systems, etc.). In the future, we are preparing to validate the model. The validation will include a significant simulation using data from a live network and intrusion detection system. The simulation will not execute active defense actions, but rather explore the consequences if the action set chosen by the model were executed on the network. By this means we hope to provide confidence that the model will perform as expected if deployed in a production environment and provide another security tool for organizations to consider.