The configuration of a computer network is constantly changing, and incorrect configuration can lead to complex attacks that compromise the security of an organization. Recent work proposes a system that can automatically detect a misconfiguration by modeling the network using Resource Description Framework (RDF) models and associated rules for inference. An inference engine is used to detect if a violation of security policy can be derived from the current configuration. While this system was able to detect security violations, it was unable to automatically fix them.

My primary goal was to extend the current system so that it can determine the best way to reconfigure a vulnerable network. We then investigated applications of this new capability to the problem of Insider Threat, the threat posed by malicious insiders using their access for sabotage or espionage. Particularly, we investigated how this system can be used to automatically ensure that the network conforms to auditing policies, so that it is not possible to silently compromise a network without being logged.

Can we efficiently determine the best way to reconfigure a network by computing the minimal hardening set (the “easiest” set of changes sufficient to secure the network)? Can we ensure that the network remains auditable using this system?

We generate Hypergraphs that represent each attack and then merge them all together into a single Attack Hypergraph. We then convert that Hypergraph to a propositional logic statements, which then gets converted to an instance of the Maximum Satisfiability (MAXSAT) problem.

That problem answers the question, “What propositions can we discard to make the system satisfiable such that we maximize the scores of the remaining propositions?” The set of propositions discarded correspond to a set of actions, which is the minimal hardening set we are looking for. Though MAXSAT is NP-Hard, fast solvers exist that we use to solve our moderately-sized problems quickly.

We generate Hypergraphs that represent each attack and then merge them all together into a single Attack Hypergraph. We then convert that Hypergraph to a propositional logic statements, which then gets converted to an instance of the Maximum Satisfiability (MAXSAT) problem.

That problem answers the question, “What propositions can we discard to make the system satisfiable such that we maximize the scores of the remaining propositions?” The set of propositions discarded correspond to a set of actions, which is the minimal hardening set we are looking for. Though MAXSAT is NP-Hard, fast solvers exist that we use to solve our moderately-sized problems quickly.

Time to compute hardening sets is independent of the number of hosts on the network, instead depending on the size of the Attack Hypergraph. More complicated attacks generally take longer to resolve.

Research Plan

Goals

Background

Research Results

Fundamental Questions/Challenges

Related Work/Interaction with Other Projects