Alex Withers Wins an NSF SI2-SEE Award

One of CyberSecurity's newest leaders, Alex Withers, wins a $499,136 award from the National Science Foundation to bring research from Professor Ravi Iyer's DEPEND group to production use.

Abstract

The cyber infrastructure that supports science research (such as the cyberinfrastructure that provides access to unique scientific instrumentation such as a telescope, or an array of highly distributed sensors placed in the field, or a computational supercomputing center) faces the daunting challenge of defending against cyber attacks. Modest to medium research project teams have little cyber security expertise to defend against the increasingly diverse, advanced and constantly evolving attacks. Even larger facilities that have with security expertise are often overwhelmed with the amount of security log data they need to analyze in order to identify attackers and attacks, which is the first step to defending against them. The challenges of the traditional approach of identifying an attacker are amplified by the lack of tools and time to detect attacks skillfully hidden in the noise of ongoing network traffic. The challenge is not necessarily in deploying additional monitoring but to identify this malicious traffic by utilizing all available information found in the plethora of security, network, and system logs that are already being actively collected. This project proposes to build and deploy, is needed in research environments, an advanced log analysis tool, named AttackTagger, that can scale to be able to address the dramatic increase in security log data, and detect emerging threat patterns in today's constantly evolving security landscape. AttackTagger will make science research in support of national priorities more secure.

AttackTagger will be a sophisticated log analysis tool designed to find potentially malicious activity, such as credential theft, by building factor graph models for advanced pattern matching. AttackTagger will integrate with existing security software so as to be easily deployable within existing security ecosystems and to offload processing and computational work onto better suited components. It can consume a wide variety of system and network security logs. AttackTagger accomplishes advanced pattern matching by utilizing a Factor Graph model, which is a type of probabilistic graphical model that can describe complex dependencies among random variables using an undirected graph representation, specifically a bipartite graph. The bipartite graph representation consists of variable nodes representing random variables, factor nodes representing local functions (or factor functions , and edges connecting the two types of nodes. Variable dependencies in a factor graph are expressed using a global function, which is factored into a product of local functions. In the practice of the security domain, using factor graphs is more flexible to define relations among the events and the user state compared to Bayesian Network and Markov Random Field approaches. Specifically, using factor graphs allows capturing sequential relation among events and enables integration of the external knowledge, e.g., expert knowledge or a user profile.