Rahul Hiran

Topic title: Keeping the Network Clean: Dynamic Alliances for Collaborative Evaluations

Abstract:

The miscreant of the Internet is becoming increasingly sophisticated and attacks are no longer insulated events. For example, correlated attacks mounted by the same source IP address to different networks are prevalent on the Internet. While some of these attacks are difficult to detect for a single network entity, collaboration among network entities can help detect (and in some cases prevent) such attacks. In this work, we present a framework that allows network entities to form alliances in the fight against miscreants. Our main focus in this work is how these alliances can be made dynamic and secure. Our system allows new members to be added to the alliance and others to be removed from the alliances, based on
their security compliance and value to the alliance. We present
effective mechanisms to identify well behaving candidate entities to promote into the alliance network and mechanisms to detect nodes which entities should be demoted. In this talk, we will discuss the framework within a simple use case example of a mail server infrastructure. We will discuss how to identify well behaving entities based on their mail sending patterns and their feedback reporting behavior about the other mail server nodes, such as to promoted them into the alliance. We will present some preliminary results using baseline policies and conclude with a discussion of more advanced policy mechanisms.