Title of Technical Presentation: **Verification of Security Response**

Desired Session/Topic Area: **Verification and Validation of Human-machine Interfaces and protocols**

Presenter Name(s): **Thomas C Eskridge, Siddhartha Bhattacharyya, Marco M Carvalho**

Titles: **Associate Professor, Research Professor, Executive Director and Associate Professor**

Address: **Harris Institute for Assured Information, Florida Institute of Technology, Melbourne, FL 39201**

Telephone Number: **321-674-8590**

Email Address(es): teskridge, sbhattacharyya, mcarvalo @fit.edu

Defending a computer network is a complex and difficult task. Computer network defense operators are frequently overwhelmed with the rate of incoming security events, and must be aware of the implications of adding or modifying network defenses before actions are taken. The increasingly frequent use of adaptive and moving target defenses makes achieving the needed awareness even more difficult, as subtle interactions between defenses can render the defenses useless or worse, cause the combination of them to become an inadvertent attack themselves.

Intelligent, semantically-enabled multi-agent systems (MAS) have been shown to provide leverage to computer network defense operators by enabling aspects of the command and control of network defenses to be represented, monitored, and maintained while ensuring that operator intentions are respected. This is accomplished in part thorough the use of semantic policies that ensure the system operates within the boundaries determined by the operator. Polices represent conditions or states of the network in which actions must be (obligation) or must not be (prohibition) taken. Operators interact with the MAS by either directing agents to take particular actions, or by modifying the policies under which the agents operate. Because the operational pace is generally too quick for direct interaction with agents, more often operators modify policies to achieve their goals. This can be to discount the importance of alerts (because they know the context in which the alert was generated), bias defense operations towards a known useful solutions (i.e., one that has worked well in the past), or to prevent an action from being carried out (such as accessing a database from a suspicious address block).

Formal verification systems use guards as part of the model-checking process in order to ensure that required constraints are not violated. The similarity between guards and semantic policies instigated the current work determining how verification can be applied to security response. In particular, we wish to verify specific performance properties and security properties of the combined defenses. Performance properties include connectivity, accessibility, latency and lag bounds, and transmission rates. Security properties include confidentiality, integrity, and accessibility. By representing the security specifications/properties as a formal model, changes or additions to the defense can be verified before they are enacted. We expect that formal analysis will identify key performance parameters that will allow us to generate runtime monitors/policies to perform checks during real-time adaptive operations.

In this early-stage work, we review the state-of-the-art in the application of verification and validation techniques to computer network security, and present a partial implementation of an integrated verification and validation with a MAS used for cyber command and control. We present the performance and security properties identified for command and control purposes, and illustrate the utility of the integrated system with an example based on an emulated enterprise network scenario.