The rapidly changing threat landscape in today's cyber world has motivated a need to perform not only experimental-based but also theoretical-based security research. In the development of a *Science of Cyber-security*, control theory has been shown to provide useful techniques and concepts for designing policies to achieve security objectives. My research brings Discrete Event Control Theory to the design and implementation of secure systems. The main goals are to formally characterize and provably achieve security objectives under different dynamic relationships between the defender and the attacker.

My doctoral research focuses on a confidentiality property called "opacity" for Discrete Event Systems (DES) modeled as partially-observable and/or nondeterministic finite state automata. The attacker is a passive observer of the system that wants to know whether or not the *secret* of the system has occurred. The system is opaque if "whenever the secret has occurred, there exists another *non-secret* behavior that is observationally equivalent." In my thesis, I have leveraged techniques from DES to (i) develop algorithms for verifying various notions of opacity, (ii) introduce a novel opacity enforcement mechanism based on event insertion, (iii) solve for optimal insertion policies with respect to a given cost criterion, and (iv) apply opacity techniques to enforce location privacy in location-based services.

Based on these results, I am interested in further investigating the control synthesis for other secure specifications. Specific future research topics are described as follows:

Probabilistic Opacity

I propose to extend the notion of opacity to a probabilistic setting. This notion of "probabilistic opacity" aims to capture scenarios where the intruder has prior knowledge of the system's transition probability, and always infers that the occurring behavior is the *most probable* one based on its observation. Probabilistic finite state automata will be used to model the systems. Probabilistic opacity holds if given any observation, there is a non-secret behavior that is more likely than the secret behavior. This study will start with the development of the algorithm for verifying probabilistic opacity. When probabilistic opacity fails to hold, we want to enforce probabilistic opacity by using a stochastic insertion function. A stochastic insertion function inserts events according to some specifications but randomizes the insertion when there are multiple choices. It enforces probabilistic opacity if the intruder, who is assumed to know the randomized strategy, can never infer that the secret has occurred based on its observation. Preliminary study has found examples for which probabilistic opacity can only be enforced when the insertion strategy is randomized. The use of stochastic insertion functions allows us to enforce a bigger class of probabilistic opacity problems. In all, this proposed work aims to develop a procedure that synthesizes systems that are probabilistically opaque. It will provide a formal framework that is more applicable to real-world confidentiality problems.

Opacity in the Distributed Architecture

I propose to further investigate opacity notions under the *distributed architecture*. In the distributed architecture, each subsystem has its own secret. We want to enforce opacity of subsystems such that each local secret is kept opaque under the interaction of the subsystems. This study will focus on exploring structural properties of automata that preserve opacity under composition. Structures and architectures that preserve certain properties under partial observation have been explored extensively in the DES supervisory control research. Hence, this study will start with leveraging and adapting results from supervisory control. This proposed work aims to provide principles that facilitate the modular development of secure systems and ensure that adding secure subsystems into a secure system results in a secure system.

Resilient Systems Under Active Attackers

In opacity problems, the intruders only passively observe the system's behavior. This passive attack model, however, is ill-suited when attackers can inject or modify data in the system. I propose to investigate security properties under active attackers. This effort will use Supervisory Control and Data Acquisition (SCADA) systems as the starting application. In SCADA systems, computation capabilities are integrated into the control of physical entities. Attackers that compromise sensors and/or actuators can send false information or block the delivery of information, potentially resulting in irreparable harm to the physical system. I propose to leverage results from supervisory control to formulate the control infrastructure. Algorithms for diagnosis problems and robust control will be used to detect compromised nodes and maintain the system's control specification when the system is being attacked. Also, I propose to bring in opacity techniques to capture sophisticated defender (i.e., system) and attacker that try to hide their detection and attack strategies. In this case, the defender wants to achieve control specifications and detect intrusion while hiding its detecting strategy; the attacker wants to damage the system without being detected. Either party may need to sacrifice one of its objectives in order to hide its strategy.

In all, the above proposed work will contribute to the Science of Cybersecurity with formal security formulations and provable design policies. The intersection of discrete event control theory and cybersecurity is a research direction that is not fully explored but well-motivated. I am also interested in exploring other fields of study and developing cross-disciplinary techniques to comprehensively capture security scenarios. These efforts will help establish a solid foundation for cybersecurity and provide design principles that can rapidly adapt to emerging threats.