A Framework for the Analysis of Cyber Attacks on Cyber-Physical Systems

Adam Hahn
The MITRE Corporation

Roshan Thomas
The MITRE Corporation

Alvaro Cardenas
University of Texas, Dallas

Complex energy management systems, such as the smart grid, are increasingly dependent on cyber systems to perform numerous critical control functions such as automatic generation control (AGC), state estimation (SE), and protective relaying functions. Understanding the cybersecurity properties of these and other cyber-physical (CPS) systems requires radically new approaches to analyzing how cyber inputs perturb physical system aspects. To this end, we propose a novel framework for analyzing cyber attacks against CPS systems. At the heart of our attack analysis framework is a multi-dimensional approach incorporating numerous axes, specifically *knowledge*, *difficulty* and *precision*.

The knowledge axis is concerned with how much control-theoretic and cyber knowledge an attacker needs to achieve a certain probability of success. Attacker's knowledge of the system may include properties associated with the physical system dynamics, control algorithms and cyber infrastructures. Knowledge of the control algorithms is tied to the degree of *observability* required to determine the current state of the system.

The difficulty axis is a measure of the viability or realism of an attack. It encompasses needs to access (e.g., one time, physical, network-based, real-time and continuous) to various elements of the control system, the number of resources needed to execute the attack, and the collective set of conditions that have to be true for the attack to succeed. Finally, the *precision* axis characterizes how precisely the attacker can manipulate the operation of the physical system to achieve the intended objective.For example, an attack that causes the random opening and reclosing of a circuit breaker may cause only minor grid inefficiencies, however, intelligently reclosing a breaker during an out-of-phase condition (e.g., the AURORA attack) could cause significant damage to the grid. Such precision may require deep knowledge of several state estimation variables and related algorithms (i.e. control-theoretic observability).

For each axis we have identified (1) a number of attributes that can be used to characterize it, and (2) specific cyber and control-theoretic vectors and related properties that manifest at the cyber-physical interface, so as to make CPS attacks viable. The cyber vectors are the traditional CIA triad (confidentiality, integrity and availability) as applied to sensor outputs, controller computations and control signal directives. These may be used to achieve a number of objectives in relation CPS operations including *degrade*, *deny*, *disrupt*, *destroy*, and *deceive*, and *exploit*. The control-theoretic properties are those of *controllability*, *stability*, *safety*, and *observability* as applied to the control laws that govern the physical system.

The proposed axes demonstrate a necessary means to analyzing the security of complex cyber-physical systems. The framework thus allows for the detailed characterization of the CPS attack space for any domain, rigorous analysis of individual attack classes and instances, and the development of related quantitative metrics to measure attacks as well as control system resiliency. We are currently studying various control systems in the production, distribution, and consumption of electric power in the smart grid. By studying the properties of various energy systems and published cyber attacks and applying our framework, we hope to better identify attack classes and their properties, the viability and precision of the attacks, and last but not least, approaches to mitigating the attacks.