Association for
Computing Machinery
Student Chapter

Indian Institute of Information
Technology Allahabad

Prof. Sandeep Shukla

ACM Distinguished Speaker

IIT Kanpur

Cyber Security of Critical Infrastructures: A Case for a Schizoid Design Approach

Topic(s):

Architecture, Embedded Systems and Electronics, Robotics , Security and Privacy , Computational Theory, Algorithms and Mathematics

Abstract

In the past, the design of cyber physical systems required a model based engineering approach, where as a first step of the design process -- a physics based mathematical model of the physical system, and a control theoretic model of the control system -- were put together in a formal or semi-formal framework. The designers would start from an abstract model, and refine it down to an implementation model in several steps, either formally or informally. The implementation model is then validated for functional correctness, performance, real-time requirements etc. Functional Safety, robustness to input assumptions, reliability under fault assumptions, and resilience to unknown adversities were considered as good design goals. With the increasing networked distributed control of large and geographically distributed critical infrastructures such as smart grid, smart transportation systems, air traffic control system etc. -- the exposure to cyber-attacks ushered in by the IP-convergence -- the design goals must consider cyber-security and cyber defense as first class design objectives. However, in order to do so, designers have to don a dual personality -- while designing for robustness, reliability, functional safety -- a model driven engineering approach would work -- whereas for designing for cyber-security and defense, the designer has to step into the shoes of a malicious attacker. For example, one has to consider the various observation or sampling points of the system (e.g. sensors to read or sample the physical environment), and think how an attacker might compromise the unobservability of those points without authentication, and what knowledge of the system dynamics or the control mechanism of the system might be actually reconstructed by the attacker. One also has to consider the actuation points of the system, and ponder the least number of such actuation points the attacker has to take over in order to disrupt the dynamics of the system enough to create considerable damage. One has to envision how to obfuscate the dynamics of the system even when certain sensing or actuation points are compromised. Also, it is known that a large percentage of attacks are induced by inside attackers. Thus perimeter defense alone cannot defend the system. In such cases, the question that one is confronted with is whether there is enough indication of an ongoing attack in the dynamics of the system itself. This approach to viewing the system from an adversarial position requires one to topple the design paradigm over its head, and we will need to build models from data, and not just generate data from models. The designer has to observe a system in action – even through partial observations, and construct a model close enough to the real system model – and then use the partial access to create damages to the because the approximate model allows her to do so. Almost like a schizophrenic duality, the engineer also has to wear the designers hat, and consider a game in which the observations are obfuscated enough to render it impossible for an attacker to build any useful model to induce clever attacks. The designer has to worry if she can construct from unobfuscated observations a dynamics quickly enough so that the difference between the expected dynamics and the real dynamics can trigger alarms to alert the system administrators. In this talk, while discussing this view of system design, we will also talk about VSCADA -- a virtual distributed SCADA lab we created for modeling SCADA systems for critical infrastructures, and how to use such a virtual lab completely implemented in simulation -- to achieve the cyber security and cyber defense objectives of critical infrastructures -- through attack injections, attack detection, and experiments on new defense mechanisms.