Chapter 110
Using Hybrid Attack Graphs to Model and Analyze Attacks against the Critical Information Infrastructure

Peter J. Hawrylak
The University of Tulsa, USA

Mauricio Papa
The University of Tulsa, USA

Chris Hartney
The University of Tulsa, USA

John Hale
The University of Tulsa, USA

ABSTRACT

The Smart Grid will incorporate computer networking technologies into the electrical generation, transmission, and distribution sectors. Thus, there will be an underlying Critical Information Infrastructure (CII) based on these network connections. This CII is vulnerable to traditional cyber or computer based attacks typically geared toward disabling devices or networks. However, the Smart Grid is also vulnerable to physical attacks where sensors are tricked into reporting false conditions that cause the control system to react in an inappropriate manner. Cyber-physical attacks blending both cyber and physical attack components are also a possibility. Techniques to model cyber-attacks exist, and this chapter presents a modeling methodology, termed hybrid attack graphs, to model cyber-physical attacks. The hybrid attack graph formalism can be applied to develop best practice guidelines and security patches for the Smart Grid. This formalism can also be applied to other cyber-physical domains as well to help bridge the gap between the physical, logical, and network domains.

INTRODUCTION

This chapter will address the use of hybrid attack graphs in modeling and analyzing attacks against the Critical Information Infrastructure (CII), as it constitutes a massive cyber physical system of vital national interest. The focus is on the CII for the electrical utility sector and examples are drawn from this domain. Supervisory control and data acquisition (SCADA) system components, such as Programmable Logic Controllers (PLCs), typically have very limited security features.

DOI: 10.4018/978-1-4666-5942-1.ch110

Traditionally, these systems have been isolated from public networks, e.g., the Internet, but that is changing. Current trends have resulted in connecting these systems to the Internet to enable better and more effective operation and use. The Smart Grid will make extensive use of public networks, e.g. the Internet, because it provides an available (deployed) and economical link to all components. As a result, attacks against the CII can now have significant physical consequences, e.g., shutting down an electrical power plant during peak demand. This chapter will illustrate how hybrid attack graphs can be used to understand and counter such threats.

The CII is used to control and make decisions about physical systems (e.g. electric power grid). The physical aspects of these systems must be taken into account when modeling possible attacks against the CII. The interplay between digital and physical control elements in these systems profoundly influences overall system behavior. Adversaries may not limit themselves to purely cyber or purely kinetic (physical) tactics to mount an attack. Blending cyber and kinetic acts may yield a composite effect not attainable through attacks launched in either domain alone. Such blended attack patterns exploit gaps in our understanding regarding the relationship between discrete and continuous domain elements. Thus, any risk analysis methodology that aspires to a comprehensive treatment of threats in the cyber-physical space must adopt a model that can capture hybrid attack vectors.

Hybrid attack graphs provide this capability by extending attack graphs to include systems and actions from the physical domain. Attack graphs enable the security analyst to identify all linkages between a compromised device and the rest of the system/network. Hybrid attack graphs extend this capability by adding linkages between cyber (computer) systems and physical systems (e.g. machinery). This provides increased visibility into the effects of an attack. The hybrid attack graph can then be analyzed to determine how best to counter and prevent the attack in a given system.

This chapter will present practical techniques for enumerating and modeling hybrid attack vectors, as well as considerations for efficient automatic generation of hybrid attack graphs. Both state based and dependency based attack graph modeling variants will be covered. Temporal and spatial aspects of hybrid attacks warrant special attention as both represent opportunities and challenges for scalable hybrid attack graph generation and analysis. Multiple scenarios, all related to CII domains will be explored, illuminating simple and illustrative examples of hybrid attack graph modeling, generation and analysis.

Applications of hybrid attack graphs in security engineering, risk assessment, and real-time threat management for the CII will also be explored. The development of risk metrics that leverage the rich information content available in hybrid attack graphs will be presented. Issues related to cognitive scalability and intuitive visual representation also will be pursued.

BACKGROUND

SCADA Systems

SCADA systems are widely employed to control the critical infrastructure and most manufacturing processes. These distributed digital systems are used to control industrial processes, linking the digital world with the physical world through sensors and actuators and are known as *cyber-physical systems* or *hybrid systems*. Often this linkage is provided with a PLC capable of executing simple logic operations to control an actuator or monitor a sensor. Typical applications of a PLC include monitoring electrical current in a transmission line and opening a circuit breaker (tripping) to disconnect the line if a fault (e.g. an overcurrent condition) is detected. In a cyber-physical system both physical and cyber (digital) conditions affect the system state. Thus, from a security standpoint cyber-physical systems present a difficult chal-