Chapter 37
Attack Graphs and Scenario Driven Wireless Computer Network Defense

Peter J. Hawrylak
The University of Tulsa, USA

Jeremy Daily
The University of Tulsa, USA

George Louthan IV
The University of Tulsa, USA

John Hal
The University of Tulsa, USA

Mauricio Papa
The University of Tulsa, USA

ABSTRACT

This chapter describes how to use attack graphs to evaluate the security vulnerabilities of an embedded computer network and provides example cases of this technique. Attack graphs are powerful tools available to system administrators to identify and manage vulnerabilities. Attack graphs describe the steps an adversary could take to reach a desired goal and can be analyzed to quantify risk. The systems investigated in this chapter are embedded systems that span hardware, software, and network communication. The example cases studied will be (1) radio frequency identification (RFID), (2) vehicle networks, and (3) the Smart Grid (the next generation power and distribution network in the USA).

INTRODUCTION

Embedded systems are systems composed of a microprocessor embedded within a larger product other than a typical desktop or laptop computer and are becoming pervasive. Embedded systems include sensors and actuators, which are controlled and monitored by microprocessors. Some examples of embedded systems are the engine control module found in vehicles, a washing machine, a cell phone, and a thermostat. Often an embedded system includes some form of network connection (e.g. RS-232, USB, CAN, RFID, or Wi-Fi) to connect to other devices. With the proliferation and networking of embedded systems, the security of these systems is of critical concern.

For embedded systems, security is addressed component by component in isolation. The goal is to secure a given component and then to do this for all components in a system. This tech-

DOI: 10.4018/978-1-4666-4707-7.ch037

nique may have worked in the past when most embedded systems were designed entirely from scratch or in-house components. However, today's embedded systems often incorporate third party intellectual property (IP) blocks that cannot always be verified or modified to fix security issues. The system-on-a-chip (SOC) design philosophy (Keating & Bricaud, 2002), built around reuse of IP blocks, requires a new approach to securing an embedded system.

Many embedded systems blend the physical (or continuous) world and the digital (or discrete) worlds. Such systems are often termed *cyber-physical systems*. The electronics in an automobile is one example of this blending of physical processes. For example, oxygen sensors provide analog signals to a digital control system that adjusts fuel mixture in a way that reduces hydrocarbon emissions. Because of this cyber-physical linkage, an attack may now be introduced into the system through both physical and cyber (software, hardware, and communications network) components. One example of such an attack is the Stuxnet worm, which targeted nuclear centrifuges using the motor to cause a catastrophic failure (centrifuge will break apart) (Broad & Sanger, 2010). Another example of cyber-physical attack is exploiting the electronic communication bus present on all modern automobiles to take control of physical variables or components (e.g. speed or door locks) (Koscher, *et. al.*, 2010). These kinds of blended attacks force a sea-change in the approach adopted by conventional IT security tools and methods. Security must be evaluated from the software, hardware, network, and physical viewpoints.

Attack graphs are one method to model and describe attacks. This chapter will describe how to use attack graphs to evaluate the security vulnerabilities of an embedded computer network and provide example cases of this technique. The systems investigated in this chapter are embedded systems that span hardware, software, and network communication domains. The example cases studied will be

1. Radio frequency identification (RFID),
2. Vehicle networking, and
3. The smart grid (the next generation power and distribution network in the USA).

First, a definition and explanation of attack graphs will be provided. Then, the methods of using these attack graphs to identify vulnerabilities and improve system security will be presented. Finally, the three example cases will be presented in separate sections. Each example case will be defined and attack graphs will be generated to enumerate vulnerabilities in that system.

BACKGROUND

Definition of Attack Graphs

An attack graph denotes one of any number of closely related formalisms that utilize graph theory to represent the state space of attacks on systems. Vertices of the graph represent individual network or system states, and edges represent state transitions generally due to the actions of an adversary. The term attack graph first appeared in the literature in 1998 (Philips & Swiler, 1998) including three features that continue to comprise the formalism: "attack templates," or generalized attacks to be employed in state transitions; configurations of individual network elements; and the topology of the network. The original formalism also included some features that are only sometimes present in modern incarnations of attack graphs such as a separate *attacker profile*, which represents a particular attacker's capabilities; and edge weights representing a *probability-of-success measure* (Philips & Swiler, 1998). Similar structures such as attack trees (Schneier 1999) and privilege graphs (Dacier, Deswarte & Kaâniche, 1996) were introduced independently around the same time.

Chaining together exploits over matching preconditions and postconditions yields a network