Chapter 47
Embedded Systems Security

Muhammad Farooq-i-Azam
COMSATS Institute of Information Technology, Pakistan

Muhammad Naeem Ayyaz
University of Engineering and Technology, Pakistan

ABSTRACT

Not long ago, it was thought that only software applications and general purpose digital systems i.e. computers were prone to various types of attacks against their security. The underlying hardware, hardware implementations of these software applications, embedded systems, and hardware devices were considered to be secure and out of reach of these attacks. However, during the previous few years, it has been demonstrated that novel attacks against the hardware and embedded systems can also be mounted. Not only viruses, but worms and Trojan horses have been developed for them, and they have also been demonstrated to be effective. Whereas a lot of research has already been done in the area of security of general purpose computers and software applications, hardware and embedded systems security is a relatively new and emerging area of research. This chapter provides details of various types of existing attacks against hardware devices and embedded systems, analyzes existing design methodologies for their vulnerability to new types of attacks, and along the way describes solutions and countermeasures against them for the design and development of secure systems.

INTRODUCTION

A few years ago almost all electronic equipment was built using analog components and devices. However, after the advent of microprocessors and microcontrollers majority of electronic equipment developed today uses digital components for design implementation. Embedded systems are finding their use in diverse applications ranging from complicated defense systems to home gadgets. Smart cards, debit and credit cards, DVD players, cell phones and PDAs are just a few examples of embedded systems that we use in our daily lives.

Under certain circumstances and conditions, a larger digital system is usually dependent upon the functions of smaller component embedded

DOI: 10.4018/978-1-4666-4301-7.ch047

systems for its function and operation. For example, a general purpose computer houses many smaller embedded systems. A hard disk, a network interface card, CD-ROM drive are examples of embedded systems used by a computer system for its operation. In addition to this, large industrial plants, nuclear power plants, passenger and fighter aircrafts, weapons systems, etc. are a few of many places where embedded systems are part of a bigger system.

With this increased usage of embedded systems in our daily lives, it is not unusual that bad guys and criminals try to take advantage of weak links in their security. Specially, the embedded systems used in financial institutions, battlefield equipment, fighter planes and industrial and nuclear plants may become targets of attack due to the importance of functions performed by them. Therefore, it is essential that these systems and the components used in them are highly dependable and their security is not compromised.

A number of security incidents related to embedded systems have been reported in the literature. For example, in 2001, Shipley and Garfinkel found an unprotected modem line to a computer system which was being used to control a high voltage power transmission line (Koopman, 2004). In another incident, a disgruntled employee in Australia released almost 250 million tons of raw sewage by causing failure of control system of a waste treatment plant through a remote attack (IET, 2005).

It is pertinent to mention here that the organizations which become target of attack may not like to publicize the incident due to various reasons. For example, it may disclose a vulnerable area of their systems or it may cause them a bad name and raise questions against security of their other assets. Furthermore, security threats against embedded systems do not propagate as rapidly as those against a standard operating system or software application. This is because majority of personal computer systems is similar and it is easier for any security threat to replicate from one system to the other. On the other hand, each embedded device is unique and it is almost impossible for a security threat to propagate from one device to the other. Moreover, a security threat against an embedded device is generally initiated at any one of the design stages before the device is built. Security threats against a software system may be programmed at any time after they have been developed and deployed. These are a few of the many reasons that we do not come to see as many security incidents reported against embedded systems as against software applications. Despite this fact, security incidents have been reported against hardware devices and embedded systems, a couple of which have been cited above and a few more will be mentioned later in this chapter.

BACKGROUND

Embedded systems security is a new and emerging area of research. It is meeting point of many disciplines such as electronics, logic design, embedded systems, signal processing and cryptography. It is closely related to the area of information and software systems security because software is an integral component of any embedded system.

First microprocessor was developed around 1971 and later innovations in this field resulted in the development of computer systems and embedded devices. Software is an integral component of the both. In particular, every desktop computer carries a critical piece of software called the operating system. It manages the hardware resources and makes it possible for an end user to operate the computer. Other software applications in a computer run on top of the operating system.

It was the software component of digital systems which was first subjected to different types of security threats and attacks and many security incidents were reported against different operating systems and software applications. This started in 1970s and continues to date. However, embedded systems security gained importance in 1990s, spe-