Chapter 58
Secure Techniques for Remote Reconfiguration of Wireless Embedded Systems

Abdellah Touhafi
Vrije Universiteit Brussel, Belgium

An Braeken
Erasmushogeschool Brussel, Belgium

Gianluca Cornetta
Universidad San Pablo-CEU, Spain

Nele Mentens
Katholieke Universiteit Leuven, Belgium

Kris Steenhaut
Vrije Universiteit Brussel, Belgium

ABSTRACT

The aim of this chapter is to give a thorough overview of secure remote reconfiguration technologies for wireless embedded systems, and of the communication standard commonly used in those systems. In particular, we focus on basic security mechanisms both at hardware and protocol level. We will discuss the possible threats and their corresponding impact level. Different countermeasures for avoiding these security issues are explained. Finally, we present a complete and compact solution for a service-oriented architecture enabling secure remote reconfiguration of wireless embedded systems, called the STRES system.

DOI: 10.4018/978-1-60960-042-6.ch058

1. INTRODUCTION

The broad diffusion of different wireless technologies like WiFi (Wireless Fidelity), GPRS (General Packet Radio Services), EDGE (Enhanced Data Rates for GSM Evolution), UMTS (Universal Mobile Telecommunication Systems), Zigbee, Bluetooth, etc. has prompted a wide interest in remote reconfiguration and remote monitoring of wireless embedded systems in several industrial environments such as car-manufacturers, healthcare, the financial sector and the entertainment industry.

Three main features are desirable in a state-of-the-art wireless embedded system: remote status checking, remote problem solving and remote upgradeability. It is, however, important that these remote techniques are reliable, have a low integration cost and are sufficiently secure. The reconfiguration or update of such embedded wireless systems can imply a change either in the system's software or in its reconfigurable hardware. The wireless nature of such kind of embedded systems makes them extremely prone to security threats. For this reason, the reconfiguration schemes must be designed very carefully, taking into account all kind of possible threats and attack schemes. Unfortunately, the increase in security can be achieved at the cost of an increased hardware complexity, which in embedded and cost-constrained systems is, most of the times, unaffordable. This brings up some key issues in the design of a wireless reconfigurable embedded system, since a new design constraint must be considered and part of the design efforts must be devoted to trade off security for cost.

We first give a thorough overview of remote reconfiguration technologies for wireless embedded systems and of the communication standard commonly used in those systems. Basic security mechanisms both at *hardware* and *protocol* level will be carefully reviewed and explained, putting particular emphasis on the possible threats and their impact level.

Protection at *protocol* level is necessary due to the fact that many off-the-shelf state-of-the-art communication modules provide little or poor protection against wireless security threats with respect to confidentiality and authentication of the configuration data. Some schemes propose to encrypt and to authenticate the bitstream to thwart security attacks but this does not prevent the replay of old bitstream versions. In fact, wireless embedded systems are particularly vulnerable to man-in-the-middle (MITM) attacks performed over the network while the system is being monitored or reconfigured. A MITM attack is a form of active eavesdropping in which the attacker establishes independent connections with the victim nodes and forwards messages between them, making them believe that they are communicating directly to each other over a private connection. As a consequence, it is necessary to develop a protection layer on top of the provided communication stack dealing with, confidentiality and authentication between three entities: user, embedded system, and service provider for updates and status monitoring. A cross-layer system-wide design approach is often required to cope with the demand for a low-cost implementation and secure wireless remote reconfigurability. An overview of different types of protocols is presented. Also a short discussion on the used algorithms is given.

Protection at the *hardware* level is studied with respect to three main categories of attacks: side-channel attacks, semi-invasive attacks, and invasive attacks. Each of the attacks can be either passive or active. A passive attack does not disrupt the operation of the system (the attacker snoops the data exchanged in the system without altering it). On the other hand an active attack attempts to alter or destroy either the data exchanged in the system, or the system itself. Invasive attacks involve direct electrical access to the internal components by