Applying Key Infrastructures for Sensor Networks in CIP/CIIP Scenarios

Cristina Alcaraz and Rodrigo Roman

Computer Science Department,
University of Malaga,
29071 - Malaga, Spain
{alcaraz,roman}@lcc.uma.es

Abstract. It is commonly agreed that Wireless Sensor Networks (WSN) is one of the technologies that better fulfills features like the ones required by Critical (Information) Infrastructures. However, a sensor network is highly vulnerable against any external or internal attacks, thus network designers must know which are the tools that they can use in order to avoid such problems. In this paper we describe in detail a procedure (the KMS Guidelines), developed under our CRISIS project, that allows network designers to choose a certain Key Management System, or at least to know which protocol need to improve in order to satisfy the network requirements.

Keywords: Critical Information Infrastructures, Sensor Networks, Key Management, Key Infrastructures.

1 Introduction

According to the European Commission, *Critical Infrastructures* consist of *"those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States."* [1]. These infrastructures depend on a spectrum of highly interconnected national (and international) software-based control systems for their smooth, reliable, and continuous operation. This information infrastructure underpins many elements of the aforementioned Critical Infrastructures, and is hence called *Critical Information Infrastructures* (CII).

CII are characterized by unique requirements for communications performance, including timing, redundancy, centers control and protection, and equipment control and diagnostics. One of the technologies that can fulfill these requirements are *Wireless Sensor Networks* (WSN)[2]. However, these networks are highly vulnerable against physical and logical attacks from a malicious adversary. Therefore, it is essential for a network designer to have the right set of tools and protocols for protecting the Wireless Sensor Network itself.

One of these tools are the *Key Management Systems* (KMS), which distributes some security credentials (i.e. keys) along the nodes of the network. However,

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 166–178, 2006.

due to the great number of existent KMS, it is not clear which KMS is suitable for a certain scenario. The purpose of this paper is to introduce the KMS CRISIS Guidelines, a tool that will help network designers into choosing the right KMS for its WSN in a C(I)IP environment. The rest of this paper is organized as follows. In section 2 we explain in more detail the challenges of protecting a CII and its relationship with WSN. In section 3 we introduce our KMS CRISIS Guidelines, and explain the procedure for choosing a certain KMS. Afterwards, in section 4, we will describe and apply our Guidelines to some actual and possible C(I)IP scenarios. Finally, we conclude the paper in section 5.

2 The Importance of WSN for C(I)IP

2.1 CIIP Challenges

In a Critical Infrastructure, the interconnected nature of networks means that single, isolated disturbances can cascade through and between networks with potentially disastrous consequences. Therefore, it is indispensable to have a resilient and robust information infrastructure that could deal with any situation, being a physical or computational attack to the system or an abnormal behavior of any component inside the overall system. Such infrastructure must be able to issue alerts and warnings in order to help human users and the information subsystems to react against adverse scenarios. Those alerts could be issued even in the case that a problem is not taking place but the context seems to be slowly changing into a problematic situation. In a worst-case scenario, the information infrastructure must be able to react and protect itself in real time, and to assure the seamless continuation of its services.

As any Information infrastructure, the CII must be thoroughly tested in order to assure that the system and its response mechanisms will work under any kind of context. However, it is usually not feasible to test and obtain results about a CII without endangering the operation of the entire system itself. As a result, it becomes imperative to create models and simulations that show how the system should behave in presence of problems. As an input to these models and any decision-making tools, it is also of vital importance to analyze an infrastructure and quantify the possible problems in order to correctly model the protection system.

In all these processes, it is essential to guarantee the security of information that is considered of critical importance, from a political, economic, financial or social standpoint. Adding Information Security provisions such as authorization, authentication, encryption, and other basic security services is not enough to manage these complex scenarios and applications, due to the complex and dynamic nature of these infrastructures. Finally, since these Information Infrastructures compose a very heterogeneous environment, it is crucial to provide a set of policies and methods to allow an effective and secure interaction of the elements of a CII, both internal and external.

As we have seen, CII are characterized by unique and complex requirements, and are vulnerable to many different types of disturbances. Although strong