Chapter 10
Security in Smart Home Environment

Georgios Mantas
University of Patras, Greece

Dimitrios Lymberopoulos
University of Patras, Greece

Nikos Komninos
Athens Information Technology, Greece

ABSTRACT

This chapter presents the concept of Smart Home, describes the Smart Home networking technologies and discusses the main issues for ensuring security in a Smart Home environment. Nowadays, the integration of current communication and information technologies within the dwelling has led to the emergence of Smart Homes. These technologies facilitate the building of Smart Home environments in which devices and systems can communicate with each other and can be controlled automatically in order to interact with the household members and improve the quality of their life. However, the nature of Smart Home environment, the fact that it is always connected to the outside world via Internet and the open security back doors derived from the household members raise many security concerns. Finally, by reviewing the existing literature regarding Smart Homes and security issues that exist in Smart Home environments, the authors envisage to provide a base to broaden the research in Smart Home security.

INTRODUCTION

Over the last decades the Smart Home development is a continuously evolving field that faces exceptional challenges. However, the recent advances in information and communications technologies have led the Smart Home development in a good level of maturity. A Smart Home is a living environment that incorporates the appropriate technology, called Smart Home technology, to meet the resident goals of comfort living, life safety, security and efficiency (Ricquebourg et al., 2006; Pohl & Sikora, 2005; Jiang, Liu, & Yang, 2004; Friedewald, Da Costa, Punie, Alahuhta, & Heinonen, 2005).

DOI: 10.4018/978-1-61520-805-0.ch010

Smart home technology achieves these goals building an environment which consists of a variety of home systems. A Smart Home encompasses four types of Smart Home systems; Home Appliances, Lighting and Climate Control system, Home Entertainment system, Home Communication system and Home Security System (Pohl & Sikora, 2005; Valtchev, Frankov, & ProSyst Software AG, 2002). Each of the above systems is characterized by different requirements (e.g. data rate, distance) based on the applications that supports. Thus, different physical media are appropriate for different Smart Home systems. In a Smart Home, the physical media that can be used by the Smart Home systems are the following: the existing wiring, a new wiring and the air. The existing wiring refers to the existing electrical wiring, the existing telephone wiring and the existing coax cabling. A new wiring requires installation of new cabling in the walls and the air refers to wireless networking (Pohl & Sikora, 2005; Jiang et al., 2004; Valtchev et al., 2002; Adams, 2002; Zahariadis, 2003).

In spite the fact that there is a high level of complexity and heterogeneity because of the various communication media and network protocols, the Smart Home systems are integrated into a well structured network, called Smart Home internal network. This integration is achieved using a central node, called residential gateway (RG), which serves as a bridge between the internal network of the Smart Home environment and the Internet. The residential gateway represents the intelligent control of a Smart Home as it manages the systems and connects them to the outside Internet world (Pohl & Sikora, 2005; Valtchev et al., 2002; Adams, 2002; HGI, 2006).

However, the heterogeneous and dynamic nature of the Smart Home internal network, the fact that it is always connected to the Internet and the fact that the household members usually open security back doors unintentionally are factors that create many security challenges in a Smart Home environment. For that reasons, security is a critical issue in Smart Home environment. The principal idea behind secure Smart Home is to preserve occupant privacy (improper eavesdropping or tampering of information) and not to allow service interference (e.g. blocking home network services) (Jeong, Chung, & Choo, 2006; Herzog et al., 2001; Thomas & Sandhu, 2004; Wang, Yang, & Yurcik, 2005; Schwiderski-Grosche, Tomlinson, Goo, & Irvine, 2004; He, 2002).

The notion of providing security in Smart Home environments relies on the maintenance of six essential properties; Confidentiality, Integrity, Authentication, Authorization, Non-repudiation and Availability. Confidentiality, Integrity, Authorization, Non-repudiation and Availability play very important roles in ensuring of Smart Home internal network security. However, Authentication can be considered as the first step in the pyramid of a security mechanism (Jeong, et al., 2006; Komninos, Vergados, & Douligeris, 2007a; Thomas & Sandhu, 2004; Schwiderski-Grosche et al., 2004; He, 2002; Bergstrom, Driscoll, & Kimball, 2001).

Following the introduction, this chapter is organized as follows. Firstly, in the second section, the concept of the Smart Home and its main components are presented. Furthermore, an overview of the main Smart Home systems is given and the role of the residential gateway in the Smart Home environment is discussed. The third section is devoted to the current Smart Home networking technology. In the fourth section, the security requirements that should be satisfied in a Smart Home are described. The fifth section concentrates on the factors that affect the security in a Smart Home environment. In the sixth section, security threats for the Smart Home internal network are discussed. In the seventh section, existing security technologies that provide security features in Smart Homes are described. Finally, the eighth section concludes the chapter.