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).

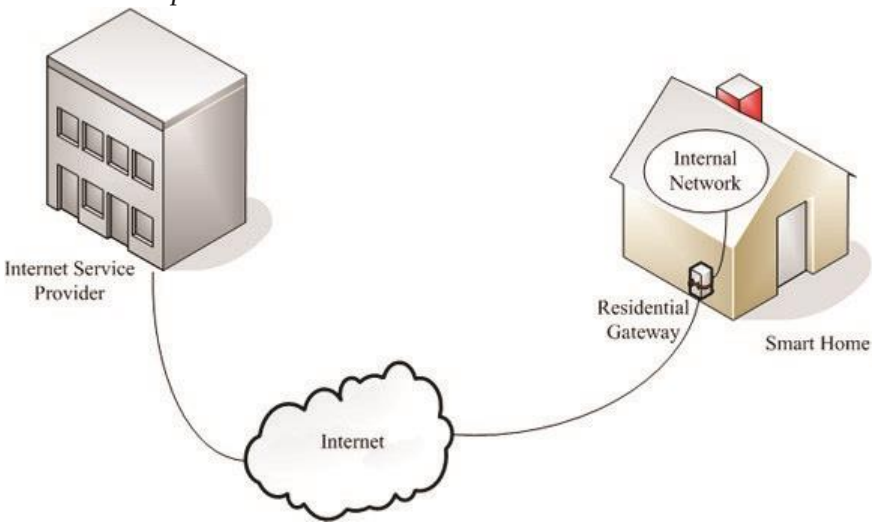
However, the heterogeneous and dynamic nature of the Smart Home internal network, the fact that it is always connected to the Internet and the fact that the household members usually open security back doors unintentionally are factors that create many security challenges in a Smart Home environment. 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.

Figure 1. Smart home concept



SMART HOME CONCEPT

It is very important to determine the main components of the Smart Home architectural model in order to be able to understand the factors that raise security breaches in a Smart Home environment as well as realize security technologies that can be applied to minimize the risk of security attacks. Smart Home can be considered that consists of three main components; the internal network, the external network and the residential gateway. These three components are presented in the Figure 1.

The internal network is the basis of a Smart Home and can consist of wired and wireless networks. The internal network of a Smart Home incorporates a combination of different communication media and protocols in order to support a number of Smart Home systems that simplify the residents' life and improve their quality of life. The external network of a Smart Home includes Internet and the service provider which is in charge to provide services over Internet to the household members. Finally, residential gateway (RG) is an always connected device located in a Smart Home and plays a very important role in bridging the internal network of the Smart Home and the outside world (Ricquebourg et al., 2006; Pohl & Sikora, 2005; Valtchev et al., 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003).

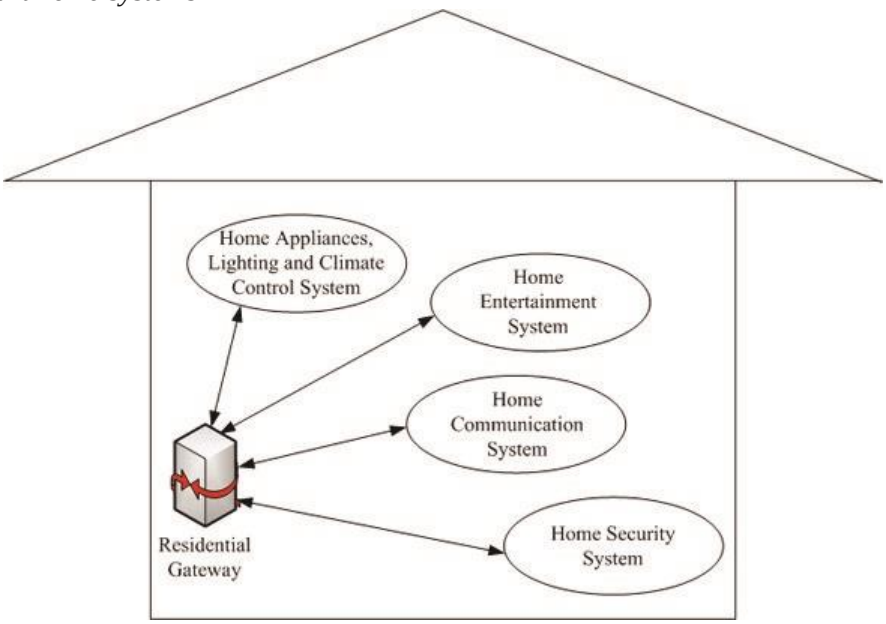
Smart Home Systems

The Smart Home internal network can integrate a variety of Smart Home systems, which provide a convenient and safe environment to the household members, as well as help them to perform their household tasks effectively. Smart Home systems can be classified into four categories (Figure 2): Home Appliances, Lighting and Climate Control system, Home Entertainment System, Home Communication System and Home Security System (Pohl & Sikora, 2005; Valtchev et al., 2002; Friedewald et al., 2005; Zahariadis, 2003; Delphinanto, 2003).

Home Appliances, Lighting and Climate Control System

Home Appliances, Lighting and Climate Control system consists of three subsystems. The Home Appliances Control subsystem monitors and controls the power outlets in Smart Home. Thus, based on this subsystem, the habitat is able to monitor the power consumption as well as switch off power outlets separately. Furthermore, the Home Appliances Control subsystem can include smart appliances that communicate with each other and the outside Internet world making habitat's daily life more comfortable and enjoyable. The Lighting Control subsystem consists of switches, lights and sensors. This subsystem monitors the intensity of light as well as the activities of the occupants in a smart domestic environment. Based on these factors the Lighting Control subsystem adapts lighting of intelligent inhouse ambient. Finally, the Climate Control subsystem includes the functions of heating, ventilating, and air-conditioning. This subsystem monitors and controls temperature and humidity in a Smart Home environment providing healthy conditions within. Additionally, Lighting and Climate Control subsystem reduces costs for heating, cooling and lighting by smart energy management helping the homeowner to save money (Pohl & Sikora, 2005; Valtchev et al., 2002; Friedewald et al., 2005; Zahariadis, 2003; Delphinanto, 2003).

Figure 2. Smart home systems



Home Entertainment System

Home Entertainment system provides the connection and communication of audio and video appliances over broadband networks serving distribution of high fidelity audio signal and high quality digital video. An Entertainment system can be consisted of a home theater, projection systems, plasma or LCD screens, a multi-channel surround sound system, satellite and digital television channels, video on demand systems, gaming consoles, a central media server, a central control system as well as a multi room audio video system for full audio and visual distribution. Digital audio is distributed from MP3 files, Internet radio and the home media server throughout the system to every room in the Smart Home. Furthermore, digital video content is distributed from the broadband connection, DVDs, PCs and the home media server to any video screen in the smart environment (Pohl & Sikora, 2005; Teger, Waks, & System Dynamics Inc., 2002; Valtchev et al., 2002; Han, Park, Jeong, & Park,

2006; Friedewald et al., 2005; Zahariadis, 2003; Delphinanto, 2003).

Home Communication System

Home Communication system provides telephone services such as conventional voice services and video conferencing calls as well as incorporates the intercommunication system of an intelligent inhouse environment for calling from room to room. Furthermore, this system contains devices such as PCs, printers, scanners, mobile phones, personal digital assistants (PDAs) and enables them to communicate with each other, to share information and a broadband connection within the Smart Home. Thus, tenants are able to chat, send emails and share data (e.g. digital photos, video) with other people in any place in the world. Finally, this system supports telecommuting for the residents (Pohl & Sikora, 2005; Teger et al., 2002; Valtchev et al., 2002; Han et al., 2006; Friedewald et al., 2005; Zahariadis, 2003; Delphinanto, 2003).

Home Security System

Home Security system encompasses identification mechanisms such as biometric recognition, voice recognition and face recognition, RFID tokens and smart cards that provide access control. Moreover, this system includes notification mechanisms such as burglar alarms that allow immediate reaction. Also, surveillance mechanisms such as CCTV can be part of Home Security system for monitoring in a Smart Home. What is more, there are solutions such as vibration shock sensors, glassbreak sensors, for the detection of an intruder to a habitat. Furthermore, there are systems which use lights that automatically switch on and off giving the impression that someone is at home. Additionally, Home Security System comprises electro-mechanical door locks, electric windows and door shutters. Finally, health and well-being monitoring for disabled and elderly people as well as children can be part of this system (Pohl & Sikora, 2005; Teger et al., 2002; Valtchev et al., 2002; Han et al., 2006; Friedewald et al., 2005; Zahariadis, 2003; Delphinanto, 2003).

Residential Gateway

In a Smart Home, the residential gateway is a network device which integrates all the different networking technologies that exist in the Smart Home internal network as well as provides access from the internal network to Internet and vice versa. The residential gateway serves as a single point of internal network convergence and distribution of both LAN-initiated and WANinitiated services. The residential gateway enables switching, routing and inter-working functions between the devices of the Smart Home systems over the internal network. This network device also supports high level distribution of advanced multimedia services over Internet broadband connectivity. Furthermore, the residential gateway supports remote control of the Smart Home systems and home appliances (Ricquebourg et al., 2006; Pohl & Sikora, 2005; Valtchev et al., 2002; Adams, 2002; Zahariadis, 2003; HGI, 2006).

Due to the variety of access network technologies, the residential gateway is able to interface with the majority of wired or wireless broadband access networks (e.g. ADSL, broadband mobile phone network, satellite link etc.). Different WAN side interfaces types can be provided by a residential gateway, but only one interface is supported at a time. Additionally, the residential gateway is able to support wired/wireless LAN interfaces towards the internal network since there are a lot of wired (HomePlug, HomePNA, Ethernet, IEEE 1394 and USB) and wireless (IEEE 802.11, Bluetooth, Zigbee and HiperLAN) networking technologies in a Smart Home. Moreover, the residential gateway provides QoS management to support services of different types at the same time. Besides, the residential gateway contains the rules for classification, queuing and priority field mappings (Zahariadis, 2003; HGI, 2006).

Furthermore, a residential gateway enables functionalities related to security of the Smart Home environment. It provides protection for the household members from unauthorized attacks and intrusions. Thus, a residential gateway encompasses a variety of security features such as firewalls, authentication mechanisms, authorization mechanisms and intrusion detection mechanisms (Kim, Lee, Han, & Kim, 2007; Zahariadis, 2003; HGI, 2006).

SMART HOME NETWORKING TECHNOLOGY

Smart Home internal network is based on various communication media and protocols (Figure 3). It is a combination of wired and wireless networks, since various transmission mediums, such as telephone lines, power lines, radio communication and wired cables are used in order to transmit signal throughout the Smart Home environment (Ricquebourg et al., 2006; Jiang et al., 2004; Teger et al., 2002; Valtchev et al., 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003). Thus, the security threats in the internal network include those derived from both wired networks and wireless networks.

Smart Home networks can be organized into three categories: existing wired networks, new wired networks and wireless networks (Figure 3). Existing wired networks reuse the existing inhome wiring, which consists of electrical wiring, telephone wiring and coaxial cabling, to transfer data. New wired networks require special cabling to distribute high-speed data and video throughout the dwelling. Finally, wireless networks use the air as transmission medium and offer solutions with “no wires” requirements (Teger et al.,

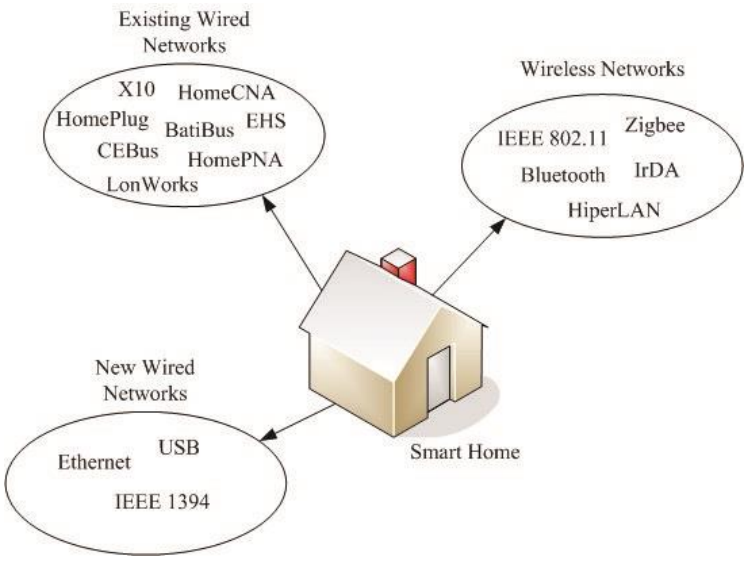


Figure 3. Smart home networking technologies

2002; Valtchev et al., 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003).

Wired networks provide more security compared to wireless networks, since they cannot be as easily tapped. It is easy for an adversary to intercept the signal or to disturb the normal operation of a wireless network, because of the fact that wireless technologies cannot control the transmission range. Furthermore, the dynamism and mobility provided by wireless networks yield more chances for adversaries to exploit vulnerabilities of the network invisibly (Schwiderski-Grosche et al., 2004; Komninos, Vergados, & Douligeris, 2007c; Krishnamurthy, Kabara, & Anusas-amornkul, 2002; Zahariadis, 2003; HGI, 2006).

Existing Wired Networks

Existing wired network technology is directly applicable to new and old houses as rewiring of the buildings is not required. The major limitations of this networking technology include the networks' structure and the interference from the original operation of the network. Based on existing wiring of a home, Powerline networks, Phoneline networks as well as Coaxial networks can be developed to satisfy the needs of the household members (Jiang et al., 2004; Teger et al., 2002; Valtchev et al., 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003).

Powerline Networks

Powerline networking makes use of the existing electrical wiring, which is already used to provide power to home appliances and lights. The main target of Powerline networking is to connect devices to each other and to Internet plugging them directly into AC wall outlets in a Smart Home. However, based on the current Powerline technologies, we need to add an adapter to each device before it is plugged into an outlet. Currently Powerline networks support low speed connections (50 Kbps to 350 Kbps) because of the small bandwidth capacity of the wire. Thus, in a Smart Home Powerline networking can be used in Home Appliances, Lighting and Climate Control system as well as Home Security system for applications with low data rate requirements. Furthermore, new modulation techniques and technologies have increased the data rate of Powerline networks enabling them to support multimedia applications such as audio and video streaming in a Smart Home (Paruchuri, Durresi, & Ramesh, 2008). However, there is possibility that the transmitted signal over the power line network leaks out of the Smart Home environment through the leaked electromagnetic wave from the electric power line. Thus, blocking filters which block off the high frequency ingredient of the signal should be installed in the power line communication network (Nishi, Morioka, & Sakurai, 2005). The main communication protocols for Powerline networks are HomePlug, X10, BatiBus, CEBus, LonWorks, and EHS (Jiang et al., 2004; Teger et al., 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003).

HomePlug is the major standard for Powerline communication. It is a simple-to-use, Ethernetclass standard and is created by the HomePlug Powerline Alliance. There are four versions of HomePlug standard. The first version, HomePlug 1.0, supports connections with data rate at 14Mbps. The second version, HomePlug 1.0 Turbo, runs at 85Mbps. The third version, HomePlug AV designed for HDTV and VoIP applications runs at 189Mbps. Finally, the last version, HomePlug Command and Control, operates at low data rate and is suitable for applications of Home Appliances, Lighting and Climate Control system (Adams, 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003).

Furthermore, HomePlug AV protocol forms virtual private LANs using cryptographic isolation. When a virtual private network is formed, a Network Membership Key (NMK) is

distributed to all station of this network. The distribution of the NMK to all stations may take place with three ways. In the first way, NMK can be provided to each station by he host directly. In the second way, it can be distributed using the Device Access Key (DAK). In the third way, it can be passed using the Unicast Key Exchange protocol.

The possession of the NMK defines each station in the network. Furthermore, another key, called Network Encryption Key (NEK), is used in this network. This key is changed periodically for security reasons. The controller of the network distributes the NEK, which is encrypted using the NMK, to all stations. The encryption which is applied is 128-bit AES to ensure that the data streams cannot be eavesdropped. Each station uses the NEK to encrypt the payloads of the data that sends in the network (Paruchuri et al., 2008).

Phoneline Networks

Phoneline networking provides an easy and inexpensive way to connect devices for sharing data, peripherals and a high-speed Internet access throughout a Smart Home using the registered phone jacks and the existing in-home telephone cabling without affecting the telephone service. Phoneline networking requires the installation of a network adapter, which supports the phone-line protocols, to each device that the user wants to connect to the Phoneline network. Then, the user connects the network adapter of the device to the telephone outlet with a standard telephone cable. In contrast to Powerline networks and coaxial networks which require physical isolation or data encryption to prevent eavesdropping, Phoneline networks do not use any method for ensuring security as they are not shared (Björklund, 2007).

HomePNA is the main industry standard for Phoneline networking and provides an additional communication channel over the existing telephone line (Jiang et al., 2004; Teger et al., 2002; Valtchev et al., 2002; Zahariadis, 2003). HomePNA is an Ethernet-based standard and is developed by the Home Phoneline Networking Alliance. Recently, there are a lot of vendors that comply with this standard. There are three versions of HomePNA, the HomePNA 1.0 providing data rate at 1Mbps, the HomePNA 2.0 running at 10Mbps and the HomePNA 3.0 operating at 100 Mbps. Therefore, Phoneline networks can handle applications of Home Communication system and Entertainment system that include applications with high data rate requirements (Adams, 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003).

Coaxial Networks

Coaxial networking makes use of coaxial cabling which is normally used for distribution of radio and TV signal in a residence. Coaxial networks are characterized by large bandwidth capabilities and can support applications of Home Communication system and Home Entertainment system (Teger et al., 2002; Valtchev et al., 2002; Zahariadis, 2003; HGI, 2006). The major standard for this technology is HomeCNA, which is developed by the Home Cable Network Alliance. However, Coaxial networking represents the minority of in-home networks for existing buildings because of small use of coaxial cabling (Adams, 2002; Zahariadis, 2003; Delphinanto, 2003). In Coaxial networks, physical isolation as well as encryption are required to avoid eavesdropping on network traffic (Björklund, 2007).

New Wired Networks

New wired networks or structured wiring networks provide high performance connectivity and high reliability. Thus, this type of in-home networks can support applications of Home Communication system, Home Entertainment system and Home Security system. The main disadvantage of new wired networks is that they can not be installed or extended easily in an existing home or apartment because of their wiring requirements. Running new data cables inside the walls of an existing brick or stone home is not an affordable solution. However, it is a good idea to run the wiring throughout the house while it is being built. The most common communication standards of new wired networking are Ethernet, IEEE 1394 and USB (Jiang et al., 2004; Valtchev et al., 2002; Zahariadis, 2003; HGI, 2006).

Ethernet or IEEE 802.3 is the most widespread wired-LAN standard for PCs and workstations. Ethernet is a mature technology characterized by simplicity in installation and configuration. This standard can support a plethora of services such as TCP/IP based data, voice and video applications in a Smart Home and is supported by a lot of vendors. In 1985, the first version, Ethernet (10Base), was defined and run at a data rate of 10Mbps. After ten years, the second version, Fast Ethernet (100Base), was published and run at 100Mbps. The third version, Gigabit Ethernet (10000Base), works at 1Gbit/s. Finally, the last version, 10Gigabit Ethernet, operates at 10Gbit/s (Adams, 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003).

Ethernet has a number of vulnerabilities that affect the network security. The main weakness is the fact that all stations in a local network share the same physical channel. Thus, an attacker can easily eavesdrop on transmitted traffic as what a station sends over the network can be received simultaneously by all the other stations of the network. Furthermore, Ethernet standard does not provide any mechanism for verification of message sender's identity or verification of message integrity. Therefore, an adversary can generate fraudulent data and insert them in the network traffic or he/she can obtains messages that are being exchanged between two legitimate communicating parties and retransmit them later as an authorized entity. These two weaknesses can be addressed dividing the Ethernet LAN in the Smart Home into sub-networks using bridges (Khoussainov & Patel, 2000).

Wireless Networks

Wireless networking is a very attractive solution for Smart Home networking providing simple installation, high flexibility and high data rate. Additionally, wireless networking does not include the cost of rewiring as well as the challenges of the existing wiring networks. What is more, wireless networks can be expanded easily in a home environment according to household members' needs. Wireless networks are used to satisfy requirements for mobility, ad hoc networking, relocation as well as coverage of areas hard to wired local area networks. Consequently, there are many applications areas for wireless networks. However, wireless networks sometimes have line-of-sight requirements and limited coverage. They can be used in all types of Smart Home systems, from Home Appliances, Lighting and Climate Control system to Communication, Entertainment and Security systems. There are a lot of residential wireless networking standards but the most dominant are IEEE 802.11, Bluetooth (IEEE 802.15.1), Zigbee (IEEE 802.15.4), and HiperLAN (Ricquebourg et al., 2006; Jiang et al., 2004; Teger et al., 2002; Valtchev et al., 2002; Adams, 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003).

IEEE 802.11

IEEE 802.11 is a set of standards and is considered as the most widespread standard for wireless local area networks worldwide. In 1999, IEEE published 802.11a and 802.11b. IEEE 802.11b is the slowest and least expensive

standard. In 2002, 802.11g was published to extend the IEEE 802.11b data rates to 54Mbps operating in the 2.4GHz band. Its range is around 50 meters. Right now, 802.11g is the most popular flavor of 802.11 for in-home networks because of its speed and reliability. Finally, IEEE 802.11n is the newest standard that is widely available and improves speed (140 Mbps) and range, but, it still in draft form (Adams, 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003).

Security in IEEE 802.11 standards is provided using Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WEP was the first security mechanism providing confidentiality, access control and data integrity in wireless communication. WEP uses RC4 encryption algorithm to protect the transmitted data. However, WEP is the most unsecured mechanism of these three, as it has a number of vulnerabilities. Transmitted packets can be easily captured and forged by attackers. Furthermore, WEP uses static keys which are rarely changed by users. WPA is a security mechanism created in response to the known serious weaknesses of WEP. WPA is a subset of the 802.11i standard. Similar to WEP, WPA uses RC4 as its encryption method. However, the strongest of these three security mechanisms is WPA2 which is based on the full 802.11i standard. This mechanism uses Advanced Encryption Standard (AES) as encryption method and provides better security than WEP and WAP (Krishnamurthy et al., 2002; Björklund, 2007; Komninos & Mantas, 2009).

Bluetooth

Bluetooth (IEEE 802.15.1) is an open standard specification that enables short-range (10cm – 10m) wireless connections for a wide range of portable and/or fixed devices. The older Bluetooth 1.0 has a maximum data rate at 1 Mbps while the newest Bluetooth 2.0 can handle up to 3Mbps. Bluetooth enabled devices communicate through short-range, ad hoc networks called piconets. Piconets are established dynamically and automatically as Bluetooth devices enter and leave radio proximity. Furthermore, Bluetooth technology supports both data and voice transmission simultaneously (Ricquebourg et al., 2006; Adams, 2002; Zahariadis, 2003; HGI, 2006; Delphinanto, 2003).

Bluetooth implements several authentication and data encryption mechanisms to provide security. The Bluetooth authentication scheme uses a challenge response method. The Bluetooth encryption scheme encrypts the payloads of the transmitted packets using a stream cipher E_0. Furthermore, any pair of Bluetooth enabled devices that desire to communicate with each other should generate a session key, called link key, using a combination of an initialization key, the device MAC address and the Personal Identification Number (PIN). However, Bluetooth has a number of weaknesses which can be exploited by adversaries to obtain keys and the PIN numbers, depending on how session initialization of the communication standard is performed (Krishnamurthy et al., 2002; Hager & Midkiff, 2003).

Zigbee

Zigbee (IEEE 802.15.4) is a wireless standard of data transmission allowing the communication of device to device with low cost as well as low data rates and low power consumption. It replaces wired solutions with low data rates requirements. Zigbee can operate at 2.4 GHz with a basic bit rate of 250Kbps. Zigbee is suited for house-oriented applications such as applications of Home Appliances, Lighting and Climate Control system as well as Home Security system (Ricquebourg et al.,

2006; Adams, 2002; HGI, 2006; Delphinanto, 2003).

Zigbee security is based on a centralized infrastructure providing a central control on security of the network. There is a centralized trust entity that is trusted by all nodes in the network and is responsible for distribution of keys and admission control of nodes requesting to access to the network. Each network can not have more than a single centralized trust entity and each device can be associated to only one centralized trust entity. However, this entity can be considered as a single point of failure and can be a security vulnerability of the network which can be exploited by malicious attackers.

Furthermore, Zigbee standard proposes three types of keys; link key, network key and master key. Link key is shared between any two devices and is used to secure their communication. Network key is a common key for all devices and is shared among all devices in the network. Network key is used to secure all broadcast communications in the network. Master key is pre-installed or derives from the centralized trust entity and is used to generate the link keys.

Additionally, Zigbee standard provides data freshness, data integrity, authentication and encryption. Data freshness is achieved using counters which are reset every time a new key is generated. Data integrity is provided by Message Authentication Codes. Network level authentication and device level authentication are provided using the common network key and the link keys respectively. Finally, Zigbee proposes 128-bit AES encryption using the common network key for network encryption and the link keys for device encryption (Baronti et al., 2007).

HiperLAN

HiperLAN is a wireless LAN standard published by European Telecommunications Standard Institute (ETSI). There are two versions; HiperLAN 1 and HiperLAN 2. HiperLAN 1 was published in 1996 and its maximum data rate is 23.5Mbps. HiperLAN 2 was published in 2000 and can handle up to 54Mbps data rate. The basic services that two versions can support are data, audio and video transmission (Zahariadis, 2003; Delphinanto et al., 2003).

HiperLAN uses schemas for mutual authentication of mobile devices, encryption of data and exchange of encryption keys. HiperLAN standard proposes five authentication mechanisms based on the challenge response approach providing mutual authentication between mobile devices and the access point. Furthermore, HiperLAN uses the DES and 3DES algorithms for data encryption. Finally, the exchange of encryption keys is based on the Diffie-Hellman protocol. In spite the fact that HiperLAN has several relatively strong security mechanisms, there are a lot of vulnerabilities (Casole, 2002).

SECURITY REQUIREMENTS IN SMART HOME

Having presented the concept of a Smart Home and described the networking technologies used to implement its systems, the security requirements for a Smart Home environment are identified. The main security objectives that a Smart Home environment must fulfil are Confidentiality, Integrity, Authentication, Authorization, Non-repudiation and Availability (Jeong et al., 2006; Herzog et al., 2001; Kim et al., 2007; Schwiderski-Grosche et al., 2004; Kangas, 2002; He, 2002; Bergstrom et al., 2001; Komninos et al., 2007c).

Confidentiality is concerned with preventing unauthorized access to certain information. In an attack at confidentiality, an adversary may use services providing information about the Smart Home's status in order to enable indirect surveillance of resident's activities in a Smart Home environment (Komninos et al., 2007a; He, 2002; Bergstrom et al., 2001; Komninos et al., 2007c; Krishnamurthy et al., 2002). Confidentiality can be achieved using

symmetric cryptographic ciphers (i.e. block or stream ciphers).

Integrity is a security service that provides prevention of unauthorized modification of information. Integrity ensures that data have not been changed, destroyed or lost during any process, such as transfer, storage or retrieval. In other words, Integrity ensures that data are consistent and correct. Integrity can be compromised by a malicious attacker who eavesdrops on the traffic to or from the internal network of a Smart Home and tampers data. Integrity can be provided using a Message Authentication Code (MAC) (Herzog et al., 2001; Bergstrom et al., 2001; Komninos et al., 2007c; Krishnamurthy et al., 2002).

Authentication is a security service related to verification of an entity based on a password or a shared secret key between the communicating parties. Authentication allows one entity to verify the identity of another entity. There are two types of authentication; entity authentication and message authentication. Entity authentication verifies the validity of the claimed identity of each entity. In other words, entity authentication confirms the identities of communicating parties. On the other hand, message authentication verifies that a message derives from the claimed entity. In a Smart Home environment, a lot of authentication mechanisms are required for user-to-device, userto-internal network, device-to-device, deviceto-internal network and user-to-service provider authentications. An adversary may pretend to be another legitimate user or entity in order to obtain critical information regarding home users or access Smart Home environment services (Jeong et al., 2006; Komninos et al., 2007a; SchwiderskiGrosche et al., 2004; Bergstrom et al., 2001; Komninos et al., 2007c; Krishnamurthy et al., 2002; Komninos & Mantas, 2009).

Authorization is the process that determines the user's access rights on a device or a network resource and what a device is allowed to do within the Smart Home environment. Authorization can also provide different access levels to guarantee that entities can only access and perform operations on network resources that they are authorized for. The devices of the Smart Home internal network can be categorized into two types; home devices and foreign devices. Regarding the home devices, the authorization mechanism is based on home user's access rights on the devices. Regarding foreign devices, the owner of each device delegates certain access rights to foreign users who have to pay when they wish to use them. However, an adversary can use forged authorizations to perform prohibited actions in a Smart Home environment (Schwiderski-Grosche et al., 2004; Bergstrom et al., 2001; Komninos et al., 2007c; Krishnamurthy et al., 2002).

Non-repudiation corresponds to a security service providing protection against denial of involvement in an action. For instance, Nonrepudiation prevents both sender and receiver from denying of a transmitted message or access to services. This service is similar to a signature by the author or recipient of a document in real life. Furthermore, this service can not prevent an entity from repudiating having performed a particular action. However, it can provide proof (i.e. proof of commitment, resource use, obligation, data origin) that can be stored and used later by a trusted third party in order to resolve disputes that arise in cases that an action is repudiated by one of the entities participated in the action. Non-repudiation can be provided using digital signatures based on public key encryption cryptosystems (Schwiderski-Grosche et al., 2004; He, 2002; Komninos et al., 2007c; Krishnamurthy et al., 2002; Stallings, 2005).

Availability ensures that network services and resources (i.e. bandwidth) are available and protected against events impacting the network such as malicious

attacks. Especially, the Smart Home internal network is exposed to direct denial of service attacks, since it is exposed to Internet directly. What is more, disaster recovery solutions are included in this service since the internal network is exposed to a variety of attacks that lead to the loss or reduction of availability (He, 2002; Komninos et al., 2007c; Krishnamurthy et al., 2002;).

FACTORS AFFECTING THE SECURITY IN SMART HOME

Security is a crucial and critical issue in a Smart Home environment. Many home users are concerned about unauthorized access into their home and about privacy of their data. However, it is not a trivial task to provide security in the Smart Home environment because of its heterogeneous nature, dynamic nature, the fact that it is always connected to Internet as well as the open security back doors derived from the household members (Jeong et al., 2006; Herzog et al., 2001; Thomas & Sandhu, 2004; Wang et al., 2005; Haque & Ahamed 2006; Schwiderski-Grosche et al., 2004; He, 2002; Ziegler, Mueller, Schaefer, & Loeser, 2005).

Smart Home internal network is an extremely heterogeneous network since it consists of a vast range of different devices, applications and communication technologies as we have already described. In a Smart Home, there are many devices such as light switches, white appliances, sensors, cameras, TVs, phones, PCs, and PDAs, with very different capabilities and requirements, and communicate with each other via wired and wireless networks (Wang et al., 2005; Schwiderski-Grosche et al., 2004; Ziegler et al., 2005). Consequently, the deployment of security mechanisms depends on the device capabilities and requirements. The capabilities of devices vary widely in terms of memory storage, battery power and computational capability (Haque & Ahamed 2006; Krishnamurthy et al., 2002). There are devices such as PCs that can easily handle complex computations and support security features. However, there are devices such as the handset of a cordless phone that they do not have the appropriate computational power because of their limited resources (i.e. memory storage, battery power and computational capability). These devices usually provide no protection or they may able to support only simple security mechanisms (Krishnamurthy et al., 2002). Thus, exploiting these devices, intruders can compromise residential networks. Furthermore, not all devices require the same level of security. It can vary from low level to high level. Different security mechanisms should be implemented depending on the requirements of each device.

Moreover, the applications supported of Smart Home Systems are also diverse. There are applications that support different types of data such as audio, video signals and low date rate sensor information, with different features. Thus, each application has security schemes that should be optimal for it. Applications that support high data rate services (e.g. multimedia applications) require security mechanisms that do not increase delay or jitter. On the other hand, applications that support low data rate services (e.g. over a sensor network) can be constrained to use complex security schemes because of power consumption (Haque & Ahamed 2006; Schwiderski-Grosche et al., 2004; Krishnamurthy et al., 2002).

Additionally, having presented the Smart Home networking technology in section “Smart Home Networking Technology”, it is clear that the internal network of a Smart Home is a completely heterogeneous network which integrates a number of different communication technologies. Each of Smart Home networking technologies has its own features and security weaknesses. For instance, wireless technologies can be easily tapped because of their broadcast nature. An attacker can intercept the signal or disturb the normal operation of a wireless communication.

On the other hand, wired technologies provide higher levels of security inherently.

In a Smart Home environment, there are also a lot of wireless devices, supporting a wide range of services, which join and leave the internal network completely arbitrarily, forming an extremely volatile ad hoc subnetwork. This ad hoc subnetwork is extremely dynamic and changes from time to time. Thus, the topology of the internal network is dynamic, which means that the required security mechanisms should be reconfigured dynamically every time that the topology is changed without home user's intervention (Thomas & Sandhu, 2004; Wang et al., 2005; Haque & Ahamed 2006; Schwiderski-Grosche et al., 2004; Krishnamurthy et al., 2002). Otherwise, the internal network suffers from several security vulnerabilities. However, the deployment of security mechanisms in an ad hoc network is a challenging issue because of its inherent dynamic nature. Thus, the security solutions regarding the ad hoc networking should be based on dynamic security mechanisms with sufficient intelligence in order to prevent security breaches.

Additionally, the expansion of the Smart Home internal network to the outside world via Internet creates many network security problems, as it is exposed to a variety of cyber attacks such as DoS attacks, malicious software, eavesdropping and so on (Jeong et al, 2006; Herzog et al., 2001; Kim et al., 2007; Kangas, 2002; Bergstrom et al., 2001). In contrast to dial up connections to Internet, Smart Home high-speed connections provide constant connectivity to Internet, which implies static IP address. The fact that the IP address does not change makes the internal network to be easily hacked, since attackers have a lot of time to guess the IP address and hack the connected devices (Herzog et al., 2001). Moreover, the internal network is subjected to all legacy security attacks of an open network since it is accessible from Internet.

First of all, malicious attackers can cause havoc in a Smart Home environment as they can intercept and modify remotely transmitted messages of networks (i.e. Powerline network, Phoneline network, wireless networks) that comprise the internal network of the Smart Home. Furthermore, malicious attackers might compromise the internal network and use it to launch attacks against other networks covering their tracks. Adversaries can also use the computing power and the resources of the compromised internal network for Denial of Service attacks against other Internet nodes. Furthermore, adversaries might gain access over Internet to confidential information of the household members eavesdropping on their Internet traffic. For example, sniffing messages of e-banking transactions, adversaries can get credit card numbers or they can learn about the behavior of the household members. Also, they can get the locking mechanism password of the home in order to burglarize it (Herzog et al., 2001; Bergstrom et al., 2001).

Thus, due to the heterogeneity of devices, applications and communication technologies in a Smart Home environment, the dynamic nature of the Smart Home internal network as well as the fast permanent connection to the outside world, there is not a single security solution that is able to provide all required security services in order to decrease the risk of security attacks. Consequently, the challenges for security insurance can be addressed with a diversity of security mechanisms, protocols and services that should be integrated and managed in the Smart Home internal network.

Finally, the household members are another factor that makes a Smart Home environment vulnerable to a rich variety of security threats. Most of the household members are usually nonprofessionals in networking as well as network security field. However, they usually build the internal network without participation of security professionals. Thus, there are always security weaknesses in the internal network which can be exploited by intruders. Additionally, household members often abuse their privileges

raising many security issues. Furthermore, in many cases, home users consider that the appropriate security measures are complicated and they are not willing to follow them because of low usability. Besides, there are cases that residents do not use security protection or follow security policies because either they do not care about security or they are not able to understand completely the threats that they are faced with (Thomas & Sandhu, 2004; Wang et al., 2005; He, 2002).

SECURITY THREATS IN SMART HOME

Smart Home security threats can be derived from the factors described in section "Factors Affecting the Security in Smart Home" and they usually attempt to compromise one or more of the security requirements for a Smart Home environment presented in section "Security Requirements in Smart Home". These threats are mainly classified into internal and external threats.

Internal Threats

Internal threats stem from within the trusted Smart Home internal network. However, they are not given the attention they deserve compared with external attacks. Internal threats can be derived from inappropriate network construction and configuration, incomplete security plan and software pitfalls.

Inappropriate Smart Home internal network construction and configuration of network enabled devices create many security breaches in a Smart Home environment. It is very important the professional design and implementation of the internal network. Additionally, it is a very critical issue the correct configuration and set up of network devices (e.g. servers), user devices (laptops, PDAs) and firewalls. Otherwise, a wrongly configured device can raise security risks. However, for a nonprofessional home user, the correct construction and configuration can be an extremely difficult and daunting task.

Furthermore, there are not complete security policies in a Smart Home environment. Any home user (young children, people lacking security skills) is allowed to use any device and access any service. Besides, any resident can change the Smart Home internal network since he\she can modify the configuration of network equipment, add or remove network devices from the internal network as well as install or uninstall software of network devices. Additionally, the security features of the Smart Home environment can be modified intentionally or unintentionally by any home user. Also, there are cases that the home users abuse their privileges (e.g. frequently changing systems' settings, downloading uncertified software). Thus, a lot of security holes for intruders can be raised when the home user does not follow security policies properly. Finally, another fact that poses many security threats to the internal network is the use of software with security pitfalls (Wang et al., 2005; He, 2002).

External Threats

Smart Home internal network is subject to a lot of security threats derived from outside malicious nodes. The types of the external threats are classified based on the way the information is compromised. There are two generic types of threats: passive and active attacks.

In passive attacks, the intruder intends to gain unauthorized access to information that is being transmitted without modifying it. The detection of passive attacks in a communication is not easy, since the intruder does not change the messages that are being exchanged between the sender and the receiver. Passive attacks can be either eavesdropping or traffic analysis (He, 2002; Komninos et al., 2007c, Stallings, 2005). These two passive attacks are described below.

Eavesdropping allows an intruder to monitor the home user traffic (e.g. telephone

conversation, email message) between the Smart Home internal network and the outside world without the consent of the communicating parties. This traffic may contain confidential information that the residents do not want to disclosure it to unauthorized third parties. Eavesdropping is the most widely identified security problem in open networks and is an attack on confidentiality of the Smart Home internal network.

Traffic analysis is a subtler passive attack as it allows an adversary to deduce information observing the traffic pattern of a communication that is taking place between one communicating party located in the Smart Home environment and one located in the outside world. Using traffic analysis, the adversary is able to infer sensitive information (e.g. home user's location, passwords) from the messages that are being exchanged even when they are encrypted and they can not be decrypted. In traffic analysis attack, the greater the number of observed messages, the more information can be extracted.

In active attacks, the adversary intends to tamper the information or generate fraudulent data into the Smart Home internal network. Active attacks can result in severe losses for the home users. The main types of active attacks are masquerading, replay, message modification, denial of service and malicious codes (He, 2002; Komninos et al., 2007c, Stallings, 2005).

In masquerading attack, an intruder gains certain unauthorized privileges pretending to be another legitimate user or entity. The intruder may impersonate an authorized home user or entity and access to the Smart Home internal network remotely in order to get sensitive information or obtain services. This attack is often combined with others attacks such as replay attack.

In replay attack, an adversary firstly obtains messages that are being exchanged between two legitimate communicating parties and retransmit them later as an authorized entity. The adversary may capture a copy of a valid service request sent from a device in the Smart Home environment, store it and then replay it in order to access the service that the home user is authorized to.

Message modification takes place when an unauthorized entity modifies contents of a legitimate message by deleting, adding to, or changing it. Furthermore, in this attack, an adversary can also create delays to some messages or change their order producing unauthorized effect. Message modification can take place when an adversary intents to hijack the communication between two authorized entities, alter a software so that it performs maliciously or change values in a data file. This attack can result in a DoS attack and is an attack on integrity.

Denial of service attack is used in cases that an adversary intents to make a network unavailable to users or reduce the availability of network services. The adversary can send countless messages to the Smart Home internal network in order to overload its resources with traffic. Thus the authorized users are not able to access the services of the home network. Additionally, the adversary can send a tremendous amount of messages to servers and devices connected to Internet so as to block the internal traffic transmitted via wired or wireless networks inside the Smart Home.

Malicious codes are software threats that cause adverse affects to the Smart Home internal network exploiting its vulnerabilities. Malicious codes are used to modify, destroy or steal data as well as allow unauthorized access. Malicious codes can be classified into two categories. The first category includes those (i.e. Trap doors, viruses, logic bombs and Trojan horses) that need a host program. They are parts of programs that can not exist independently of some actual application software. The second category consists of those (i.e. worms and zombies) that are self-contained programs and can be scheduled and run by the operating system.

Furthermore, malicious codes can be categorized on those that do not replicate and those that do. The former are parts of programs that are to be activated when the host program is invoked in order to perform a specific function. The latter contains parts of programs or independent programs that when they are executed they produce one or more copies of themselves in order to be activated later on the same system or another system.

Each of the malicious code has different threat to network security as they have their own characteristics. Malicious codes are distributed combining network communication and multiple attacking methods. They are distributed via emails, web pages, instant communication tools, software pitfalls, etc. The security threats of malicious codes have the highest risk in a Smart Home environment compared to corporation networks due to lack of home user's awareness about network security and data protection.

SECURITY TECHNOLOGIES FOR SMART HOMES

The most essential security technologies for making a Smart Home internal network secure are authentication and authorization mechanisms. Both mechanisms are required in order to restrict any malicious entity from accessing the Smart Home internal network. Furthermore, use of firewalls is another intrusion prevention mechanism that is important to increase security in Smart Home environment. However, intrusion prevention mechanisms alone are not sufficient for the Smart Home internal network because of its complexity and heterogeneity. Therefore, the use of intrusion detection systems (IDS) is also required.

Authentication Mechanisms

Authentication process includes entity authentication and message authentication. Entity authentication ensures the authenticity of the entity and message authentication verifies that the received message derives from the right sender. There are mechanisms for entity authentication as well as message authentication.

Entity authentication mechanisms support two processes; identification process and verification process. In identification process, an entity (e.g. home user) requests access to a network claiming a certain identity based on an identifier. The verification process is based on three approaches; proof by knowledge, proof by possession and proof by property (Kim et al., 2007; Kangas, 2002; Komninos & Mantas, 2008, 2009).

The proof by knowledge approach takes into consideration what the user knows. This approach usually checks a secret password or an identifier (ID) of the user that request access. The authentication mechanisms based on this approach called ID-password-based authentication mechanisms. The proof by possession approach depends on what the user possesses. This approach is based on the ownership of a smart card that should be connected during the login process. The authentication mechanisms that follow this approach called smart card-based authentication mechanisms. The proof by property approach is based on what the user is. In this approach, the verifier measures certain biometrics properties (e.g. fingerprint, iris, retina) of the user. The authentication mechanisms based on this approach called biometric-based authentication mechanisms.

Additionally, the entity authentication mechanisms can be divided into two categories; authentication mechanisms for intra-domain, and authentication mechanisms for inter-domain (Kim et al., 2007). In contrast to Intra-domain authentication mechanisms taking place in the Smart Home environment, inter-domain authentication mechanisms are applied out of the Smart Home environment. Authentication mechanisms for intra-domain include the authentication mechanisms based on proof by knowledge, proof by possession and proof by property approaches.

However, authentication mechanisms for interdomain include the authentication mechanisms based on proof by knowledge and proof by possession approaches. Authentication mechanisms using biometric information are not used for inter domain authentication. It happens because once biometric information is disclosed to malicious attackers the user can not exchange the exposed biometric information for new one as the modification of human body is very difficult. Thus, it results in serious privacy violation in cases that biometric information is revealed. Consequently, it is not logical to use biometric-based authentication mechanisms in applications that require biometric information to be transferred over Internet (Kim et al., 2007; Yun-kyung, Hong-il, & Hyung-kyu, 2006).

Message authentication mechanisms are achieved using public key cryptosystems and digital signatures (Kangas, 2002). In public key cryptosystems, each communicating party has a pair of keys. One is used for encryption and the other for decryption. The key used for encryption is known to everyone and is referred to as public key. On the other hand, the key used for decryption remains secret and is known as private key. The private key and the public key are related mathematically. But, the private key can not be derived from the public key in a reasonable amount of time. In public key cryptosystems, the sender encrypts a message with the recipient's public key and only the entity (i.e. recipient) with the corresponding private key can decrypt the encrypted message (Stallings, 2005). Furthermore, digital signatures are used in public key cryptosystems. Digital signatures are produced using sender's private key. A message signed with sender's private key can be verified by the entity that knows the sender's public key.

In a Smart Home Environment, the authentication mechanism challenges the home user to provide his unique information (e.g. password, smartcard, fingerprint). If the authentication mechanism can verify that the shared secret was presented correctly, the home user is authenticated directly. Furthermore, a home user is required to be authenticated only one time to access any network resource or service. If the authentication does not succeed, this leads to rejection or termination of the access and the creation of a report to a security management center. Furthermore, there are cases that the home user desires to access a remote application server which performs its own authentication. In these cases, the user is identified by the residential gateway and it does the required authentication with the remote server instead of the user. It is happens because the residential gateway has an authentication mapping function, which achieves mapping between authentication mechanisms for intra-domain and authentication mechanisms for inter-domain (Kim et al., 2007).

Authorization Mechanisms

The purpose of authorization is to control the authenticated entity's access rights on network services and resources. Additionally, authorization contributes to reduce the harmful consequences of exposure to malicious accesses. Thus, authorization mechanisms are used to determine what level of access a particular authenticated entity should have on network services and resources in a Smart Home environment. For authorization within the Smart Home internal network, the existing authorization mechanisms can be used. The existing authorization mechanisms can be classified into three categories; server-based authorization mechanisms, peer-to-peer authorization mechanisms and certificate-based authorization mechanisms (Kim et al., 2007; Kangas, 2002).

Server-based authorization mechanisms are used in client-server communication model. In this mechanism, the server generates and keeps authorization rules.

Server-based authorization mechanism is the simplest authorization mechanism.

Peer-to-peer authorization mechanisms are based on peer-to-peer communication service model. In this mechanism, a peer manages the authorization rules or requires help of a designated authorization server. This mechanism is more complicated than the server-based authorization mechanism because of a number of constraints such as database maintenance and hardware specifications of peer's machine.

Finally, certificate-based authorization mechanisms refer to authorization infrastructures, where Authorization Certificates (ACs) are used for authentication and access control simultaneously. AC establishes authorization access rights between a subject and a resource (Kim et al., 2007; Kangas, 2002; Stallings, 2005).

All the above three categories of authorization mechanisms use an Access Control List (ACL) schema or a Role-based Access Control (RBAC) schema. Access Control List (ACL) schema includes a list of permissions attached to an object. ACL establishes relationships between subjects (i.e. entities) and objects (i.e. resources). ACL determines the entity allowed to access the object and what operations are allowed to be performed on the object. ACL schema defines access rights of entities to the resources in terms of write, read and execute permissions. First of all, when an entity requests to perform an operation on an object, the list is checked in order to decide whether to proceed with the operation or not. ACL schema includes two models; discretionary and mandatory. In discretionary access control model, the owner of an object is able to have full control access to the object. In mandatory access control model, the authorization mechanism enforces restrictions that override the permissions stated in the ACL. Role-based Access Control (RBAC) schema is a newer alternative approach to discretionary access control model and mandatory access control model. In Role-based Access Control (RBAC) schema, an intermediate component, called role, is used between a subject and a resource (Kim et al., 2007; Kangas, 2002; Stallings, 2005).

Intrusion Prevention: Firewalls

A firewall is a hardware device or software running on another device which inspects the information passing through it in order to prevent unauthorized Internet entities from accessing private networks connected to Internet. A firewall examines all network traffic entering or leaving the private network and blocks the network traffic that does not conform to a defined set of rules based on security criteria (Stallings, 2005; HGI, 2006).

The firewall techniques used in order to control the network traffic are packet filtering, proxy service and stateful inspection. In packet filtering method, firewall analyzes packets, entering or leaving the private network, against a set of filters and accepts or discards them based on user-defined rules. Firewall provides a private network with the capability to perform coarse-grain filtering on IP and TCP/UDP headers, including IP addresses, port numbers and acknowledgment bits. However, in this method it is difficult for the user to configure the firewall. Furthermore, this method is vulnerable to IP spoofing attack.

In proxy service method, firewall retrieves all information entering and leaving the private network and then sends it to the requesting entities. Thus, firewall hides the true IP addresses of the private networks devices from malicious adversaries.

In stateful inspection method, firewall monitors the state of network connections (i.e. TCP, UDP) passing across it and stores information (i.e. IP addresses, ports sequence numbers, etc.) about them in a state table. Thus, filtering decisions are based on the information that has been stored based on the prior packets that have passed through the firewall. Firewall is able to distinguish legitimate packets for different types of connections. Thus, only packets matching a known connection state are accepted by the firewall. However, firewalls that follow the stateful inspection technique are not very efficient for applications that include

IP addresses and TCP/UDP port information in the payload. To have higher level of security, firewalls should combine packet filtering with application gateways. Application gateways recognize the specific packets and analyze their payloads in order to obtain the required information and make policy decisions (Stallings, 2005; HGI, 2006).

All the above firewall techniques are not competitors. A Smart Home environment can employ all of them together to provide defence in depth. As we have already discussed in section "Smart Home Concept", the residential gateway is the official access point to the Smart Home internal network. All traffic transmitted from Internet to the internal network or to Internet from the internal network passes through the residential gateway. Thus, a firewall can be installed on the residential gateway in order to block all unauthorized accesses or suspicious data. The installed firewall monitors and analyzes all traffic between the internal network and Internet to decide whether it corresponds to the criteria of the Smart Home security policy.

Intrusion Detection

Intrusion detection is used as a second line of defence to protect the Smart Home internal network because once an intrusion is detected, a response can then take place to minimize damages. In case that an intruder succeeds in his attack over the Smart Home internal network, intrusion detection systems (IDS) can detect this attack and stop the activities of the intruder. In the Smart Home internal network, both Network-based IDS and host-based IDS can be used. Network-based IDS are used in wired networks where traffic monitoring takes place at switches, routers and gateways. However, host-based IDS are used in ad hoc networks where there are not such traffic concentration points. Host-based IDS are concerned with what is happening on each individual node of the ad hoc network (Komninos, Vergados, & Douligeris, 2007b; Komninos & Douligeris, 2009).

Intrusion detection techniques are classified into two categories; misuse detection and anomaly detection. Misuse detection technique requires audit data for analysis and compares these data to already known attack patterns stored in large databases. In cases that any comparison between the audit data and the known attack patterns results in a match, an intrusion alarm is set. The main advantage of misuse detection technique is the fact that it can accurately and efficiently detect instances of known attacks. However, this technique is not able to detect the newly invented attacks.

On the other hand, anomaly detection technique is based on statistical behaviour. Anomaly detectors look for behaviour that deviates from normal network activity. First of all, this technique requires the collection of audit data for analysis. Then, the audit data is transformed to a format statistically comparable to the profile of a user generated dynamically and updated based on the user's usage. In cases that any comparison between the audit data and the user's profile results in a deviation that crosses a set threshold, then an intrusion alarm is activated. The main advantage of anomaly detection technique is that it can detect unknown or new intrusion without requiring prior knowledge of the intrusion. The main disadvantage of this technique is that it may not be able to describe what the attack is (Stallings, 2005; Komninos & Douligeris, 2009).

CONCLUDING REMARKS

In this chapter, we have presented the concept of the Smart Home itself as well as its systems and the used networking technologies in order to perceive the security issues of Smart Homes. However, Smart Home security is of extreme

importance since it affects the privacy of the household members. Thus, a variety of important security issues in Smart Home environments were discussed. Especially, the security objectives of a Smart Home as well as the main factors that increase the level of difficulty to provide security in a Smart Home environment were described. Furthermore, the threats that intend to compromise the security requirements were examined. Finally, existing security mechanisms that provide security features in a Smart Home environment were presented.

In a lot of cases, most of the home users are not security-aware enough to realize the implications of Smart Home environments. However, the importance of Smart Home security is going to be raised in the future because of the increasing complexity and heterogeneity of the Smart Home internal networks and the increasing use of remote working habits of the home users. Thus, there are requirements that should take place in order to reduce the risks of security attacks in a Smart Home environment. First of all, the main requirements for ensuring security in a Smart Home environment are the correct network design and construction as well as the correct configuration of network devices (e.g. firewalls, servers etc.) by professionals in networking and network security. Furthermore, operating systems and application software should be installed or configured correctly. Moreover, the correct creation of complete security policies is obligated. Security policies specify the home user's privileges and responsibilities. Additionally, user's privileges should be restricted to avoid security breaches. Finally, the correct installation and use of a reliable virus defense system is required.

REFERENCES

Adams, C. E. (2002). Home area network technologies. *BT Technology Journal*, *20*(2), 53–72.

Baronti, P., Pillai, P., Chook, V. W. C., Chessa, S., Gotta, A., & Hu, Y. F. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee Standards. *Computer Communications*, *30*(7), 1655–1695.

Bergstrom, P., Driscoll, K., & Kimball, J. (2001). Making Home Automation Communications Secure. *IEEE Computer*, *34*(10), 50–56.

Björklund, H. F. (2007, March). *Wiring Devices and Technologies in Home Environment*. Paper presented at the TKK T-110.5190 Seminar on Internetworking.

Casole, M. (2002). WLAN security – Status, Problems and Perspective. In *Proceedings of European Wireless 2002*. Florence Italy.

Delphinanto, A., Huiszoon, B., Rivero, D.S., Hartog, F., Boom, H., Kwaaitaal, J., & Wijk, P. (2003). *Home Networking Technologies Overview and Analysis*. Residential Gateway Environment, Deliverable D3.1.

Friedewald, M., Da Costa, O., Punie, Y., Alahuhta, P., & Heinonen, S. (2005). Perspectives of ambient intelligence in the home environment. *Telematics and Informatics - Elsevier*, *22*(3), 221-238.

Hager, C., & Midkiff, S. (2003). An Analysis of Bluetooth Security Vulnerabilities. In *Proceedings of Wireless Communications and Networking Conference* (pp. 1825-1831). New Orleans, LA.

Han, I., Park, H., Jeong, Y., & Park, K. (2006). An Integrated Home Server for Communication, Broadcast Reception, and Home Automation. *IEEE Transactions on Consumer Electronics*, *52*(1), 104–109.

Haque, M., & Ahamed, S. I. (2006). Security in Pervasive Computing: Current Status and Open

Issues. *International Journal of Network Security*, *3*(3), 203–214.

He, G. (Spring 2002). *Requirements for Security in Home Environments*. Paper presented at Residential and Virtual Home Environments – Seminar on Internetworking, HUT TML Course T-110.551.

Herzog, A., Shahmehri, N., Bednarski, A., Chisalita, I., Nordqvist, U., Saldamli, L., et al. (2001). Security Issues in E-Home Network and Software Infrastructures. In *Proceedings of the 3rd Conference on Computer Science and Systems Engineering in Linköping* (pp. 155-161). Norrköping, Sweden.

Home Gateway Initiative (HGI) (2006). Home Gateway Technical Requirements: Release 1.

Jeong, J., Chung, M., & Choo, H. (2006). Secure User Authentication Mechanism in Digital Home Network Environments. In Sha, E., Han, S.-K., Xu, C.-Z., Kim, M. H., Yang, L. T., & Xiao, B. (Eds.), *Embedded and Ubiquitous Computing* (pp. 345–354). Springer.

Jiang, L. Liu, D., & Yang, Bo. (2004). SMART HOME RESEARCH. In *Proceedings of the Third International Conference on Machine Learning and Cybernetics* (pp. 659-663). Shanghai.

Kangas, M. (Autumn 2002). *Authentication and Authorization in Universal Plug and Play Home Neworks*. Paper presented at Ad Hoc Mobile Wireless Networks – Research Seminar on Telecommunications Software, HUT TML – Course T-110.557.

Khoussainov, R., & Patel, A. (2000). LAN security: problems and solutions for Ethernet networks. *Computer Standards & Interfaces*, *22*(3), 191–202.

Kim, G. W., Lee, D. G., Han, J. W., & Kim, S. W. (2007). Security Technologies Based on Home Gateway for Making Smart Home Secure. In Denko, M. (Eds.), *Emerging Directions in Embedded and Ubiquitous Computing* (pp. 124–135). Springer.

Komninos, N., & Douligeris, C. (2009). LIDF: Layered intrusion detection framework for adhoc networks. *Journal in Ad Hoc Networks*, *7*(1), 171–182.

Komninos, N., & Mantas, G. (2009). Intelligent Authentication and Key Agreement Mechanism for WLAN in e-Hospital Applications. In Feng, J. (Ed.), *Wireless Networks: Research Technology and Applications). Nova Science Publishers Inc*.

Komninos, N., & Mantas, G. (2008). Efficient Group Key Agreement & Recovery in Ad Hoc Networks. In *Proceedings of the 2nd IET International Conference on Wireless, Mobile & Multimedia Networks* (pp. 25-28). Beijing, China.

Komninos, N., Vergados, D., & Douligeris, C. (2007a). Authentication in a Layered Security Approach for Mobile Ad Hoc Networks. *Journal in Computers & Security*, *26*(5), 373–380.

Komninos, N., Vergados, D., & Douligeris, C. (2007b). Detecting Unauthorized and Compromised Nodes in Mobile Ad-Hoc Networks. *Journal in Ad Hoc Networks*, *5*(3), 289–298.

Komninos, N., Vergados, D., & Douligeris, C. (2007c). Multifold Authentication in Mobile Ad-Hoc Networks. *International Journal of Communication Systems*, *20*(12), 1391–1406.

Krishnamurthy, P., Kabara, J., & Anusasamornkul, T. (2002). Security in Wireless Residential Networks. *IEEE Transactions on Consumer Electronics*, *48*(1), 157–166.

Nishi, R., Morioka, H., & Sakurai, K. (2005). Trends and Issues for Security of Home-Network Based on Power Line Communication. In *Proceedings of the 19th*

International Conference on Advanced Information Networking and Applications (pp. 655-660).

Paruchuri, V., Durresi, A., & Ramesh, M. (2008). Securing Powerline Communications. In *Proceedings of the IEEE International Symposium on Power Line Communications and Its Applications* (pp. 64-69). Jeju city, Jeju Island.

Pohl, K., & Sikora, E. (2005). Overview of the Example Domain: Home Automation. In Pohl, K., Böckle, G., & van der Linden, F. J. (Eds.), *Software Product Line Engineering Foundations, Principles and Techniques* (pp. 39–52). New York: Springer.

Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Dalahoche, L., & Logé, C. (2006). The Smart Home Concept: our immediate future. In *Proceedings of the 1st IEEE International Conference on E-Learning in Industrial Electronics.*

Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops.

Valtchev, D., & Frankov, I., & ProSyst Software AG. (2002). Service Gateway Architecture for a Smart Home. *IEEE Communications Magazine*, 126–132.

Wang, J., Yang, Y., & Yurcik, W. (2005). Secure Smart Environments: Security Requirements, Challenges and Experiences in Pervasive Computing. In *Proceedings of NSF Pervasive Computing Infrastructure Experience Workshop.*

Yun-kyung, L., Hong-il, J., & Hyung-kyu, L. (2006). Secure Biometric Recognition method in Home Network. In *Proceedings of the 32nd Annual Conference of the IEEE Industrial Electronics Society* (pp. 3745-3749). Paris.

Zahariadis, T. B. (2003). *Home Networking Technologies and Standards*. New York: Artech House.

Ziegler, M., Mueller, W., Schaefer, R., & Loeser, C. (2005). Secure Profile Management in Smart Home Networks. In *Proceedings of the 16th International Workshop on Database and Expert Systems Applications.* Copenhagen, Denmark.

Schwiderski-Grosche, S., Tomlinson, A., Goo, S. K., & Irvine, J. M. (2004). Security Challenges in the Personal Distributed Environment. In *Proceedings of IEEE 60th Vehicular Technology Conference.* Los Angeles.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices*. Upper Saddle River, NJ: Prentice Hall.

Teger, S., & Waks, D. (2002). *System Dynamics Inc* (pp. 114–119). End-User Perspectives on Home Networking. IEEE Communications Magazine.

Thomas, R. K., & Sandhu, R. (2004). Models, Protocols, and Architectures for Secure Pervasive Computing: Challenges and Research Directions. In