# A Review on Security in Smart Home Development

Rosslin John Robles[1] and Tai-hoon Kim[1]

[1]*School of Multimedia, Hannam University, Daejeon, Korea*
*rosslin_john@yahoo.com, taihoonn@hannam.ac.kr*

### *Abstract*

*A smart home or building is a home or building, usually a new one that is equipped with special structured wiring to enable occupants to remotely control or program an array of automated home electronic devices by entering a single command. Conventional security systems keep homeowners, and their property, safe from intruders. A smart home security system, however, offers many more benefits. Home automation technology notifies homeowners of any problems, so that they can investigate. In this paper, we discuss smart home and security, we also review the tool related to smart home security.*

***Keywords:*** *Smart Home, Security, Automation, Protection*

## 1. Introduction

Smart homes connect all the devices and appliances in your home so they can communicate with each other and with you. Anything in your home that uses electricity can be put on the home network and at your command. Whether you give that command by voice, remote control or computer, the home reacts. Most applications relate to lighting, home security, home theater and entertainment and thermostat regulation. Security has been an important issue in the smart home applications. Conventional security systems keep homeowners, and their property, safe from intruders. A smart home security system, however, offers many more benefits. On the following chapters, we discuss smart home, smart home security and related tools in smart home security.

## 2. Smart Home Systems

A smart home or building is a home or building, usually a new one that is equipped with special structured wiring to enable occupants to remotely control or program an array of automated home electronic devices by entering a single command. For example, a homeowner on vacation can use a Touchtone phone to arm a home security system, control temperature gauges, switch appliances on or off, control lighting, program a home theater or entertainment system, and perform many other tasks. [1]

The field of home automation is expanding rapidly as electronic technologies converge. The home network encompasses communications, entertainment, security, convenience, and information systems. [1]

A technology known as Powerline Carrier Systems (PCS) is used to send coded signals along a home's existing electric wiring to programmable switches, or outlets. These signals convey commands that correspond to "addresses" or locations of specific devices, and that control how and when those devices operate. A PCS transmitter, for instance, can send a signal along a home's wiring, and a receiver plugged into any electric outlet in the home could receive that signal and operate the appliance to which it is attached. [1]

One common protocol for PCS is known as X10, a signaling technique for remotely controlling any device plugged into an electrical power line. X10 signals, which involve short radio frequency (RF) bursts that represent digital information, enable communication between transmitters and receivers.

In Europe, technology to equip homes with smart devices centers on development of the European Installation Bus, or Instabus. This embedded control protocol for digital communication between smart devices consists of a two-wire bus line that is installed along with normal electrical wiring. The Instabus line links all appliances to a decentralized communication system and functions like a telephone line over which appliances can be controlled. The European Installation Bus Association is part of Konnex, an association that aims to standardize home and building networks in Europe.

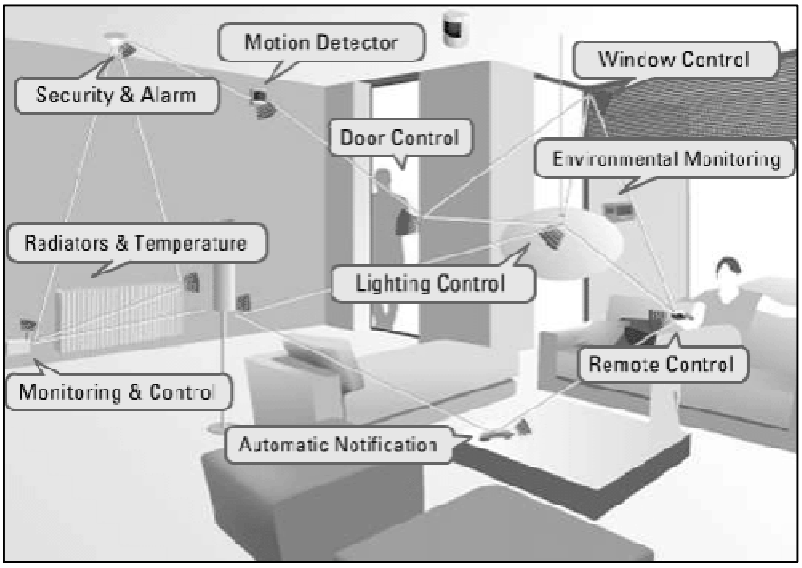

Figure 1. Smart Home Technology Automation

Echelon Corp., the creator of the LonWorks system, is helping drive adoption of an open interoperability standard among vendors in the control networks industry. LonWorks is an open standard for network automation and control for the building, transportation, industrial and home markets. The American National Standards Institute (ANSI) has adopted the protocol underlying LonWorks control networks as an industry standard. The LonMark Interoperability Association is made up of more than 200 controls companies mission working on standard to integrate multi-vendor systems based on LonWorks networks. [2]

### 2.1. Smart Home Software and Technology

Smart home technology was developed in 1975, when a company in Scotland developed X10. X10 allows compatible products to talk to each other over the already existing electrical wires of a home. All the appliances and devices are receivers, and the means of controlling the system, such as remote controls or keypads, are transmitters. If you want to turn off a lamp in another room, the transmitter will issue a message in numerical code that includes the following:

- An alert to the system that it's issuing a command,
- An identifying unit number for the device that should receive the command and
- A code that contains the actual command, such as "turn off."

All of this is designed to happen in less than a second, but X10 does have some limitations. Communicating over electrical lines is not always reliable because the lines get "noisy" from powering other devices. An X10 device could interpret electronic interference as a command and react, or it might not receive the command at all. While X10 devices are still around, other technologies have emerged to compete for your home networking dollar.

Instead of going through the power lines, some systems use radio waves to communicate, which is also how WiFi and cell phone signals operate. However, home automation networks don't need all the juice of a WiFi network because automation commands are short messages. The two most prominent radio networks in home automation are ZigBee and Z-Wave. Both of these technologies are mesh networks, meaning there's more than one way for the message to get to its destination.

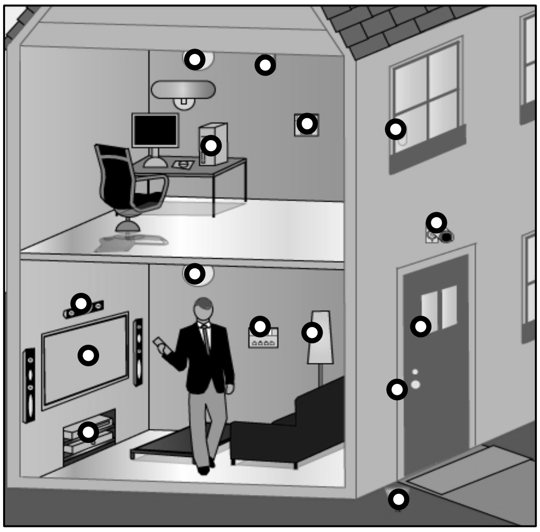

Figure 2. The dots represent devices that could be connected to your smart home network.

Z-Wave uses a Source Routing Algorithm to determine the fastest route for messages. Each Z-Wave device is embedded with a code, and when the device is plugged into the system, the network controller recognizes the code, determines its location and adds it to the network. When a command comes through, the controller uses the algorithm to determine how the message should be sent. Because this routing can take up a lot of memory on a network, Z-Wave has developed a hierarchy between devices: Some controllers initiate messages, and some are "slaves," which means they can only carry and respond to messages.

ZigBee's name illustrates the mesh networking concept because messages from the transmitter zigzag like bees, looking for the best path to the receiver. While Z-Wave uses a proprietary technology for operating its system, ZigBee's platform is based on the standard set by the Institute for Electrical and Electronics Engineers (IEEE) for wireless personal networks. This means any company can build a ZigBee-compatible product without paying licensing fees for the technology behind it, which may eventually give ZigBee an advantage in the marketplace. Like Z-Wave, ZigBee has fully functional devices (or those that route the message) and reduced function devices (or those that don't).

Using a wireless network provides more flexibility for placing devices, but like electrical lines, they might have interference. Insteon offers a way for your home network to communicate over both electrical wires and radio waves, making it a dual mesh network. If the message isn't getting through on one platform, it will try the other. Instead of routing the message, an Insteon device will broadcast the message, and all devices pick up the message and broadcast it until the command is performed. The devices act like peers, as opposed to one serving as an instigator and another as a receptor. This means that the more Insteon devices that are installed on a network, the stronger the message will be. [3]

### 2.2. Setting Up a Smart Home

X10, Insteon, ZigBee and Z-Wave just provide the technology for smart home communication. Manufacturers have made alliances with these systems to create the products that use the technology. Here are some examples of smart home products and their functions.

- Cameras will track your home's exterior even if it's pitch-black outside.
- Plug your tabletop lamp into a dimmer instead of the wall socket, and you can brighten and dim at the push of a button.
- A video door phone provides more than a doorbell -- you get a picture of who's at the door.
- Motion sensors will send an alert when there's motion around your house, and they can even tell the difference between pets and burglars.
- Door handles can open with scanned fingerprints or a four-digit code, eliminating the need to fumble for house keys.
- Audio systems distribute the music from your stereo to any room with connected speakers.
- Channel modulators take any video signal -- from a security camera to your favorite television station -- and make it viewable on every television in the house.
- Remote controls, keypads and tabletop controllers are the means of activating the smart home applications. Devices also come with built-in web servers that allow you to access their information online.

The keypad will send a message to your lamp. These products are available at home improvement stores, electronics stores, from technicians or o-nline. Before buying, check to see what technology is associated with the product. Products using the same technology should work together despite different manufacturers, but joining up an X10 and a Z-Wave product requires a bridging device.

In designing a smart home, you can do as much or as little home automation as you want. You could begin with a lighting starter kit and add on security devices later. If you want to start with a bigger system, it's a good idea to design carefully how the home will work, particularly if rewiring or renovation will be required. In addition, you'll want to place strategically the nodes of the wireless networks so that they have a good routing range.

The cost of a smart home varies depending on how smart the home is. One builder estimates that his clients spend between $10,000 and $250,000 for sophisticated systems. If you build the smart home gradually, starting with a basic lighting system, it might only be a few hundred dollars. A more sophisticated system will be tens of thousands of dollars, and elements of home theater systems raise the cost of a system about 50 percent. [3]

### 2.3. Benefits of Smart Home

Smart homes obviously have the ability to make life easier and more convenient. Home networking can also provide peace of mind. Whether you're at work or on vacation, the smart home will alert you to what's going on, and security systems can be built to provide an immense amount of help in an emergency. For example, not only would a resident be woken with notification of a fire alarm, the smart home would also unlock doors, dial the fire department and light the path to safety.

Smart homes also provide some energy efficiency savings. Because systems like Z-Wave and ZigBee put some devices at a reduced level of functionality, they can go to "sleep" and wake up when commands are given. Electric bills go down when lights are automatically turned off when a person leaves the room, and rooms can be heated or cooled based on who's there at any given moment. One smart homeowner boasted her heating bill was about one-third less than a same-sized normal home. Some devices can track how much energy each appliance is using and command it to use less.

Smart home technology promises tremendous benefits for an elderly person living alone. Smart homes could notify the resident when it was time to take medicine, alert the hospital if the resident fell and track how much the resident was eating. If the elderly person was a little forgetful, the smart home would perform tasks such as shutting off the water before a tub overflowed or turning off the oven if the cook had wandered away. It also allows adult children who might live elsewhere to participate in the care of their aging parent. Easy-to-control automated systems would provide similar benefits to those with disabilities or a limited range of movement.

## 3. Security Technology

As the technology mature and the interest on the internet increases, network security has become a major concern to companies throughout the world. The fact that the information and tools needed to penetrate the security of corporate networks are widely available has increased that concern. Because of this increased focus on network security, network administrators often spend more effort protecting their networks than on actual network setup and administration. Tools that probe for system vulnerabilities, such as the Security Administrator Tool for Analyzing Networks, and some of the newly available scanning and intrusion detection packages and appliances, assist in these efforts, but these tools only point out areas of weakness and may not provide a means to protect networks from all possible attacks. Thus, as a network administrator, you must constantly try to keep abreast of the large number of security issues confronting you in today's world. [4]

### 3.1. Protecting Confidential Information

Confidential information can reside in two states on a network. It can reside on physical storage media such as a hard drive or memory, or it can reside in transit across the physical network wire in the form of packets. These states present multiple opportunities for attacks from users on your internal network, as well as those users on the Internet. We are primarily concerned with the second state, which involves network security issues. The following are five common methods of attack that present opportunities to compromise the information on your network: [4]

- Network packet sniffers
- Password attacks
- IP spoofing
- Man-in-the-middle attacks
- Distribution of sensitive internal information to external sources

When protecting your information from these attacks, your concern is to prevent the theft, destruction, corruption, and introduction of information that can cause irreparable damage to sensitive and confidential data. This section describes these common methods of attack and provides examples of how your information can be compromised. [4]

## 4. Smart Home Security

Conventional security systems keep homeowners, and their property, safe from intruders. A smart home security system, however, offers many more benefits. Home automation technology notifies homeowners of any problems, so that they can investigate. Artificial intelligence programs keep track of the homeowner's habits, and other important information, and notify emergency personnel when necessary. [5]

### 4.1. Smart Home Fire Protection

Smart home security system offers much more protection than the typical fire alarm. This type of system checks carbon monoxide levels as well as watching for signs of fire and monitors all areas of the home. In the event of a fire, the smart home security system can alert the homeowner and notify emergency services. Artificial intelligence programs are even able to pinpoint the location of the fire, and provide that information to fire department personnel as they respond. [5]

### 4.2. Access Control

Security codes, motion detectors, and cameras provide information to a smart home security system, allowing it to determine whether an individual is a resident, a cleared visitor, or an intruder. Motion detectors trigger an alert, letting the artificial intelligence program know that there is someone or something to be evaluated. Facial recognition software and security codes allow the security system to allow residents into the home, while based on pre-programmed information restrict access to other individuals. [5]

Whenever smart home security system detects someone who is unknown, it can provide video of the visitor to the homeowner. Visitors that are welcome can be given clearance and allowed in the house remotely. Unwelcome visitors can be ignored, and individuals attempting to break in will trigger a call to the police. [5]

### 4.3. Artificial Intelligence Programs Protect the Homeowner

Intruders and fires are not the only dangers in a home. A smart home security system also protects residents from unanticipated health problems. Using the same cameras and motion detectors that protect the outside of a home, smart houses can learn about the habits and normal movements of the residents. When the resident does something unexpected, and does not resume normal activities, the smart home can alert family members or emergency services. This aspect of a smart home is particularly helpful for the elderly, or those in fragile health. [5]

## 5. Technology and Researches in Smart Home Security

Many smart home devices provide home automation technology, but the smart home security system offers many benefits that can ensure the safety of the homeowner. In this section, we review the tools related to Smart Home Security.

### 5.1. Smart Home Networks User Authentication Using Neural Network

This authentication scheme has two phases: the user registration phase and user authentication phase. First, authorized users have to register in the authentication system by giving their username and password. In second phase, i.e., the user authentication phase, the system validates the legitimacy of the users. [6]

In the user registration phase, the system administrator obtains the training patterns from usernames and passwords to train the neural network. The registration process is described as follows:

1. Each user chooses a proper username and password and gives them to the system administrator.
2. The system applies a one-way hash function to the username and password and the result is used as the training pattern. So, the training pattern consists of hashed username, as the input of the neural network, and the corresponding hashed password, as the desired output of the neural network.
3. Before training the neural network, the system needs to normalize the ASCII codes of the characters of the training patterns.
4. The system administrator uses these training patterns for training the RBF network. After training process, the system administrator stores the RBF network weights in the system.

In the user authentication phase, the authentication system uses the trained RBF network and applies the same one-way hash function to authenticate the legality of the users. The authentication process is described as follows: [6]

1. The system applies the same hash function on the entered username and password.
2. The system extracts an output through the trained neural network.
3. The system compares the output of the RBF network with the hashed password. If the results are equal, the user is recognized as an authorized user. Otherwise, the user is rejected as an illegal user.

### 5.2. Sentry@Home

Smart Home environments typically are equipped with different kinds of sensors and tracking devices for context-aware service provisioning. While on the one hand, people want to take advantage of the comfort and added value of personalized context-aware services, privacy and traceability becomes a serious concern on the other hand. The question arises, how we can build up trust into inherently untrusted services in a potentially hostile environment? How can it be guaranteed that eventually all sensitive data is deleted or safely stored away? The Sentry@HOME concept, as part of our User-centric Privacy Framework, addresses these concerns.

Sentry@HOME is designed to become an integral part of the user's home environment; seamlessly embedded into the Smart Home software infrastructure.. The Smart Home itself then can be leveraged to act as a privacy proxy for a tracked individual. On behalf of the user it constitutes the central privacy enforcement point for all privacy-relevant accesses to private or sensitive data. We are confident that our contribution, the combination of Smart Homes and a privacy-aware infrastructure, substantially adds to the success of personalized pervasive computing systems.

### 5.3. Defending DDoS Attacks Caused by Spam

Distributed Denial of Service (DDoS) attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. DDOS attack through spam mail is one of the new versions of common DDoS attack. In this type, the attacker penetrates the network by a small program attached to the spam mail. After the execution of the attached file, the mail server resources will be eaten up by mass mails from other machines in the domain results denial of services.

This defense mechanism is a multi layer approach to defend the DDoS attack caused by spam mails. This approach was implemented in the mail system and monitored the results. The result shows that our approach is very effective. The approach has six layers. This approach is a combination of fine tuning of source filters, content filters, network monitoring policy, general email policies, educating the user & timely logical solutions of the network administrator. Fine tuning of source filters reject the incoming connections before the spam mail delivery. The content filters analyses the contents of the mails and blocks the incoming unwanted mails. Network monitoring approach provides general solution to identify the attacks prior to the attack and also during the attack. Business houses should educate the user about possible attack scenarios & reacting ways to it. The logical solutions of the network administrator play an important role during the attack period and even post attack period. The combination of these layers provides best methodology to stop the DDoS attacks established though spam mails.

## 6. Conclusion

Smart Home is a residence that uses a Home Controller to integrate the residence's various home automation systems. The most popular Home Controllers are those that are connected to a Windows based PC during programming only, and are then left to perform the home control duties on a stand-alone basis. Integrating the home systems allows them to communicate with one another through the home controller, thereby enabling single button and voice control of the various home systems simultaneously, in preprogrammed scenarios or operating modes. Security has been an important issue in the smart home applications. In this paper, we discussed smart home and security, we also review the tool related to smart home security.

## References

[1] Vendela Redriksson (2005) "What is a Smart Home or Building" http://searchcio-midmarket.techtarget.com/sDefinition/0,,sid183_gci540859,00.html#

[2] SearchCIO-Midmarket.com Definitions - smart home or building http://searchcio-midmarket.techtarget.com/sDefinition/0,,sid183_gci540859,00.html

[3] Molly Edmonds “How Smart Homes Work - Setting Up a Smart Home” http://home.howstuffworks.com/home-improvement/energy-efficiency/smart-home1.htm

[4] CISCO Press, "Internetworking Technologies Handbook", Chapter 51 - Security Technologies http://users.freenet.am/~file/DownDB/CISCO_PDF/SecurityTechnologies_CISCO.pdf

[5] Victoria Nicks (2009) "AI Enhances the Smart Home Security System" http://artificialintelligence.suite101.com/article.cfm/ai_enhances_the_smart_home_security_system

[6] Shahbaz Zahr Reyhani and Mehregan Mahdavi "User Authentication Using Neural Network in Smart Home Networks", International Journal of Smart Home, Vol. 1, No. 2, July, 2007

[7] Susana Alcalde Bagüés, Andreas Zeidler, Fernandez Valdivielso, Ignacio R. Matias, "Sentry@Home - Leveraging the Smart Home for Privacy in Pervasive Computing", International Journal of Smart Home, Vol. 1, No. 2, July, 2007

[8] Dhinaharan Nagamalai, Cynthia Dhinakaran and Jae Kwang Lee, "Novel Mechanism to Defend DDoS Attacks Caused by Spam", International Journal of Smart Home, Vol. 1, No. 2, July, 2007

## Authors

### Rosslin John Robles

He received his B.S. in Information Technology from Western Visayas College of Science and Technology, Philippines. He is currently a Multimedia integrate Masters-Ph.D. Student at Hannam University, Korea. His research interests are Software Engineering, Web Development and IT Security.

### Tai-hoon Kim

He received B.E., M.E., and Ph.D. degrees from Sungkyunkwan University. Now he is a professor, School of Information & Multimedia, Hannam University, Korea. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments.