*Review of Business and Technology Research, Vol. 13, No. 1, 2016, ISSN 1941-9414*

# SECURITY IN THE IOT: SMART HOME AND CAR

**Jaymee P. Arputham, Young B. Choi**

College of Arts & Sciences
Regent University
1000 Regent University Drive
Virginia Beach, Virginia 23464
U.S.A.
e-mail: jaymarp@mail.regent.edu | ychoi@regent.edu

**Abstract**

This paper discusses the Smart car/ Smart home network as enabled by the IoT infrastructure. It presents new landmarks and challenges to the world of home and personal network communications. With so much information traveling over the Internet, it is important to address the security threats to people's privacy, digital assets, and access; as it pertains to their homes and personal property such as vehicles. This paper will explore various methods and designs that can be used to build the smart home/smart car network securely and maintain this security.

In order to secure the smart home/smart car network, I explored various proven security practices that are employed with other aspects of network security. I looked at some security concerns that are prevalent to the smart home/smart car network. The purpose of this is to secure communications between the technologies involved in this network. Therefore, I studied the applications of VPN tunneling, encryption, biometric authentication, and user authentication. All of these tools can be used to create an effective standard of security for the smart home/smart car network.

*Keywords:* The Internet of Things (IoT), security, smart home, smart car, encryption, VPN, education, biometric authentication, IoT best practices.

## Introduction

We live in a world of interconnection. The internet has reached a level of maturity that enables people to connect to each other, information, and resources in incredible ways. People now have the ability to access whatever resources they want in the palm of their hand (smartphones). Technology is rapidly improving and evolving. This brings changes in the business and home environments. The internet of things (IoT) is one of these technologies that are bringing about significant change in the world of business and the home. This is essentially accomplished by the significant amount of interconnectivity that the IoT offers.

This interconnectivity is not without challenges. With this level of interconnectivity comes many security concerns. With so many interconnected devices sharing information with each other; the IoT becomes a prime target for users with malicious intent. This becomes especially true in the smart home/smart car network. In order to defend against inevitable attacks, it is best to employ standard security protocols to secure the IoT, at least in the personal consumer/smart home environment (Perumal, Sulaiman, Sharif, Ramli, Leong, 2013). This paper is primarily concerned with the smart home/ smart car network and provides some methods and standards for securing the IoT of the smart home/smart car/smart network.

## Materials and Methods

I researched the IoT and its implications for day to day life and business. IoT essentially enhances many of the technologies that are available to us. For example, we all have homes and some of these homes have security systems. Home security systems are not considered new technology. However, the smart home is relatively new technology. Smart homes are capable of managing the home based on the home owner's preferences. For example, a Smart home can adjust the temperature based on the home owner's ideal temperature at a specific time (Piyare, Lee. 2013). IoT takes this level of convenience even further and will allow the homeowner to control things like the home's temperature from his car while he is driving home. This, however, can raise questions of security. What happens if the home owner's car is broken into? Could the car be used by a malicious user to disarm the home's

security system? If the car is connected to the home via the Internet, does the car even need to be broken into? Through this paper, I have gathered the useful and dangerous implications of the smart home network and gathered them in one place for thoughtful consideration about the nature, dangers, and benefits of the smart home network. In addition to this, I have provided some thoughts for consideration on a standardized security protocol for the smart home/ smart car on an everyday consumer level (Keoh, Kumar, 2013).

**The Smart home/Smart car network**

The smart home/smart car network represents the future direction of modern living. This type of technological advancement will impact our day to day lives; in a way similar to the Internet and smartphones. This network will allow us to manage our homes and lives in a much deeper way. For example, we will be able to change the temperature of our homes while driving home from work with a simple voice command to the computer in our car (Javale, Mohsin, Nadanwar, Shingate, 2013). We will be notified by our smart refrigerators that we are running low on milk, while on the road. Then, we could tell the refrigerator to place an order for milk at our favorite grocery store; our car GPS would then change our directions to stop at the grocery store on the way home to pick up the milk that has already been ordered and paid for. These kinds of technological innovations will be extremely helpful in bettering and enriching our day to day lives. Unfortunately, with this increase in interconnectivity, there is also an even greater increase in vulnerability. Therefore, when building the smart home/smart car network security and privacy should be one the biggest concerns, perhaps even the biggest concern (Bangali, Shaligram, 2013).

**Security concerns within the smart home network**

The smart home network is a series of improvements on existing networking technologies. These improvements have a lot of benefits that will, for the most part, better everyone's lives. However, many of these technologies operate over the Internet. The most public and insecure network. Therefore, many of the problems that are inherent to the Internet are also going to be concerns of the smart home network (Jing, Vasilakos, Wan, 2014).

Because of this, the smart home network is vulnerable to phishing, Dos, viruses, worms, and espionage just to name a few. As of right now, the majority of the population does not own smart homes and smart cars that are interconnected to each other. Many people do not have to worry about someone remotely hacking into their car's camera and watching them. They don't have to worry about someone hacking into their cars and shutting it off in the middle of the highway. They don't have to worry as much about someone hacking into their refrigerator's computer and ordering one million dollars' worth of groceries that they don't need. This is because these technologies are not a standard part of our lives; like the Smartphone and tablet are. Therefore, it is imperative that the smart home/smart car network is built from the ground up with security in mind. I have provided some theories on how to secure this network below (Sicari, Rizzardi, Grieco, Coen-Porisini, 2014).

**Smart home network access**

The first layer of the TCP/IP model is the network access layer. This layer is the first level of access and defense. In the context of the smart home, this is where the user will authenticate his or her account access information. I propose a three-layer model of authentication and verification at this layer; in order to verify user access and authentication. The three components of this authentication will be something the user is, something the user knows, and something the user has. It will take all three of these factors to grant access and verify the user.

Something the user is could be a biometric check. For example, retina scanning, voice recognition, facial recognition, and fingerprint scanning could all be used to verify the user's identity. Only of these methods could be used or all of them, depending on the situation and requirements of the user. However, it should be standard protocol for the user to use at least one method. Fingerprint authentication would be one of the simplest methods, many smartphones, tablets, and laptops already come with this technology (El-Basinoi, El-Kader, Fakhreldin, 2013).

Something that the user knows could be a passphrase, pin, number, or pattern. This would provide other means of authentication and verification one the biometric check had been passed. Just like the biometric authentication the user could employ more than one tool at the same time. For example, the user could input a passphrase and afterward be prompted to draw a pattern. However, the user should have to use at least one of these methods after passing the biometric authentication step. This method alone is not very secure. However, when used in conjunction with other methods of authentication it can be useful in securing access to protected systems (Cirani, Ferrari, Veltri, 2013).

The final method of authentication within the network access layer would be something a user has. This could be an item such as a car key, an electronic token, or a card the user carries. The electronic token could be attached to a key chain or be embedded into a ring or necklace and could be used with smartphones, tablets, laptops, cars, and homes. The car key or house key could be used to access the IoT network in the car and home respectively.

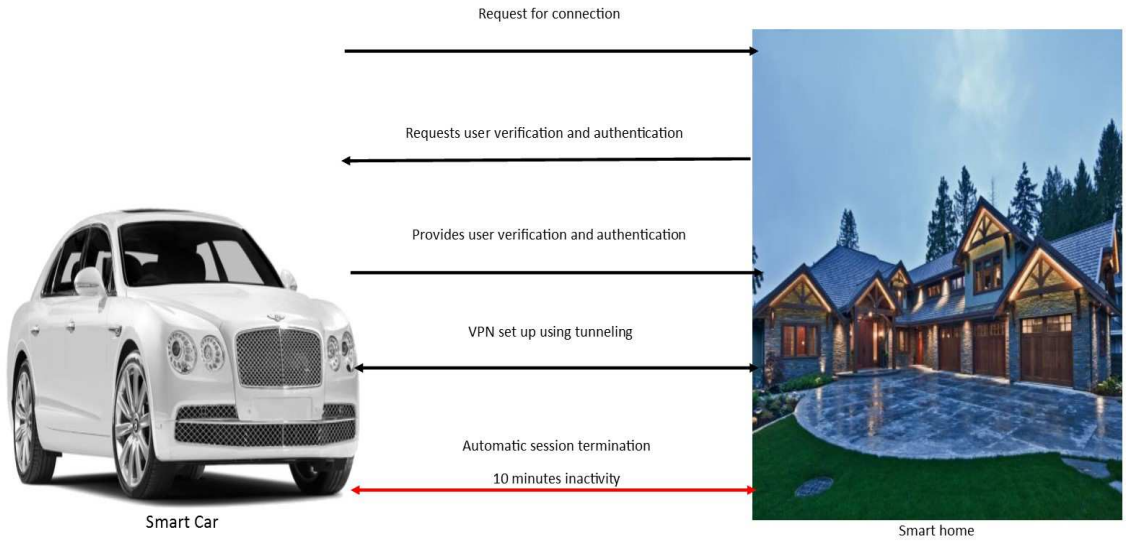
This final method of authentication will be requested only once the other two methods are met. Using this three-point authentication, users will be able to have peace of mind and will be able to securely access their smart home/smart car networks (Riahi, Natalizo, Challal, Mitton, Lera, 2013).

**Data encryption and secure communication**

Once the user's identity and access have been verified, the user is now connected to the internet and has reached the internet layer of the TCP/IP model. From here the user will be able to send and receive data over the public internet from other users and devices. Such as smart home to smart car. While the security at the network access layer served to restrict access to only those individuals that are authorized to use the systems; it doesn't offer any means of protection for the information that is being sent between the connected systems. The IoT has to operate over the Internet and this leaves it quite vulnerable to users with malicious intent. There are already many methods to secure traffic at the internet and transport layer. For example, IPsec in the internet layer of the TCP/IP model is available for use. There is also the use of TLS/SSL as well as VPN tunneling via public key encryption; to encrypt the entire interaction between two or more smart devices. There should also be an automatic session timeout feature. Similar to what is currently being used in online and mobile banking. The issue is not primarily in the technology, instead, the issue is with users behind the technology. You can have the most secure system technologically; but if you have weak security policies, weak user knowledge/education, and too much user freedom you can leave your systems vulnerable.

Therefore, I am suggesting universal minimum security standards for use within IoT smart home/smart car technologies. If the user is not forced into 3-point authentication, then the user will most likely not do it. If the user is not forced to use VPN tunneling and automatic session termination, they will more than likely not do it. This standard will contain 3 key principles. First 3-point user authentication, VPN tunneling once the user identity and connection is established, and finally automatic session termination within 10 minutes of user inactivity.

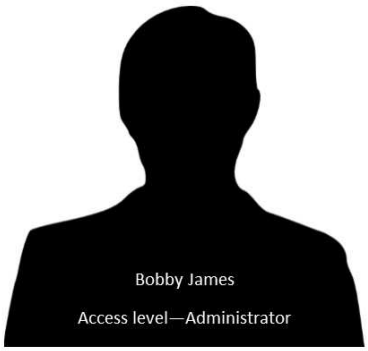
This is not a perfectly secure method and cannot prevent every single attack from being successful, but it does at least force the user to use some minimum security standards when using their smart home/smart car IoT services. These steps will authenticate the user's identity via three-factor authentication. It will establish the kinds of rights and privileges that this user has. Finally, it will automatically terminate the transmission after a certain period of time. This will help to prevent unauthorized access to the smart home/smart car network. Users should automatically log off once they have finished their business within the network. However, human error is one of the largest causes of failed security. This automatic log off will at least help to circumvent the folly of human forgetfulness. I have attached a diagram depicting the interaction between a smart car and smart home using these standards.




**Smart home network security**

In addition to 3-point authentication, data encryption, and automatic session termination. I suggest the user's home network, which is the center of their personal IoT service be outfitted with some basic security features that are currently not common to home users. First, I suggest that the smart home/smart car network should have its own dedicated router. This router could obviously run off the household's ISP, but it would set aside specifically for IoT related processes for the smart home/smart car. This router should not broadcast its SSID and should have a host-based intrusion detection system.

Instead of broadcasting its SSID, the router would store user profiles. These profiles would contain user data such as level of access and acceptable MAC addresses associated with the user profile. For example, if Bob is the main owner of the smart home network, his account would have administrator level privileges. He could change, modify, and delete to his heart's content. Within his profile, he would register devices via MAC address that he would use to access his smart home/smart car. He could register devices such as his smartphone, smart watch, computer, tablet, laptop, car, SUV, and even T.V. Any device that is not on the list for the user Bob would not be able to connect to the smart home network. Even if it has passed the three-factor authentication. A sample user profile is attached below.




**Authorized Devices**

Device 1 (Smart car)

IP – 192.168.0.2

MAC - FF:00:FF:00:FF:00

Device 2 (Smart phone)

IP – 192.168.0.3

MAC - FF:00:FF:00:FF:01

Device 3 (Tablet)

IP – 192.168.0.4

MAC - FF:00:FF:00:FF:02

Device 4 (Laptop)

IP – 192.168.05

MAC – FF:00:FF:00:FF:03

Device 5 (smart watch)

IP – 192.168.0.6

MAC – FF:00:FF:00:FF:04

The router would also have a host-based intrusion detection system. Its job would be to monitor traffic on the network and alert the administrator accounts of unusual activity. For example, if a new account is created the HIPs would alert Bob via e-mail or text message that a new account has been created. Bob would then verify whether or not he approved the creation of this new account. Other examples would be new IP addresses on the network or new MAC addresses added to a profile. All of these events would alert the user. This feature keeps the user informed about what is going on in the smart home/smart car network.

These services and technologies could be offered as part of a smart home technology suite. Much like home security systems are offered; it could even be part of a home security package. The user could pay a monthly fee, for support, monitoring, archiving, and remote management of his smart home network. The company could create their own proprietary software and mobile apps that work in conjunction with each other to create a useful, responsive, and secure environment for the user

.

**Results and Discussion**

The most important aspects of maintaining security in the smart home/smart car network at the user level are controlling access and monitoring activity. This is why I have proposed a method of authentication and access using three-factor authentication and automatic session timeout. This will help ensure that only authorized users can access the network. In order to monitor activity, I suggest that the network should have its own dedicated router that is not connected to the home network with IDPS functions and unicasting. This will also help to control access to the smart network but will also be able to monitor traffic on the network and will be able to alert administrators of potential intruders or suspicious activity.

**Conclusions**

The IoT has the potential to change the way we live our day to day lives. This is especially true of smart cars and smart homes. These technological advancements will improve the quality of our lives significantly. However, with this increased interconnectivity comes increases in security and privacy risks. Therefore, it is important to build the smart car and smart home network with security in mind throughout the entire process. Unlike many of our other technologies, security and privacy should not be an afterthought of the smart home and smart car network. The network must be built to not only allow interconnectivity and convenience, but must also be built to ensure privacy and security.

References

Bangali, J., Shaligram, A. (2013). Design and Implementation of Security Systems for Smart Home based on GSM technology. *International Journal of Smart Home, Vol. 7, No. 6,* pp. 201-208.

Cirani, S., Ferrari, G., Veltri, L. (2013) Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview. *Algorithms, Vol. 6*, PP 197-226.

El-Basioni, B., El-Kader, S., Fakhreldin, M. (2013) Smart Home Design using Wireless Sensor Network and Biometric Technologies. *International Journal of Application or Innovation in Engineering & Management, Vol. 2,* pp. 1-17.

Javale, D., Mohsin, M., Nandanwar, S., Shingate, M. (2013) Home Automation and Security System Using Android ADK. *International Journal of Electronics Communication and Computer Technology, Vol. 3*, pp. 1-4.

Jing, Q., Vasilakos, A., Wan, J., (2014). Security of the Internet of Things: Perspectives and challenges. Springer Science + Business Media, New York, NY, pp. 1-21.

Keoh, S., Kumar, S., (2014) Securing the Internet of Things: A Standardization Perspective. *ResearchGate, pp. 1-13.*

Perumal, T., Sulaiman, N., Sharif, K., Ramli, A., Leong, C. (2013) Development of an Embedded Smart Home Management Scheme. *International Journal of Smart Home Vol. 7*, pp-1-12.

Piyare, R., Lee, S., (2013) Smart Home-Control and Monitoring System Using Smart Phone. *ICCA 2013, ASTL Vol. 24*, pp. 83 - 86

Riahi, A., Natalizio, E., Challal, Y., Mitton, N., Lera, A., (2013) A systemic and cognitive approach for IoT security. Military Academy of Tunisia, Nabeul, Tunisia, pp. 1-6

Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini., (2014) Security Privacy and Trust in the Internet of Things: The Road Ahead. *Computer Networks 76,* pp.146-164