Home Automation Security and Vulnerabilities

Spring 2014

EEL4789 – Ethical Hacking and Countermeaures

Dr. Alexander Pons

by

Henry Flefel

Luis Puche

Elvin Blen

Miguel San Martin

Joseph Hickman

In 2012 a survey conducted by the National Association of Home Builders showed that home automation was listed as one of the most desired features in a new home. Todays home automation systems are capable of controlling just about any devices in a home. This is made possible through the use of several different control protocols, the most popular being the Z-Wave protocol. In 2012 the market for home automation was a 3.4 billion dollar industry with nearly 1.5 million systems having been shipped to consumers. By the year 2017 the market size is expect to grow to 5.5 billion dollars and the estimate number of system shipped to consumers will be 8.0 million. With so many homes beginning to use these system one is compelled to ask the question. Are these system secure?

"Last year the Federal Trade Commission received more than one-quarter million stolen identity complaints--and that's just the reported case" (Marian Merritt, Norton Identity Theft Primer). For a malicious hacker, to gather the required information for identity theft purposes is not hard. That is, if the victim is not aware of how easy they are making this process for them. Besides usual wireless network sniffing, email scams and other cracking procedures, home automation has introduced quite a few more tools for mischievous objectives.

One of the most common features of smart homes is audio and video capabilities. Among other amenities, like smart air conditioning and lights, security surveillance is the usual tool for people who want to protect valuables, sensitive information, safeguard loved ones or simply automate process that require supervision. But this technology comes with a price, much bigger than the monetary one. Privacy can be invaded by a criminal and the information that he or she can gather goes beyond bits and bytes. What you eat, movies you watch, your daily schedule and other information can be collected if someone cracks into your home surveillance system (which most automated homes have), home server (which most automated houses use to support the system) or any other information cluster you use. For example, if your credit card information in stolen, it would be suspicious if it is used to buy a car, or something small but delivered to another address. But what would happen if the attacker buys a TV from amazon and asks to be shipped at your own address when he or she knows you are not at home? It is just a matter of timing, and waiting for a couple of minutes for UPS to arrive with the package and steal it from your doorstep. You know it wasn't you, but for Amazon, UPS and your bank it looks absolutely normal.

Many other techniques and attacks can be performed with information gathered from smart homes, so it is important to know what to do to prevent it. Check for shoulder-surfers when entering PIN numbers or other sensible data. Also, destroy any data storage device properly, especially if it is encrypted. People tend to think that due to encryption, you are save to throw away your CD, but what you are doing is actually giving away the necessary parts for someone to decipher the key, saving time for when they crack into your network and find an encrypted drive in your server (to which they will already have the key). For CDs, microwave is the best bet. For drives, a "shredder" or multi-pass writer is a program that rewrites the information in different ways and multiple times before cleaning the bits to all ceros. Magnetic drives (such as Hard Disk Drives) have other techniques of data recovery so the microwave or directly drilling holes in it will fully destroy it. This information is collected by dumpster-diving, so try to keep your trash can inside your garage until the cleaning personnel comes to collect them. Knowing what not to do is also important: "No reputable business or agency will send you an unsolicited email requesting personal or financial information from you" (Internet Security article from www.identitytheft.info). Much more information is available from that site and many others. A practical list can be found at http://netsecurity.about.com , but remember to inform yourself about the security risks and best methods to be safe from time to time, as they evolve with time.

Best Practices in Home Networks

Anyone may ask, how do I secure my home from trespassers? With the rising popularity of Smart Homes and connectivity to the internet one could say that homes can become bigger and better targets the more integrated they become.

Port Forwarding: This is one of the most commonly used methods to output either Smart home systems or CCTV (Security Cameras). Done usually at the gateway of the home, the modem is bridged and everything is managed at the router.

The DVR might be easily compromisable as users tend to either not change the administrator passwords. Even more alarming is the number of loopholes that come with camera systems. Personally having worked on the field, most chinese-made DVRs have ways to access their content with backdoor passwords. Commonly Anonymous and Anonymous to gain full access to all functions.

For the main players in a Smart Home environment a common practice for installers was to port forward directly to the system ports. Some of these completely unsecured and allowing real-time modifications through the use of proprietary programs that were cracked and available on the net. At this point, anything within a home could be controlled remotely, blinds, door locks, gates, and garages all compromised.

So what might be the alternative? Simply put, a VPN is more secure for a smart home however more costly to setup or the proprietary service that companies offer to access their own systems

Securing Network Wirelessly: Having a strong WPA2 security with WPS mode disabled can make a huge difference. As we have learned, WEP is unsecured, and some of the older Automation Systems only work through WEP encryption, systems that sometimes have not been updated to a more secure encryption.

However, the most secure of encryptions can be cracked by social engineering, Guests in a home are often given the WiFi password, this is a problem when the system itself is connected to the same network and once unsecured, anyone nearby can gain access. Providing any of these details will always be a risk and for that, if there's any suspicion that the wireless will be left alone then changing the password frequently is one of the best practices.

Ethernet based: This is the obvious, how about intercoms? Some intercoms are wired directly. If a person with a screwdriver can go over to the gate, remove the intercom and connect directly to the home network to then disable security and stop the cameras then the whole home is open for robbery. Outdoor antennas are the same; one could freely gain access from an unsecured antenna and connect their own access point.

Paying attention to which wires are exposed is critical; having equipment inside walls will make it unlikely that anyone will try to break in. Installing sensors that immediately alert the homeowner that that the intercom has been opened can make a huge difference.

What to remember: For most systems, the network is the first and the only line of defense is the network itself. Taking special care of plugging all the holes in your own network should be any homeowner's priority as we sink deeper into the controlled home environment.

Looking through a set of black glasses

Hackers are everywhere attempting to compromise our information for ill-intentioned actions such as stealing our credit card information (for the obvious purpose), social security numbers and just about any information that may be valuable to you (blackmail perhaps?) or them. As the smart-home industry rises there is greater risk of hackers compromising and entering what we once thought of as "sacred ground", our home. How does this work exactly? Let us take a quick look at how a black hat (aka hacker) will most likely go through the process of breaking in by walking through a door or window completely unnoticed or without an alarm. First, he/she scouts for a prospect (most likely someone who has nice material objects, is somewhat flashy with their assets), after finding a subject he/she will start on reconnaissance (legally and/or illegally) to provide a more solid background on you and learn the ins and outs of your schedule/lifestyle; after gathering all this information they will develop a strategy on attacking your home and execute that plan.

Tools of the trade

So once all the planning is set, exactly how does it work? Well like we all know, the internet is full of viruses and malware that can reap our information and cause harm to our computers; smart-homes are now on the menu for viruses and malware because smart-homes use technology involving radio waves and protocols that can be compromised just like any other computer. The U.S. market for smart-homes is nearly entirely occupied (80%) by devices equipped with the Z-Wave protocol which is now known to be quite vulnerable to attack. How does the attack work though? There is a small-circuit board that can pick up the radio wave frequencies that the Z-Wave protocol uses which can be easily equipped to a laptop via serial communication; what does this mean?

This means that a hacker can view all the packets in the air being sent from a home-owner to their smart-homes and access information critical to the security of that house including the ID of the Z-Wave home device. A hacker would then use Z-Force, software developed to read and inject packets to a Z-Wave home device to literally tell the front door to unlock and maybe even turn on the light while disabling the alarm! Now there are a few steps in order to complete the somewhat simple attack which consists of:

1. Identify the home ID of the Z-Wave smart-home device
2. Use the set-temporary key command and confirm the device is now running your temporary key
3. Now that you and the home device have the same key, send commands over!

As you can see, it's not much. This is a pretty easy way of literally walking into the bank and taking all that you can without a security guard telling you otherwise.

Z-Wave is an ITU certified proprietary communication protocol that was developed by Sigma Designs for use in home automation systems. It uses a low-power wireless technology design that makes it ideal for remote control applications in low cost home control networks. The protocols primary function is to communicate short control messages in an efficient and dependable manner from a controlling device to one or more compatible devices in the network. The protocol was designed with two main device types categorized as controlling devices and slave nodes. The controlling devices send out commands to other devices in the network while the slave nodes can either execute received commands or forward commands intended for other slave nodes located outside of the controlling devices signal range. There can only be on primary or master controlling device in a given network. This controller is the only device that is capable of adding and removing other devices on the network. This ensures that the master controller always has complete knowledge of the network topology. Every Z-wave network has a 32 bit unique identifier also know as Home ID. This ID is used to maintain different Z-wave networks separate. This Home ID is pre-programmed into all control devices. All slave nodes initially have the Home ID set to zero. Before a slave node can communicate on a Z-wave network it must first be assigned a Home ID by the controller on that network.

In July 2013 at the annual Black Hat conference security researchers Behrang Fouladi, Sahand Ghanoun presented their security assessment of the popular Z-wave protocol. Their research found two security vulnerabilities in the Z-wave protocol that would potentially allow an attacker to control slave nodes installed in a Z-Wave home automation network. By using a fairly inexpensive RF transceiver from Texas Instrument (model CC1110) and software utility called Z-Force an attacker could sniff the Z-wave protocol communication in any network. This will allow an attacker to start building a network map of the nodes installed as well as obtaining the 32 bit unique Home ID.

The first security vulnerability was found to be in the protocol used when adding slave nodes for the first time to the network. Z-wave uses a "Custom Key Establishment Protocol" to deliver a new encryption key from the controller to the slave node so that all future communication can be encrypted. However instead of using public-key cryptography to encrypt and send the new key the controller and node use a temporary pre-shared key to encrypt the new key. This “set key” message could be intercepted and decrypted using the Z-Force utility. This vulnerability was not considered critical since it would require any potential attacker to be in close proximity when the slave node was being added. However an installer could exploit this vulnerability and later use the information to mount an attack at a later time.

The second security vulnerability a by far the most dangers was found in the communications between slave nodes and controls. The research should that the slave nodes did not authenticate communication coming from controllers. If an attacker was to inject a “set message” with a new Home ID the slave node would accept the packet and register with the controller even though it was already registered with another Home ID. This would allow an attacker to install a rouge controller or use the Z-Force software to send control commands to the devices.

Educating Your Children About Social Engineering Therefore Less Reliance on Technology Against Hackers and Better Home Protection

Items that protect your children when they are home; safety Latches and Locks, Anti-Scald devices, smoke detectors, window guards, edge bumpers, outlet covers, door stops and holders and most importantly a web filter. All of these are technological items but what about the social/intellectual side of security. Many have heard of the many technological advances in home security and the many ways hackers circumvent these defensive measures but given that our children and teens are losing the concept of privacy via social media and are always “connected” it is easier for a hacker to invade your home, the private domain where every member of the family should be secure in all dimensions. Not to mention, what are we protecting, is just our privacy and possessions what about the mind and the minds of the children. “More than anything you guard, protect your mind, for life flows from it.”

Given that the home is the fortress its greatest weakness is not just the children/teens that inhabit it but that fact that everything is connected. Organized crime has gone to the internet to steal more than what is possess in the home just attackers who may want to hurt children and teens. The primary threats to juveniles in the home today are their peers cyberbullying via social media and adults that would want to harm them. Since every device has a keyboard, screen, camera and microphone surrounding everyone including children there obvious positive use is self-revealing but its possible use as a gateway to harm is not. Computers do automatic updates and antivirus programs are running and firewalls are up but what if the attacker already has access to your children which is often the case. Just as it is unrealistic to block every communications port on your computer and still be productive, it is just as unrealistic to block your child's every medium to the outside world. The primary method of attack in a social engineering attack is a prolonged communications with the target/victim. As the target develops trust in the attacker the attacker get closer to obtaining their goal.

The best defense is education, educating children on the threats they face and how they should react. Train them to ask themselves critical questions such as how well do I really know this person, why would they ask me certain questions, should I ask my parents for their opinion. Teach them how information is valuable asset and that they should share as little as possible. Teenagers often act impulsively without giving complete and proper thought to the consequences. Educate them on how to create a proper password, what is generally safe to download, log out of systems when they are done and configuring privacy settings. Most importantly, being open and honest through constructive non-emotional conversations. The children of the future will need to taught the importance of privacy and how to maintain it. Unfortunately parents must also conduct their own surveillance gradually decreasing such surveillance as children grow older, wiser and more trustworthy and increase surveillance if the inverse is true. Just as children are educated to be vigilant on the street they should be equally as vigilant while using the internet and that just because they are in the physical safety of the home that physical safety can be threatened by their actions virtually.

There is no substitute for good parenting. Much like many corporations have Counterespionage divisions, electronic surveillance departments and security training at the end of day individual wisdom and education are the only true defenses against social engineering.

1.http://en.wikipedia.org/wiki/Social_engineering_%28security%29

2.http://kotaku.com/5948617/confessions-of-a-teenage-xbox-hacker

3.http://www.washingtonpost.com/blogs/she-the-people/wp/2014/02/14/cellphones-social-media-are-new-tools-in-teen-dating-abuse/

4.http://us.norton.com/identity-theft-primer/article

5.http://www.identitytheft.info/internetsecurity.aspx

6.http://netsecurity.about.com/od/newsandeditorial1/a/aaidenttheft.htm