SECURING THE DIGITAL HOME

Ken Morse, CTO SP Video Software and Solutions, Cisco Systems

ABSTRACT

The home is getting more and more connected. Smart sensors are monitoring systems and activities and, in many cases, working together to enhance the efficiency and capability of your home. It’s the dream of the Internet of Things (IoT), and it’s becoming a reality in our homes. But the smart home can become a security nightmare because every connected device is a new potential entry point for cyberattacks.

Criminals are looking for vulnerabilities to gain access to connected devices in the home to steal personal data and even break into the premises. Once inside, they can quickly pivot to target service provider networks and content and mount larger-scale attacks

This paper looks at the common attack scenarios and presents an approach to mitigate this challenge, which, if unchecked, will result in a lower adoption rate by consumers.

1. INTRODUCTION

Your smart thermostat automatically adjusts the temperature when you’re away. Your washing machine and dishwasher communicate with each other to save on power and water costs. Connected surveillance cameras remotely notify you when the package you’ve been waiting for is delivered to your doorstep. And your connected TVs, tablets, and home audio equipment put the world’s digital content at your fingertips.

It’s the dream of the Internet of Things (IoT), and it’s becoming a reality in our homes. But the smart home can become a security nightmare because every connected device is a new potential entry point for cyber-attacks.

Criminals are looking for vulnerabilities to gain access to connected devices in the home to steal personal data and even break into the premises. Once inside, they can quickly pivot to target service provider networks and content and mount larger-scale attacks.

This paper provides an overview of the challenges of securing the home against these attacks and presents an approach to secure the home via a combination of capabilities in the residential gateway and cloud through a development known as HomeGuard.

2. THE EXPLOSION OF THE INTERNET OF EVERYTHING

Technology is quickly changing the way we interact with the world around us. Today, companies are developing products for the consumer market that would have been unimaginable a decade ago: Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. These are all examples of the Internet of Things (“IoT”), an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people. The IoT explosion is already around us, in the form of wearable computers, smart health trackers, connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn't a mobile phone, tablet, or traditional computer.

Consumer adoption of network-connected devices, such as in-home smart appliances and wearable technology, is on the rise. Thirty percent of consumers already own or plan to purchase an in-home IoT device in the next two years. In-home IoT devices include smart thermostats, self-driving vacuum cleaners and smart refrigerators.

While consumer adoption of connected technology will be more gradual in the short term, widespread adoption will be inevitable over the next five years. Figure 1 below illustrates one analysts' view of the adoption rates of various connected technology.

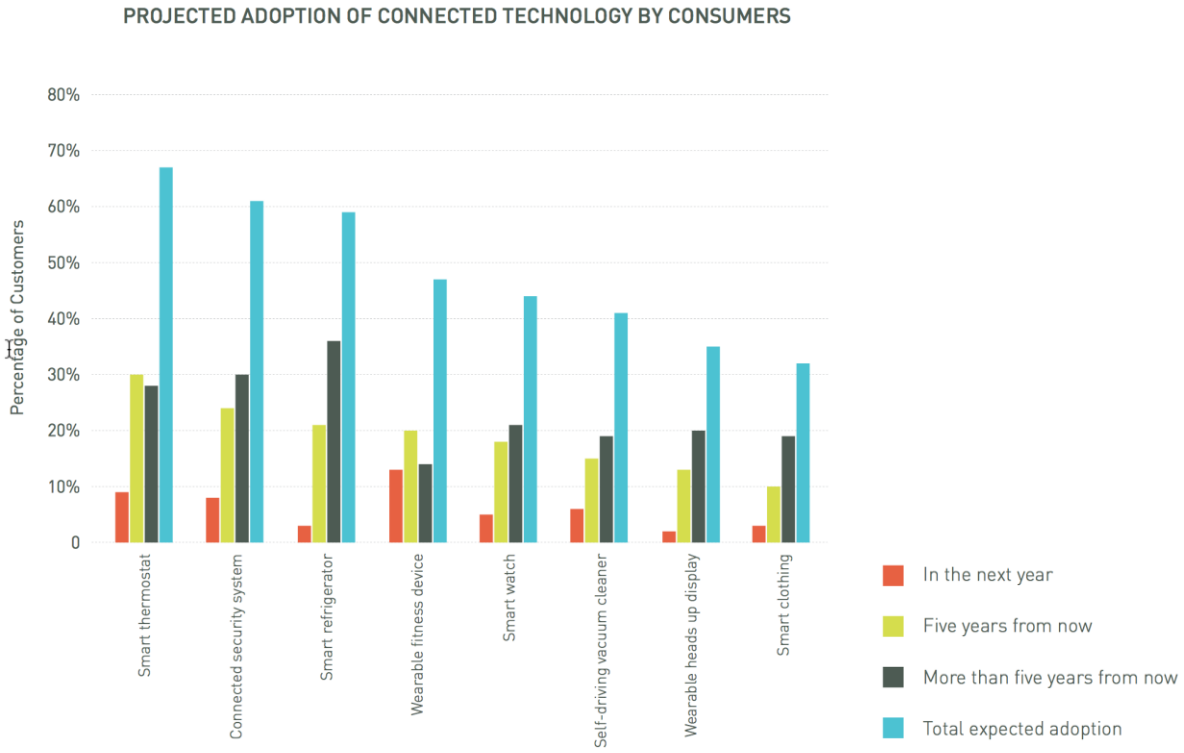

Figure 1 – Connected Technology Adoption Rates

(Aquity Group – Internet of Things: The Future of Consumer Adoption Report, 2014)

Currently, 7 percent of consumers own a wearable IoT device and 4 percent of consumers own an in-home IoT device. Nearly two-thirds of consumers plan to buy an in-home device in the next five years and wearable technology ownership will double by 201 - increasing from 7 percent in 2014 to 14 percent by 2015. By 2016, wearable technology is expected to double again and reach a total of 28 percent adoption rate.

These new developments are expected to bring enormous benefits to consumers. Connected health devices will allow consumers with serious health conditions to work with their physicians to manage their diseases. Home automation systems will enable consumers to turn off the burglar alarm, play music, and warm up dinner right before they get home from work. Connected cars will notify first responders in the event of an accident. And the Internet of Things may bring benefits that we cannot predict.

However, these connected devices also will collect, transmit, store, and potentially share vast amounts of consumer data, some of it highly personal. Given the rise in the number and types of connected devices already or soon to be on the market, the Federal Trade Commission in the US held a series of meetings to investigate the implications that could arise from this.

They identified three areas of concern within the consumer home network.

1. Access and misuse of personal information collected and transmitted to of from the device
2. Attack on consumer’s network or other systems
3. Use of vulnerabilities to create safety risks

3.1 Access and Misuse of Personal Information

IoT devices, like traditional desktop and laptop computers, can be exploited to enable intruders to access and leverage personal information collected and transmitted to or from the device. Smart TV’s represent an IoT device that is not dissimilar to a traditional computer in terms of the functionalities it offers today such as Internet surfing, application downloading and sharing content on the consumers home network. Hence, any security vulnerabilities on such a device could put the information stored on it or transferred through it at risk. Given the nature of Internet browsing and the ability of such devices to store passwords and other sensitive information the breaching of such a device could facilitate fraud or identity theft. There are countless other IoT devices coming to market that also leverage general Internet connectivity and as such as more of these devices are installed in consumer homes they may increase the opportunity for personal information to be compromised.

3.2 Attack on Consumer’s Network or Other Systems

Secondly, any security vulnerabilities in a given device can be used to enable attacks on the consumers’ home network or to the Service Providers’ network to which it is connected. This is of great concern to Service Providers who understand that a compromised IoT device could be used to launch a denial of service attack. As more IoT devices are seeded in the market the spectre of large scale denial of service attacks rise as this proliferation of devices enables the attackers to assemble large numbers of devices to utilise. From a Service Provider perspective it is critically important to contain as many of these as possible within the home domain as it will drive incremental costs if they have to be contained further upstream in the network.

3.3 Use Vulnerabilities to Create Safety Risks

The third area of interest is when cyber-attacks are used to exploit security vulnerabilities to create risks to physical safety. There have been documented examples of hacking into cars and even airliner systems and with the rise of IoT devices in the home that manage the local environment this becomes important in the connected home. For example, intelligent thermostats detect when the house is occupied and connected door locks enable remote unlocking of the house. If both of these are compromised it could be used to indicate not only when, but offer a simple mechanism, for intruders to enter a house. One area of concern around these devices is that the communications protocol, carried over WiFi or Bluetooth, can, in many cases, be easily recorded for subsequent playout and access.

Given the focus on low-cost for IoT sensors there is a concern that if vulnerabilities are found after deployment they may not be addressable in the device itself and hence an alternative solution must be found if replacement is to be avoided. In addition, many of the manufacturers operating in the IoT sensor marketplace may not have the appropriate financial incentives to address such issues given the low-cost nature of the solutions. Finally, many of the companies providing IoT devices may not have the necessary security knowledge to ensure such designs follow best practice from a security perspective.

3.4 Privacy Concerns

Security risks alone are not the only items that are of concern. Equally important is the risks associated with privacy based on the data flowing from the Internet of Things. Many of these are familiar to the world of Internet and Mobile devices such as financial information, health information and geo-location. Others are based on the collating of personal information over time such as locations, habits and personal environment over time. Access to this kind of data collection may allow an entity to infer additional information that can compromise the individual or system.

This paper does not address these privacy concerns directly, however, the papers' focus on security within the IoT home indirectly addresses them. It is however clear that the perceived risks to privacy and security could result in a lowered consumer confidence resulting in the IoT technologies not realising their full potential and reducing their adoption within consumer homes. With this in mind it is vital to promote the protections that are put in place with any potential solution.

4. THREAT-CENTRIC SECURITY MODEL

When you step back and look at the larger problem of securing the connected home, it becomes immediately clear that you cannot rely on "point-in-time" solutions. Because the home network keeps changing - with new devices announced and brought into home seemingly every day, and new malware and attack models being created almost as quickly. It is possible to harden the hardware and software against an attack that hit the home yesterday, but that is not going to protect the home from an attack tomorrow against some newly discovered vulnerability.

Hence there is a need to continually analyse the home network environment before, during, and after an attack, in order to:

- Identify suspicious traffic and block attacks before they hit your customers' data and devices
- Recognize and react to attacks in progress, and lock them down before they spread to other devices and your own network and content
- Understand what an attacker was trying to do, so you can take fast, effective steps to block that attack in all your other customers' networks

It’s important to remember that when considering connected home cyber-attacks, it is not just an individual trying to attack one customer’s computer or smart thermostat. Usually, criminal hackers today are working for large crime syndicates. So if they find a vulnerability that allows them to exploit a particular smart TV and gain access to something they can profit from, they won’t just go after one customer’s home. They’ll launch an attack against all of the millions of consumers that have bought that TV.

When you use an attack continuum approach, you are expanding the security strategy beyond an individual home to the entire customer base. Maybe a new, day-zero threat will gain entry into the first or second home it attacks. But over time, and not very much time, the system will recognise the pattern and report it back to the security operations center, so it can be blocked in all of the other customer networks.

Using this attack continuum approach—again, the same approach used with major global corporations and government customers that are protecting highly sensitive networks and data, it is possible to look at attacks as they occur and understand their common patterns. The incentive for the attack can be ascertained along with its technology and business impact. With this determination the system can quickly identify the right protection mechanism and remediate it across the entire network.

This paper has introduced the concept of continuous analysis in the connected home but what does that mean exactly? It’s an ongoing, four-step process:

- See
- Learn
- Adapt
- Act

4.1 See

The environment must start by monitoring the infrastructure in the residential network, under the premise that you can’t protect what you can’t see. Hence the home network must be continually monitored to discover every new device that gets added. For each of these devices a fingerprint is created. With this knowledge it is possible to know where every instance of, for example, a particular Smart TV exists so it is possible to share information about that device with every other home where it exists. It is important to note that customers’ privacy is protected, the information is used merely to know, based on the capabilities and fingerprint of the specific device, how to apply security rules later on, and to share this information to protect the rest of your customers.

4.2 Learn

With the knowledge of the devices in place it is then possible, via automated systems, to turn this data into actionable security and threat information. For a given home, the device and traffic patterns can be correlated with what is being monitored in other homes, and across the Internet, including the dark parts of the web where cybercriminals share information about vulnerabilities. With this knowledge it is possible to put suspicious or malicious network behavior in the right context.

For example, the system doesn’t just see a strange spike in traffic from a thermostat to some unusual endpoint; instead it is able to understand what the consequences are of the attack and the method of operation for the attacker.

4.3 Adapt

Once the system understands what a threat is doing, it can automate the process of adapting the security policies in response to it. One of the biggest concerns consistently mentioned about connected home security is that it has to be totally transparent to the consumer. People say, “My parents will never understand how to operate a network security appliance in their home.” Hence it is important that all of these processes are entirely automated. The system should not rely on the consumer interaction to enable protection of their home network.

If more sophisticated consumers are comfortable interacting with their home security solution, then they can log into a portal to add more information about a specific device on their network. With this additional data the system will gain even more information to protect them more effectively. However, it is important to note that the system can run autonomously without any required input from the consumer.

4.4 Act

Finally, the system needs to act and uses a set of automated tools to create rules around a new threat, in the form of new attack signatures, and deliver those to every home that might be vulnerable in order to block the attack. Given the dynamic and timely nature of attacks on the Internet these updates are delivered in near real-time to ensure that attacks are caught as quickly as possible. The back-end systems are continuously monitoring across the deployed networks and if a repeating attack pattern is recognised then a new security envelope is generated to protect the consumers’ network.

5. BUILDING BLOCKS TO SECURE THE DIGITAL HOME

Given the challenges the HomeGuard solution leverages a set of building blocks working on conjunction to deliver an enhanced security and privacy solution for the consumer’s home network with additional protection against attacks on the Service Provider network originating from the home.

The building blocks are outlined in the following paragraphs and include:

- Home IPS
- Device Discovery
- Access Control
- M2M Control
- Privacy
- Posture Assurance

5.1 Home IPS

Enterprise and commercial systems are protected today using Network Intrusion Detection Systems (NIDS) and Network Intrusion Prevention Systems (NIPS) that have the ability to perform real-time traffic analysis and packet logging on IP networks. The opportunity is to apply these mechanisms of signature-based threat defense and anomaly detection, to the connected home environment. The HomeGuard solution uses Snort, the same IPS engine that’s revolutionised the enterprise security market.

5.2 Device Discovery

In order for home IPS to work, it needs to be able to see the home environment, including all of the connected devices deployed in the home network.

This is critical to make sure that it applies IPS signatures and security rules in efficient and effective ways, without causing network disruption on one end or false positives on the other.

To do that, a device discovery capability that keeps tabs on what’s inside the residential network of a specific home, including both service provider CPE devices and consumer retail devices is leveraged. The discovery mechanism can use a range of different techniques to identify devices based on signatures provided in their communications with the network.

5.3 Access Control

Access control is a critically important aspect to securing the home network. For instance, any web server today can discover many home webcams. It’s not hard for a criminal to find an IP address of a webcam, gain access to it, and, with that information, see what is in the home.

HomeGuard implements a secure network VPN connection to assure secure, encrypted communication between devices and outside applications. This is a critical element of protecting consumer privacy and the physical premises.

Returning to the prior example of the webcam; by using VPN connections between the webcam and the application, the system can make sure that only that subscriber or other users they authorise can access it.

The access control mechanisms also include capabilities to quarantine a suspicious device. If a device is detected that is creating lots of suspicious traffic, suggesting it may be infected or a source of an attack, or something that’s being attacked by other devices, it can be put in a quarantine subnet and make sure it functions but can’t send information outside its specific subnet.

5.4 M2M Control

Another area of attack profile that can be detected is when a device starts to communicate with a device within the home that is unexpected. For example, it may be normal for the clothes dryer to talk with the washing machine. But if the washing machine is trying to see what’s happening with the smart TV, it may be the start of an attack or some other malicious behavior. Given the position of the platform in the residential gateway it can control information and communication between devices to block off potential avenues of attack. It monitors that traffic and reports suspicious activity. Subsequently it can alert the user that their connected endpoint is behaving strangely, alert the vendor that there may be a vulnerability, or just block the device from interoperating on the home network.

5.5 Privacy

Privacy is an important consideration and HomeGuard monitors all video and audio streams in the home network to make sure the user’s privacy is protected.

There are a wide variety of consumer services now that use streaming audio and video within the home such as Skype, WebEx, FaceTime, etc. The system can recognise if someone is intercepting or manipulating those streams providing an additional layer of protection for content streaming to, and from, new devices in the home.

5.6 Posture Assurance

One data point that is known from industry research is that most consumer devices installed in the home still have the default credentials, like “admin” for the user name and some simple password. Which makes it very easy for an attacker to gain access to a webcam or some other device and manipulate it.

To protect against this the system carries out a passive discovery on all connected devices in the home to make sure the credentials aren’t set to default.

If there are identified vulnerabilities in that device, the system alerts the user the that it needs to be patched or changed. To enhance the probability of those changes being implemented the system enables the consumer to jump right to the application window that enables them to either fix the vulnerability or change the credentials. This automation maximises the opportunity that the consumer will address the identified vulnerability.

6. SUMMARY

As has been discussed, the dream of the Internet of Things (IoT) is becoming a reality in our homes today. However, the smart home can become a security nightmare because every connected device is a new potential entry point for cyber-attacks. The paper has introduced the concept of a cloud/client software solution that interoperates with residential gateways to provide enhanced security and privacy management capabilities to address securing the home network and insulating the Service Provider network from attacks originating out of the consumers’ home.

It is however clear that the perceived risks to privacy and security could result in a lowered consumer confidence resulting in the IoT technologies not realising their full potential and reducing their adoption within consumer homes. With this in mind it is vital to promote the protections that are put in place with any potential solution.