UDC 621

SECURITY PROBLEM ON THE INTERNET OF THINGS NETWORKS

Olena G. Grygorenko, Galyna D. Sozonnik

Institute of Telecommunication Systems
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

Aymen Mohammed Khodayer Al-Dulaimi

Al-Farahidi university, Baghdad, Iraq

Background. The number of IoT devices is increasing every year. At the same time, the number of data transmitted by these systems over networks is growing. Smart devices do not need a powerful processor, and the amount of memory is usually measured in kilobytes, so antivirus software and firewalls are not installed on such devices. Cybercriminals are increasingly exploiting the vulnerabilities of such home networks for the purpose of extortion or simply hooliganism. There is a security problem in the Internet of things networks that needs to be solved.

Objective. The aim of the article is to identify the main causes of vulnerabilities in smart home systems and networks and to offer protection.

Methods. As methods, we consider the most common attacks on smart home systems

Results. The main security features on the Internet of things are timely software updates, changing default settings, multi-factor authentication, encrypting traffic on your home network, installing a firewall on your home router and filtering traffic. When managing devices through a browser and remotely connecting to your home network via the Internet, you must use a VPN.

Conclusions. The proposed methods for ensuring security in the networks of the Internet of things can protect smart devices and the network from attack by intruders.

Keywords: Internet of Things; IoT network; smart home systems; home network; multi-factor authentication; IP cameras.

Introduction

Throughout the development of mankind, people have always strived for comfort and various amenities. Smart home and other smart devices are modern, fashionable, technological. For example, the ability to remotely connect to the system and give it a command to heat the air in the apartment to the required temperature, heat food, provides convenience for people in everyday life. Opening a door with a fingerprint is a reality today.

However, such smart devices receive, process and transmit data, so the question arises of data security and the safety of such smart systems. Cybercriminals can hack into networks, devices and gain access to all kinds of data and even organize DDoS attacks from devices on a home network. Therefore, it is relevant to consider the security problem of gadgets for a smart home and determine the necessary measures and means of protection.

Problems protecting smart devices

Smart home appliances include highly specialized devices. A smart socket or thermostat does not need a powerful processor, and the amount of memory is usually measured in kilobytes. Therefore, antivirus software is not installed on such devices. As for firewalls or other means of protection, it is hardly possible to implement them at the device level.

The second problem is passwords. Many IP cameras and other gadgets come with a standard password. In the user manual, the manufacturer usually asks for a password change. As practice shows, many consumers do not change passwords, even specialists sometimes forget about it or are lazy about it.

The functions of the device control center of a smart home can be performed by a smartphone, tablet, smart TV or fridge (that is, an ordinary fridge with a tablet built into it). Therefore, if you access the control center, you can receive any data from the system, which can lead not only to disruption of the devices, but also to more serious consequences. For example, Hikvision's products and their cameras popular among consumers hack very simply [1,2].

The minimum damage received by attackers from breaking into a smart home will allow them to use the Internet connection for free. More problems will come from intercepting data from the network, including logins, passwords, and so on. Sensitive information is usually encrypted by browsers and smartphones, but vulnerabilities are everywhere.

The main threats to smart home systems and their consequences

The smarter the house, the more serious the consequences of a hacking can be. If the consumer has smart devices that control everything from doors and windows to thermostats, lighting and water heaters, then hacking can be really life-threatening.

An example [3] is the incident with the Samantha and Lamont Westmorland family from Milwaukee, Wisconsin, who bought a smart thermostat, doorbell, and Google Nest security camera. Hackers broke into their home network, turned on terrible music through the camera and began talking to victims through a gadget, and then raised the room temperature to 32 degrees.

At first, the Westmorelands thought it was some kind of failure, but having suspected something was amiss, they changed the password. When this did not help, so they had to call the provider and set a new network identifier.

If hackers blocked smart windows and doors, and then raised the temperature, they would be able to engage in extortion, actually threatening the life and health of the owners of the smart home. And so it's just petty hooliganism.

Google recommends two-factor authentication.

Another terrible threat is smart cars. If you can still do something with an increase in temperature in the room, then if you break into the on-board computer of a car speeding, there will be a disaster. Yes, and for unlocking the doors they can extort money, especially if it is comparable to the price of new glass.

You can find vulnerabilities for hacking smart thermostats. Andrew Tierney and Ken Munro of Pen Test Partners have developed a ransomware for a smart thermostat [4]. Its capabilities were demonstrated at the DefCon conference.

The researchers explained: the popular thermostat (the brand was not named) works under the control of the operating system (OS) on the Linux kernel and does not check which files it launches. If the owner wants to change the picture on the thermostat display, instead of the image, he can run malware pre-copied to the device's memory. As a result, the hacker can control the temperature of the thermostat or block the device so that the owner can not do anything. Then the cybercriminal extorts money, and for many it is easier to pay than to fight.

The possibilities of breaking smart locks are determined by the methods of opening them:

- recognize the owner's smartphone, which went to the door, via Bluetooth;
- remotely - using the command in the application sent via the Internet;
- voice command, which the voice assistant perceives on the smartphone and transmits it to the smart device.

The transmitted data is encrypted, but this is not enough.

For example, if the potential victim's iPad or iPhone lies close to the locked door, nothing prevents the attackers from using the Siri program and saying in the entrance: "Hi, Siri. ¬ Open the door! " A smart lock, knowing that the owner's gadget is nearby, will easily let criminals in. Usually only an unlocked device perceives voice commands. However, many users unlock the devices they use at home.

You can also crack a smart lock by infecting a smartphone or tablet with a virus. The malware is able to seize control of the lock and imitate the action to open it. This is easier than intercepting encrypted data packets and decrypting them.

Some models are equipped with a physical button that authorizes a new device. If one of the user's guests uses this technique, he will make the lock recognize his smartphone as trusted, and thus will be able to penetrate the room.

Most models of home IP cameras can be configured very simply: just connect the gadget to your home network and then go to a specific IP address in a browser or install the manufacturer's application on your smartphone. Therefore, Internet cameras are subject to significant threats from cybercriminals.

Newer models typically use an encrypted https connection. Older and / or cheaper cameras exchange data with a smartphone through a cloud service. In this case, the cameras send unencrypted requests to the cloud. Retrieving the session ID with which traffic is encrypted is not difficult, especially if the hacker is connected to the same Wi-Fi access point.

In addition, on many cameras, the manufacturer sets a standard and / or unchangeable password (root, etc.). Knowing the manufacturer's IP address and camera model, a hacker can download software for it from the manufacturer's website, find this password

and gain full access to the gadget, which poses a significant threat.

Most often, attackers use users' IP cameras to launch DDoS attacks on known resources or mine cryptocurrency from them.

For example: a woman bought a Chinese second-hand camera to monitor her puppy while she was at work, and access to the video stream of the camera was directly on the manufacturer's website, which is a clear security risk.

Hacking a video camera can also be done through the so-called "port forwarding" [5]. At the same time, users open a specific port on the router in order to be able to remotely connect to their home camera via the Internet. This opens up opportunities for hackers to attack. Exploits are used in a similar way to gain access to the camera control panel, which allows, in particular, extracting unencrypted video from device drives [5].

Another vulnerability is that many manufacturers leave service entrances to cameras that are accessible through a browser. For example, for Foscam the address is in the format xxxxxx.myfoscam.org:88, at the beginning you need to substitute two letters and four digits [5].

The Shodan search site allows you to find tens of thousands of cameras that are "available" for hacking [5]. Requests like netcam city: Moscow, netcam country: RU, webcamxp geo: 55.45,37.37 in Shodan will also show a lot of useful information.

Examples of queries on Google are as follows [5]:

- inurl: "wvhttp-01"
- inurl: "viewerframe? Mode ="
- inurl: "videostream.cgi"
- inurl: "webcapture"
- inurl: "snap.jpg"
- inurl: "snapshot.jpg"
- inurl: "video.mjpg"

In the search site for the Internet of things, ZoomEye cameras can be seen at the request of device: webcam or device: media device.

Similarly, Censys, at the request of 80.http.get.body: "DVR Web Client", will display a list of cameras connected to the IP DVRs. At the request of metadata.manufacturer: "axis", Axis cameras can be seen. The camera owners are unaware.

Smart light bulbs can also pose a threat to users. White hackers Colin O'Flynn and Ial Rowen have significantly cracked the popular Philips Hue smart lamps [6]. They found vulnerability in the Hue Bridge, through which the lamps are controlled, and controlled them from a distance of 200 m.

Through this vulnerability, cybercriminals can not only control lighting, but also intercept or replace data packets that are sent inside the home network without protection. In an experiment, Rowan and O'Flynn made the lamps blink at a frequency of more than 60 Hz. The human eye is not sensitive to this frequency, and a telescope with a special light sensor mounted in front of the window can easily receive data from the home network. The data transfer speed will turn out small, up to 10 Kb per day, but sufficient for the theft of logins and passwords.

Through the lamps, malware can also be introduced into the home system. The bridge communicates with devices using the ZigBee encoded wireless standard, the main key from which hackers have long been uploaded to the Internet. Since devices within the network do not control the signature of the transmitted data when updating the firmware, you can start a fake update and conduct DoS attacks, for example.

Philips has already closed the vulnerability and released a patch for bridge software and a mobile application. However, vulnerabilities may also appear in third-party applications. Also, you can hack smart devices with the help of a drone.

Developers of the Internet of things systems simplify everything as much as possible in order to save resources and time. The result is smart device vulnerabilities and opportunities for cybercriminal attacks. Researchers at Pen Test Partners found that the Samsung RF28HMELBSR smart fridge does not check SSL certificates when establishing an SSL connection, and warned of a threat [4].

Vulnerability allowed for attacks Man-In-The-Middle. And since the information from the "Google Calendar" was displayed on the display of the smart fridge, an attacker who hacked the smart device and connected to the same network could easily get an account from email and other services. Connecting to the network in which the fridge is located is quite simple. For example, you can create a fake Wi-Fi access point or organize deauthentication of a real user.

Russian developer Anna Prosvetova found a vulnerability in Furrytail Pet Smart Feeder smart animal feeders, which were sold on the Xiaomi Youpin platform [5]. She studied the system API and accidentally realized how to access all of these feeders on the planet. The discovered vulnerability allows obtaining data on Wi-Fi networks of the owners of feeders and see how much food is in each feeder. An attacker can set up a schedule for a separate feeder or

run a script for all feeders at once to pour too much food for all animals or, conversely, delete a schedule and deprive pets of dinner. Finally, you can make the feeder download and install the dummy firmware. After that, you can restore the gadget only in the factory. There are no software warranties.

The number of hacking devices for smart home

The number of attacks on IoT systems is increasing every year. According to Kaspersky Lab, in the first half of 2019, smart homes and industrial systems attacked an average of 20 thousand times in 15 minutes [7].

Through the TCP service, attackers tried to reach remote administration systems based on Telnet and RDP, servers and databases. Researchers found 50 honeypots (points at which vulnerabilities were specially left to collect data on attacks). They estimated that since the beginning of the year, these points have been attacked 105 million times with 276 thousand unique IP addresses [7].

The main wave of attacks came from China - 30%. Brazil came in second place (19%), which was the leader last year. The top five are Egypt (12%) and the USA (8%).

Statistics for the first half of 2018 and 2019 are presented in Table 1.

Table 1. Source countries for Telnet attacks on Kaspersky Lab [7]

2018		**2019**	
Brazil	28%	China	30%
China	14%	Brazil	19%
Japan	11%	Egypt	12%
USA		Russia	11%
Greece	5%	USA	8%
Turkey	4%	Vietnam	4%
Mexico	4%	India	4%
Russia	3%	Greece	4%
South Korea	3%	South Korea	4%
Italy	2%	Japan	4%

Analysts said [7] that hackers use both brute force attacks and known vulnerabilities. The most popular login / password pairs were the following: support / support, admin / admin, default / default and root / vizxv (this pair is common in Chinese smart technology).

Most often, hacked devices infect Mirai family of malicious software, which is easy to assemble for any hardware architecture. Mirai makes the smart gadget of a botnet part and possibly an accomplice in crime. Also infect Hajime, NyaDrop and Gafgyt (it is Bashlite) [5].

Securing smart home systems

One of the first and easiest ways to protect smart home systems is to change the default password. You need to set a complex password for the control panel of the smart home, as well as the home Wi-Fi network and the router itself. When managing devices through a browser When managing devices through a browser and remotely connecting to your home network via the Internet, you must use a VPN (virtual private network), which, for example, is built into the Opera browser.

The next step to security is the constant and timely updating of software on smartphones, tablets and smart home gadgets. You need to use two-factor authentication where possible. A bad idea is to use the Jailbreak IOS operation on Apple devices, which allows you to install unlicensed software and gain full access to the file system not only to users, but also to attackers. There is evidence that such devices are vulnerable to contactless hacker attacks [8].

To control a smart home, it is advisable to use specialized controllers, for example, based on the Raspberry Pi, which are less prone to hacking and are more configurable.

For security, you should also not purchase cheap Chinese devices, especially smart locks, IP cameras and the like, which have many vulnerabilities and are simply hacked. In addition, for such devices, firmware updates are usually not released.

In the home network, you also need to use a firewall on the router, replacing the default settings. A firewall allows you to securely control remote access and block unwanted traffic based on user-defined rules.

It is advisable to set filtering by region for access to the home network. A method of protection is also encryption of traffic within the home network. on the router you need to activate the WPA2 protocol (Wi-Fi Protected Access, 2) - Personal and use a secure connection.

Fig. 1 presents a home network security management scheme.

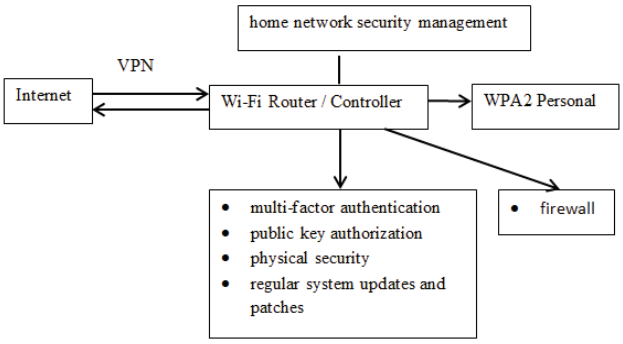

Fig.1 - Home network security management scheme

Conclusion

The article discusses common vulnerabilities in the Internet of things networks and the effects of attacks on smart systems.

Quantitative indicators of attacks on the Internet of things networks are presented.

Priority tools and measures are proposed to protect the security of home systems and networks.

References

[1] https://hikvision.org.ua/uk/articles/zlom-reyestratoriv-ta-ip-kamer-hikvision-chastyna-2.

[2] John Honovich. US Embassy Ukraine Specifies Hikvision, Published on Feb 12, 2018, https://ipvm.com/reports/ukr-hik

[3] Ashley Sears. 'Felt so violated:' Milwaukee couple warns hackers are outsmarting smart homes, - posted 10:14 pm, september 22, 2019, https://fox6now.com/2019/09/22/felt-so-violated-milwaukee-couple-warns-hackers-are-outsmarting-smart-homes/

[4] Andrew Tierney. Thermostat Ransomware: a lesson in IoT security, - 08Aug 2016, https://www.pentestpartners.com/security-blog/thermostat-ransomware-a-lesson-in-iot-security/

[5] Shestakova Kseniya. Your nudes in LIVE mode. How to hack a smart home, even a camera and a power outlet, https://www.iphones.ru/iNotes/chem-opasen-umnyy-dom-kak-vzlamyvayut-vashi-umnye-lampy-i-rozetki-chtoby-oni-shpionili-i-ddos-ili-10-23-2019

[6] Colin O'Flynn. A LIGHTBULB WORM? Details of the Philips Hue Smart Lighting Design Colin O'Flynn – August 1, 2016. (Black Hat USA 2016 White Paper) http://colinoflynn.com/wp-content/uploads/2016/08/us-16-OFlynn-A-Lightbulb-Worm-wp.pdf

[7] Den Demeter, Marco Preuss, Yaroslav Shmelev. The Internet of Things (IoT): a history of malware. - October 15, 2019, https://securelist.ru/iot-a-malware-story/94900/

[8] Sumra, Husain. 'Hacking Team' Data Breach Confirms Firm's Ability to Infiltrate Jailbroken iPhones.

Григоренко О.Г., Созонник Г.Д., Аймен Мохамед Кодайєр Аль-Дулаімі.
Проблема безпеки в мережах інтернету речей

Проблематика. Кількість пристроїв інтернету речей збільшується з кожним роком. При цьому зростає число даних, які передаються цими системами, мережами. Смарт пристроям не потрібен потужний процесор, а обсяг пам'яті зазвичай виражається в кілобайтах, тому антивірусне програмне забезпечення і брандмауери на такі пристрої не встановлюють. Кіберзлочинці все частіше використовують уразливості таких домашніх мереж з метою вимагання або просто хуліганства. Виникає проблема безпеки в мережах інтернету речей, яку необхідно вирішувати.

Мета досліджень. Метою статті є визначити основні причини вразливостей систем і мереж розумного дому і запропонувати засоби захисту.

Методика реалізації. В якості методів використовується розгляд атак на системи розумного дому, що зустрічаються найбільш часто.

Результати досліджень. Основними засобами забезпечення безпеки в мережах інтернету речей є своєчасне оновлення програмного забезпечення, зміна налаштувань за замовчуванням, багатофакторна аутентифікація, шифрування трафіку в домашній мережі, установка на домашньому маршрутизаторі брандмауера і фільтрації трафіку. При управлінні пристроями через браузер і віддаленому підключенні до домашньої мережі через Інтернет необхідно використовувати VPN.

Висновки. Запропоновані способи забезпечення безпеки в мережах інтернету речей дозволяють захистити смарт пристрої та мережу від атак зловмисників.

Ключові слова: інтернет речей (Internet of Things); мережі IoT; системи розумного дому; домашня мережа; багатофакторна аутентифікація; IP-камери.

Григоренко Е.Г., Созонник Г.Д., Аймен Мохамед Кодайер Аль-Дулаими.
Проблема безопасности в сетях интернета вещей

Проблематика. Количество устройств интернета вещей увеличивается с каждым годом. При этом растет число данных, передаваемых этими системами, по сетям. Смарт устройствам не нужен мощный процессор, а объем памяти обычно выражается в килобайтах, поэтому антивирусное программное обеспечение и брандмауэры на такие устройства не устанавливают. Киберпреступники все чаще используют уязвимости таких домашних сетей с целью вымогательства или просто хулиганства. Возникает проблема безопасности в сетях интернета вещей, которую необходимо решать.

Цель исследований. Целью статьи является определить основные причины уязвимостей систем и сетей умного дома и предложить средства защиты.

Методика реализации. В качестве методов используется рассмотрение наиболее часто встречающихся атак на системы умного дома.

Результаты исследований. Основными средствами обеспечения безопасности в сетях интернета вещей являются своевременное обновление программного обеспечения, изменение настроек по умолчанию, многофакторная аутентификация, шифрование трафика в домашней сети, установка на домашнем маршрутизаторе брандмауэра и фильтрации трафика. При управлении устройствами через браузер и удаленном подключении к домашней сети через Интернет необходимо использовать VPN.

Выводы. Предложенные способы обеспечения безопасности в сетях интернета вещей позволяют защитить смарт устройства и сеть от атак злоумышленников.

Ключевые слова: интернет вещей (Internet of Things); сети IoT; системы умного дома; домашняя сеть; многофакторная аутентификация; IP-камеры.