DOI: https://doi.org/10.30837/csitic52021232903

Securing the Internet of Things via VPN technology

Mykhailo Hunko[1]
Igor Ruban[2]
Kateryna Hvozdetska[3]

[1] Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, hunko@ieee.org,
[2] Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, ihor.ruban@nure.ua
[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, kateryna.hvozdetska@ieee.org

Abstract. The speed at which the Internet of Things is evolving these days looks promising for the smart environment of the future. Along with the popularity of smart devices, concerns about the security of IoT devices are also growing because they are inherently resource-constrained, heterogeneous and they suffer from a lack of standard security controls or protocols. In particular, because of their inability to support today's secure network protocols and security mechanisms, standard security solutions are not suitable for dynamic Internet of Things environments that require large and smart infrastructure deployments. Current Internet of Things environments use predominantly cloud-based approaches so that data can be exchanged in unlimited quantities, leading to additional security and privacy risks. While standard security protocols such as virtual private networks have recently been implemented for certain Internet of Things environments, the implementation models presented have few variations and are virtually unscalable for any dynamically scalable Internet of Things deployment.

Keywords: *Internet of Things; Virtual Private Network; security; data.*

I. INTRODUCTION

As IoT devices become more available and widespread, people should consider using more sophisticated security features to keep their data safe from getting stolen. The IoT has revolutionized how much more useful the everyday household devices we use in our daily lives can become if they are connected to the Internet. It is now possible to control the lights in the house while you currently outside, remotely watch the house through video monitoring, control the temperature with a special app, turn on the kettle, and so on. It's okay to say that your phone easily fits into this category because of the ability to completely track you: the smartphone can record, stream, and geolocate you[1].

One thing that may escape people's attention is that all this data, by definition, can be used against its owners. Individually, the pieces of information stolen may seem insignificant, but if you put them together into one single "portrait," that data becomes valuable personal information. This does not mean that companies do not care about the security of their products, but it requires energy and resources, which these devices often lack - for a variety of economic reasons.

The reality is that information about your health, bad habits, purchases, location, and even any passing talk is all recorded in whole or in part by these various devices - and these devices can be vulnerable to some kinds of leaks, so the phrase "IoT Security" is considered by some people like a pun.

So, satisfying the security needs of the IoT is one of the most important parts. We need a functional end-to-end security

a model that can ensure security, privacy, and confidentiality throughout the IoT system lifecycle, including design, deployment, and operational phases.

II. MAIN PART

IoT devices connect via an Internet connection and speak to their destination to achieve whatever it is you've asked the device to do. The problem comes when people, somewhere along the way, intercept that data, make a copy of it and then use it for their purposes.

A VPN solves this problem by encrypting all traffic from point A (the device) to point B (the VPN server). Many companies that allow employees to work remotely will require those employees to connect to the company's business network with a VPN for this very reason; sensitive data always takes a secure route to or from the local network.

If someone gains access to the captured data, they won't be able to do anything significant with it. A VPN not only encrypts traffic - it usually allows you to choose an exit point - basically anywhere in the world. This means that it provides the ability to hide not only what data is being transmitted, but also where it's being sent from globally, and from which IP it's taken. It creates a mask of privacy that all your traffic is passed through.

When you have this mask, attackers cannot attack your IoT devices because they cannot see them in any way to get access. This makes it much more difficult to produce targeted botnet and DDOS attacks because you are anonymous from a traffic point of view. Setting up this router level will protect all data accessed and transmitted from any device on your network, including all of your IoT devices.

So, as well as mitigating direct attacks and masking traffic from nefarious middle-men, a VPN naturally hides your content from all potential snoopers. This can include advertisers, trackers, government agencies, and your ISP. Because, to the outside world, you're using a different IP to your actual IP, it becomes next to impossible to directly link your activity to your ISP-provided IP. The ability to effectively spoof your IP address to anywhere in the world can have downsides, especially when it comes to geo-locked applications – but the correct configuration will usually find a work-around.

There are three most popular methods to harm IoT devices: botnet attacks, Man-in-the-Middle attacks (MITM), General Sniping

DOI: https://doi.org/10.30837/csitic52021232903

IoT devices are a prime target for botnets. A botnet is a series of Internet-connected devices, joined by a hacker, that can perform a large-scale attack, such as a distributed denial of service (DDoS) attack on a massive scale. A botnet can remain dormant until an attacker sends a command over the Internet, and because IoT devices typically have no anti-virus protection, it can be difficult to detect and remove them. The main problem is that many IoT devices are relatively simple compared to PCs and smartphones, so a sophisticated security architecture is often not a primary goal for smart device manufacturers. [2].

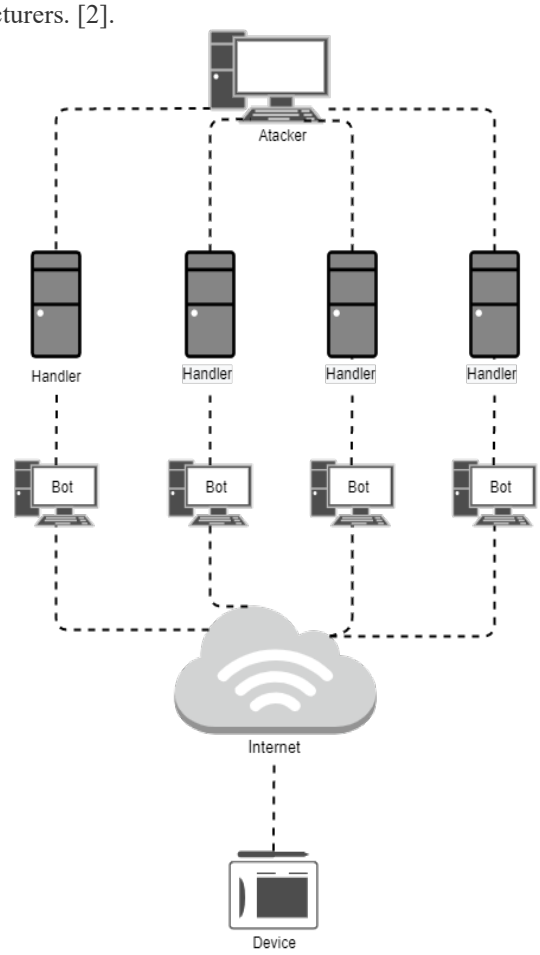

Figure 1. Scheme of DDoS attack via bots

The basis of a Man-In-The-Middle (MITM) attack is the unauthorized intervention of a third person, controlling the interception of messages and access to information like a fisherman in a river (Figure 2). MITM attacks are an ideal way for cybercriminals to view or modify sensitive information and even hack into user accounts.

Either of these actions can have huge consequences for the victim, whether it's an individual, a corporation, or a cloud-based network connected to multiple companies or brands. MITM attacks increase the importance of encrypting traffic so that it is unreadable in transmission, even if someone intercepts it.

Man-In-The-Middle attacks are especially effective against IoT devices that have not been properly secured by the manufacturer. Many solution providers leave the manufacturer's default passwords in place during installation.

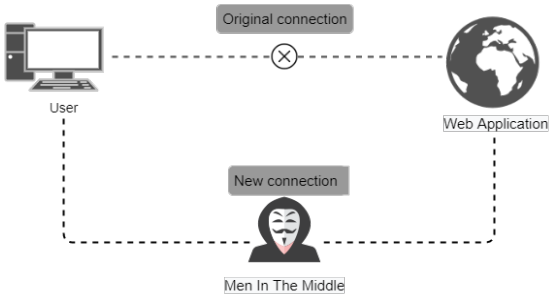

Figure 2. Scheme of MITM attack

Hacking into a device or gateway can be as easy as brute-forcing the default password for that model of the device. Moreover, unlike a Web browser, where you can check "HTTP" (secure) in the address bar to make sure the site is secure, IoT devices have no such standard protocol. They have no way to alert the user if the security certificate has expired or is otherwise invalid.

The banal reason to use VPN is general snooping. When every device is connected to the Internet, Internet Service Providers (ISPs) and the government agencies that control them have access to a huge amount of your data. With IP addresses in the public domain and easily readable traffic, they can monitor all of your daily activities. This is another reason to encrypt all of your Internet traffic. So, in addition to preventing direct attacks and masking traffic from nefarious middlemen, a VPN naturally hides your content from all potential snoopers. This can include advertisers, trackers, government agencies, and your ISP.

Besides, when a device is connected to a VPN, all traffic to and from the device is encrypted [3]. The encryption used by top-tier VPN providers is usually 256-bit AES, which is considered military-grade encryption.

III. CONCLUSIONS

IoT development has a long way to go before fully-secured, standardized, and trustworthy devices are normalized in the market. As such, businesses need to step up their game to help protect against attacks and ensure information doesn't fall into the wrong hands.

A VPN is a great solution for most users, especially those with an increasing number of connected IoT devices. The security and privacy benefits, which it brings, play a big role in protecting user's home and sensor-based IoT devices from attacks.

REFERENCES

[1] Коваленко А.А. Моделі транзитної комутації гетерогенних мереж / А.А. Коваленко, А.В. Аніщенко // Проблеми інформатизації. Тези доповідей шостої міжнародної НТК. – Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Харків: НТУ «ХПІ», 2018. – 14-16 листопада 2018. – С. 78.

[2] Lyu, M.; Sherratt, D.; Sivanathan, A.; Gharakheili, H.H.; Radford, A.; Sivaraman, V. Quantifying the reflective DDoS attack capability of household IoT devices. In Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks; ACM: New York, NY, USA, 2017; pp. 46–51.

[3] Vitalii Tkachov, Anna Budko, Kateryna Hvozdetska and Daryna Hrebeniuk. Method of Building Dynamic Multi-hop VPN Chains for Ensuring Security of Terminal Access Systems // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T): Kharkiv 06-09 oct. 2020, Kharkiv