# Securing a Home Network by Using Raspberry Pi as a VPN Gateway

**Conference Paper** · April 2018

CITATIONS
3

READS
3,754

**3 authors:**

Bogdan Jeliskoski
University American College Skopje
**3** PUBLICATIONS **3** CITATIONS
SEE PROFILE

Biljana Stojcevska
University American College Skopje
**22** PUBLICATIONS **66** CITATIONS
SEE PROFILE

Адријан Божиновски
University American College Skopje
**29** PUBLICATIONS **97** CITATIONS
SEE PROFILE

# Securing a Home Network by Using Raspberry Pi as a VPN Gateway

Bogdan Jeliskoski, Biljana Stojcevska, Adrijan Bozinovski
School of Computer Science and Information Technology
University American College Skopje
Skopje, Macedonia
bogdan.jeliskoski@live.com, { stojcevska, bozinovski }@uacs.edu.mk

**Abstract— The need of home Internet of Things (IoT) applications is rapidly increasing as the ease of access and diversity of technologies is growing. Securing the network is the first thing to consider before connecting any IoT device on the Internet. The central theme in this paper is providing protection for IoT devices in a home network and their safe connection to the Internet. The security threats and risks of using IoT devices on the Internet are outlined and discussed and a solution for security in an IoT home network is presented. The protection used in the IoT home network is based on a Raspberry Pi device that is installed as a Gateway on the internal network, with all IoT devices connecting to it as their gateway, or via VPN tunnels. The paper explains the problems, challenges and the role the gateway plays in protecting the devices on the network and presents an analysis of the results of the testing of the presented solution.**

***Keywords— Internet of Things; Raspberry Pi; network security***

## I. INTRODUCTION

The modern way of life would be inconceivable without quick and easy access to information and would be difficult to imagine without computer networking systems that connect different or similar devices in one whole. The need for network connectivity naturally arises primarily from the need for continuous exchange of information.

Today, there is a large number of devices that are used for Internet connectivity, and, according to purpose, they are commonly divided into consumer, infrastructure, and business applications [1]. It is inevitable to mention Internet of Things (IoT) in the field of network connectivity and information transfer. IoT is seen as the next stage of an information revolution in which there should be a connection to everything in the world. IoT contributes to the modernization of services that a person can receive through the network connection, or the Internet [2] [3].

IoT represents interconnection of devices that incorporate software, electronics, actuators and sensors which are connected in a network in order to achieve easier and faster information exchange. The idea of IoT is to primarily overcome the gap between the physical and the computer world, where physical objects and devices would be integrated into a seamless information network and physical objects could be active participants in the processes of information exchange. Such advanced technology offers the opportunity to connect people, systems and processes and finds huge application in all spheres of modern life.

IoT devices are used in modern cars with built-in sensors, in modern medicine (for example, for monitoring the work of the heart), the chipping of animals, city transport, video surveillance, environmental monitoring, various field operations that help firefighters save people, or in modern households, to name a few applications. But the emergence of more applications and their availability for users makes them more vulnerable to a wider range of security weaknesses [4] [5].

## II. IOT AND SMART HOMES

### A. *Internet of things*

The term Internet of Things was first used in 1998 to distinguish itself from other related terms, but also to present the vision of IoT is a network of networks, through which a large number of objects, devices, objects and sensors are connected while requiring minimal human intervention. IoT enables physical devices, vehicles, home appliances and other objects that are characterized by electronic, software, sensory, actuarial, and connectivity to exchange information [4] [6].

A feature of each IoT device is that it has a built-in unique computer system that is capable of working internally within the existing Internet infrastructure. The number of such devices on the Internet is constantly increasing. According to the assumptions of experts and researchers in the field, by 2020 the number of such devices and facilities will be as much as 30 billion, and the global market value of IoT will reach 1.7 trillion dollars [1] [3] [6] [7] [8].

IoT enables devices and facilities to be managed and controlled remotely via an existing network infrastructure, creating greater opportunities for direct integration of the physical and computer world. All this is done to facilitate and improve the efficiency and accuracy of reduced human intervention, as well as economic benefits. IoT is also an example of a more general class of cyber-physical systems that encompass technologies applicable from smart networks, virtual centers, smart and modern homes and cities, and intelligent information transport [6] [9] [1] [10].

IoT has a huge and wide range of uses in almost all areas of contemporary living. Because of this, IoT devices are characterized as a mixture of information, hardware, software and service. However, the main function of IoT devices is the collection and dissemination of useful information through different technologies among different devices [1] [10].

### B. *IoT application in homes*

The application of IoT technology and the solutions resulting from the use of such devices in the home make the place of living more comfortable and pleasant. IoT technology and devices occupy a large part of modern homes, primarily in the field of automation. This system provides its users an opportunity to control all devices in the home including lighting, heating, air conditioning, security systems, home maintenance etc. The benefit of IoT devices is based primarily on ease of use, connectivity and functionality. In addition, they contribute to long-term benefits and create an ecological home by automating some functions such as switching off lights or electronics. According to a large number of people, one disadvantage associated with the use of this technology in homes is certainly the high price [11] [12] [13].

IoT devices can be used to monitor and control mechanical, electrical and electronic systems used in different types of homes (for example, houses, apartment buildings or institutions of different types). Some of their areas of application are:

- integration of the Internet with energy management systems in order to create energy efficient and smart homes managed by IoT,

- applications for monitoring energy consumption and monitoring the behavior of visitors in the home,

- integration of smart home appliances with future applications,

- providing assistance in the operation of people with disabilities and older people, etc.

Devices that are connected in the system can be managed even from a distance, so, for example, the air conditioner in a home or office can be switched on to operate at a certain temperature through the mobile phone before the person arrives there. The idea is that through these applications users can do more things at the same time. IoT technology thus contributes to providing consumers with a greater quality of life [13] [14].

Smart technology of this type is in fact a generic platform that consists primarily of hardware devices, sensors and software applications. Information is collected through the sensors and injected into the applications, from which the appropriate action and solution originated. For example, a water sprayer placed in the yard for irrigation of grassy surfaces can recognize the rain and switch off to save energy.

There are many examples of IoT applications and we will mention some of them in the remainder of this section.

Much of the IoT technology refers to virtual help. The Ubi application acts as a voice activated by the computer, and can perform tasks related to reading, voice memos, performing notifications on certain events, audio calendar, e-mail, and so on. The application uses a microphone and speakers and also has sensors for monitoring the environment (temperature, lighting, air pressure and humidity).

The Netatmo application determines the air quality and offers solutions for smart homes. In order to determine the air quality, it collects information about the temperature, humidity and amount of $CO_2$ in the air. This application sends a warning to the user when needed [4].

WeMo is another type of application from the wide range of IoT technology used to turn on or off electronic devices from anywhere. For this purpose, it uses Wi-Fi, but it can also be set up automatically (for example, turn on devices at sunrise) [4].

The Lockitron application is used to lock the door through the phone, and the user can authorize members of the family so they can unlock them via their phones using the Internet [4].

Blufitbottle is a drinking water bottle that records the user's hygiene habits but also remembers the hydration [4].

## III. PROTECTION OF SMART DEVICES WITH VPN AND IOT GATEWAY

According to many researchers, the biggest disadvantage of IoT technology is the lack of technical standards (hardware and software variations among devices that are connected). The IoT's amorphous computational nature is also a security issue, since operating system kernel errors often deter users. Other researchers believe that IoT is becoming a "powerhouse" tool, which creates a supervisory society where technology is routinely used. According to them, people are gradually losing control of their own lives and are driven by sensors and self-managing devices. In addition, the American Civil Liberties Union has expressed concerns about the IoT, believing it impedes people's control over their own lives [15] [16] [17] [18].

However, for IoT users, the greatest threat is privacy protection. While smart technology can reduce or eliminate human intervention, it also increases the potential for hacking or major crashes. Certain problems can also arise by generating a large number of unnecessary information that will make smart devices produce misguided conclusions [17] [18]. The overall understanding of IoT is essential to the basic security of users. A growing number of surveys are focused on the IoT invasion and the threats arising from the application. Many consumers are willing to give up smart technology to preserve their privacy and security [19] [20] [21].

The great concern is that the communication channel in IoT technology is not only realized between the person and the machine, but also between the machines. And, in these circumstances, the guarantee of control, access, authorization, privacy and protection is a major problem. Accordingly, data security in the devices itself is necessary, but also security when transmitting messages from one device to another [6].

Security challenges can generally be divided into three groups [4]:

- system security;

- network security;

- security of the IoT application.

The research presented in this paper is concerned about network security and proposes a solution that is based on a VPN (Virtual Private Network) gateway.

The main reason for choosing an open VPN over PPTP is in this project is that a PPTP protocol is not completely secured, meaning it is limited to:

- MPPE-128 encryption, using RC4 encryption with a 128 bit key
- MS-CHAPv2 authentication-using SHA-1
- strong passwords (minimum 128 bits of entropy)

The cryptosystem used for VPN encryption is RSA 2048, using certificate file.

A VPN gateway is a type of network device that connects two or more devices or networks to a shared infrastructure. Its role is to enable connection (communication) among multiple devices or networks located in different locations. In other words, it can be said that VPN gateway is a virtual private network that provides a private and encrypted channel through which communication is accomplished, as can be seen in Fig. 1. With the development of technology, this type of configuration develops, becoming more accessible for every type of computer, phone or tablet. VPN-enabled applications provide users with secure Internet access. VPN is used for secure connectivity by creating a cohesive network, avoiding space constraints and security-related issues in the transmission of information [5] [22] [23].

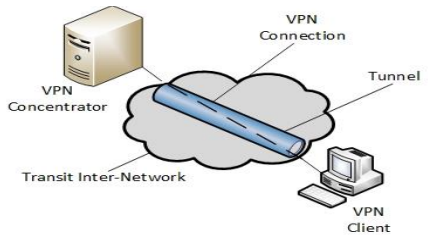


Fig. 1. A VPN network

VPN gateway can be a router, server, firewall, or similar device with data transfer capabilities. The VPN device is easily applicable to most operating systems on any computer, phone or tablet. Most often this device is a router [23].

The VPN system is created by establishing a point to point connection through the use of virtual protocols and tunneling links or encrypted data traffic. The part of the link in which private messages are entered is called a tunnel. Messages transmitted through the tunnel are encrypted, a process that is professionally referred to as a virtual private network connection. This system provides a number of benefits and access from a distance. Computer designers are constantly working to perfect the system to enable full customer support [24].

Although the VPN cannot completely save the user's anonymity, it can increase privacy and security. For this purpose, it uses authentic remote access using tunneling protocols and encryption techniques. The VPN security system provides [24]:

- confidentiality through encrypted data,

- authentication of the sender so that unauthorized users cannot access the network,

- detection of all intrusions through direct messages to the user.

The configuration line for VPN setup are as follows:

```
ca /etc/openvpn/ca.rsa.2048.crt
auth-user-pass /etc/openvpn/login
crl-verify /etc/openvpn/crl.rsa.2048.pem
```

Generation of certificate and private key for the server is issued with:

```
./build-key-server server
```

The VPN server is using a PKI (public key infrastructure). There are two important things to be addressed for the PKI:

- Public key, (a separate certificate), and a private key for the server and client.
- Master Certificate Authority (CA) certificate and key used to sign certificates for the server and client.

The server also supports a two way authentication, which is based on certificates. The client will be authenticated with the server's certificate, while the server must authenticate the client's certificate.

The server and the client, both will authenticate the other one with verification that the presented certificate was previously signed by the "master certificate authority" (CA), and then testing information in the authenticated header will be conducted.

The clocks on the server and a client must be in the same sync, or certificates will not work.

This security model has a number of desirable features from the VPN perspective:

- The server owns a certificate or key.
- The server will accept connection only on whose certificates are signed by the master CA certificate. The server can sign verification without access to the CA private key. This gives freedom to store CA key on separate server.
- If in some way, a private key is compromised, its certificate can be added to a "certification revocation list" (CRL). With this, a CRL will reject the compromised certificates.
- Client specific access right can be used, based on embedded certificate fields.

Therefore, the design of the VPN meets most security objectives: confidentiality, integrity and authenticity [24].

Using LZO compression is optional with the VPN server. This compression is fast, and 1 byte per packet for incompressible data may be added. The default setting for the VPN server is adaptive compression. With this compression, the VPN server will sample the compression process in some predefined time for measuring its efficiency. If the data is

already compressed, the efficiency of the compression will be low, giving the server option to disable the compression for a period of time, until the next cycle of testing.

DNS security can be used for enhancing the VPN server, but not as a primary protection, because the client could use own DNS settings, and bypassing the secured DNS, placed on the router or internet gateway.

IoT gateways are compact, smart and secure products that are part of the network connection. An IoT gateway contributes to bridge the gap between smart devices in the home and the place (user equipment such as phone, computer, tablet) where information is manipulated and stored and they can use wireless or wired local networks (LAN, WiFi, 3G, Zigbee and RF) [25].

## IV. Raspberry Pi as a VPN Gateway

Raspberry Pi is a very small (credit card sized) computer that plugs into a computer monitor, keyboard and a mouse. This device is using Raspbian, which is a Debian-based computer operating system especially designed for Raspberry Pi [26]. For security reasons, applying security patches and updates is necessary.

In Fig. 2, a Raspberry Pi model 3B is presented. The pin-out mapping in Raspberry Pi 3B model is shown in Fig. 3.

Fig. 2. Raspberry Pi model 3B

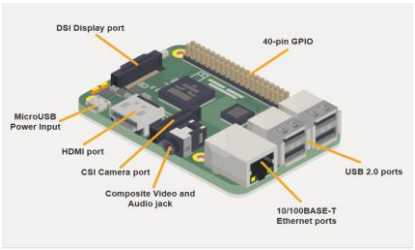


Fig. 3. Raspberry Pi 3B pin-out mapping [26]

For better security, it is recommended to create a separate user –working with "root" privileges is not recommended. A newly created user `iotuser` is added to the list of users with root privileges with the following command:

```
iotuser ALL=(ALL) ALL
```

The network topology designed is displayed in Fig. 4, where all network elements are shown.

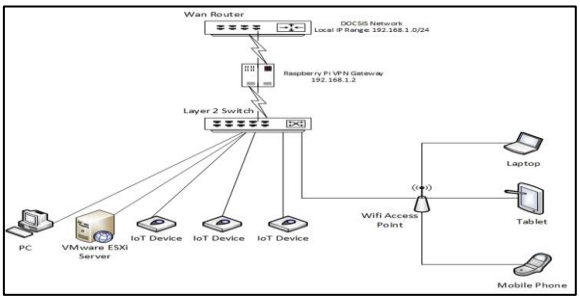


Fig. 4. Network topology

The local network setup of the DOCSIS (Data Over Cable Service Interface Specification) router used in the project is as follows:

- WAN Router IP: 192.168.1.1
- Subnet Mask: 255.255.255.0
- DHCP Range: 192.168.1.2-192.168.1.254

For easier setup, the Raspberry Pi is given a static address, right after the WAN router, 192.168.1.2.

For the VPN encryption to work properly, the NTP (Network Time Protocol) [27] is needed. If the time is not correct, the server will reject the client. The checking of synchronization with NTP servers is done with the command ntpd –p.

Next, other network devices are configured such that their default gateway is set to be the Raspberry Pi. The IP address of the gateway is the same as the IP address of the Raspberry Pi, i.e., 192.168.1.2, and public DNS servers from Google 8.8.8.8 and 8.8.4.4 are used. Other secure DNS servers can be used, ex. Comodo Secure DNS [28]. Also, 192.168.1.2 can be used in DNS servers as well.

It is recommended to install dnsmasq [29] in the Raspberry Pi device to ensure that all DNS traffic goes through the VPN. With dnsmasq, the Raspberry Pi device will accept DNS requests from all local LANs and then will forward requests to the external DNS servers.

Another security measure that can be used is blocking of all local LAN Internet access if the VPN goes down, so no device could have inbound or outbound traffic. Specifically, the traffic will not be routed through the existing Internet connection if it is unprotected and thus exposed to security risk. This is accomplished by using iptables [30]. The commands bellow illustrate how the iptables configuration is performed:

```
sudo iptables -A OUTPUT -o tun0 -m comment --comment "vpn" -j ACCEPT

sudo iptables -A OUTPUT -o eth0 -p icmp -m comment --comment "icmp" -j ACCEPT

sudo iptables -A OUTPUT -d 192.168.1.0/24 -o eth0 -m comment --comment "lan" -j ACCEPT

sudo iptables -A OUTPUT -o eth0 -p udp -m udp --dport 1198 -m comment --comment "openvpn" -j ACCEPT

sudo iptables -A OUTPUT -o eth0 -p tcp -m tcp --sport 22 -m comment --comment "ssh" -j ACCEPT
```

```
sudo iptables -A OUTPUT -o eth0 -p udp -m udp --dport 123 -m comment --comment "ntp" -j ACCEPT

sudo iptables -A OUTPUT -o eth0 -p udp -m udp --dport 53 -m comment --comment "dns" -j ACCEPT

sudo iptables -A OUTPUT -o eth0 -p tcp -m tcp --dport 53 -m comment --comment "dns" -j ACCEPT

sudo iptables -A OUTPUT -o eth0 -j DROP
```

Connecting one Raspberry Pi with another would improve the IoT network security even more. This is very convenient if there are two remote locations that need control of IoT devices. For example, a user that owns a summer house would benefit from interconnecting the home network with the summer house network. A VPN tunnel can be opened among the VPN gateways, connecting the two Raspberry Pi devices. With that, full access control can be specified on both locations, thus enabling secure communication among network devices. This can be achieved with static public IP addressing of the routers.

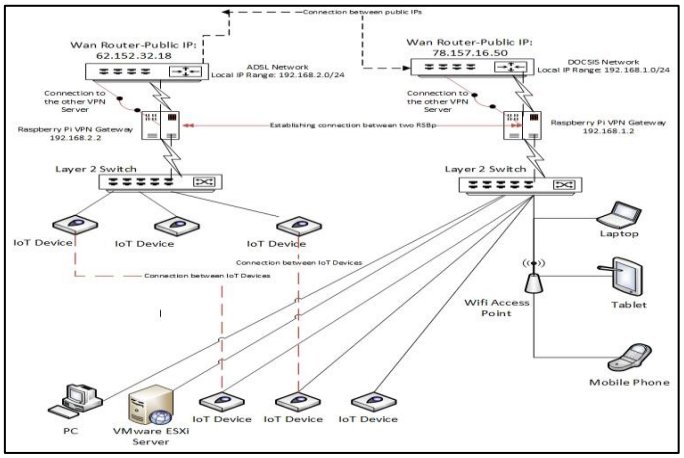


Fig. 5. A Concept of interconnecting two VPN Gateways using Raspberry Pi devices

Mainly, the performance of the VPN server depends on the hardware used. The throughput is limited to the speed of the CPU. High performance CPU e.g. multi-core CPU can handle more multiple VPN request at the same time.

Raspberry Pi is a cheap solution for setting up a VPN server. This solution can be limited, but it will be sufficient for most home and small business needs, where users will feel no difference that they are using VPN instead of a direct connection.

## V. CONCLUSIONS

The ability to quickly and easily transmit information is an important component of human life. The functionality of IoT is of paramount importance. The goal is to create a "better world" in which the physical world will know what we want, what we like and what we need without further instructions.

The smart home can be defined as a space equipped with computers and information technology that meets human needs, which contribute to greater comfort and fun. Despite all the benefits offered by the "smart" home, it is still a rare phenomenon. But, IoT technology is an inevitable part of life in the future.

There are many reasons for which users would hesitate to accept the concept, security and privacy being among the foremost. One way to increase the security and privacy of users is by using a VPN and IoT Gateway, which was the method applied in this project. The main outcome is the understanding of the security threats and risk of using IoT devices on the Internet, the needs of such a device, its performance and the role it plays in protecting the devices in the network.

Further work will focus on detailed testing of the system in order to determine whether and how much the offered solution with Raspberry Pi as a gateway to a virtual private network will provide security protection.

## REFERENCES


[1] Vermesan, O., Friess, P., "Internet of Things: converging technologies for smart environments and integrated ecosystems", ISBN: 978-87-92982-73-5, River Publishers, 2013.

[2] Haller, S., Karnouskos, S., and Schroth, C., "The Internet of Things in an enterprise context", https://doi.org/10.1007/978-3-642-00985-3_2, Springer, Berlin, Heidelberg, 2009.

[3] Lochab, K., Yadav, D. K., Singh, M., and Sharmab, A. "Internet of Things in cloud environment: services and challenges", International Journal of Database Theory and Application Vol.10, No.5, 2017, pp.23-32.

[4] Perera, C., Liu, C. H., and Jayawardena, S., "The emerging Internet of Things marketplace from an industrial perspective: a survey", IEEE transactions on emerging topics in computing, arXiv:1502.00134v1, 31 Jan 2015.

[5] "An Internet of Things", accessible at https://www.postscapes.com/internet-of-things-examples/ (last accessed on October 4, 2017).

[6] Vongsingthong, S., Smanchat, S., "Internet of Things-a review of applications & technologies", accessible at https://www.researchgate.net/publication/308711274_INTERNET_OF_THINGS_A_REVIEW_OF_APPLICATIONS_AND_TECHNOLOGIES (last accessed on March 18, 2018).

[7] Hsu, C. L., Lin, and J. C. C. Lin "An empirical examination of consumer adoption of Internet of Things services: network externalities and concern for information privacy perspectives", doi:10.1016/j.chb.2016.04.023, Published online April 2016.

[8] Kang, W. M., Moon, S. Y., and Park, J. H., "An enhanced security framework for home appliances in smart home", doi:10.1186/s13673-017-0087-4, Published online: March 2017.

[9] "Internet of Things: science fiction or business fact?" accessible at http://www.locate-now.com/tags/Harvard%20Business%20Review.pdf (last accessed on March 18, 2018).

[10] Mattern, F., Floerkemeier, C.,"From the Internet of Computers to the Internet of Things", https://doi.org/10.1007/978-3-642-17226-7_15, Springer, Berlin, Heidelberg, 2010.

[11] "Internet of Things (IoT)", accessible at http://www.gatewaytechnolabs.co.uk/internet-things (last accessed on September 27, 2017).

[12] Harper, R., "Inside the smart home", ISBN 1–85233–688–9 Springer-Verlag, London Limited, 2003.

[13] Demiris, G., Hensel, B. K., "Technologies for an aging society: a systematic review of smart home applications", IMIA and Schattauer GmbH, 2008, p.33-40.

[14] Mulvenna, M., Hutton, A. Coates, V. Martin, S. Todd, S., Bond, R.,and Moorhead, A., "Views of caregivers on the ethics of assistive

technology used for home surveillance of people living with dementia", doi: 10.1007/s12152-017-9305z, Published online: January 2017.

[15] La Diega, G, N., Walden, I., "Contracting for the 'Internet of Things': looking into the nest", Research Paper No. 219/2016. SSRN 2725913, February 2016.

[16] Thomas, D. R., Beresford A. R., and Rice, A., "Security metrics for the android ecosystem", accessible at https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf (last accessed on December 3, 2017).

[17] "Panopticon as a metaphor of the Internet of Things – Why not? But if it were the opposite?" accessible at https://www.theinternetofthings.eu/sites/default/files/Rob%20van%20Kranenburg/Panopticon%20as%20metaphor%20for%20the%20IoT_GS%20Dec2011.pdf (last accessed on September 27, 2017).

[18] "The societal impact of the Internet of Things", accessible at http://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf (last accessed on November 2, 2017).

[19] "Disruptive civil technologies", accessible at https://www.hsdl.org/?abstract&did=485606 (last accessed on April 30, 2017).

[20] "Igniting growth in consumer technology", accessible at https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf (last accessed on September 18, 2017).

[21] Aleisa, N., Renaud, K., "Privacy of the Internet of Things: a systematic literature review (extended discussion)", arXiv:1611.03340, Available online: September 2016.

[22] McEwen, A., Cassimally, H., "Designing the Internet of Things", ISBN 978-1-118-43063-7, John Wiley and Sons, Ltd, 2014.

[23] "The ABC's of VPN Configuration", accessible at https://www.techopedia.com/2/30433/networks/the-abcs-of-vpn-configuration (last accessed on January 3, 2018).

[24] "Virtual Private Networking: An Overview", accessible at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2000/bb742566(v=technet.10) (last accessed on March 18, 2018)

[25] "Internet of Things gateway solutions", accessible at http://www.supermicro.com/products/system/compact/ (last accessed on January 26, 2018).

[26] "Raspberry Pi 3 model B", accessible at https://raspberry.piaustralia.com.au/raspberry-pi-3-model-b (last accessed on August 29, 2017).

[27] "Network time protocol-NTP", accessible at http://www.ntp.org/ (last accessed on March 5, 2018).

[28] "Comodo secure DNS", accessible at https://www.comodo.com/secure-dns/ (last accessed on February 7, 2018).

[29] "Dnsmasq", accessible at http://www.thekelleys.org.uk/dnsmasq/doc.html (last accessed on March 14, 2018).

[30] "IPtables", accessible at http://ipset.netfilter.org/iptables.man.html (last accessed on January 13, 2018).