A Case Study on Hardware Firewalls and Trojans

Amber Chou, Harry Chu, Kimiya Ghobadi, Brandon Gong

NOMENCLATURE

IC	Integrated Circuits
DoS	Denial of Service
DDos	Distributed Denial of Service
MITMA	Man in the Middle Attack
IP	Internet Protocol

ABSTRACT

This paper is designed to give a basic knowledge of an essential part of network defense and security, the firewall. It will also provide information about common threats to firewalls, such as Hardware Trojans, and about how the firewall or the user may be able to deal with such threats. This report will examine a new system of Hardware Trojan classification, how Hardware Trojans pose as a threat, and how they can be detected. Along with that, two alternative solutions for preventing malicious activity are presented, in the event that the firewall is unable to successfully detect and neutralize the malware.

INTRODUCTION

A firewall is a boundary that prevents or slows the spread of dangerous technological events between two networks [1, 2]. Firewalls are designed to keep out intruders and maintain the security of the system. All traffic between the two networks must pass through the firewall, which is able to block some traffic while allowing others through according to the rules set by the network administrator [3]. Based on those rules, network traffic is allowed in and out.

A secure firewall must have: [4, 5].

- A resistance to any type of security compromise, such as a virus.
- A fail-safe, in case the firewall is broken through and there is not a user that has direct access to the firewall.
- The ability to monitor the resources of the system it is guarding.
- Strong proxy authentication.
- Auditing/accounting capabilities.

There are two types of firewalls: software/personal and hardware/network firewalls [6, 7]. Software firewalls are usually inside a device protecting it and the information contained inside. Hardware firewalls are stand-alone devices that usually attach to an internet device and protects an entire network, including all internal personal computers, from outside attacks. They can protect the Integrated Circuits (ICs) against Hardware Trojans.

Hardware Trojans are modifications/alterations to the original circuit made by adversaries in an effort to exploit the hardware or use its mechanisms to gain access to data and/or software running on the circuit [8]. Hardware Trojans threaten not only the security of sensitive and important devices used for military and financial purposes, but basic home appliances as well.

The breach Hardware Trojans create may result in alterations to the operation of the device, the leaking of sensitive information, or a Denial of Service (DoS) attack. Hardware Trojans are one of the common types of viruses that affect personal computers or PCs. Today's ICs are becoming increasingly vulnerable to malicious activities and alterations. In order to reduce the cost production of ICs, more and more manufacturers outsource parts of the IC design and fabrication to other companies. The outsourcing provides an opening for the malicious manipulation of the design of the IC without the original company's knowledge [9]. This allows for the implementation of Hardware Trojans during the design or fabrication of ICs.

Hardware Trojans can be inserted only by the designers of the IC. During the first or the second phase of the design, the designer can insert the Hardware Trojan, however, during the testing phase they have to make sure that the Trojan cannot be detected. If it is detected, the designers are the ones testing it in order to hide the Trojan. This way the IC will be called safe, and the developers will be able to put it on the printed circuit board. This method will enable designers to attack any device in which this IC will be implemented.

Detecting Hardware Trojans can be very difficult, and in some cases impossible, due to different factors such as which state the Trojan was inserted into the IC. Computer scientists have came up with several different methods to make detecting Hardware Trojans easier. These methods are divided into two groups: destructive, and non-destructive which divides into several branches that may include the need for a healthy model of the IC.

LITERATURE REVIEW

I. FIREWALLS

There are two types of firewalls - software firewalls and hardware firewalls. Since software firewalls localized are only on personal computers, if there is a virus on a network, then the computer would be protected while the rest of the network is exposed. A software/personal firewall can hide a computer from port scans and can block hacking and hacking attempts. Its main feature is controlling the network traffic allowed into the programs on the computer. It can block or terminate access if it suspects an intrusion from the outside [7, 10].

For example, if someone were to receive an email with a worm or Trojan attached to it, the software firewall should be able to detect the malware and terminate it. Hardware firewalls do the same, but they usually do it better. Hardware firewalls are generally connected to the router before the switch, so they can monitor all information going in and out of the network, thus protecting all devices on the network. Another advantage of hardware firewalls versus software firewalls is that malware that successfully infiltrates a system can bring down software firewalls, but cannot do the same with hardware firewalls [11]. All in all, it is best to pair hardware and software firewalls together. The following sections A, B, and C outlines the different types of attacks.

A. ACCESS ATTACKS

In an access attack, the attacker tries to access a network or a device on a network through inappropriate means. The security is supposed to ensure that only authorized users can access the network. There are three main types of access attacks: password attacks, trust exploitation, and man-in-the-middle attacks [12].

- Password attacks are fairly straightforward. The attacker somehow obtains a password to the network, and such attackers can be internal. The attacker can now do whatever they desire to do.
- Trust exploitation occurs when a client and a server are set up to trust each other's information. An attacker could compromise the server and then connect to the client, and the trust allows in whatever the attacker sends.
- Man-in-the-middle attacks (MITMA) occur when an attacker intercepts transmissions and can control the communication. Attackers are positioned between two parties, receives packets, can do whatever they want with the packets, from stealing information to changing the conversation altogether.

B. DENIAL OF SERVICE ATTACKS

The goal of a DoS attack is to deny a service usually available to a user. There are three main forms of DoS attacks: DDoS (Distributed Denial of Service) attack, smurf attack, and TCP SYN attack [12].

- A DDoS attack occurs when multiple systems are compromised and used to send a DoS attack to a target. The target is overwhelmed and cannot provide service for its users.
- A smurf attack occurs when a spoofed IP address sends multiple ping requests to a target.
- A TCP SYN attack occurs when the attacker sends a SYN request, or a connection request to a device with a spoofed IP address, but the attacker does not recognize the returning SYN-ACK request, meant to establish a two-way connection, causing the connection queues to fill up and not accept new connection requests.

DoS attacks can have many goals, including blackmail and sabotage. Attackers can keep attacking one’s system until the system owner gives the attacker what they want. Or they can attack to make the target’s service look bad or to cost them money [13].

C. RECONNAISSANCE ATTACKS

A reconnaissance attack occurs when an attacker surveys the network and collects data for future uses. The attacker can get important information for hacking the network such as open ports and the IP addresses of the devices connected to the network.

There are four main methods of gathering data: packet sniffers, ping sweeps, port scans, and information queries [12].

- A packet sniffer is a piece of software that captures data sent over the network and is decoded and viewed by the attacker.
- Ping sweeps send ping requests to different IP address simultaneously to see which IP address responds.

- A port scanner is a piece of software that scans a network for open ports. Gathering this information can assist in attacking the network in the future.
- Information queries are sent through the Internet to determine the IP address from a hostname or vice versa.

All of these methods have the ultimate goal of obtaining information that could potentially prove useful for future attacks on the network.

II. HARDWARE TROJAN CLASSIFICATION

There have been several proposed Hardware Trojan taxonomies that classify them based on inherent attributes of Hardware Trojans. Trojans remain dormant until they are triggered and they are typically activated only under very specific conditions. Some common characteristics of Trojans are: [8]

- leaving the physical form and the number of inputs and outputs of the original IC unchanged.
- being at least 3-4 orders of magnitude smaller than the original circuit.
- being able to remain undetected during regular test phases.
- operating stealthily during normal IC operation.

The first detailed taxonomy for Hardware Trojans was developed by Wang, Tehranipoor, and Plusquellic. Wang and his colleagues sectioned the Trojan taxonomy into three main categories according to their physical, activation, and action characteristics [14].

A. PHYSICAL CHARACTERISTICS

The physical characteristics category describes Trojans that change the physical parts of the IC itself. They can be split into 4 subcategories: [14]

- Distribution - where the Trojan is located on the physical form of the IC.
- Structure - how the layout of the chip has to be changed in order for the Trojan to be implemented, which could result in changes of the chip physically as well.
- Size - the number of components in the IC that were added, deleted, or compromised as a result of the Trojan [9].
- Type - this category can be further divided into two classes:
    - Functional - Trojans that are realized through the addition or deletion of transistors or gates.
    - Parametric - Trojans that are realized through the modifications of existing components.

B. ACTIVATION CHARACTERISTICS

The activation characteristics category refers to the trigger/situation that prompts a Trojan to become active and carry out its malicious functions [14]. Activation characteristics fall into two subcategories:

- Externally activated - Trojans can be triggered by an antenna or a sensor that can interact with the outside world.
- Internally activated - this category can be further divided into two classes:

  - ○ Always on - the Trojans are always active and are able to disrupt the chip's functions at any time.
  - ○ Conditional - the Trojans are inactive or dormant until a specific condition is met. These conditions may rely on an internal logic state or on the output of specific sensors.

C. ACTION CHARACTERISTICS

Action characteristics are the effects and types of the malicious functions caused by the Trojan [2]. These characteristics can be divided into three subcategories:

- Transmit information - Trojans that send key information to an adversary.
- Modify specification - Trojans that change the chip's properties, such as modifying existing wires and transistors.
- Modify function - Trojans that change the chip's functions through adding logic or removing or bypassing existing logic.

A reorganized and extended version of this taxonomy was put forward my Rajendran et al. in 2010 which added consideration of a design phase, abstraction level, and location. The design phase indicates the different phases a Hardware Trojan can be implemented during the creation of the IC. The abstraction level refers to the phase in which the alteration occurs. Location describes where the Hardware Trojan is located on the physical layout of the IC.

III. IMPLEMENTATION OF HARDWARE TROJAN ON AN IC

Designers of ICs are able to implement Trojans at two steps: either the first step, which is the specification phase of the IC, or at the second step when they are designing the IC. In the specification phase, the designers specify the system's characteristics such as delay, power, and target environment. In this phase, the designers are able to change these characteristics of the IC, which can cause longer delay time or other problems. In the designing phase, the designers are able to use third-party IP blockers or standard cells that can be infected with the Trojans. During the fabrication phase, the designers create masks that, if changed, can cause serious troubles. In the next phase, which is the testing phase, the designers make sure that the Trojans can stay secret, and will not show up as a problem. However, the testing phase can be used only if the IC is trustworthy. Usually the designers change a part of the design to make it untestable or follows the specific actions to keep the Trojan a secret so they can use it later. During the last phase which is the assembly phase, the developers assemble the chip and other hardware components on a printed circuit board, which will result in the attackers later on finding a gap, and attacking a computer in which the hardware was implanted [15].

IV. DETECTION OF HARDWARE TROJAN

Detecting Hardware Trojans can be either very difficult, or, in some cases impossible, since each method of detection can only be used to find one type of Hardware Trojan, and every day, new Trojans are being created and used on the ICs. Therefore, researchers are working hard to find new methods for detecting Trojan without destroying the IC. As of now, researchers such as Tehranipoor, Chakraborty and other famous computer scientists were able to come up with two main branches for detecting a Hardware Trojan: destructive and nondestructive. Through the destructive method, the suspicious IC will be destroyed during the process of detection. For detection a method called *reverse engineering* is used; which is very costly and time consuming, and in some of the cases cannot be beneficial. This method also requires a “golden reference,” which is a healthy model of the IC that is being tested [16].

The second main branch of detection is non-destructive, which means the use of different methods that will not destroy the IC while testing. It has two sub branches: invasive and non-invasive. In non-invasive testing the IC will not be changed, and the Trojan can be detected through two methods: assistive and preventive. The non-invasive method will modify the tested IC when a Trojan is detected. This method, like the destructive method, needs to use a healthy sample of the IC. The IC that is being tested will be compared to the healthy IC. There are two times to detect a Hardware Trojan through a non-invasive method, either at runtime or test-time. However, with all these methods available, there are times that Hardware Trojans cannot be detected either because that the aforementioned methods cannot detect that type of Trojan or if the Trojan is inserted at a different stage that does not match the needed stage for testing [16].

PROJECT DESCRIPTION

Firewalls have never and will be 100% effective. There will be times when malware bypasses the firewall. Hardware Trojans are especially difficult to detect and eliminate. When Hardware Trojans infiltrate devices, machines, etc., they can cause disastrous consequences from stealing information, to tearing down firewalls, to spreading to all personal and/or network contacts and infecting them too. The specific case we are focusing on in this report is Stuxnet. Stuxnet was hybrid malware that contained elements from Worms, Trojans, Rootkits, and Viruses. It was built to disrupt or destroy Iran’s nuclear program and it was so successful that it crippled uranium-enrichment facilities across Iran. Stuxnet is introduced into a system via an infected USB stick. It then infects and replicates itself within Microsoft Windows machines and networks inside Iranian Nuclear Power Plants. Then, it seeks out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment, such as centrifuges [17]. If the system is a target, Stuxnet compromises it, exploiting vulnerabilities. In Iran, the malware then caused the centrifuges to spin so fast that they broke, simultaneously informing technicians that nothing was wrong.

One of the most alarming things about this malware is that it can be carried from one computer to another on a USB stick. If an uninfected USB drive was to be introduced to an infected computer, Stuxnet could hide itself within that USB drive and spread into the next machine that reads that USB drive [17]. What we wish to achieve in our research is a theoretical way to prevent and/or combat the threat that Stuxnet and similar malware pose.

In addition to that issue, from information gained through reviewing many articles about Hardware Trojans, their classification, insertion, and detection methods, we were able to create our own charts and graphs for classification and steps of IC creation, implementation and detection.

Method

To solve this problem, we can download on the desired device a virtual machine that is solely devoted to the purpose of scanning a USB when it is connected the desired device. If there is a Hardware Trojan or any other virus on the USB, it will attack or destroy the virtual machine, not the hardware and software of the actual device. If a lot of malware activity that can cause trouble is detected, the device that the USB is connected to can send electric shocks to destroy the USB, and prevent the problems.

The creation of the new taxonomy drew heavily upon three existing methods of classification. Two of those methods were reviewed in the literature review section [14] [16]. The third method was proposed by Moein et al. [18]. Their classification sorts Hardware Trojans through eight categories: insertion, abstraction, effect, logic type, functionality, activation, physical layout, and location. In this study, a new taxonomy of Hardware Trojans was created based on the previously mentioned classifications.

Process (or Processes)

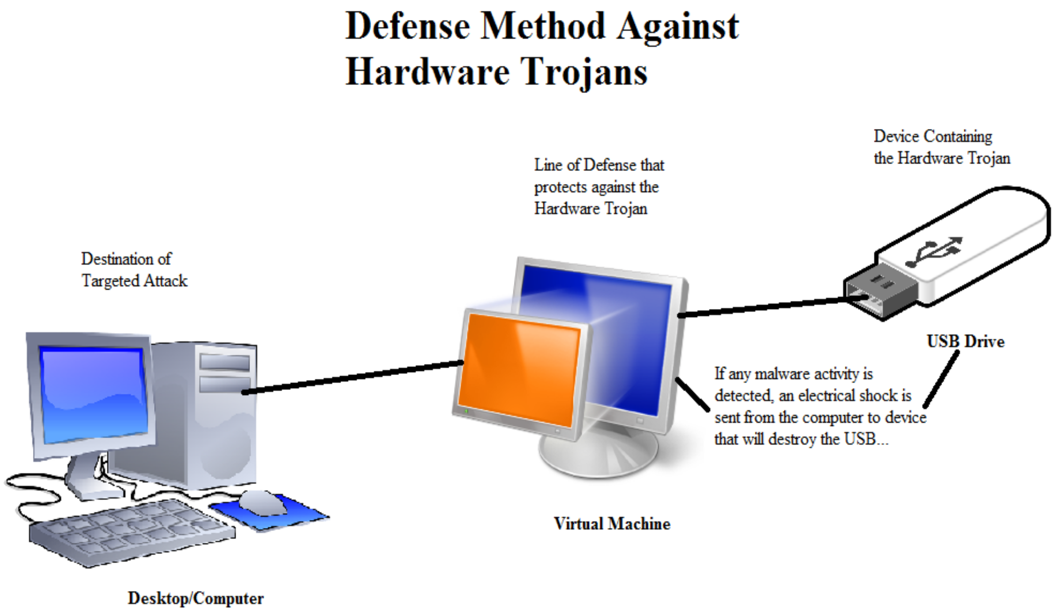
Defense Method Against Hardware Trojans
Device Containing the Hardware Trojan
Line of Defense that protects against the Hardware Trojan
Destination of Targeted Attack
USB Drive
If any malware activity is detected, an electrical shock is sent from the computer to device that will destroy the USB...
Virtual Machine
Desktop/Computer

Fig. 1 A diagram explaining how to defend against Hardware Trojans.

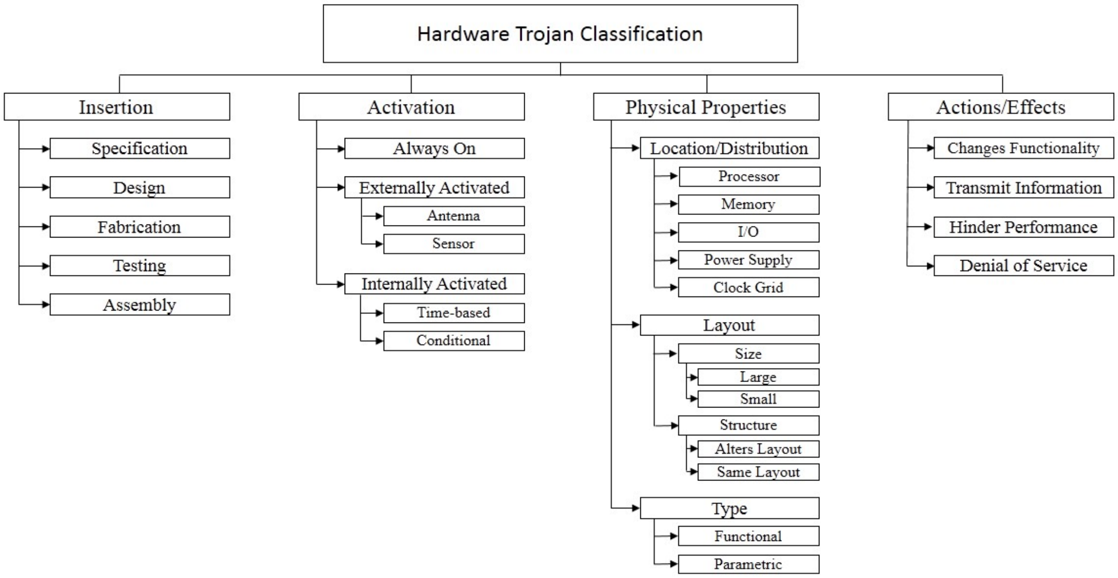

Fig. 2. A proposed classification of Hardware Trojans based on insertion, activation, physical properties, and actions/effects.

Figure 2 Was created through thorough analysis of previously proposed classification methods. The layout was designed based on the main categories into which Hardware Trojans can be classified and the subcategories that fall under them.

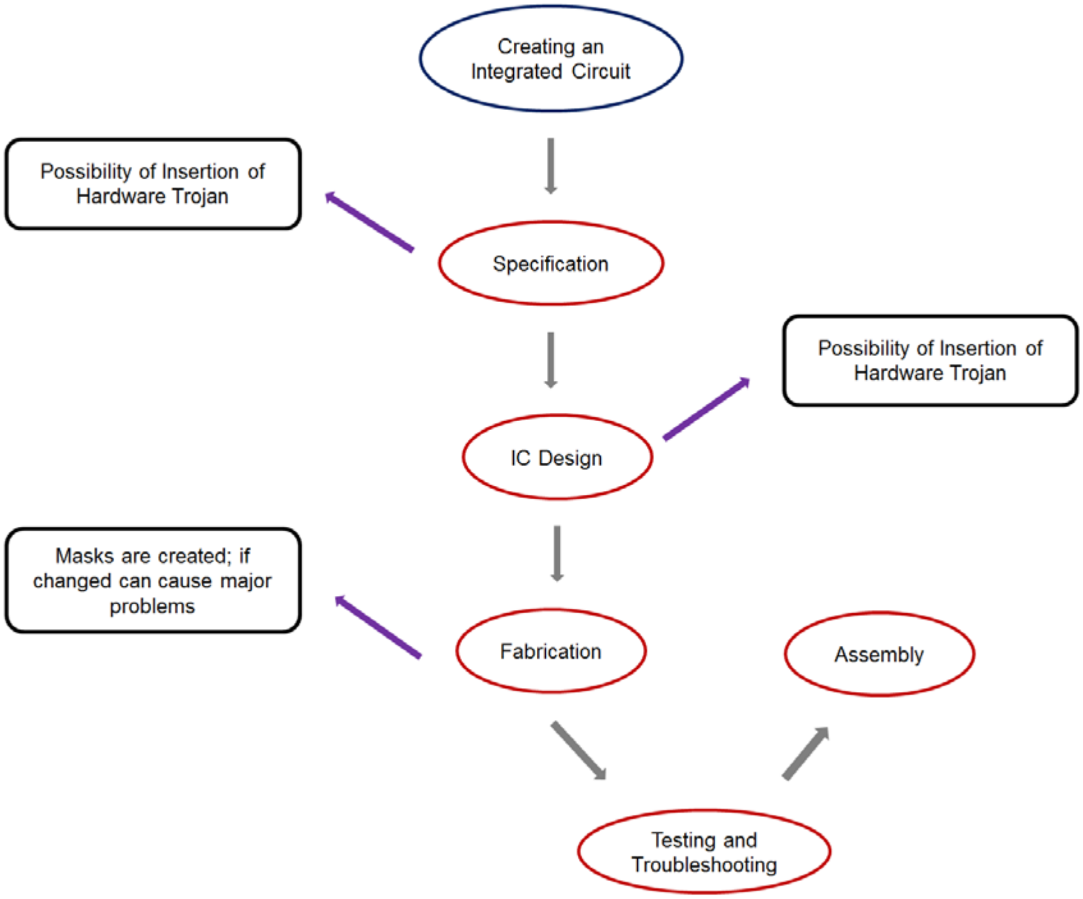
Creating an Integrated Circuit
Possibility of Insertion of Hardware Trojan
Specification
Possibility of Insertion of Hardware Trojan
IC Design
Masks are created; if changed can cause major problems
Fabrication
Assembly
Testing and Troubleshooting

Fig. 3. Steps of designing an IC and possibility steps of Hardware Trojan insertions

In figure 3 which shows IC design and Hardware Trojan insertion, the red ellipticals represent the steps of IC design, while the black rectangles represent the locations of possible Hardware Trojan implementation.

Conclusion

The focus of this report has been to introduce a new method for preventing Hardware Trojans from being transmitted. In order uncover a solution, we researched extensively to understand how Hardware Trojans and firewalls function and relate to each other. There were many limitations in our work. One of those limitations was time. There simply was not enough time to thoroughly study the topic and understand its nuances. Another limitation was being unable to test our solution due to lack of resources. These limitations led to a less technical report and our understanding of the topic could be improved. This solution is also only applicable to this specific situation with Stuxnet and similar types of malware. Future research could focus on recording the resulting data of our solution and see how effective it can be. Further research could also focus on expanding and/or manipulating the current solution to be able to cover different types of malware.

ACKNOWLEDGEMENTS

The authors of this research report would like to give their deepest gratitude to the research mentors Mr. Shahab Tayeb and Mr. Elliot Ploutz. The fabrication and completion of this project required a lot of guidance and assistance, and the writers were extremely fortunate to have such patient and knowledgeable mentors present. This team would further like to thank Dr, Zhan, Ms. Longo, and Ms. Wainscott. Dr. Gina Sully and the Writing Center heavily impacted the outcome of this report and their aid was greatly appreciated. This research team would also like to acknowledge and thank the U.S Department of Defence for funding this summer program and providing them with this incredible opportunity.

REFERENCES

[1] M. Rouse, "What is firewall? - Definition from WhatIs.com", *SearchSecurity*, 2016. [Online]. Available: http://searchsecurity.techtarget.com/definition/firewall. [Accessed: 13- Jul- 2016].

[2] N. DuPaul, "Firewall Security", *Veracode*, 2014. [Online]. Available: http://www.veracode.com/security/firewall-security. [Accessed: 13- Jul- 2016].

[3] "What is a firewall?", *Paloaltonetworks.com*, 2016. [Online]. Available: https://www.paloaltonetworks.com/documentation/glossary/what-is-a-firewall. [Accessed: 13- Jul- 2016].

[4] J.Tyson, "How Firewalls Work", *HowStuffWorks*, 2000. [Online]. Available: http://computer.howstuffworks.com/firewall.htm. [Accessed: 13- Jul- 2016].

[5] K. Ingham, *A History and Survey of Network Firewalls*, 1st ed. Albuquerque: ACM Journal Name, 2016, pp. 1-6.

[6] V. Beal, "Differences Between Hardware & Software Firewalls - Webopedia", *Webopedia.com*, 2016.[Online].Available:http://www.webopedia.com/DidYouKnow/Hardware_Software/firewall_types.asp. [Accessed: 13- Jul- 2016].

[7] "Internet Security, AntiVirus, AntiSpam, AntiSpyware | Security Advice Center | McAfee", *Home.mcafee.com*,2016.[Online].Available: https://home.mcafee.com/advicecenter/?id=ad_ost_hvsf. [Accessed: 13- Jul- 2016].

[8] N. Jacob, D. Merli, J. Heyszl and G. Sigl, "Hardware Trojans: current challenges and approaches," in *IET Computers & Digital Techniques*, vol. 8, no. 6, pp. 264-273, 11 2014.

[9] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," in *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10-25, Jan.-Feb. 2010.

[10] W. Contributors, "Personal firewall", *Wikipedia*, 2016. [Online]. Available: https://en.wikipedia.org/wiki/Personal_firewall. [Accessed: 13- Jul- 2016].

[11] M. Desmond, "What You Should Know About Firewalls", *PCWorld*, 2016. [Online]. Available: http://www.pcworld.com/article/117557/article.html. [Accessed: 13- Jul- 2016].

[12] D. Minutella, J. Cioara and H. Stevenson, "CCENT Exam Prep: General Network Security | Introduction | Pearson IT Certification", *Pearsonitcertification.com*, 2016. [Online]. Available: http://www.pearsonitcertification.com/articles/article.aspx?p=1151753. [Accessed: 13- Jul- 2016].

[13] "Prevent Denial of Service (DoS) Attacks", *Applicure.com*, 2016. [Online]. Available: http://www.applicure.com/solutions/prevent-denial-of-service-attacks. [Accessed: 13- Jul- 2016].

[14] Xiaoxiao Wang, M. Tehranipoor and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, Anaheim, CA, 2008, pp. 15-19.

[15] R. Karri, J. Rajendran, K. Rosenfeld and M. Tehranipoor, "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," in *Computer*, vol. 43, no. 10, pp. 39-46, Oct. 2010.

[16] Beaumont, Mark, Bradley Hopkins, and Tristan Newby. *Hardware Trojans-prevention, detection, countermeasures (a literature review). No. DSTO-TN-1012. DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) COMMAND CONTROL COMMUNICATIONS AND INTELLIGENCE DIV, 2011.*

[17] D. Kushner, "The Real Story of Stuxnet", *IEEE Spectrum: Technology, Engineering, and Science News*, 2009. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. [Accessed: 13- Jul- 2016].

[18] S. Moein, T. A. Gulliver, F. Gebali and A. Alkandari, "A New Characterization of Hardware Trojans," in *IEEE Access*, vol. 4, no. , pp. 2721-2731, 2016.