Vulnerability Scanning of IoT Devices in Jordan Using Shodan

Haneen Al-Alami, Ali Hadi
Department of Computer Science
Princess Sumaya University for Technology
Amman, Jordan
haneen.alami@gmail.com, a.hadi@psut.edu.jo

Hussein Al-Bahadili
Faculty of Information Technology
University of Petra
Amman, Jordan
hbahadili@uop.edu.jo

***Abstract*— Internet of Things (IoT) is an advanced automation and analytics system which exploits networking, sensing, big data, and artificial intelligence technology to deliver complete systems for a product or service. These systems allow greater transparency, control, and performance when applied to any industry or system. Due to their unique flexibility and ability to accommodate any environment, IoT systems attract a wide range of industrial, civilian, commercial, and military applications across the globe. They enhance data collection, automation, operations, and much more through smart devices and powerful enabling technology. However, there are many challenges facing the widespread usage of IoT, such as security, privacy, interoperability, standards, and emerging economies and development. In this paper, we concern with security and privacy of IoT, where we perform a vulnerability scanning of IoT devices in Jordan using the IoT search engine Shodan. The vulnerability scanning results is analyzed and presented to show how IoT devices could be an easily attacked and how they could be exposed by hackers. The research outcomes should encourage IoT users in Jordan to be aware and watch out the security of their IoT devices to maintain high level of security and privacy.**

Keywords*— *IoT; Security; Shodan; Vunerability Scanning; Jordan

I. INTRODUCTION

Nowadays, the Internet of Things (IoT) emerges as an advanced technology widely deployed in several fields including industry, transportation, energy, home, environment monitoring, healthcare, agriculture, irrigation, water resource management, and wellbeing applications [1-3]. IoT provides an added value service allowing users to easily supervise their environments and helping them make suitable decisions. IoT is likely to improve the quality of people's lives, reduce power consumption, create new markets and new opportunities, increase economic growth, and be a momentum for competition.

Many research efforts focus on collecting, processing, and analyzing data coming from different connected things. Others proposed novel processing and communication architectures, technologies, and management strategies. IoT systems can leverage wireless sensor networks (WSNs) to collect and process data and use cloud technologies, peer-to-peer systems, and big data paradigms to provide computation and analysis capabilities [1].

The most pressing challenges and questions related to the technology include: security, privacy, interoperability, and standards (e.g., legal, regulatory, and rights), and emerging economies and development [4, 5]. However, the main challenge to the widespread usage of IoT is clearly the security and privacy issues. Indeed, IoT is based on the large number of wireless sensors which involve accuracy, accessibility, availability, and confidentiality problems. Thus, the security problems start from the data collection phase and continue throughout the collected data life cycle going through the transmission, storage, and processing phases. On the other hand, the increasingly invisible, dense, and pervasive collection, processing, and dissemination of data in the midst of people's private lives give rise to serious privacy concerns.

The tracking of personal details of lifestyle, activities, habits, and preferences would potentially be accessible for third or unauthorized persons to disclose. Through the power of machine learning, someone can then analyze and make predictions about future behaviors of people or process. The current personal data protection approaches are based mainly on security techniques like data encryption or access control mechanisms. However, the privacy threats in the IoT outstrip these solutions and provoke serious challenges like tracking and profiling leakage, accountability and responsibility, and privacy by design paradigm [6, 7].

Shodan [8] and Censys [9], which are search engines that index Internet-facing devices, have brought the light on how much the IoT is vulnerable to be exposed and have become a reliable tool for researchers and security professionals in the field of IoT as it is for hackers who use it to pick an easy target or do more. To that end, a large-scale vulnerability analysis on IoT field could be carried out using Shodan and it is an operative method to determine some statistics through a passive scan on how a specific country is exposed to outsiders to maintain an acceptable level of security and privacy.

In this paper, we concern with security and privacy of IoT, where we scan IoT devices in Jordan to identify any vulnerabilities using an IoT search engine, namely, Shodan [8]. The vulnerability scanning results is analyzed and presented to show how IoT devices could be an easily hacked. Thus, IoT device users in Jordan should be aware of the seriousness of the security challenge, and they should maintain a high level of security measure and updated security tools.

978-1-5386-1986-5/17/$31.00 ©2017 IEEE

II. IoT and Security Challenges

The Internet is a global network that connects smart devices, such as computers, laptops, tablets, notebooks, and smartphones together through networks devices, such as routers and switches. The ability of information exchanging that the Internet provided, have played a significant role in humanity development in different aspects. This is what makes the world take another step and expand the Internet concept to include our daily routine devices in order to improve productivity and efficiency, a term commonly referred to as the IoT [1, 2]. Fig. 1 illustrates some of the components that could be part of IoT systems.

Fig. 1. Some of the components of IoT system.

IoT security and privacy are the special considerations required to protect the information of individuals from exposure in the IoT environment, in which almost any physical or logical entity or object can be given a unique identifier and the ability to communicate autonomously over the Internet or similar network [4, 5].

The key difference between traditional Internet and IoT is the presence of embedded devices which are devices with specialized system designed for special purpose with minimum resources. IoT are being used in several disciplines, including public health, transportation, industrial infrastructure and home appliance [10]. This comes up with new challenges in the aspect of security and privacy [6]. The main security challenges of IoT are [7]:

A. *Enormous number*

The enormous number of Internet-connected devices increases the risk of any potential attack, where it is notable that the number of distributed denial-of-service (DDoS) attack through IoT botnet increased during the last few years [11]. According to Arbor Network [12], the DDoS attacks increased in frequency and size where the number of DDoS attacks in 2016 is the double size of attacks in 2015 and the average attack size increased to 931 Mbps in 2016 with prediction to reach to 1.2 Gbps by the end of 2017. More details about the security and privacy of IoT can be found in Arbor Network report [12].

B. *Privacy*

IoT devices use sensors to collect information about device/user activities in order to take an action with minimum human interaction, these devices are easily tracked, as well as, the users. Also, the nature of collected information maybe not indefinite. Using these devices in our daily routine lead to serious privacy issues [5, 6].

C. *Resource-constraint*

IoT are devices with constrained resources, in other words, with limited battery life, processing and storage capabilities. These devices are going online using traditional Internet protocols. Hence, they use small packets size according to their capabilities and that leads to a packet fragmentation which will degraded the device efficiency with respect to quality and security. Furthermore, using cryptographic algorithms to ensure confidentiality and integrity is a challenge due to energy limitation [13].

III. Cyber-attacks against IoT

Misconfiguration of IoT and disregarding security patches are serious threats that may result in critical attacks. In comparison with other fields, the attacks against IoT have their own status. In one hand, the targeted devices have cost constraints that make any security controls expensive [14]. On the other hand, the availability of IoT devices always has a higher priority, not to mention the privacy issues since the targeted devices are in our routine. Two types of cyber-attacks have been spotted from real-life attacks targeting IoT during the last years, one is modifying the configuration and the other is controlling the device as a bot [15].

A. *Disregard security patches*

Many devices in IoT have insecure Web interface, insufficient authentication, insecure software or insecure network services which make the devices vulnerable exposed to attackers, who may alter the firmware, change the execution of software or even encrypt a file according to their intent.

A good example is the recent attack on 12 May 2017, Wannacry ransomware [16], where an attacker exploits remote code execution vulnerabilities on the Microsoft Server Message Block 1.0 (SMBv1) in the way the server handles certain requests [17].

Microsoft released a security patch on 14 March 2017, but this attack proved that many organizations around the world have not patched their systems which gave the attackers the opportunity to launch the attack and inject their malware that will encrypt the files with specific extensions, demanding for a ransom to send victims the decryptor so they can retrieve their files. Moreover, this malware will spread to Internet and any unpatched device in the same network.

B. *Default username and password*

The growing number of insecure IoT has brought a massive botnet attacks, such as Mirai [18, 19], which is the most popular IoT bot that was used in several DDOS attacks in 2016, one of them on 21st October 2016, where an attack was deployed through enormous army of malware-infected IoT targeted DYN servers, a major provider of domain name space (DNS) services to other companies such as PayPal, Twitter and GitHub. Home routers, IP cameras and digital video recorders (DVRs) with default password were employed and generated massive amounts of bogus traffic to overload targeted servers.

IV. Scanning for Vulnerable Devices

Scanning for vulnerable devices is the first step that is taken by attackers who attempt to target IoT devices or launch an attack through them. The information about the targeted device, default username and password, available exploits or open ports could be easily obtained from product manuals or from public resources on the Internet. The attacker uses this information and attempts to access the device in intent to alter its configuration or have a full control of the device, yet researchers and security professionals can follow these steps to assess the surrounding IoT devices and do vulnerability analysis as a defense approach.

A. Shodan

Shodan is a search engine for the IoT [8]. To put it in another way, it is a search engine of service banners while Shodan do its scan independently by probing all TCP/IP-connected ports, meta-data from responsive servers are retrieved and indexed. Then, this information is made available to users to make quarries and search among large-scale indexed IoT devices. However, the results are neoteric since Shodan do the scan constantly. This great ability of Shodan to search and index the vulnerable devices makes it an efficient reconnaissance tool which provides the attacker with a wide range of easy-targeted devices from home routers to industrial devices. Yet, it is a powerful tool, while the number of IoT devices is increasing exponentially, to do security assessment and obtain statistics of vulnerable devices with open ports or default passwords.

B. Vulnerability scanning procedure

Shodan was used to search indexed IoT devices to find vulnerable services and devices located in Jordan and analyzed the data of the vulnerable services and devices to obtain some statistics on the captured vulnerabilities, and then to use these statistics to warn the community about how they could be an easy-target and how their devices could be exposed and even take part in worldwide attacks. Shodan provides several filters that we applied to our queries to find open ports, devices such as routers and cameras, industrial control systems (ICS) and specific vulnerabilities, as well as, to do general scan. It is crucial to note that we do search for vulnerable device without attempting to access any spotted device, download files, modify device configuration or do any further tests.

C. Services

In this work, we investigate the vulnerabilities of a number of standard Internet services (such as HTTP, FTP, RDP, SMB) [20]. TCP port 80 is the first port to search in Shodan which will retrieve all devices with enabled hypertext transfer protocol (HTTP) service, such as home routers and Web cameras. These devices will be with open Web interface that is a way to access the device directly specially if there is no or weak authentication method. 200 OK is Standard response for successful HTTP requests, which give the ability to do more filtration on Shodan results, as in Fig. 2.

Fig. 2. HTTP successful connection banner.

The file transfer protocol (FTP) has many security faults since it is a plain-text protocol and does not use any encryption mechanism, all transmitted data is visible to anyone being able to capture the traffic including username and password. This makes the devices with enabled FTP vulnerable and exposed to several attacks such as brute force attack and FTP bounce attack where the attacker can use the device in man-in-the-middle (MITM) attack. Another alternative for FTP is to access your server remotely using virtual private network (VPN) or to use FTP over the secure socket layer (SSL) protocol [21].

FTP by default is listening on TCP Port 21 and if the provided password is correct the FTP server responses with reply code 230. This code can be used to filter devices with Port 21 opened and respond with login successful as shown in Fig. 3.

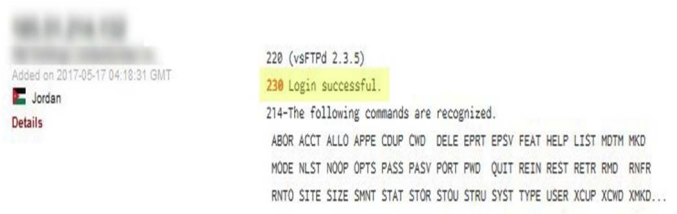

Fig. 3. FTP login successful banner.

Remote desk protocol (RDP) is running on Port 3389. It is another critical service that has security bugs, which expose many devices to different attacks, such as MITM attack and pass the hash attack [22].

Another service to search in Shodan is server message block (SMB) service [23], as mentioned previously the vulnerability in this service caused the devices with enabled SMD version1 being infected by Wannacry ransomware. The SMB is a critical service that had been reported for much vulnerability that caused several attacks. US-CERT recommended blocking all versions of SMB at the network boundary by blocking TCP Port 445 [23].

The SMB is enabled by default on Windows 7, Windows 8, Windows Server 2012 and other operating systems. There are other services with security fault, such as Telnet which is not recommended to be used by security experts in remote login on all conditions; yet it is still used. Telnet use TCP Port 23 and sometimes TCP Port 2323 is used as alternative port. These ports are registered to be related to Mirai botnet where attackers attempt to control vulnerable IoT devices and infected them with Mirai malware using Telnet [23].

D. Devices and vulnerabilities

Home router is the gateway for the entire connected devices in your home such as personal computers, smart TV, mobile phones, Web cameras, home device controllers, and baby monitor. If an attacker is able to intrude the router and control it, all connected devices can be accessed as well as transmitted data. Many products of home routers have vulnerabilities that the attackers can benefit from to control them such as cross-site request forgery (CSRF) and default password, which are still used by many users despite all warnings and recommendations.

For user convenience and accessibility, many products are not secured by default; this is because original manufactures want to ensure ability of the user to setup their product easily. Unfortunately, many users do not configure and secure their devices. This is the case with home routers and also Web cameras that are widely used nowadays to monitor their houses all the time. One of the security issues of Web cameras and other home appliance that they use universal plug and play (UPnP), which is an application to automatically forward ports on home router and makes connected devices in home network visible to each other as well as to IoT malwares [24].

The UPnP protocol has critical security issues. However, it is enabled by default in many routers and other IoT devices such as printers, Web cameras and other smart devices where the purpose of using UPnP is to seamlessly connected devices in the same network and achieving users convenient. Yet convenient, has its drawbacks where UPnP would allow malwares, trojans or worms to bypass the firewall integrated in the router and infect connected devices in the same network. Another security concern is UPnP library that the device is used; although it could has security faults in its implementation.

SDK UPnP [25] and MiniUPnPd [24] portable are examples of UPnP library. SDK UPnP provides support for building UPnP-compliant control points, devices, and bridges on several operating systems. However, it has vulnerabilities that could lead to stack buffer overflow. On the other hand, MiniUPnPd is a lightweight implementation of the UPnP Internet gateway device (IGD) daemon, which is a common communications protocol of automatically configuring port forwarding on a local network.

Also, MiniUPnPd have many security vulnerabilities, the latest reported one was on May 2017, have a common vulnerability scoring system (CVSS) score of 7.5 which could lead to DOS attack. Other vulnerability on MiniUPnPd version 1 could lead to remote code execution, and have CVSS score of 10 [26, 27].

Using Shodan to search for these devices and products is possible; also, searching for devices with specific vulnerabilities such as Heartbleed and Ticketbleed which are software vulnerability in the OpenSSL and TLS/SSL stack of F5 BIG-IP respectively that could leak client's information and password, and in some cases attackers could obtain server's private key encryption [20, 21].

E. Industrial control system (ICS)

Industrial control systems (ICSs) were not designed in the first place to be connected to the Internet, where it's purpose is to monitor and control the operation of associated devices locally. Then, as IoT is being developed and can be used everywhere, most ICSs is implemented as IoT devices connected over the Internet to collect and exchange data aiming to enhance ICS performance, minimize downtime, maximize assets utilization and use big data analysis to make intelligent decisions [29]. On the other hand, connecting ICS to the Internet need indispensable security improvement. ICS used in many critical sectors such as transportation, energy, gas and oil, water, electricity and manufacturing, where attacking such ICSs is a serious issue as it risk the system availability [29].

An example of ICS that is used in Jordan is Moxa NPort devices [30]. On Dec. 2016, there were eight vulnerabilities on Moxa NPort devices was reported. Three of them have CVSS score of 9.8, make them classified as critical risk, they can be exposed by an attacker giving him an administrative control through brute-force attack to bypass authentication or retrieving the administration password. Also, the attacker could be able to update the firmware without authentication allowing remote code execution. Another three have CVSS score above 7.0, which make them classified as high risk, they can lead to availability issues, giving the attacker ability to do buffer-overflow attack allowing him to execute a shell code, and also a cross-site request forgery attack is possible [30].

Lantronix is another ICS that is used in Jordan. Much vulnerability in these devices have been reported since 2005, the latest one was in May 2016 with CVSS score of 10.0, the vulnerability could allow remote attackers to obtain root access via unspecified vectors [31].

V. Numerical Results

The main objective of this research is to find vulnerable devices in Jordan using Shodan search engines, and analyze these results to estimate some statistics. In this work, we started by performing a general scan to find all IoT devices that exist in Shodan database, then we filtered the results according to types and products. Moreover, a search for devices that are vulnerable for Heartbleed and Ticketbleed vulnerabilities was performed.

The Heartbleed vulnerability is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. The Ticketbleed vulnerability is software vulnerability in the TLS/SSL stack of F5 BIG-IP appliances allowing a remote attacker to extract up to 31 bytes of uninitialized memory at a time. This memory can potentially contain key material or sensitive data from other connections. Ticketbleed is similar in spirit and implications to the well-known Heartbleed vulnerability. It is different in that it exposes 31 bytes at a time instead of 64 KB, requiring more rounds to carry out an attack, and in that it affects the proprietary F5 TLS stack, not OpenSSL.

A. General scanning results

A search for IoT devices in Jordan using Shodan on May 17, 2017 retrieved 40,849 results. Most of them are in Amman, Irbid, and then Salt. The most common organizations are listed in descending order: Jordan Data Communications Company LLC, Linkdotnet-Jordan, Orange-Jordan and DAMAMAX Jordan. Fig. 4 shows the top using services in Jordan. The HTTP has the largest number which is expected. The number of devices with enabled Telnet is more than twice as big as SSH which is not supposed to be. Since as mentioned before Telnet services is not recommended to use and the key difference between Telnet and SSH is that all transmitted data in SSH are encrypted and secured from eavesdropping. Yet this does not mean that the SSH is 100% secured service. Another thing to mention is the number of expired SSL certificates is 202 out of 2543 SSL certificates, which means 7.9% of the total certificates were expired.

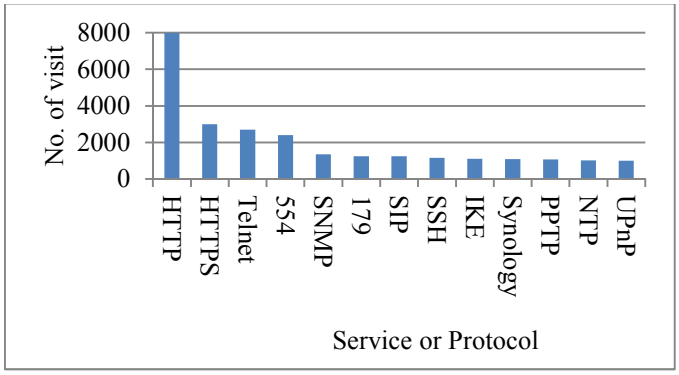

Fig. 4. General scanning results.

B. Services

The results are filtered according to the type of services into successful-unsuccessful HTTP and successful-unsuccessful FTP services. It is found that 62% of HTTP connections were successful connections (32% unsuccessful connection) while only 8% of FTP connections had a successful login (92% unsuccessful login). In SMB service, Shodan shows that 41% of SMB services disabled the authentication and 26% anonymous login successful. Shodan could take a screen shots from connection if the device is vulnerable to do so, and it is found to be that 35% from RDP connections have a successful screenshot.

C. Products

We also search for common Web camera products, routers and other home appliance in Jordan using Shodan. The search outcomes are given in Table I.

Table I - Search outcomes for IP camera in Jordan using Shodan.

Products / # of Devices					
IP Camera	***No.***	***Routers***	***No.***	***Others***	***No.***
Hikvision	297	Cisco	63	Samsung Smart TV	1
Avtech	27	Micro-httpd	53	Dahua DVR	57
Netwave IP Cam	16	TP-Link	47		
vvtk-http-server	7	Linksys	8		
hipcam	3	GoAhead-Webs	3		
ReeCam IP Cam	2	Apache httd	1		

D. Vulnerabilities

We search for devices that are exposed to Heartbleed and Ticketbleed in Jordan using their CVE codes, CVE-2014-016 for Heartbleed and CVE-2016-9244 for Ticketbleed. The results were 16 devices for Ticketbleed and 41 devices for Heartbleed, which indicates that the number decreased by 69% since Jan. 2017, where a historical data in Shodan shows that the number of exposed devices to Heartbleed was 135.

E. Industrial Control Systems (ICS)

The number of employed ICS in Jordan is very low in comparison to USA and Japan which is expected. However, the industrial sectors are critical and ICS need to be secured. 53 ICS devices were found in Shodan database in May 2017, and this number is almost quadruple the number of ICS devices in Dec. 2016, which was just 14 devices. This may indicate that Jordan is moving toward connecting ICS to the Internet. The results show three types of products which are Moxa Nport, Lantronix and N5N. Fig. 5 shows number of devices. The first two types as mentioned before are reported for critical vulnerabilities and they use port 4800 and port 30718, respectively. The last type, N5N uses port 1001 with automated tank gauge service. Other used services are shown in Fig. 6.

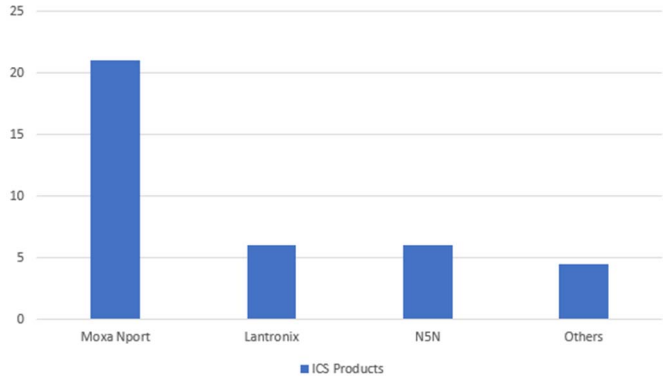

Fig. 5. ICS Products.

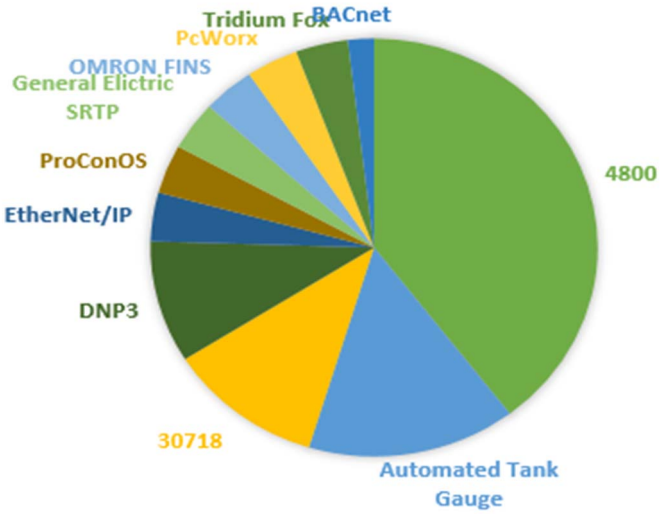

Fig. 6. ICS Services.

F. Universal Plug-and-Play (UPnP)

Searching for devices with UPnP enabled in Jordan retrieved 4175 results that are equivalent to 9.2% of all publicly available IPs in Jordan. Shodan results provide us with some knowledge about the products available as shown in Table II. The results are filtered to figure out what UPnP libraries used by the devices, and we found that 72.6% of devices used Portable SDK with size of 3029 devices. Another library is Miniupnpd has a number of 95 devices, over 38% used MiniUPnPd version 1.0 which is vulnerable to critical risk and are exposed to remote code execution attack. Table III lists the available MiniUPnPd versions.

Table II - Products enabled UPnP in Jordan

Product	***# of Results***
Intel UPnP reference SDK	39
Avtech AVN801 network camera	27
Allegro RomPager	26
Sonos	7
TwonkyMedia UPnP	2

Table III – MiniUPnPd versions in Jordan

Version	***Percentage (%)***
MiniUPnPd Version 1.0	39
MiniUPnPd Version 1.2	44
MiniUPnPd Version 1.4	4
MiniUPnPd Version 1.6	13

VI. CONCLUSIONS

This paper presents a large-scale vulnerability scanning for IoT devices in Jordan using Shodan to warn the community about IoT security issues and how they are highly vulnerable and can be exposed by an attacker. The paper points-out the critical cyber-attack against IoT and presents statistics about vulnerable devices in Jordan using Shodan. From the results, IoT users must be very aware and need to follow recommendations of security experts about disabling vulnerable services and turning off unused services. Users need to patch their devices, download latest update for their services, secure their devices, configure them probably, and change the default usernames and password as well as select strong one.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito. The Internet of Things: A Survey. Computer Networks, Vol. 54, No. 15, pp. 2787–2805, 2010.

[2] David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. Cisco Press, Jun. 2017.

[3] L. Da Xu, W. He, and S. Li. Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics, Vol. 10, No. 4, pp. 2233–2243, 2014.

[4] Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Qureshi, and Saleem Ullah. Security Issues in the Internet of Things (IoT): A Comprehensive Study. International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, No. 6, pp. 383-388, 2017.

[5] J. S. Kumar and D. R. Patel. A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications (IJCA), Vol. 90, No. 11, 2014.

[6] M. Abomhara and G. M. Køien. Security and Privacy in the Internet of Things: Current Status and Open Issues. Proceedings of International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1-8, 2014.

[7] Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Qureshi, and Saleem Ullah. Security Issues in the Internet of Things (IoT): A Comprehensive Study. International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, No. 6, pp. 383-388, 2017.

[8] John Matherly. The Complete Guide to Shodan: Collect. Analyze. Visualize. Kindle Publisher, 2016.

[9] Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, J. Alex Halderman. A Search Engine Backed by Internet-Wide Scanning. Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS'15), Denver, Colorado, USA, October 12-16, 2015.

[10] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna. Internet of Things in Healthcare: Interoperability and Security Issues. IEEE International Conference on Communications (ICC), pp. 6121–6125, 2012.

[11] P. Schaumont. Security in the Internet of Things: A Challenge of Scale. Proceedings of Europe Conference & Exhibition on Design, Automation & Test (DATE), Lausanne, Switzerland, March 27-31, 2017.

[12] Arbor Networks. Worldwide Infrastructure Security Report. Special Report Volume XII, 2017.

[13] T. Heer, O. Garcia-Morchon, R. Hummen. Security Challenges in the IP-based Internet of Things. Wireless Personal Communications, , Vol. 61, Issue 3, pp 527–542, 2011.

[14] H. Ning, H. Liu, and L. T. Yang. Cyberentity Security in the Internet of Things. Computer, Vol. 46, No. 4, pp. 46–53, 2013.

[15] Elisa Bertino and Nayeem Islam. Botnets and Internet of Things Security. Computer, Vol. 50, Issue No. 02, pp. 76-79, Feb. 2017.

[16] Murali Somarouthu and Prashanth Giri. Using Server Message Block (SMB) in iDRAC9 of Dell EMC PowerEdge Servers. Dell EMC Technical White Paper, Dell EMC Server Solutions, September 2017.

[17] Savita Mohurle and Manisha Patil. A Brief Study of Wannacry Threat: Ransomware Attack 2017. International Journal of Advanced Research in Computer Science (IJARCS), Vol. 8, no. 5, pp. 1938-1940, 2017.

[18] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, Y. Zhou. Understanding the Mirai Botnet. Proceedings of the 26th USENIX Security Symposium, USENIX Association, pp. 1093-1110, Vancouver, Canada, August 16–18, 2017.

[19] Robert Graham. Mirai and IoT Botnet Analysis. RSA Conference. San Francisco, USA, 13-17 February 2017.

[20] Williams Stalling. Cryptography and Network Security Principles and Practices. Pearson, 7th Edition, 2017.

[21] Behrouz A Forouzan and Debdeep Mukhopadhyay. Cryptography and Network Security. McGraw Hill Education (India) Private Ltd., 2011.

[22] Aaron Johns. Mastering Wireless Penetration Testing for Highly Secured Environments. Packt Publishing, 2015.

[23] SMB Security Best Practices. https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices, US-CERT, 2017.

[24] MiniUPnP Project HomePage. http://miniupnp.free.fr/.

[25] Portable SDK for UPnP Devices. http://pupnp.sourceforge.net/.

[26] CVE Details. https://www.cvedetails.com/vulnerability-list/ vendor id-12591/product_id-24263/Miniupnp-Project-Miniupnpd.html

[27] Common Vulnerability Scoring System. https://www.first.org/ cvss/.

[28] Morgan Stanley. The Internet of Things and the New Industrial Revolution. http://www.morganstanley.com/ideas/industrial-internet- of-things-and-automation-robotics, April, 2016.

[29] O. Andreeva, S. Gordeychik, G. Gritsai, O. Kochetova, E. Potseluevskaya, S. Sidorov, A. Timorin. Industrial Control Systems Vulnerablities Statistics. Kasbersky Lab Report, 2015.

[30] Moxa NPort Device Vulnerabilities. https://ics-cert.us-cert.gov/ advisories/ICSA-16-336-02.

[31] CVE Details. https://www.cvedetails.com/vulnerability-list/vendor_id-3160/Lantronix.html.