A study on Emerging Cyber Technologies, Threats and Prevention in Information Security

[1]Ms. Shazia Ali, [2]Dr. Sadia Husain, [3] Manju Sharma,
Faculty of Computer Science and Information Systems
Jazan University- Jazan, Kingdom of Saudi Arabia

Abstract: *As continuously new technologies are evolved new threats and risks are making way and making information security a tedious task, where organizations, institutions and individuals are spending on latest technologies the question that arise is are we secured enough ? Information security plays an important role in the ongoing development of information technology, as well as Internet services. Making the Internet safer (and protecting Internet users) has become integral to the development of new services and policies for any organization. In this paper we will highlight the latest threats evolved with emerging cyber technologies their impact and how it can be prevented.*

Keywords: *Cloud Threat, Big data, Ransomware, Malware, Mirai botnet, Dark Web, IOT*

I. Introduction

Continuous research and studies have shown non-technical issues are as important as technical issues in preventing malicious access and protecting personal and organizational information. Information Security has always played a pivotal role in information technology, where continuous efforts are made by intruders and hackers to breach the security and harm the users. Recent threats like Ransomware, threats to cloud computing, drones jacking, etc. which are covered in sections below gives a brief idea on what could possibly be the matter of concerns in coming years and how we can deal with it.

When a new technique is developed, its effectiveness is not measured until it is ready for deployment. Once deployed and exposed to the real world to work with, feedback from the user determines its effectiveness, at this stage, intruders experiment and discover ways to evade this type of defence and develop countermeasures to reduce its value. As businesses are expanding enormously over internet, information security has been hot topic among users and organizations, where very little is known about how to actually secure the data and personal information which could either be personal or organizational. Now days where dark web like portals are making way for terrorists or criminals to misuse or hack, we are also evolving into new techniques or software's on how these attacks can be prevented.

A study conducted by hackmageddon and statistics published by them for the month of January 2017(figure 1) shows the motivation behind attacks with a wide predominance of events driven by Cyber Crime (77.5%) ahead of Hacktivism (13.5%) and, respectively, Cyber Espionage (6.7%) and Cyber Warfare (2.2%)[1].

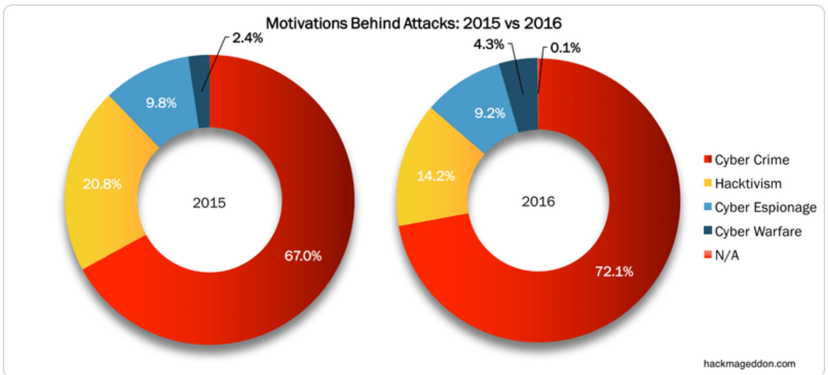

Figure 1: Motivation Behind Attacks 2015 vs 206

The main finding from the **Top 10 Attack Techniques (Figure 2)** is the percentage of unknown attacks soaring to 33.1% in 2016. Account Hijackings also experienced a noticeable growth to 15.1% from 8.8% in 2015. Targeted attacks reported a light growth (11.6% vs 10.5%), similarly to DDoS (11.3% vs 9.7%) and malware (8.0% vs 6.4%). Last but not least, both SQLi and defacement attacks reported a considerable drop (maybe related to the decreasing impact of hacktivism among the motivations), while malvertising is essentially stable (1.8% vs 2.1%)[1].

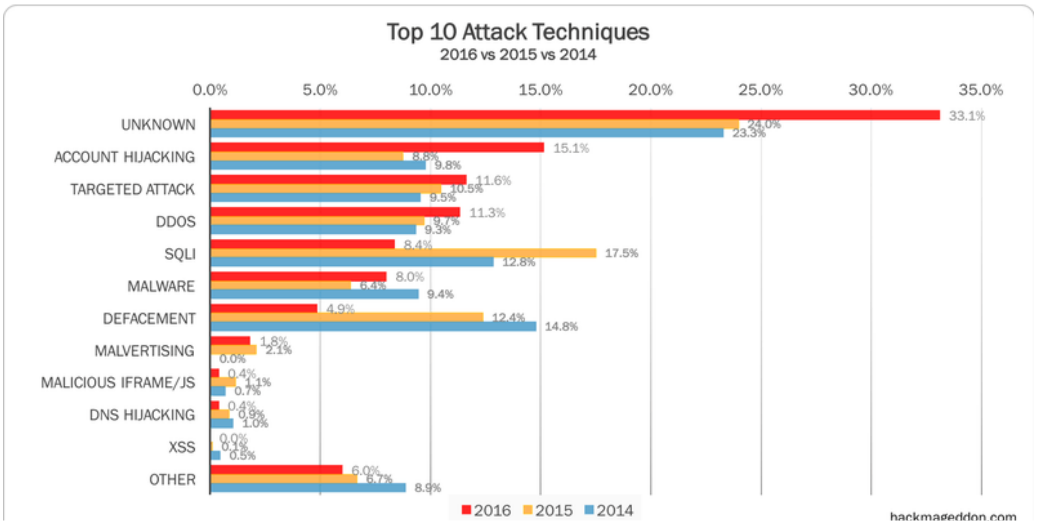

Figure 2: Top 10 Attack Techniques

The **Top 10 Distribution of Targets (Figure 3)** confirms, also for 2016, industries and governments on top of the attackers' preferences. Unlike 2015, single individuals stand at number three, pushing organizations out of the podium. This matches the soar in account hijackings that we have seen in the Top 10 attack techniques charts [1].

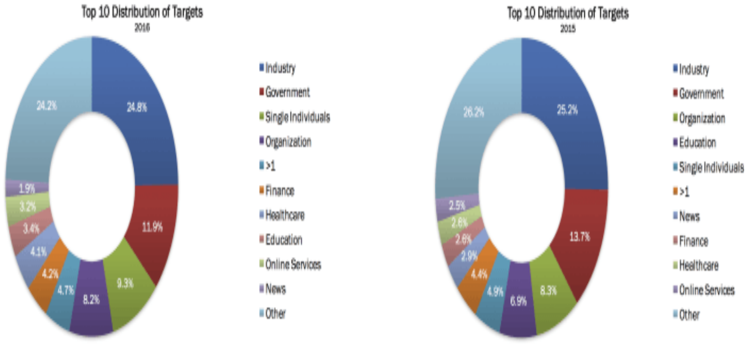

Figure 3: Top 10 Distribution of Targets

II. Emerging Technologies

2.1 Cloud Computing

Cloud computing has become an integral part of information technology with the use of remote servers to save, manage and process data rather than saving on local system. The cloud market will accelerate faster in 2017 as enterprises seek to gain efficiencies as they scale their compute resources to better serve customers, says Forrester Research in a new report.

With the advancement of modern society, basic essential services (utilities) are commonly provided such that everyone can easily obtain access to them. Today, utility services, such as water, electricity, gas, and telephony are deemed necessary for fulfilling daily life routines. These utility services are accessed so frequently that they need to be available whenever the consumer requires them at any time. Consumers are then able to pay service providers based on their usage of these utility services. In1969, Leonard Klein rock, one of the chief scientists of the original Advanced Research Projects Agency Network (ARPANET) project which seeded the Internet, said: ''As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of 'computer utilities' which, like present electric and telephone utilities, will service individual homes and offices across the country''. This vision of the computing utility based on the service provisioning model anticipates the massive transformation of the entire computing industry in the 21st century whereby computing services will be readily available on demand, like other utility services available in today's society. Similarly, computing service users (consumers) need to pay providers only when they access computing services. In addition, consumers no longer need to invest heavily or encounter difficulties in building and maintaining complex IT infrastructure. Hence, software practitioners are facing numerous new challenges toward creating software for millions of consumers to use as a service, rather than to run on their individual computers [2].

Nevertheless, as with any new technology, cloud computing has been related with a number of security risks. While the cloud computing continues to evolve and address these security & compliance requirements, organizations are left to wonder if cloud computing is a benefit for IT value optimization or misery for enterprise risk management.

2.2 IoT (Internet of Things)

The "Internet of things" (IoT) is becoming an emerging topic of conversation where many people don't know the phrase IoT. So what basically is IoT, it is the concept of basically connecting any device to the Internet (and/or to each other). This includes everything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. The new rule for the future is going to be, "Anything that can be connected, will be connected."

The analyst firm Gartner says that by 2020 there will be over 26 billion connected devices... That's a lot of connections (some even estimate this number to be much higher, over 100 billion). The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things.

Security is a big issue that is oftentimes brought up. With billions of devices being connected together, what can people do to make sure that their information stays secure? Will someone be able to hack into your toaster and thereby get access to your entire network? The IoT also opens up companies all over the world to more security threats. Then we have the issue of privacy and data sharing. This is a hot-button topic even today, so one can only imagine how the conversation and concerns will escalate when we are talking about many billions of devices being connected. Another issue that many companies specifically are going to be faced with is around the massive amounts of data that all of these devices are going to produce. Companies need to figure out a way to store, track, analyze and make sense of the vast amounts of data that will be generated [3].

2.3 Drones

Drones, also called unmanned aerial vehicles (UAVs), have no human pilot on board, and instead are either controlled by a person on the ground or autonomously via a computer program. These are becoming increasingly popular, not just for war and military purposes, but also for everything from wildlife and atmospheric research to disaster relief and sports photography. Drones are becoming the means for researchers for surveying the ground for archaeological sites, illegal hunting and harvest damage, spying, and even whooshing inside storms to study the wild storms.

More than 10,000 unmanned aircraft are expected to be roving the skies by 2020 for search and rescue, power-line monitoring, scientific research and other uses that will become less costly than if the same tasks were carried out by humans [4]. With increasing number of drone security will be a big issue.

2.4 Big Data

A large number of applications, such as large scale sensors, information monitoring, web exploring, data from social networks like Twitter and Facebook, surveillance data analysis, and financial data analysis, deal with a large stream of data input, and consequently require an alternate ideal model of real-time data processing [5][6].

Several of these applications are approaching the bottleneck of current data streaming infrastructures and require real time processing of very high-volume and high-velocity data streams (also known as big data streams). The complexity of big data is defined through V4's: 1) volume – referring to terabytes, petabytes, or even Exabyte's (10006 bytes) of stored data, 2) variety – referring to unstructured, semi-structured and structured data from different sources like social media (Twitter, Facebook etc.), sensors, surveillance, image or video, medical records etc., 3) velocity – referring to the high speed at which the data is handled in/out for stream processing, and 4) veracity – referring to the quality of data. These features introduce huge open doors and enormous difficulties for big data stream computing. A big data stream is continuous in nature and it is important to perform real-time analysis as the lifetime of the data is often very short (data is accessed only once) [7] [8].

III. Latest Threats

Some Threats to be listed which may be a matter of concern in the year 2017:

3.1 Cloud Threats:

As more and more organizations are shifting focus on saving data on clouds and using cloud computing more, cloud computing security is at risk. As per McAfee Labs 2017 Threats Predictions November 2016: Cloud service providers are building trust and gaining customers. Increasing amounts of sensitive data and business-critical processes are shifting to public and hybrid clouds. Attackers will adapt to this shift, continuing to look for the easiest ways to monetize their efforts or achieve their objectives [9].

3.2 IoT Threats:

The **Internet of things** (stylized **Internet of Things** or **IoT**) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

As per my literature review the year 2017 will bring a large scale IoT security breach, with e-commerce, manufacturing plants, and government organizations at the biggest risk, according to experts. In the past year, IoT security has quickly emerged as a hot issue with multiple threats against the enterprise such as the Mirai botnet (**Mirai** (Japanese for "the future") is malware that turns computer systems running Linux into remotely controlled "bots (Software Robot", that can be used as part of a botnet in large-scale network attacks) It primarily targets online consumer devices such as remote cameras and home routers, that affected Twitter, Amazon, and Netflix. What's most alarming, however, is that it's likely only the beginning as more companies deploy IoT sensors and devices across their networks. The Threats n affects will be seen more in 2017 as IoT increases and more and more organizations get evolved.

3.3 Ransom Ware

Ransomware is a growing threat that encrypts a user's files and holds the decryption key until a ransom is paid by the victim. This type of malware is responsible for tens of millions of dollars in extortion annually. Worse still, developing new variants is trivial, facilitating the evasion of many antivirus and intrusion detection systems. In this work, we present CryptoDrop, an early-warning detection system that alerts a user during suspicious file activity. Using a set of behavior indicators, CryptoDrop can halt a process that appears to be tampering with a large amount of the user's data. Furthermore, by combining a set of indicators common to Ransomware, the system can be parameterized for rapid detection with low false positives. Our experimental analysis of CryptoDrop stops ransomware from executing with a median loss of only 10 files (out of nearly 5,100 available files). Our results show that careful analysis of ransomware behaviour can produce an effective detection system that significantly mitigates the amount of victim data loss [10].

3.4 Drone jacking

Drones (Unmanned Ariel vehicle) which have become more and more talk of the town these days. Some consider this as a toy for fun some may use it for intruding privacy. What started as a fun toy for kids and a slightly expensive hobby for fanatics has really taken off. Drones are well on the way to becoming a major tool for transporters, law agencies, photographers, the news media, or be it covering the telecast of cricket match and more. We cannot deny the fact that drones are becoming more valuable to businesses and government agencies. As we know Amazon made its first ever delivery of product via drone in December 2016 in US and also dominos delivered its pizza in New Zealand via drone, such is the acceptability and increasing craze for using drones to reduce delivery times and attract more customers[11].

In the coming year we could see hackers deploy drone over offices or houses for intruding privacy or intercept official communication which could be a major threat to cyber security. As per David Latimer, a researcher on the project, said large companies have not properly prepared for this threat. "A drone could just go land on the roof, sit there and record people's keystrokes, and access the internal network over the wireless".

3.5 Threat to Big Data

Establishments have become very dependent on big data, using it in almost every major decision that they have to make. While data analysis is certainly helpful in many areas, some businesses are starting to forget that human intuition is also important. By taking humans almost out of the process, many fear that decisions may begin to suffer. Big data isn't always correct, and using it as the only basis for decisions could result in poor decisions, security vulnerabilities, and other issues. Business owners need to question the validity of their data, their code, and all other information to make certain that the information they're using is correct and current.

Many efforts on big data are focused on the 3V challenges today. However, the flourishing of big data relies not only on the promised solutions for 3V challenges, but also on the security and privacy challenges in big data analytics. It is likely that if the security and privacy challenges are not well addressed, the concept of big data cannot be widely accepted. For example, when big data is exploited in the healthcare context, it could save the health care industry up to US$450 billion. Nevertheless, as patients' data are very sensitive, privacy issues become a major concern when exploiting big data in healthcare. Similarly, when big data is exploited in smart grid, a utility company can collect customers' data every 15 minutes in a residential area to structure conservation programs that analyze existing usage to forecast future use. Although this kind of big data analytics can lead to a strong competitive position for the utility company, the near-real-time data generated every 15 minutes may be abused to disclose the privacy of customers. More important, once the reported data is fabricated, big data analytics become useless [12].

There are many more threats like these which could be evolving in future just to name few we have listed above

IV. Prevention

Now arises a question can these threats be prevented if yes then how or at least if we can reduce the impact of the risk which would be good. Below we are listing the prevention techniques which can be resorted to minimize the threat effect.

4.1 Information Security Awareness

Nowadays Very little attention is paid in organization regarding to security awareness among the users, making them the weakest link in any organization. As a result, currently, cyber criminals are putting significant efforts to research and develop advanced hacking methods that can be used to steal money and information from the general public. Additionally, the high internet penetration growth rate in the world and the limited security awareness among users is making it a pretty target for cyber criminals. Hence more and more training programs should be deployed in organization, as many users have limited or no knowledge about security awareness.

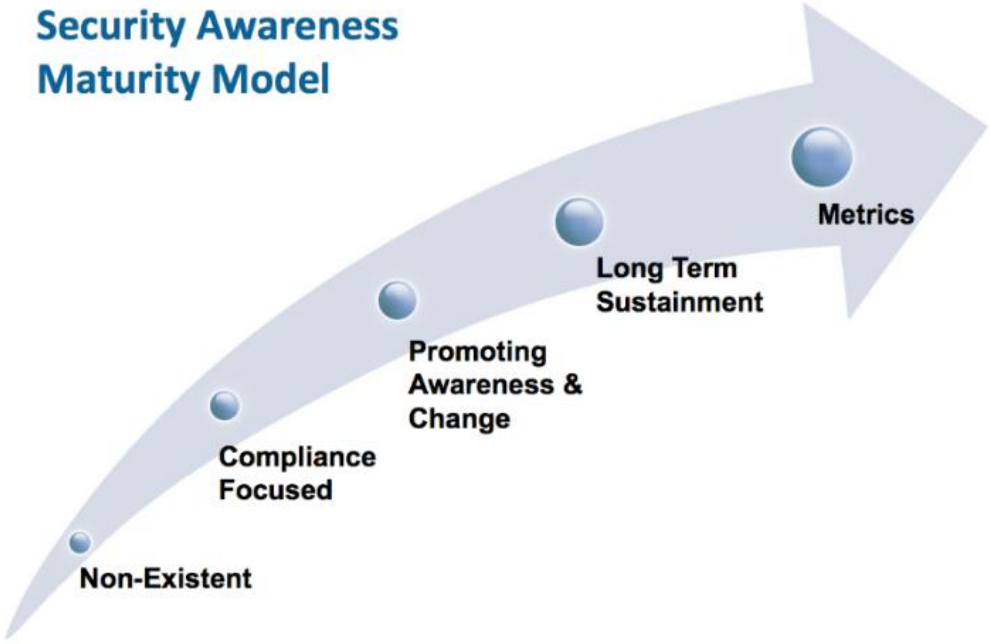

Figure 4: Security Awareness Model

As we can see from the figure 4 starting from the non-existent security level to promoting security awareness which eventually lead to long term solutions for security.

Generally user education is considered one of the most important and widely-used approaches in fighting phishing attacks. Several organizations have launched awareness campaigns to educate the user on the meaning of phishing attacks and how to detect such attacks and avoid falling victims to them [13].

4.2 Making attacks less Profitable

According to Robert Dethlefs May 01, 2015 Cyber-attack became more profitable than drug trade. Cyber criminals run highly organized and collaborative enterprises that operate with troubling and destructive efficiency. Juniper Networks conducted a study that found that global cybercrime takes in larger profits than the illegal drug trade. “The cyber black market has evolved from a varied landscape of discrete, ad hoc individuals into a network of highly organized groups, often connected with traditional crime groups (e.g., drug cartels, mafias, terrorist cells) and nation-states,” the report said. And even when the goals of the attackers are not monetary gain, the costs can be enormous. Though not a penny of its cash was stolen, the attack on Sony last December cost the entertainment company billions of dollars through the release of data. Types of data stolen can include financial data, personal health information (PHI) and associated insurance information [14].

4.3 Law Enforcement on Information Security

While the web has brought businesses near without restriction for countries to get involved and do business together, many terrorists, extremist groups, hate groups, and racial-supremacy groups are also using Web sites and other online tools. We refer to the part of the Web used for such illegitimate and malicious purposes as the Dark Web. As everyday more and more information is sent, stored, and analyzed online, more and more governments are creating laws in an attempt to control it. However, the law passed by one country may be different or even directly opposing to that passed by another, leaving worldwide businesses stuck in the middle. These laws may restrict the free exchange of information, even if that was not the original act, and all businesses are going to have to deal with the fallout.

The result is that some technology companies have come in direct conflict with governments by telling them that they will not hand over certain information or decrypt specific data. This is an ongoing discussion in the information security industry, and so far, there has been no clear indication of how regulations, which is often trying to put rules on past situations, can keep up with the always changing world of data security.
Hence the security and law agencies should come together for fight against crime and ensure smooth business across borders by applying strict measures, laws and enforcing regulations so as to reduce the impact of threats.

4.5 Known System Vulnerabilities

As per report publish by Peter Davidson in beta news. It’s much easier to buy software or make use of open-source programs than it is to spend the time and money to develop one in-house. However, these commercially available programs often come complete with known vulnerabilities that hackers are more than willing to take advantage of. That’s why you have to do your research into software before you buy it [15].

V. Conclusion

Computer technology is more and more ubiquitous; the penetration of technology in society is a welcome step towards modernization but society needs to be better equipped to handle with challenges associated with technology. New hacking techniques are used to penetrate in the network and the security vulnerabilities which are not often discovered create difficultly. As the technologies are evolving based on human needs the more we are getting prone to hackers and threats which are going more persistent and sophisticated by the day. Now it’s time for Academia, industry and government to work together in bold new ways to solve the grand challenges of Information security. To combat today’s sophisticated Threats and meet we need a multilayer approach to threat prevention. In this paper we highlighted the latest threats to Information security emerged with technologies like cloud computing, IOT, Drones, Big Data etc. We also discussed the literature on prevention techniques which can be resorted to minimize the threat effect.

References

[1]. http://www.hackmageddon.com/2017/03/02/january-2017-cyber-attacks-statistics/

[2]. Future Generation Computer Systems 25(2009)599–616 Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility Rajkumar Buyyaa, b, ∗,CheeShinYeoa, Srikumar Venugopala,James Broberga,Ivona Brandicc

[3]. Forbes:https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#28ae2da11d09

[4]. Hacking drones: K Wesson, T Humphreys - Scientific American, 2013 - nature.co.

[5]. A. Arasu, B. Babcock, S. Babu, M. Datar, K. Ito, I. Nishizawa, J. Rosenstein, J. Widom, STREAM: the stanford stream data manager (demonstration description), in: Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data, 2003, p. 665.

[6]. Journal of Computer and System Sciences (www.elsevier.com/locate/jcss): A dynamic prime number based efficient security mechanism for big sensing data streams ☆ Deepak Puthal a,∗, Surya Nepal b, Rajiv Ranjan b,c, Jinjun Chen a- Volume 83, Issue 1, February 2017, Pages 22–42

[7]. B. Albert, Mining big data in real time, Informatica 37 (1) (2013) 15–20

[8]. M. Dayarathna, S. Toyotaro, Automatic optimization of stream programs via source program operator graph transformations, Distrib. Parallel Databases 31 (4) (2013) 543–599.

[9]. McAfee Labs 2017 Threats Predictions November 2016: https://www.mcafee.com/au/resources/reports/rp-threats-predictions-2017.pdf

[10]. 2016 IEEE 36th International Conference on Distributed Computing Systems Crypto Lock (and Drop It): Stopping Ransomware Attacks on User Data Nolen Scaife University of Florida scaife@ufl.edu Henry Carter Villanova University henry.carter@villanova.edu,Patrick Traynor University of Florida traynor@cise.ufl.edu Kevin R.B. Butler University of Florida butler@ufl.edu

[11]. Drone jacking: https://www.ft.com/content/a06a1f5c-505f-11e6-8172-e39ecd3b86fc

[12]. R. Lu et al., “EPPA: An Efficient and Privacy-Preserving Aggregation Sheme for Secure Smart Grid Communications,” IEEE Trans. Parallel Distrib. Sys. , vol. 23, no. 9, 2012, pp. 1621–31

[13]. D. Timko, “The Social Engineering Threat”, Information Systems Security Association Journal (ISSA), January 2008.

[14]. Making Attacks less profitable: http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/

[15]. Known system Vulnerabilities: https://betanews.com/2016/07/22/7-information-security-trends-currently-dominating-the-market/