International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Cyber security Attacks: Exploiting weaknesses

Lama Alhathally, Mohammed A. AlZain, Jehad Al-Amri, Mohammed Baz, Mehedi Masud

Abstract*: Due to the technology growth throw the years, Hackers are evolution a divers and sophistication methods to attack systems security. Mostly these attacks occur to get personal benefits from harming the system physically by steeling and destroying devices that contain precious information or non-physically (logically) by alter and eavesdrop on sensitive data and more than that. This paper surveys aim to discuss the most common cyber security attacks types, what the mechanisms that used in these attacks and how to prevent the system from these threats. In particular, it concentrates on exploiting the system vulnerabilities to steal information and gain benefits from it.

***Keywords* : Meltdown, spectre, phishing, Ransomware.**

I. INTRODUCTION

Accordingly, to the expanding of technical knowledge in recent years the cybercrimes have been increasing rabidly[5] . In other words, the cyber-attacks techniques and tools are evolving lately.

Intruders improve methods to reach and control confidential information for individuals or organizations in order to gain personal benefits [14] [6] [9] [7].

Consequently, hackers are exploiting any software or hardware vulnerabilities to profit by misusing the unauthorized data[8] [12] [1]. For instance, meltdown and specter attack happened because of the processor weakness [28] [12] [4] . Furthermore, they can steel or leak sensitive data by taking advantage of this disadvantage [28]. In like manner, they can use another way to get personal information by either phishing or Ransomware attacks. Phishing happened by using malwares or social engineering to have private data[23]. On the other hand, Ransomware idea is to encrypt [2] [3] [36] and lock the information by using malicious then request money to return it back [20] [19].

The remainder of this paper is structured as follows. Section 2 will be a short explanation to each attack. Section 3 describes meltdown and spectre and how it considers security attack. Section 4 discusses phishing types and how to avoid being a victim. Section 5 explaining Ransomware attack functioning and risks on system security. Section 6 is an analysis to the previous four attacks. Section 7 will conclude this paper.

Manuscript published on January 30, 2020.
* Correspondence Author
Lama Alhathally*, MSc Cybersecurity, Taif University, Saudi Arabia. Bachelor degree in Computer Science.
Mohammed A. AlZain, Associate professor, College of Computers and Information Technology at Taif University in Saudi Arabia
Jehad Al-Amri, Faculty of Computers and Information Technology at Taif University, Saudi Arabia.
Mohammed Baz, Computer Engineering Department in College of Computers and Information Technology in Taif University
Mehedi Masud, Professor in the Department of Computer Science at the Taif University, Taif, KSA

II. BACKGROUND

Cyber-attacks nowadays not only targeted different types of establishments but also individuals as well. In general, there is insufficiency to recognize the variety of attacks effects that might cause a complication to prevent information. There are many definitions to cyber-attacks but all these definitions share the same goal, which is, affected the data integrity, confidentiality and availability[14] [7] [11] [10].

Attacks can be categorized to:

- Meltdown vulnerability misused out-of-order implementation in common processors such as x86, ARM and PowerPC that lead to breakdown the memory isolation limits between user and kernel space. As a result of it a personal info will leak to other programs [24] [28].
- Spectre attack happened because of the new processors that enhance the computer performance by predicting and speculating execution. To explain, when the processes need address that is in memory to make calculate, the CPU will not wait until the value is being read. Moreover, the CPUs are going to try to predict the destination and complete the implementation. When actual value arrived the CPU will ignore it because of that these calculation are not true in executions so victim memory and registers can be accessed and manipulate[27].
- Phishing is a way to steal secretive data from users through pretend as a well-known source [14].
- Ransomware This attack started in 2012 and spread-out globally since then. The main idea of this attack is to encode and locked the data until the attacker get ransom payment[20].

III. MELTDOWN AND SPECTRE ATTACK

Meltdown and spectre are examples of Speculative execution, which is a microarchitecture technic where it used to develop CPUs functioning. Lately, implementing speculative instructions lead to have a bad impact on the cash and other structure even though when this instructions executing is not happening or their influence do not appear [25]. Consequently, the latest meltdown and spectre attacks take advantage of this risk to revel secret information where it's unauthorized to access [36]. To illustrate, attackers can misused these data or sabotage it by exploiting speculative execute code that read confidential information[25] [27] [28] [30] [18].

Hence meltdown and specter attacks are exemplary of speculation attack these attacks misuse three assets of speculative implementation in new processors[25].

1) Branch forecasting and authorization test are executed hidden in the pipeline if there is fail in executing it will produced when the instruction is obligated, which allow the speculation instructions to enter info that is outside the authorized area[25].
2) Speculative commands leave behind side issue in micro-architectural constructions for instance cashes that can be indicate by applying popular method such as Flush+reload [38] and prime+probe[29] side channel attacks[25].

The branch prediction can mistrain or pollute. Where it is distributed in all the programs that are operating on the same physical core [27] [18]. This will allow the code run in one domain to misuse branch prediction and operate it in another[25]. Furthermore there are divers alternative of Spectre and Meltdown attacks in this section will discuss how it work and classify them based on how it impact on speculative execution [25].

```
unsigned char secret;
dummy = array[secret * 64];
```

Fig. 1. Secret-revealing gadget [25]

- A common Gadget: this attack goal is to read the restrict content of the memory and register by reading a small piece of the code which is called gadget. For instance, a simple example of gadget is revealed in Figure 1. Suppose variable secret keep a private value that is used as an index into byte array. In case that processor hypothetically implements this code, the memory entrée will be established therefore data will hold by the cache data. With attention to that the secret variable manage, which cache array, will renew by speculation execute hardware. The multiplicative process grantee that divers values of the variable will save in another cache sets. In order to this activity in many scenarios the position of the data and instructions in prey memory is not hidden, therefore the attacker can check CPU cache. As a result of this behavior he can detect the secretive value of the variable. To explain if the hacker knows cache set S0 can be accessed when the value of secret is 0, he can assume that the value can be 1 (mod n) where n is equals to the number of sets in the cache. In addition, if the hacker uses a collection of cache side channel attacks he can detect the cache updates. Notably, in regular execution this code will not be implemented or else the result in cache channel will be leaked. An attacker in speculation attack uses assets 1 and 2 where it defined above to activate the gadget to implement speculatively by the target.

```
if (offset < array1_size)
y = array2[array1[offset] * 64];
```

Fig. 2 code for an alternative attack [25].

- Spectre (Alternative 1): this alternative of the attack can be showed by the code displayed in Figure 2. In this code, the target procedure reads the values from *array1* by using the *offset* that is afforded by the invader. After that the output value is used to make an entrée in *array2*. As it explained before, enter to *array2* can exploit by invader to determine the index value. Since the invader is controlling the *offset*, he controls the index also. For this reason, the invader can select *offset* value to read a random memory address where it lead to cache access monitoring by the invader[38] [29] [22]. Despite that, *if* statement makes sure that no unauthorized entrée to the memory can be permitted. Sadly, the hacker can force the target procedure to implement out of boundary memory entrance and take advantage of speculative execute and branch prediction by the coming technique [25]:

a) The hacker will implement the code repeatedly with the value of *offset* when *if* statement is always correct. As a result, this will improve the branch predictor to guess reciprocal branch continuously not – taken[25];

After that the hacker will erase *array1_size*

b) from cache, pushing the CPU to take *array1_size* value from the memory, in order to postpone the perfect improvement to the branch prediction and to make a huge speculation gap[25];

c) Overall, hacker will add malevolent offset. Moreover, the branch prediction will guess that the branch is not- taken as a result to the two-memory entrance, which expose the saved value at the hacker chosen location [25].

- Spectre (alternative 2): in this alternative the victim might not have the gadget or *offset* value is not managing by the hacker. For these reasons the hacker can avoid it by stealing the control of the speculation implement. Specially, when CPU face unclear branch direction, CPU will instantly begin the speculating executing commands at this location. Based on **assets 3** the hacker can make the victim branch polluted to take control of the speculation execution flow and to send it to any program address that have gadget commands. This is similar to the return-oriented programming attack [17] [25].
- Meltdown attack: this attack-abused asset no.1 by accessing the memory via speculation executing in order to that the pipeline and commands rearrangement approval checked will happened after that. To illustrate, let suppose that the client program which want to read the kernel memory. This action will be rejected but the speculation commands will lead to store needed information into caches by a secondary carrier, So the hacker can read the supreme kernel.

Kernel memory has all the memory in use so the hacker can damage or destroy the memory in the system because of this reason it considered a vary dangers attack. Furthermore, this attack needs capability to be endured and recovered from segmenting failed after the omission is rise. Instead of that, if the hacker has the control on the code, he can bypass the omission by leaving the gadget in the back of misprediction branch [25].

IV. PHISHING ATTACK

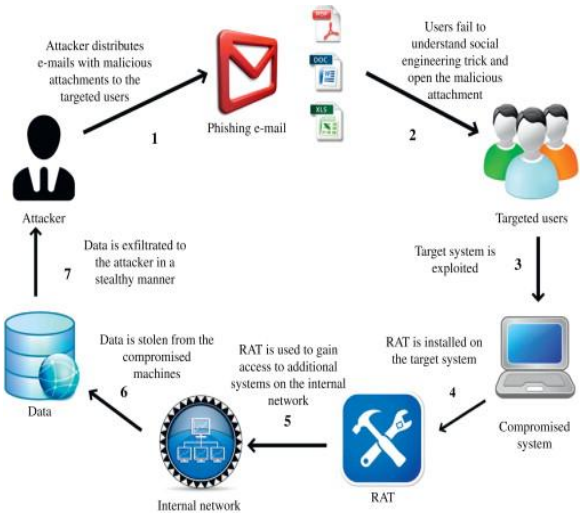

Fig. 3 phishing attacks [37]

Phishing is sociological method accustomed to avoid technological monitoring executed to diminish threats of security in information systems. Human are the most vulnerable entity in and security system. Phishing is focusing on this vulnerability and taking advantage of people nature to enter the system or to steal their personal belonging [33].

V. TYPES OF PHISHING ATTACKS

In this section will explain briefly the diverse type of phishing attack [37].

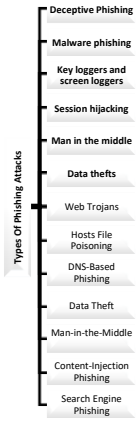

Fig. 4 Types of phishing attacks[37]

A. Deceptive Phishing

Misleading phishing is the trick massages, which needed to approve account information. Where these messages ask the user to insert their info again for several reasons such as fabricated account fees, some annoying account modification and latest uncharged utility where it requires a fast act. In addition, many malevolent websites mailed to numerous receivers wish that any target to unsuspected this massages and open it and enter their personal info to have it gathered[37].

B. Malware Phishing

This means the fraud that includes operating a mischievous program on targets computers. This malicious software can received as a massage attachment or a file that can be download from untrusted sites where there are some minor companies who is usually does not update their software regularly[37].

C. Key Loggers and Screen Loggers

This kind of malicious trace the information when entered from the user keyboard and the important data will transmit to the attacker via web. Hackers reach targets web-browser throughout tiny programs that operate immediately when the web-browser is opened. Moreover, this process will be the same in the system folders, hardware drive and monitor display[37].

D. Session Hijacking

This type of phishing is to observe the victim's actions when they log in to their accounts or making any transactions and enter a personal data. Furthermore, the poison program will implement unapproved activates. For example, the will transfer money and the victims will know nothing about [37].

E. Web Trojans

This type is happened when the target sign in his data will gather and send to the attacker [37].

F. Host File Poisoning

Attackers will monitored until the victims opened a URL to enter site and then they will search about the host name and send the fake location that is similar to the real site and then their data will be taken[37].

G. Data Thefts

The secretive information is saved in computers. Additionally, the targets are taking the information with no knowledge that it belonged to these users. Usually, this data is user's personal info such as credit or debit card numbers, and sensitive password. However, company's private data also could be stolen by take secretive files, employee reports, communication info, and much more. Attackers gain benefits from trade a confidential data with money to their contestants in order harm this company[37].

H. DNS Based Phishing

This means alters the host files. Attackers replace a fake location so if any one open the site it will send them to forge website. Targets have no knowledge that it's forge website.

In other words, they will enter a private info where it will attack by attackers and they might be in another area[37].

I. Content – Injection Phishing

In this kind attackers substitute the real data with forge data in the site whish misleads the targets to provide their personal data[37].

J. Man in The Middle

In this attack attacker will eavesdrop on the communication between the site and users. When the users insert their personal info attacker will observe their info without breaking the session between target users and website. After that attacker will exploit this data when targets are offline [37].

K. Search Engine Phishing

Hackers will design a website for forge merchandises, search engine will give the web pages' indexes. Then, the hackers will watch until unwary consumers enter their secret data as a step of the purchase process such as sign in or payment info. Note that these fake websites offer their services by a tempting cost[37].

VI. EMERGING ATTACK VECTORS

Lately, users became more conscious about the traditional phishing attacks and how to detect and prevent these kinds of attacks. As a result of that, attacker evaluate new ways to cope up with these changes and to keep deceive people and computer systems. There are several developing attacks techniques and fresh victims for attackers[33].

A. Social Media

Social network is the best environment of data for attackers. Facebook and twitter became as a digital journal of human's days. Journals in the past were protected so no one can read it. Nowadays, everyone on the social networks can see each other thoughts at the timeline. Hackers can take advantage of this info to make a phishing plan on targets throw their Facebook account. Most users post their email address and phone numbers in their profile where this giving the attacker the chance to exploit it and do phishing on victims or hacked their accounts. Facebook has a weakness to XSS. According to Acunetix, "Something as simple as a Facebook post on your wall can contain a malicious script, which if not filtered by the Facebook servers will be injected into your Wall and execute on the browser of every person who visits your Facebook profile" [33].

B. Short Message Service (SMS)

Fig. 5 Smishing[33]

The spasm method in this example was a prize. The message parallels with the announcement of Apple's Ipad III [33].

There is a new attack called Smishing due to that mobile phone nowadays is net allowed. Basically this spasm used in emails and lately developed to reach texts message. This is renewing to a previous method named war dialing. Where the hackers use the PC router to automatic called a bunch of phones number and saves the phone numbers which response by classifying it on that answer it a fax device or PC. The recent technique is to use this old method to search for mobiles number and then direct an enormous text messages that lead receivers to malevolent sites [33].

C. Craigslist

The fraud is happening in both sides consumer side and dealer side in deals. These frauds categories involve in break Craigslist's suggested rule where it is not finishing the deal personally [33].

a. Consumer Side

The trend deception on consumer side of Craigslist deals is in apartments lease. The Deceptive person will put an advertisement announcement on the website where it includes some photos of the apartment and the location. He will offer a cheap price to trick the target. The target will find this offer is attempting so he will give a fast response to get the deal. The Deceptive person will ask the target for a deposit to make sure the target will get the lease. This deal will be like it never happened and the target will not return his money[33].

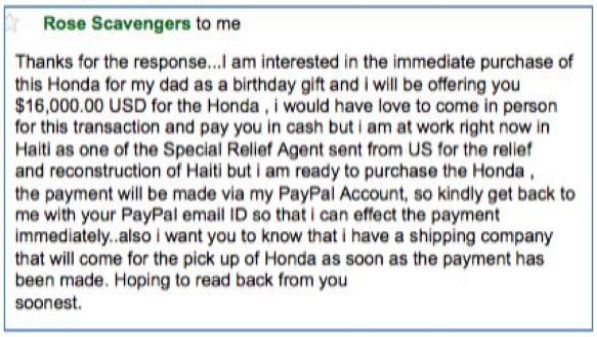

Fig. 6 Craigslist Example [33]

b. Dealer Side

In dealer side deceiving attack, the target is the dealer. The process is that consumer is offered deals by more than one dealer. However, the problem is that the consumer requires the product to be sent. For example, in fig 6 the attack shows a typical thinking of the deceiver. In this text message the consumer gain the dealer confidence by offering extra fees and attracting the dealer attention throw mentioning that this consumer is having a job in Haiti [33].

VII. SOME VARIOUS ANTI PHISHING

The main goal of phishing attack is to steal secret data via technology such as PIN and bankcards info from several victims. According to Engin Kirda and Christopher Kruegel [26], this attack has been rising in this couple of years furthermore they offered a proctection method called AntiPhish. This method is an app, which is hidden in the user web-browser, and it traces the client data and thwarts them from opening a harmful sites[37].

Madhusudhanan Chandrasekaran Ramkumar Chinchani Shambhu Upadhyaya [16] offeres a modern method named Phony that is inevitably detecting and analyzing phishing threat. This method is to protect the client by giving a forge data to the site.

Furthermore, it's capable of detecting many threats and it also work as a web-browser addition that diminishes the phishing attacks in the web [37].

Craig M. McRae Rayford B. Vaughn [31] described a recent technique to detect fake website by applying web bugs and honey pot. These bugs will form as an image and it will collect info about client[37].

Venkata Prasad Reddy, V. Radha, Manik Jindal [34]suggests two methods to prevent from deceptive attacks. First method is depending on spoofing alerting that used white list. Second method is a web-browser addition that affords a reliable frame devoted to enter the password and display a photo. The web-browse addition makes a divers password by Pwdhash++. The white lists include data that is comfortable to the clients. Writer used Levenshtein alter space algorithm to do comparison between the URL that chose by the client and in the white-lists. There is another comparison between the IP addresses for the two URLs. If it found matched to the IP addresses in the list then this is a trusted website otherwise it will be a fake website. Pwdhash++ include id key that display when Pwdhash++ started. The second method likewise use photo in the background that assign to particular client. When Pwdhash++ started this photo will show in the website otherwise it will be a forge website. Writer ends by telling that effectiveness of spoof guard and Pwdhash is rising via guarding clients from deceptive attacks [37].

VIII. RANSOMWARE ATTACK

Nowadays, people usually save their important data and perform usual work in computers and electronics devices. Mostly, these devices have a vulnerable security protection as a result it becomes an easy goal to hackers who use several attacks. Ransomware attack is a kind of malicious which block people from using their data. They either lock the computer monitor or lock the folders and they unlock it by requesting money. The recent Ransomware categories encode particular folder on affected system and make targets trade the decoding key by an online fees using special way [13].

Attackers who implement Ransomware attack use Bitcoin to get the ransom fees. There are another options to pay such as iTunes and Amazon gift cards. In addition, if the target pays the ransom fee it does not assure that getting the encoding key or recovering the affected system or unlocked the folders. This attack can affect the system by several ways. For instance, it is reach the system as a spam mail, or download from malevolent websites that take advantage the system vulnerabilities [13].

Ransomware can propagate in numerous methods, involving [15]:

- By taking advantage of program that is aimed to take advantage of a specific weakness and implement the code.
- It can spread by detachable devices such as flash drive and outer hard disk that work automatically, take advantage of folders browsers, DDL insertion or designed implementation.
- Sharing files throw networks similar to detachable devices.
- By exploring the Internet throughout mobiles which can be not secure because it put the system in danger by opening a harmful links or files.
- Also by email attachment and malevolent URLs on social media [15].

A. Ransomware Attack Stages

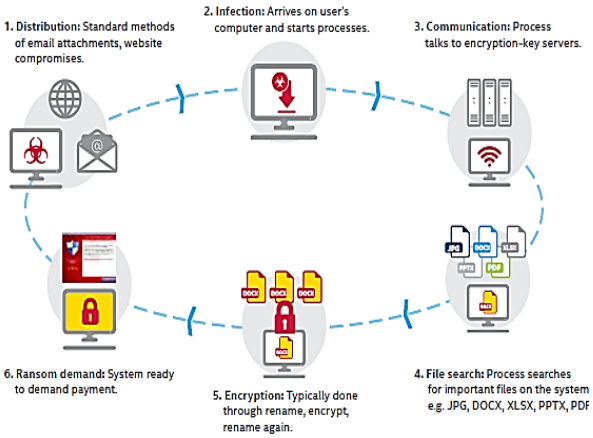

Fig. 7 Ransomware attack steps [13]

Ransomware attack stages:
This attack uses six stages to propagate. Moreover, it used a typical technique to spread out.

- First, it's propagated throughout phishing attacks, which include email phishing or download from untrusted sites.
- Second, when the binary reaches the target PC, it's infected the target system by making procedures that is required to finish the malevolent actions. It might include latest complex actions.
- Third, in this stage it will connect to encoding key server to have the public key that required to encoding data.
- The fourth stage is searching for files in organized way. To illustrate, it explores for a valuable file that target could not repeated it simply such as files ends with jpg, docx , xlsx, pptx, and pdf.
- Fifth stage is to encode the file through relocating and changing of the file name.

Finally, request the ransom by controlling the target monitor and ask target to pay [13]

B. WannaCry Ransomware

This attack is one of Ransomware attacks that expanded globally targeting PCs that using Microsoft windows as an operate system. It encrypts information and requests targets to pay ransom in Bitcoin. The attack established on May 12, 2017. Just in a day this attack poison over 230.000 PCs in more than 150 states. Kaspersky India was the most country infected by this attack[13].

This was the hugest attack in past and it damaged 130.000 computers over 100 states as Mikko Hypponen mentioned, he is a chief research officer at a Helsinki-based cyber security company called F-Secure.

In addition, he adds that Russia and India are the most affected because they used windows XP that has the highest chance to attacked or infected. Government PSc over 18 departments in Andhra Pradesh's Chittoor, Krishna, Guntur, Visakhatpatnam and Srikakulam regions were infected [13]. Yet the targets were worldwide spreader, they were infected by the exact cyber-attack. This attack focused on targets that save their important files in digital form and cannot be recovered if it is damaged or stolen. That will lead targets to pay ransom to get them back. Throughout Wannacry attack most the targets were enforced to pay the fees to get their important files back fast. The hackers provide the direction and target guide in 28 languages in because these attacks design to attack people in different nations. Moreover, if the protection program of the targets removes the decoding application and close pop – up frame that contain the description, the background will be changed and give a required info. Furthermore, the ransom will increased from 300$ to 600$ after three days and the file cannot be recovered after seven days[35].

Fig. 8 Example of massage showed up by The Wannacry Ransomware [13].

C. Advices to prevent Ransomware attack

Protection is crucial to maintain the system secure. It's an advice for consumers to preserve the operate system and update their software. Take advantage of all trusted security recourses. Save another copy of a valuable documents offline. As mentioned before Ransomware can be spread via diverse ways such as electronic Mails, Ads, and harmful websites. Ransomware is limiting the system usage in several methods when imposing the system. It is organized to three kinds: Scare -ware, Lock-Screen, and Encoding[32].

Here are several methods to evade Ransomware:

- Antiviruses programs must be updated.
- Junk mail must not open or resent.
- Take a regular back up to the system.
- Make sure that operating system, antivirus, browsers, Adobe Flash Player, Java, and other software are up-to-date.
- Maintain the Windows Firewall running and properly organized every time.
- Improve the safety of Microsoft Office components (Word, Excel, PowerPoint, Access, etc.).
- Filtering EXEs in email.
- Use good reputation anti-viruses' software.
- Restoring the system to a clean back up.
- Make sure to stop sharing the files.
- Turn off idle wireless connections, such as Bluetooth or infrared ports.
- Don't open malicious URLs in email.
- Don't enter insecure websites.
- Write the website address better than clicking on it on address bar [32].

IX. ANALYZING ATTACKS

Table.1 analyzing the four attacks based on reading and understanding. [21].

Security Attack	Recent Fashion security attack	Preceding attacks qualities
Meltdown	Attacker takes advantage of the out-of-order implementation on current processors that allow reading memory content including sensitive data[28].	
Spectre	Spectre attack are exploiting recent processor feature to enhance performance by branch prediction and speculative execution to leak target data[27].	
Phishing	Substitute trusted sites addresses with a fake one to get secret data[21].	Gains data via fake emails, text messages or phone calls[21].
Ransomware	Capability to spread out globally. Capability to rush system folders. Quick repetition and infect PCs in similar net [21].	Require target communication to infect PCs or networks. Cannot infected PCs globally because it not quick[21].

Based on the previous table it obvious that hackers during the years became smarter and evolving their method based on the technology growth. As it shown in phishing attack they used to change the domain address of a well-known site to gain users data. On the other hand, they improve their ways during the years until they can be abled to trick users by fake emails, SMS and phone calls to gain secretive info. Furthermore, Ransomware attacks are improving too.

In the past, attackers needed user interaction to make the attack. In contrast, nowadays, attackers can infect the PCs of many users quickly and the communication is not required. Indeed, meltdown and spectre are a result of a misuse of modern processor disadvantage that allow attacker to gain access to data without permission [27] [28] [21].

X. CONCLUSION

Technology is evolving rabidly during the time that leads to evolving in the attacking techniques. Hackers usually searching for any whole to exploit it in order to steal confidential data and gain profits from it either by sell it to opposite or trade it with money. This paper summarizes the most exploiting attacks that is trending nowadays. In first section, meltdown and spectre attack. The second section, explain phishing attack functioning and mentioned several types of phishing with an examples. In the fourth section, clarify Ransomware attack and how it works. Indeed, analyze the fourth attacks in table.

REFERENCES

1. M. A. AlZain, Data security, data management and performance evaluation in a multi-cloud computing model, (2014).
2. M. A. AlZain, Utilization of Double Random Phase Encoding for Securing Color Images, International Journal of Computer Applications, 975 (2018), pp. 8887.
3. M. A. AlZain and J. F. Al-Amri, Application of Data Steganographic Method in Video Sequences Using Histogram Shifting in the Discrete Wavelet Transform, International Journal of Applied Engineering Research, 13 (2018), pp. 6380-6387.
4. M. A. AlZain, A. S. Li, B. Soh and M. Masud, Byzantine Fault-Tolerant Architecture in Cloud Data Management, International Journal of Knowledge Society Research (IJKSR), 7 (2016), pp. 86-98.
5. M. A. AlZain, A. S. Li, B. Soh and M. Masud, Managing Multi-Cloud Data Dependability Faults, Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth, IGI Global, 2019, pp. 207-221.
6. M. A. Alzain and E. Pardede, Using multi shares for ensuring privacy in database-as-a-service, 2011 44th Hawaii International Conference on System Sciences, IEEE, 2011, pp. 1-9.
7. M. A. AlZain, E. Pardede, B. Soh and J. A. Thom, Cloud computing security: from single to multi-clouds, 2012 45th Hawaii International Conference on System Sciences, IEEE, 2012, pp. 5490-5499.
8. M. A. AlZain, B. Soh and E. Pardede, A byzantine fault tolerance model for a multi-cloud computing, 2013 IEEE 16Th International Conference On Computational Science And Engineering, IEEE, 2013, pp. 130-137.
9. M. A. AlZain, B. Soh and E. Pardede, Mcdb: using multi-clouds to ensure security in cloud computing, 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, IEEE, 2011, pp. 784-791.
10. M. A. AlZain, B. Soh and E. Pardede, A new approach using redundancy technique to improve security in cloud computing, Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), IEEE, 2012, pp. 230-235.
11. M. A. AlZain, B. Soh and E. Pardede, A new model to ensure security in cloud computing services, Journal of Service Science Research, 4 (2012), pp. 49-70.
12. M. A. AlZain, B. Soh and E. Pardede, A survey on data security issues in cloud computing: From single to multi-clouds, Journal of Software, 8 (2013), pp. 1068-1078.
13. T. Anjana, Discussion On Ransomware, Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks, International Journal for Research Trends and Innovation, 2 (2017), pp. 310-314.
14. A. Bendovschi, Cyber-attacks–trends, patterns and security countermeasures, Procedia Economics and Finance, 28 (2015), pp. 24-31.
15. M. A. BRANQUINHO, RANSOMWARE IN INDUSTRIAL CONTROL SYSTEMS. WHAT COMES AFTER WANNACRY AND PETYA GLOBAL ATTACKS?, WIT Transactions on The Built Environment, 174 (2018), pp. 329-334.
16. M. Chandrasekaran, R. Chinchani and S. Upadhyaya, Phoney: Mimicking user response to detect phishing attacks, Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, IEEE Computer Society, 2006, pp. 668-672.
17. S. Checkoway, L. Davi, A. Dmitrienko, A.-R. Sadeghi, H. Shacham and M. Winandy, Return-oriented programming without returns, Proceedings of the 17th ACM conference on Computer and communications security, ACM, 2010, pp. 559-572.
18. D. Evtyushkin, D. Ponomarev and N. Abu-Ghazaleh, Jump over ASLR: Attacking branch predictors to bypass ASLR, The 49th Annual IEEE/ACM International Symposium on Microarchitecture, IEEE Press, 2016, pp. 40.
19. O. S. Faragallah, M. A. Alzain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem and B. Soh, Block-based optical color image encryption based on double random phase encoding, IEEE Access, 7 (2018), pp. 4184-4194.
20. S. Y. A. Fayi, What Petya/NotPetya ransomware is and what its remidiations are, Information Technology-New Generations, Springer, 2018, pp. 93-100.
21. A. M. Gamundani and L. M. Nekare, A Review of New Trends in Cyber Attacks: A Zoom into Distributed Database Systems, 2018 IST-Africa Week Conference (IST-Africa), IEEE, 2018, pp. Page 1 of 9-Page 9 of 9.
22. D. Gruss, C. Maurice, K. Wagner and S. Mangard, Flush+ Flush: a fast and stealthy cache attack, International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2016, pp. 279-299.
23. B. B. Gupta, A. Tewari, A. K. Jain and D. P. Agrawal, Fighting against phishing attacks: state of the art and future challenges, Neural Computing and Applications, 28 (2017), pp. 3629-3654.
24. Z. Hua, D. Du, Y. Xia, H. Chen and B. Zang, {EPTI}: Efficient Defence against Meltdown Attack for Unpatched VMs, 2018 {USENIX} Annual Technical Conference ({USENIX}{ATC} 18), 2018, pp. 255-266.
25. K. N. Khasawneh, E. M. Koruyeh, C. Song, D. Evtyushkin, D. Ponomarev and N. Abu-Ghazaleh, Safespec: Banishing the spectre of a meltdown with leakage-free speculation, 2019 56th ACM/IEEE Design Automation Conference (DAC), IEEE, 2019, pp. 1-6.
26. E. Kirda and C. Kruegel, Protecting users against phishing attacks with antiphish, 29th Annual International Computer Software and Applications Conference (COMPSAC'05), IEEE, 2005, pp. 517-524.
27. P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz and Y. Yarom, Spectre attacks: Exploiting speculative execution, arXiv preprint arXiv:1801.01203 (2018).
28. M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, Y. Yarom and M. Hamburg, Meltdown, arXiv preprint arXiv:1801.01207 (2018).
29. F. Liu, Y. Yarom, Q. Ge, G. Heiser and R. B. Lee, Last-level cache side-channel attacks are practical, 2015 IEEE Symposium on Security and Privacy, IEEE, 2015, pp. 605-622.
30. G. Maisuradze and C. Rossow, Speculose: Analyzing the security implications of speculative execution in CPUs, arXiv preprint arXiv:1801.04084 (2018).
31. C. M. McRae and R. B. Vaughn, Phighting the phisher: Using web bugs and honeytokens to investigate the source of phishing attacks, 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), IEEE, 2007, pp. 270c-270c.
32. S. Mohurle and M. Patil, A brief study of wannacry threat: Ransomware attack 2017, International Journal of Advanced Research in Computer Science, 8 (2017).
33. M. Rader and S. Rahman, Exploring historical and emerging phishing techniques and mitigating the associated security risks, arXiv preprint arXiv:1512.00082 (2015).
34. V. P. Reddy, V. Radha and M. Jindal, Client Side protection from Phishing attack, International Journal of Advanced Engineering Sciences and Technologies (IJAEST), 3 (2011), pp. 39-45.
35. N.-B. Schirrmacher, J. Ondrus and T. C. F. Tan, Towards a Response to Ransomware: Examining Digital Capabilities of the WannaCry Attack, PACIS, 2018, pp. 210.
36. G. K. Sodhi, G. S. Gaba, L. Kansal, E. Babulak, M. AlZain, S. K. Arora and M. Masud, Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code, Indonesian Journal of Electrical Engineering and Computer Science, 12 (2018), pp. 1297-1304.
37. V. Suganya, A review on phishing attacks and various anti phishing techniques, International Journal of Computer Applications, 139 (2016), pp. 20-23.
38. Y. Yarom and K. Falkner, FLUSH+ RELOAD: a high resolution, low noise, L3 cache side-channel attack, 23rd {USENIX} Security Symposium ({USENIX} Security 14), 2014, pp. 719-732.

AUTHORS PROFILE

Lama Alhathally A MSc Cybersecurity student in Taif University, Saudi Arabia. Bachelor degree in Computer Science.

Mohammed A. AlZain has achieved his PhD degree from the Department of Computer Science and Engineering at La Trobe University, Melbourne, Australia in Sept 2014. Dr. AlZain's PhD research is in Cloud Computing Security. His thesis title was "Data security, Data management, Performance evaluation for a multi-cloud computing model". He has received his Bachelor degree in Computer Science from King Abdulaziz University, Saudi Arabia in 2004, and then achieved his Master's degree in Information Technology from La Trobe University in 2010. Currently, Dr. AlZain is Associate professor in the College of Computers and Information Technology at Taif University in Saudi Arabia. His area of interest includes Cloud Computing Security, Information Security, and Distributed Systems.

Jehad Faisal Al Amri is a professor assistant in Computer Informatics. He graduated from the Centre for Computing and Social Responsibility at De Montfort University June - 2013. The thesis title is "An Analysis of the Influence of Cultural Backgrounds of Individuals upon their Perspective towards Privacy within Internet Activities". Currently, he is a lecturer at the Faculty of Computers and Information Technology at Taif University, Saudi Arabia.

Mohammed Baz received the Ph.D. degrees from the University of York, in 2015 in the field of applications of statistical inference on designing communication protocols for low-power wireless networks. Mohammed is the author of a number of published papers in recognized conferences and has acted as a reviewer for anumber of IEEE journals including IEEE Transaction on Vehicular Technology, IEEE Access journal, and IEEE Wireless Communications Letters. Now, Dr. Baz works for Computer Engineering Department in College of Computers and Information Technology in Taif University and has been a member of multiple committees related to academic fields as well as participant in research projects. Moreover, he has taught several courses and supervised several capstone projects.

Mehedi Masud is a Full Professor in the Department of Computer Science at the Taif University, Taif, KSA. Dr. Mehedi Masud received his Ph.D. in Computer Science from the University of Ottawa, Canada. His research interests include cloud computing, distributed algorithms, data security, data interoperability, formal methods, cloud and multimedia for healthcare. He has authored and coauthored around 50 publications including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. He has served as a technical program committee member in different international conferences. He is a recipient of a number of awards including, the Research in Excellence Award from Taif University. He is on the Associate Editorial Board of IEEE Access, International Journal of Knowledge Society Research (IJKSR), and editorial board member of Journal of Software. He also served as a guest editor of ComSIS Journal and Journal of Universal Computer Science (JUCS). Dr. Mehedi is a Senior Member of IEEE, a member of ACM.