Cyber-Attacks on the Network.

(March 10 2022)

L Velec, IEEE, Faculty of Arts and Science.

University of Wisconsin Rivers Falls.

Department of Art Science,

Engineering Department of University of Wisconsin Rivers Falls.

Professor: Jacob Hendricks

Author: Lissette I, Velec. (Lissette.velec@my.uwrf.edu).

ABSTRACT: **—**In the recent decades, cyber threats have increased. In the era of covid and wars, many companies are not highly prepared to combat such attacks.

This make Cyber Threat intelligence with Figures (CIF) need to optimize resources and focus on this great conflict that affect us all. Globally we find ourselves in an environment where cybersecurity attacks have increased by more than 20 percent. This makes us have a risk of cyber threats, cybercrimes that take risks from our data. Internet architecture and infrastructure of Things (IoT) it has had many technological advances, providing technologically advanced solutions that have allowed different innovations and implementations in different systems. Besides, he manages many advances but he is also a threat.

INTRODUCTION:

I

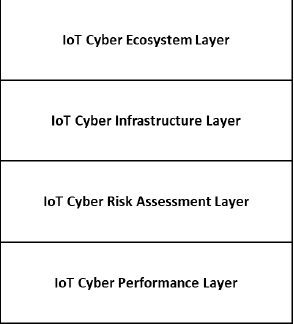
N IoT Cyber-security-attacks an IoT system consists of several sections: The first would be the perception applications, the second network, and finally the application. These systems that are composed in layers have threats in the network. These layers are used to write the architecture of the IoT system as it collects all the information on devices. The IoT network layer transmits information privately wirelessly or by wires. Consequently the application is providing services for people who want to customize them. **[[1]](#footnote-1)‘**Things’’ through internet embedded with an electronic chip, sensors, and other forms of hardware. Each device is uniquely identified globally by Radio Frequency Identifier (RFID) tags.

There is a lack of monitoring and wireless devices that would be mobiles and the contradiction and incompatibility that the network systems exist. There are currently different types of attacks on IoT networks. Based on the declines, that exists in cybersecurity and shortcomings. There is a lack of monitoring and wireless devices that would be mobiles and the contradiction and incompatibility that the network systems exist. There are also individual cyber warriors who with their knowledge can infiltrate or copy filtering software systems, and can infiltrate entities or organizations. Many of these programs that are manipulated by anonymous netizen groups that do not belong to any affiliation can have page flows from even an entire city or country. The problems that challenge the enormous security of applications, devices, and users, could be the context of any of the internet is somewhat complicated. This is due to being something to reach and popularity of the cloud this serves as intermediate management of business systems. on the cloud. Segmented security solutions Examples, firewall applications at the perimeter of a variable network do not actually protect data is now on the move across devices, clouds, networks. We also add the data centers that exist that they are the ones that house our confidential information of the companies they also address security challenges that generate the visualization in the cloud that rethinks the security states. [[2]](#footnote-2) “Currently, malicious attacks are more easily abrupt due to the growing number of IoT networks”. The malware attacks are usually planned to infect the privacy of IoT nodes, computer systems, and smartphones over the internet” How to prevent attacks? They are different types of attacks. There are these advances that have not yet had a real impact on user protection, if block chain technology is used to cover these IoT problems; they intend to close this gap. It sounds contradictory but based on the decentralization of transactions. These DoS deny attacks are an attacker attacking or attempts to prevent the legitimacy of users accessing information or services. These DoS attacks happen when an attacker floods a network with information when searching for a URL. But in reality they only have one amount at a time since an attacker overloads the server with applications and these requests cannot be processed quickly. Then the denial of service appears as the site cannot be accessed. Internet networks are subject to countless attacks, since they have a variety of direct and indirect attacks. It is actually a concern as it represents a great threat to multiple services. The development of an exchange system has become global. There are several contexts in the social, economic and cultural aspects, since these are the basis for the regulatory systems to give in to the unification that favors trade. The economic, social and cultural contexts that underlie the regulation systems give in to the unification that favors international trade.

1. Prevention of Cyber – Attacks.

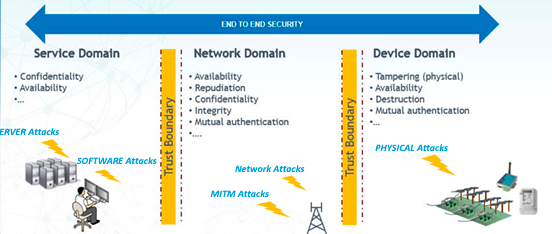
In reality there is no consensus that is global in relation to illicit conduct. Many people think that everything can be solved using technology on many occasions if it is true, but this is not completely true since there are many failures. The data traffic in the networks of users and passwords could be obtained illicitly to commit computer fraud, they can also be used to distort and alter machinery and there are also specialized teams in capturing and intercepting information. There is no type of solution that can actually protect a company or individual users from cyber-attacks, even large corporations have suffered from these vulnerabilities over the years. But we must ask ourselves why this happens? The question is something unknown in security systems. Of course risks can be reduced and these vulnerabilities are considered difficult to attack a company or different entities. However, also an easy and effective method to know if you are part of a bot is to see if the inputs connections of your computer are open and check if those loop holes are open. You could only windows + r to open the run window, in that console type cmd and hit enter, you will get the command prompt console in which you will place netstat -ano, It will show you a list of established external connections and show the port it uses, left-click on the taskbar and go to task manager, also then go to the task manager details tab and compare and stop all the tasks you are not doing or disconnect the strange connections. This is not a guarantee but it helps to stop or prevent cyber-attacks. However **[[3]](#footnote-3)“**A simple example of Network Denial is characterized by an attacker that logs into a router at the border of an organization’s network and stops it from transferring data. Example of the results in the blocking of all traffic on a network and isolates the target organization, temporarily preventing it from transmitting any information in or out using computer networks**”**.

There are many updates that solve bugs, including cybersecurity ones, you have to find an antivirus or malware that protects computers in a certain way so that our files are protected from any type of malicious attack. Passwords must also be set or generated. There are effective tools for generating passwords. Every time you want to enter the networks, it is recommended to write the address directly. This is a defense method that identifies the page that will be visited. Also the downloads made could be threats and we must know the nature of where it comes from and if it is effective.



1. Example of an Abstract Model Cyber Risk model.

Firewalls are a system that protects and prevents networks. This control system between the networks. The firewall can classify depending on the type of use. This traffic going in and out of the computer. Here we can observe the entities and relationships between their related attributes. These relationships are between many IoT administrations in reality they do not have the experience to develop different IoT situations. In reality, the network market will never stop. People who develop different types of technologies are always providing their IoT team with their new innovations for the security of different transfers. Today there are new developments such as 5G which actually has no server and foggy IoT systems. Also, AI will also show protection and potential for prevention in case of detection and recovery in real-time and take action for IoT systems with improvements than other platforms that are already traditional. IoT platforms must offer comprehensive solutions that unify wired devices and applications from multiple vendors.



2. Example Figure IoT Threats.

1. General Category of Cyber Security Threats.

Threats are acts that are made by people who want to extort or harm. These groups or individuals who have experience in data theft want to disrupt information systems. These cyber threats include a number of malwares and denial of services, there is also no doubt that there are injection attacks that we have described above. These cyber threats also have no doubt that they originate from a variety of sources and internal connections could be terrorists and hackers. There are also employees, contractors, groups or an independent individual who abuse to do malicious acts.[[4]](#footnote-4) “Malware refers to software programs designed to damage or perform other unwanted actions on a computer system”.

lll Vulnerabilities.

Deep learning is something automatically that a model can perform tasks in different ways directly, such as images, text, sounds, among others. This is implemented through the architecture of neural networks, it would be more like network layers, and if there are more layers, the network will be more extensive. Also the demand for service of various applications between the cloud has grown immensely, as there is a growth of these vulnerabilities. There are organizations that direct how to encourage the proper use of cloud services. Cloud Security Alliance is a type of non-profit organization that promotes best practices on how to use the cloud. [[5]](#footnote-5)**“**This paper discusses the vulnerabilities of the API in cloud management software. Based on these vulnerabilities, this paper will demonstrate how eavesdropping on cloud API authentication services

and API exhaustion attack can be initiated. To address the threat due to the vulnerabilities of the API, we need to detect on-going attack which exploits the vulnerabilities**”**

Organizations that are vigilant in surveillance have fallen victim to vulnerabilities in the cloud, network, etc. There are countless services but without any I exist since it does not really guarantee not to have an attack. There are companies with figures that encrypt their authentications to provide better security. Let's say that there is software that is monitoring the packets that are in traffic movements between users, which could be public or independent institutions, this service could easily steal the names of users and much more information. These hacking attacks redirect network traffic to your computer instead of being the destination server. Example if a student opens a remote session let's say with a server the computer you want to attack act as a ghost an invisible driver and all kinds of information between the remote service and the innocent user is captive. We explain that in this way the hacker gathers the passwords etc without the server or user being aware of this situation. There is also a category of services that claim to be good but are insecure, such as NFS or NIS, these are developed in LAN Local area network but have been extended to be used in Wide Area Network WAN. NFS Network file system has no authenticity that can prevent a hacker.

1. Evaluation of Vulnerabilities.

We must think about how to know how to protect ourselves to fight the enemy. We have to protect and carry out currently available technology procedures that, in reality, sometimes do not provide or guarantee that the system is secure. It should also be noted that routers can to a large extent secure the gateways that are in the networks, firewalls also in a certain way ensure some type of glitch in the networks. There is a wide range of encrypted streams. Actually, the system implementing the routers configures them correctly and the firewalls can prevent us from an attack and warn us of harmful activity. To achieve this, we have to know how to configure it. There are also companies that are responsible for constant surveillance on the networks. There are dynamic resources, but it is somewhat complex since many do not have the necessary experience for these changes. An example must be protected if the applications of servers, networks, etc., which we wish to deliberate, stay updated. It is something extensively complex since there are virus worms in the software that are constant if we are not aware of what happens technologically. We must continue to review vulnerabilities and prevent evaluating nearby and future problems. These simple practices will make security systems deliver results and indicate the confidence of our networks. Example if you would have to make a vulnerability in your personal home, you would check it to see if the windows are closed or the door if there is a gas leak. Likewise, it would verify if you had vulnerability in the networks, assuring you of your identity as that of your family.

How to secure our net against Cyber-Attacks.

Secure topologies The LAN base is a network architecture, it provides physical and logical and that is between distance with transmission medium nodes. In reality, every case is different since there are several options. to implement it. The physical topology that pertains to the number of IEEE electrical and electronic engineers these topologies are for LAN connections. The ring. Connect the knots in two connections. They are known as token rings. There are no Ethernet connections using this ring topology. In reality, these rings are not used as they would be commonly used, there are configurations for example in libraries or universities. The bus topology, nodes connected in a cable backbone, does not require as much cabling and is effective. But the backbone cable makes it somewhat of a fault if you have to go offline it's actually somewhat controversial because they are used in end-to-end LANs using coaxial cables. the star topology the nodes are connected through where the communication that the hub would be passes. there is a single point of failure in the central hardware connecting these nodes.

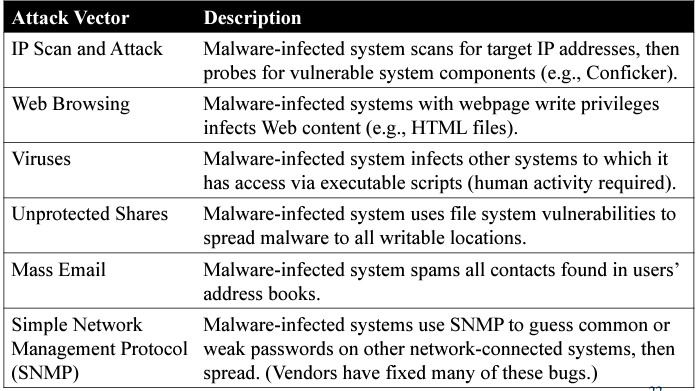


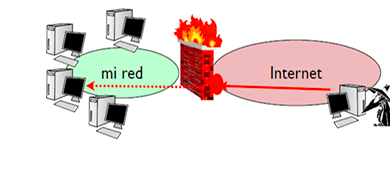
Figure Types Malwares Damage the Red.

lll Conclusion

As we added in this investigation, we can conclude that there are a large number of cyber attacks due to mishandling and lack of experience. We have listed certain technological risks as can be prevented to avoid damage to networks. The elements that we identify that make up the concept of cybersecurity would be the technology as it should be used and the analysis of the risk that it entails. We also mention organizational groups and the organized structure provide effective tools and plans how to combat this evil in independent technological levelexposure.

1. Evaluation of the Cyber attacks.

Networks and private entities control what we can do. The router and firewalls with elements to convince and establish existing policies as we can access the networks. In the graphics you provide we can observe the types of attacks and how we can avoid said attack. You have to have objectives like knowing and when to use the development of IoT Fires walls router architectures and binary configurations is a development methodology. Implementing it is crucial to develop protection models in order to reach a solution. Set up some scenarios like documenting abuses, attacks that have been recorded recently, and security checks so you could determine and be prepared for an optimization build of protection that will be adjusted to meet the given restrictions.

IIV References

1] M. I. Sharif, A. Lanzi, J. T. Giffin, y W. Lee, W. Impeding Malware Analysis Using Conditional Code Obfuscation. In NDSS Symposium 2008. Internet Society.

2]  *FARHAN ULLAH, F. A. R. H. A. N*. (*2019, August 13*). *Cyber securitythreats detection in internet of things* <https://www.researchgate.net/publication>. *https://ieeexplore.ieee.org/stamp*. *Retrieved March 10,*

*3]* Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-turjman, F., & Mostarda, L*. (2019). Cyber security threats detection in internet of things using Deep Learning Approach. Retrived from IEEE Access*

*4]* Van Camp, C., & Peeters, W. (2022). *A world without satellite data as a result of a global Cyber-Attack. Space Policy*, [*https://doi.org/10.1016/j.spacepol.2021.101458*](https://doi.org/10.1016/j.spacepol.2021.101458)

*5]* Faisal, M., Azzid, M., & casarin, zolidah. (2020*). API Vulnerabilities In Cloud Computing Platform: Attack And Detection. International Journal of Engineering Trends and Technology, 1–14*.

6] IDELIS. *(2022, February 25). 2021 AWS Cloud Security Report. Fidelis Cybersecurity. Retrieved March 11, 2022, from https://fidelissecurity.com/resource/report/aws-cloud-security-report*

7] K. Rieck, Computer security and machine learning: Worst enemies or best friends? en First SysSec Workshop (SysSec), IEEE, march. 2022, pp. 107-110.

8] S. Khandelwal (2014, may.), Police ransomware malware targeting Android smartphones [en línea], disponible en: http://thehackernews.com/2022/05/ police-ransomware-malware-targeting.html.

9] E. Gandotra, D. Bansal, y S. Sofat, “Integrated framework for classification of malwares, en Proceedings of the 7th International Conference on Security of Information and Networks. ACM, Sep. 2014, p- 417.

1. *FARHAN ULLAH, F. A. R. H. A. N*. (*2019, August 13*). *Cyber securitythreats detection in internet of things* <https://www.researchgate.net/publication>. *https://ieeexplore.ieee.org/stamp*. *Retrieved March 10, 2022.* [↑](#footnote-ref-1)
2. Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-turjman, F., & Mostarda, L*. (2019). Cyber security threats detection in internet of things using Deep Learning Approach. Retrived from IEEE Access.*  [↑](#footnote-ref-2)
3. Van Camp, C., & Peeters, W. (2022). *A world without satellite data as a result of a global Cyber-Attack. Space Policy*, *https://doi.org/10.1016/j.spacepol.2021.101458* [↑](#footnote-ref-3)
4. CISA. (2021, September 7). Report cyber incidents. Cybersecurity and Infrastructure Security Agency CISA. Retrieved March 10, 2022, *Retrieved From* https://www.cisa.gov/reporting-cyber-incidents [↑](#footnote-ref-4)
5. Faisal, M., Azzid, M., & casarin, zolidah. (2020*). API Vulnerabilities In Cloud Computing Platform: Attack And Detection. International Journal of Engineering Trends and Technology, 1–14*. [↑](#footnote-ref-5)