EasyChair Preprint

№ 9133

Confronting and Intrusion Detection Techniques of Cyber-Attacks in Wired and Wireless Communication Networks

Konstantinos Mavrommatis

October 26, 2022

TITLE

Confronting and intrusion detection techniques of cyber-attacks in wired and wireless communication networks

Author: Konstantinos I. Mavrommatis

School of Engineering, Informatics Computer Engineering Department, University of West Attica, Greece, kmavrom@uniwa.gr

Abstract

This publication aims to study the attacks that telecommunications networks face every day. Thus, the tools that have been developed through new technologies are presented in detail in order to successfully deal with these attacks. Some of these tools are more effective and others less effective depending on the form of attack. As a conclusion is that very significant steps have been taken in confronting with attacks by intruders by introducing a new and wide field of study in the networks.

Additional Keywords and Phrases: Sniffing, MAC Spoofing, IP Spoofing, DDoS, Cash Poisoning, Evil Twin Attack, War Driving, Rogue AP, TCP Syn Flood

Introduction

Information security is considered a major issue in modern computing systems. The development as well as the use of increasingly modern systems can offer significant advantages but may also create significant malfunctions regarding the protection and availability of a network's data. Thus, the satisfaction of the users' requirement for the data of a network to be secure, is one of the most basic conditions for the utilization of new technologies. For this reason, security combined with quality and performance is considered necessary for an organization's network to function properly as the services it provides are mostly based on new technologies.

In this paper, the reader has the opportunity to study basic concepts and security issues of networks and the attacks also received by the networks are described in detail, as well as their forms and the way in which they are attacked. More specifically, the most well-known forms of attacks are mentioned such as: sniffing, Cash poisoning, Mac Spoofing, IP spoofing and distributed denial of service, etc.

In conclusion, it has been proven in practice that the forms and manner of attacks carried out on networks are effectively dealt with through the various tools that have been developed to combat and mitigate them to a very large extent.

Confronting of Cyber Attacks

In this paper, the most well-known forms of attacks are presented, how they work and how to deal with them. In particular, sniffing, Mac Spoofing, IP Spoofing, DDoS, Cash poisoning, evil twin attack, man in the middle are presented. In order to make it more understandable how the specific attacks work, examples of their operation are listed.

Sniffing

Sniffing refers to the process through which the data transmitted with the help of transmission channels such as in a TCP/IP network are interpreted and decoded. Sniffer is an application that performs the entire Sniffing process. It is also defined as a network protocol analyst. However, its mode of operation is divided as follows: a) The indiscriminate mode: through which the Sniffer has the ability to extract information from the data circulating in the network and from the devices connected to the system, b) The mode no doubt: through which the sniffer can extract information and data that ends up in the system. The data that can be stolen concerns sensitive information such as: user credentials (passwords and other details of their accounts), card numbers, e-mails, etc. Sniffing can cause dangerous attacks that are not easily detected. For this reason, sniffing could also be distinguished in a passive type of attack where the attackers can pass unnoticed through the network. Vulnerable to sniffing attacks are protocols in which either the password or data is sent in clear text. Examples of such protocols are: telnet, http, SMTP, IMAP and FTP.

But how are these types of attacks carried out by attackers? The attacker carries out a sniffing attack to be able to extract information that is sensitive and may also concern data related to technical details of the network in order to carry out more attacks of this type. In practice, this can happen using commercial software tools. However, there are three ways in which Sniffing attacks are carried out on a network: a) wireless sniffer, which is exclusively designed to extract data from wireless networks; It is also called wireless packet sniffer or wireless network sniffer., b) external sniffer, where in this type it is possible for the sniffer to monitor the incoming and outgoing traffic from an external location to a web server gathering relevant information. In short, sniffing when performed from a location that is external uses the corresponding software tools, c) internal sniffer, which is designed to exploit an organization's internal network. In particular, the attacker in this case adapts a machine to the internal network and activates the sniffer trying to extract information and data from computers connected through the network. Thus, the term sniffing is related to data and information that can be stolen. The ways in which sniffing can be applied are described as follows: a) Through the LAN, where attackers can install a sniffing tool scanning all the IP addresses of the computers that make up the network and are connected. Thus, information such as: open ports, active hosts, etc. can be stolen, b) through a sniff protocol, where attackers try to extract information regarding the protocols used by the network. Thus, attackers attempt to specify a list of protocols and information received. When the list of protocols is compiled, it is separated according to the type of attack in order to develop the appropriate sniff. More specifically, if the list of protocols includes UDP, then a UDP Sniff will be created, which will try to decipher all the details associated with applications such as DNS and Telnet, c) in the case of ARP Sniff, the attackers scan all network IP addresses as well as MAC addresses. Having received this information, attackers can perform spoofing attacks, router attacks, etc., d) by stealing the TCP session, which will capture the traffic route between the source and the destination. Attackers in this case are interested in knowing more and more about the ports in use by the network, the IP addresses and the services offered in order to attack. Having all these elements, the attackers have the possibility to create sessions between the communicating devices acting as a man in the middle contributing in this way to the interruption of services but also to the recording of sensitive data, e) Sniffing at the application level, the attacks that will be carried out at the application level are done through the list of active applications of the victim. Thus, attackers attack the data packets in order to extract the necessary information about the applications either by stealing them or to carry out more attacks depending on the nature of each application they want to attack. As for example the attack carried out on the user's credentials etc. f) Web Password Sniffing, it is known that all communications carried out on the internet are done through the http protocol. Attackers can capture and steal an http session where by analyzing it they can cause attacks and cookie

poisoning. Although SSL contains security mechanisms in http, sniffing tools are much more drastic as websites prove vulnerable to them [1].

Sniffing attacks are generally divided into two categories: a) PacketSniffing: where network packets are monitored. The above can be done by introducing a program which will monitor the network data packets creating a copy which is forwarded to the attacker b) Network Sniffing, this type of attacks have a different form. Sniffing Client is implemented by actions in the user's batch languages, and includes Sniffing server side, which takes part on the server side using communication protocols. Browser Sniffing which uses websites and web applications to detect attacks. This form of Sniffing uses information from the browser cache as well as its history. In this way attackers can extract the information from the network by installing a sniffer tool. Also, another form of attack is content sniffing which is also called MIME Sniffing. This form of attack attempts to mimic any changes made to web applications as attackers essentially attempt to change the content or even the format of the file. This format hurts both sides both the client and the server. To avoid the attack by the attackers there should be adjustment in the content and options of the browser. Also, password sniffing attack can extract very sensitive and private information such as user credentials.

However, Sniffing attacks at the network layer of the OSI model can be performed in the following three ways: a) based on IP address where sniffing tries to extract network packets based on IP filter, b) MAC-based initiation, where it works in a similar way as in case a with the exception that sniffing tries to extract network packets based on MAC address filters, c) ARP-based, where sniffing it makes use of the ARP request-reply message where it then attacks its memories resulting in redirecting the attacker's interest depending on the configuration that has been completed.

MAC Spoofing

The MacSpoofing attack is another form of attack on information packets and works as follows. The attacker searches the network for valid MAC addresses. It then tries to act as one of them by masquerading as the default gateway and copying all the information forwarded to it without being noticed. The above function gives important information to the attacker regarding the applications used by the system. As a result, the CAM information on the switch is spoofed as shown in the figure below.

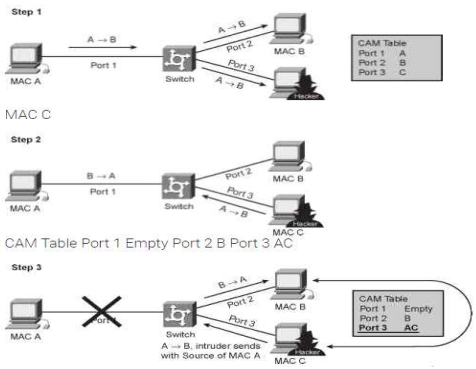

Figure 1: Mac Spoofing Attack (via Cisco.com - Certified Expert)

From the figure it follows that out of devices A, B, C in the CAM table, device C is the attacker. After spoofing the MAC address of the device A, the attacker i.e. device C, sends a fake IP address. The switch then relearns the MAC address and changes the MAC table entries. When device B communicates with device A, the switch will send the packet according to the entries

in the CAM table where, according to the figure, it is on port 3. Until device A sends packets again, nothing changes in flow that the data has as a result of which the attacker receives and also monitors the already active packets thus ensuring the maintenance of his connection until the network administrator intervenes. However, to mitigate this kind of attack, a very good network design should have been done beforehand as the attacker behaves very cleverly. One solution that could mitigate the attack is to use private VLANs as ports are restricted to a VLAN that communicates with other ports on the same network. Another method in conjunction with port security is the use of DCHP monitoring mechanisms. This ensures only valid DCHP servers are active on the network. However, such a mechanism ensures reliable data flow between client and server. Also, using DHCP Snooping in combination with DAI (Dynamic ARP Inspection) is the best solution. So, when a broadcast message is sent for an IP address, the attacker gets it. Except that the message broadcast is sent to all ports except the source port. This way the network does not allow sending either positive or negative confirmations from untrusted sources. Untrusted DHCP messages are usually received by the firewall or some external network. The DHCP Snooping table contains items such as IP and Mac addresses, network number, and all such information that corresponds to untrusted interfaces. Of course, the DHCP table does not include data about hosts or their connection to trusted interfaces. Configuring both trusted and untrusted sources is possible by setting the switch to prevent illegitimate frames. However, DHCP Snooping cannot stop an attacker from attacking Mac addresses. DAI defines how valid an ARP packet is based on the binding of Mac addresses to IP addresses stored in a DHCP database. In practice, this means that only valid addresses are allowed and are for devices on the network that are authorized. Attackers because they are smart expect some network bounce for devices that are not active [2].

At this level the error detection and correction techniques are based on sending the data ensuring that the sequence of bits conforms to a rule which is accepted and described below: a) the detection of the error: the receiver of the data understands that the data does not conform to the accepted rule, b) correction of the error, when the recipient of the data proceeds to replace a part of data that conforms to the accepted rule. In wire media that are considered reliable, the most common practice is to detect the error and retransmit the data. In media that are not considered reliable and are usually wireless media, error detection and correction is considered essential. Figure 2 below illustrates the error detection and correction technique. In order to detect errors, the following techniques are used: a) the parity check and b) the CRC technique (Cyclic Redundancy Check, c) Multiple Access Check. In Parity checking, a simple error detection check is performed by adding a bit to the end of the data. The parity check concerns even parity where a logic 1 is added thus ensuring the presence of an even number of logic 1s and odd parity where the addition of logic 1 ensures the presence of an odd number of logic 1s.

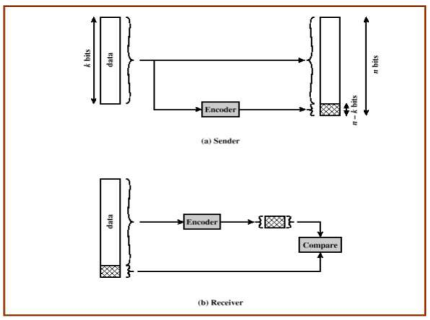

Figure 2: Error Correction and Detection Techniques (via Cisco.com - Certified Expert)

The CRC (Cyclic Redundancy Check) technique is based on the addition of one more bit in order to create a new word where if divided by a certain word it will give a remainder of zero.

More specifically, in the transmission phase, the bits that will be added to the end of each word are calculated and then it is sent. During reception, the received word is divided and if the remainder is zero then the error is detected. Finally, in the last technique, which concerns multiple access control, the use of common transmission media is based on the adoption of rules that are common to both the control and the use of the medium. However, the content of the rule can take several forms but in the case of networks the technique that is most common is carrier sensing multiple access where in this case the user detects if there are transmissions and waits until the medium is available again, in collision detection when multiple simultaneous broadcasts are taking place on the shared medium [3].

IP Spoofing

The main protocol used to communicate over the internet is IP. This protocol contains elements such as its own header with all the necessary components accompanying it which indicate the source as well as the destination of the packet. These details are necessary and have already been formed before sending the package. However, if the packet's source header address is not legitimate and is spoofed, then the packet will appear to have been sent from some other source. From the above, it follows that IP address spoofing is also called IP Spoofing. This technique is used by attackers to cover their identity. Primarily, the IP Spoofing technique is used for spamming and phishing attacks but also with DDoS distributed denial of service. However, IP Spoofing is a problem that does not have an easy solution. For example, attacks such as: DDoS and TCP SYN with spoofed IPs flood and clog the network. Phishing messages cost the victims of the attacks quite a lot in losing money and the phisher is not easily traced. The above are important cases that need to be addressed. However, there are ways to defend against spoofing. Modes of defense can be distinguished in the following categories: a) Prevention before transmission, b) prevention during transmission and c) prevention after transmission.

In the first case, according to network filtering also defined as network ingress filtering, the traffic is forwarded if the IP address belongs to the network and enough time is required for its development on the Internet. However, the filter prevents the network from being used as a victim of spoofed addresses. However, the network did not encounter spoofed network packets. Also, in this case, filtering requires each node in the network to be deployed before it is implemented and additional configurations are required from the routers [4].

In the second case, according to route filtering (RBF), ingress filtering is extended based on the network topology. In this case, suspicious information is collected autonomously and updates are made when there are changes in the routing table.

In the third case, the defense based on TTL (Time to Live) of the packet is proposed by calculating the total path of the packet from the source to the destination. The TTL value is accurate and cannot be easily faked. The TTL field of an IP address header also defines the lifetime of the packet. Each time a packet reaches the destination its initial value is subtracted to obtain the total hop count of the packet.

Alternative, the table entries and the update made to the routing when changes are made and the filtering of a spoofed packet using the table information. The system is managed in the first case with the Clouseau system and in the second case with the use of RBF. Management with the Clouseau system involves the TCP data packet arriving at the router, observing its retransmission from the source. At the same time, RBF filters the packets that are fake by comparing the expected interface with the incoming one. However, RBF works best in smaller networks, and for this reason it is a problem to detect a spoofed packet in a

larger network with more computers and autonomous systems. Of course, if the spoofed packet is sent from one network to another, it is treated as if it came from another interface. In the SMP method (Spoofing Prevention Method), the router that is closest to the destination of the packet has the ability to confirm the authenticity of its address. Routers also inspect the packet and its destination-related tags. Each source-destination pair of the network has a unique key and is known from the beginning to both the source and the destination and is also used as an identity mechanism for incoming packets. However, the keys are present in the packets when routers send them but are removed when the key is authenticated. So, when the ISP detects an attack on the network the way they defend and protect themselves is by only allowing packets originating from the SPM network to be sure there will be no traffic disruption. Yet another method to limit IP spoofing is Distributed Packet Filtering (Park, et. al., 2001). In this case, a set of paths is calculated and the best path is selected. So, in the DPF, the shortest path is applied. However, if the packet arrived from an interface that is not expected, the packet will be dropped. Of course, DPF has the ability to locate the attacker, however the detection of the attacker's location can be path-based and has the ability to minimize the attacker's network as a very small network range. If spoofed network packets are filtered and located close to the attacker, attacks can be detected. The packet that leaves the network and goes to the next router has its own signature. NLT (Neighbor Link Table) contains information about network topology, interface and previous router. In order to detect forged packets, the NTL is queried for their signature. Also, SAVE (Source Address Validation) is a protocol that collects information to validate the address of the packet entering the network. This protocol contains anti-spoofing mechanisms throughout the network, recording the path the packet has traveled and ensuring the correct path. And RBF can limit the IP addresses that are under attack. However, both DPF and SAVE improved RBF by forwarding only packets originating from correct interfaces. Verifying the source of forwarding packets to counter spoofing is considered an effective countermeasure [5].

Distributed Denial of Service (DDoS)

A DDoS-Distributed Denial of Service (DDoS) attack is related to the attempt to degrade Internet systems or web servers by constantly flooding them with data. Such attacks can be simple attacks that are a bit of a nuisance or even involve the disruption of an organization. It usually involves a large group of distributed computers colluding with each other at the same time trying to "spam" a website or service provider with data requests. The way this happens is by using and installing malware on users' systems. As mentioned, these attacks are carried out by a large number of computers to achieve their goal. However, to achieve the control of many machines the easiest and most economical way is that of exploits. Attacks of this type take control of Wi-Fi cameras with passwords that are already defaulted in order to create a large botnet. When the botnet is ready, attackers find the right time to attack by sending the initiation to all its nodes and then sending their requests to the target server. If the attack manages to bend the external defenses very quickly all systems are overwhelmed resulting in server shutdown [6].

In order for a system to withstand attacks it must be prepared. In other words, systems should have alerts built in to detect an attack early and terminate it without affecting users. However, it is possible to block the IP addresses, using the firewall, or even shut down the traffic of the primary system and switch it to a backup. Of course, there are other response plans that organizations can implement. DDoS attacks have different forms as described below: a) application level attacks: this form aims to exhaust network resources, with the aim of stopping access to websites. Thus, attackers send a complex request such as database access and even downloads which are large as the server tries to respond to it. However, if these

requests are many and sent in a short period of time the system will slow down. For example, an http flooding attack is a typical example of an application layer targeting a web server, b) protocol attacks: these attacks target the networking layer of the systems by flooding the basic networking services as well as the firewall with requests to the target. More specifically, the services of a network operate with a priority queue where the first request is entered and after it is processed then the second request is entered and so on. However, a DDoS attack can make the queue so long on a system that doesn't have that many resources to deal with it. More generally, the services of a network with regard to the requests that are in the queue, work as follows: the first request that is entered is also the first one that leaves the queue. So, the first request that enters the queue is processed, released, and the next one is entered, and so on. Thus, one form of such an attack is the SYN flood. For example, this format in a TCP/IP transaction consists of three directives. The first is called SYN and is the first part of a request, the second is called ACK and is the response given by the target and the third is called SYNACK and is the response message thanking for the message received. Thus, in a SYN attack, packets are created with fake IP addresses. More specifically, the target sends an ACK to a virtual address from which it never receives a response, waiting for responses to terminate, which in itself consumes system resources. Another form of attack is the so-called Volumetric attacks which aim to create a large enough volume of transaction traffic in order to block the target by constantly requesting the target resulting in an increase in the response size, essentially blocking the server [7].

Cash Poisoning

Cash Poisoning is a cyber-attack where attackers inject information that is fake into a domain name system cache called DNS or a web cache with the ultimate goal of extorting information from users. Such an attack occurs when an attacker tries to disrupt traffic from a server that is legitimate to a server that is dangerous. Thus, the attacker enters fake information such as a website address that is corrupted into the cache leading to redirecting users to dangerous websites. This attack is an extremely dangerous attack not only because it creates problems for the traffic of legitimate websites but mainly because the users who fall victim to these attacks are really exposed to malware and interception of their data. When a web cache is poisoned, the attacker exploits the server to serve malicious HTTP (HTTP) responses to network users.

Thus, cache poisoning occurs when false information is entered causing the web browser to return incorrect responses to network users. The responses users receive usually direct them to different websites than the ones they intended to visit. DNS resolvers are not able to verify cached data. This fact means that the false information remains stored in the cash memory until the expiration of the TTL. Although cache poisoning does not actually disconnect the real website from the true IP address, if the false information remains in the cache, network users will continue to be directed to the wrong websites. The inherent risks associated with cache poisoning are malware infection, interception of user data, and blocking of security updates. The first case enables attackers to install malware on users' systems through automated downloads. The second case may lead to a breach of users' personal data and the third case may prevent important security updates of the users' security systems which are exposed to viruses [8].

The response to a malicious attack can take on other dimensions if there is caching in the browser memory that users use or in the web cache that is accessed by several users. However, if the response to an attack eventually succeeds in being cached in a web cache that is shared, it results in users using it continuing to download malware until the cache is flushed.

The same is true of programs used by individual users who will continue to receive malicious content until the cache is cleared. However, attacks by attackers are considered successful when: a) the code of the service is vulnerable and allows filling the HTTP header field with many more, b) a crafted message is sent which is stored in the buffer memory, c) forces the server of the temporary memory to proceed with the liquidation of its substantial content, d) proceed to send the next request where the previous content entry essentially constitutes the response to this request. This form of attack is actually considered not so easily feasible in a realistic environment due to the fact that it must satisfy many conditions. However, the cachepoisoning attack is more easily performed as it allows distinguishing HTTP response and web application vulnerabilities. From the attacker's point of view, it is considered important that an application allows the header field to be populated with more than one by making use of CR (CarriageReturn) and LF (LineFeed) characters [9].

However, the execution of the requests should be done during a connection when the previous ones are satisfied. Probably this form of attack is considered problematic for cache poisoning and is caused by the difference in the connection model of the cache server and the applications that process the requests. Essentially, this form of attack could be more effective on other servers. Finally, this technique faces problems related to the length of the URL where positioning the response header is practically impossible to match the request with the page being poisoned.

Evil Twin Attack

This type of attack is cyber spoofing and aims to trick users into connecting to a fake Wi-Fi access point that tries to mimic a legitimate network. Once the user is connected to an eviltwin network, hackers have access to everything. These attacks owe their name to their ability to mimic legitimate Wi-Fi networks, so that one cannot easily tell the difference. The eviltwin attack is extremely dangerous and not easily detectable. Hackers prefer crowded locations such as coffee shops, airports, etc. to carry out their attack. This is because these parties have multiple access points with the same name, so the fake network can easily go unnoticed. Then, a new hotspot is created using the same SSID as the legitimate network. In this way, they have the possibility to use any common devices such as phones, computers, etc. In addition, hackers can also set up a captive portal page where the user is required to enter a password or even other information to connect to the network. So, hackers can easily reproduce these details by tricking users into sending their login details. Additionally, a hacker can move their device or router even closer to potential victims, creating a stronger signal.

War Driving

This form of attack maps access points and detects possible exploitation of connections in wireless networks. To do this, you need a computer, a wireless Ethernet card, and an antenna that can be mounted in a car. Because the wireless network extends beyond a building, any outside user has the ability to hack into the network by gaining free internet access to resources and files. The attack can be done very easily by using a directional antenna and a GPS to map the locations of the 802.11b access points [10].

Companies with wireless LANs are encouraged to add security controls to ensure that only intended users have access. Safeguards include using the Wired Equivalent Privacy (WEP), IPsec or Wi-Fi Protected Access (WPA) encryption standard, along with a firewall or DMZ.

The term comes from a somewhat similar approach to hacking the phone system called war calling. Hacking a private network can be illegal and at least one person has been prosecuted.

Rogue Access Points (Rogue AP)

Rogue Access Points are essentially a "rogue access point" in any wireless access point that is installed on the wired network infrastructure without the consent of the network administrator, essentially giving access to the wired network that is not authorized. In many cases APs are characterized as rogue and installed by users who want wireless access when it is not available.

TCP Syn Flood

In this attack the attacker sends TCP connection requests at a faster rate than the target machine can process resulting in network saturation. The following figure describes the TCP Syn Flood attack process. The steps of the attack include; By establishing a "three-way handshake" between the client and the server, information is exchanged as follows: a) the client wishes to connect by sending a sync message to the server, then b) the server confirms that it received the message to the client by sending syn-acknowledgment (synchronization and confirmation) and c) the client in turn responds with another acknowledgment message and the connection is restored. When a flood attack is carried out the attacker sends continuous packets that are repeated to each port of the target server using a fake IP address. The server unaware of the attack receives many messages that are legitimate requests to communicate from each of its ports. Thus, the attacker either does not send the expected acknowledgment of the packet or never receives the message in the first place. In any case the server receiving the attack waits for confirmation of the packet for a period of time [5].

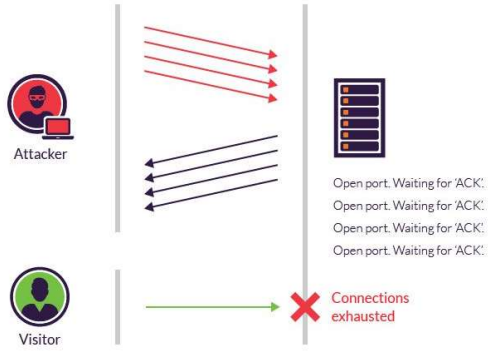

Figure3: TCP Syn Flood Attack (via imperva.com)

Conclusion

In this paper, an attempt was made to present the types of attacks on wireless and wired networks as well as the ways to deal with them. An extensive research was carried out regarding the attacks received by the networks, their forms as well as the ways and methods mainly used were described. It also describes the tools that attackers use to carry out an attack. Some of these attacks turned out to be more damaging than others. Indicative sniffing and DDoS appear to be the most destructive exploiters of network resources.

From the research and development review it emerged that researchers have focused their attention on developing packet transmission defenses thus giving credit to the customer and the implementing ISPs. Filtering on a network has been shown to work effectively but only prevents attacks from its own network. However, looking at things from the other side, adopting policies to defend against packet destination side attacks can introduce new problems. Investing in defense policies to counter attacks is proving to be a promising solution with good results in practice. However, the protocols that perform the routing continue to evolve. Implementing an algorithm with different routing seems to be not an easy task to implement a defense mechanism against attacks that is compatible with everyone. Thus, if the routing involves multiple distribution of IPs, it makes it more difficult to try to develop an effective political defense against attacks.

References

[1] Aman K, Sudesh J, Sunil M. (2012). Comparative Analysis between DES and RSA Algorithm's. International Journal of Advanced Research in Computer Science and Software Engineering. ;2(7):386-391.

[2] Qadri, S., & Pandey, K., (2012). Tag Based Client-Side Detection of Content Sniffing Attacks with File Encryption and File Splitter Technique. International Journal of Advanced Computer Research. 2(5), No-3: 215-221.

[3] Karthik S, Muruganandam A. (2014). Data encryption and decryption by using triple DES and performance analysis of crypto system. International Journal of Scientific Engineering and Research. ;2(11):24-31.

[4] Shraddha D. (2016). Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java. International Journal of Computer Trends and Technology. 2016;35(4):179-183.

[5] Preetha M, Nithya M. (2013). A study and performance analysis of RSA algorithm. International Journal of Computer Science and Mobile Computing. 2013;2(6):126-139.

[6] Alotaibi, B., & Elleithy, K. (2015). An empirical fingerprint framework to detect Rogue Access Points. In Systems, applications and technology conference (LISAT), 2015 IEEE Long Island (pp. 1–7). IEEE.

[7] Yang, L. X., Li, P., Yang, X., Wen, L., Wu, Y., & Tang, Y. Y. (2017). Security evaluation of cyber networks under advanced persistent threats. arXiv preprint arXiv:1707.03611.

[8] Wortman, P. A., Tehranipoor, F., &Chandy, J. A. (2018, June). An Adversarial Risk-based Approach for Network Architecture Security Modeling and Design. In 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-8). IEEE

[9] Välja, M., Korman, M., &Lagerström, R. (2017, April). A Study on Software Vulnerabilities and Weaknesses of Embedded Systems in Power Networks.In Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids (pp. 47-52), ACM.

[10] Span, M. T., Mailloux, L. O., Grimaila, M. R., & Young, W. B. (2018, June). A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems. In 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-8). IEEE.