Indian Journal of Science and Technology, Vol 9(40), DOI: 10.17485/ijst/2016/v9i40/98588, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Design and Implementation of a Defense System from TCP Injection Attacks

G. Ranjith, J. Vijayachandra*, B. Prathusha and P. Sagarika

Department of CSE, Warangal Institute of Technology and Sciences, Warangal – 506342, Telangana, India;
gyaderlaranjith@gmail.com, vijayachandra.phd@gmail.com, prathushabonagani@gmail.com,
pochala.sagarika@gmail.com

Abstract

Data and Information Security are the major concerns in the modern network world. The most widely used and reliable transport protocol is TCP over internet. As it is most widely used network, which is facing a security breach from the TCP injection Attacks. We discussed different attacks such as Spoofing Attacks, IP Address Spoofing Attacks, ARP Spoofing Attacks, Man–in Middle Attacks, TCP-Session Hijacking and even we concentrated on Advanced Persistent Threat. We exposed different security measures against packet sniffing, packet modification and IP Spoofing. The mathematical analysis is given for the authentication mechanism to protect the data from the different risks, threats and attacks. We also focused different security measures and protocols at transport level such as secure sockets layer and transport layer security protocols. We designed and implemented the defense system to protect against the Advanced Persistent Threat and other attacks, and research issues in networks and Cloud Computing. An experimental analysis is given along with In-depth analytics and mechanisms regarding the threats in transit and TCP Session Hijacking. Network data and information security methods such as packet filters design methods and implementation are provided along with the mathematical analysis and experimental output.

Keywords: Advanced Persistent Threat, Defense in Depth, Multi-path TCP, TCP-Injection Attack

1. Introduction

Transmission Control Protocol is an important transport protocol over the Internet, TCP-injection attacks on connections at transit, at browser level and at higher levels such as web-server level. This attack poisons web with malicious objects such as spoofed web-pages for a long period of time, and even the scripts such as cross-site scripting, phishing attack, cross-site request forgery and pharming attacks. The Attacks exploits the IP, TCP and HTTP protocols. Network Interface Card plays a major role in the network communication system, where of unique identification is possible for each host in a network, which is done with the help of mac address. The network interface cards major responsibility is to detect and identify the address of the host. It is even possible at the situation of the address corresponding to multicast hardware group in which the host is a member of and broadcast mac address[1].

The Risk at this level is an intruder or a hacker who can reprogram the Firmware of Network Interface Card using the media access control address that is the hardware address of another host where the data packets are accepted at the host based on the addressed packets addressed to that host. To make an intrusion identification complex task and to escape from the detection of Intrusion the intruder puts back a copy of packets to the network[2].

Network Protocols should able to secure against risks, threats, attacks and able to identify vulnerabilities., Transmission control protocols should able to secure from most common attacks such as the spoofing attacks, where they can't eavesdrop on packet at rest or at transit. Even it should secure against the pharming where it should be capable to identify fake IP Addresses, there is an interpretation that it cannot be realistic for a spoofing attack to inject traffic into TCP connection, for the

*Author for correspondence

cause of the TCP implementations randomizes the 32-bit sequence numbers to the 16-bit client port[3].

Here we furnish some of the attacks to defense system from TCP injection attacks, by making to grasp the port address of the client in sequence and there by connection is injected by the traffic. Here we discuss the attacks from those major procedures that are bearing the address of ports that remains for obtaining the sequence numbers. Each and every attack is used by medullary which means each and every port that is identified by learning attacks can be utilize with the help of a sequence number that each learning attack provides execution. This concept provides different attacks that may have different pure-requests as well as different performance properties[4].

Let us learn/know about the different procedures that are involved in an attack where the client relies on the security procedures that are provided by the third party auditor, where the client convention of the global internet protocol ID counter, which relies on the client convention where the sender chooses the internet protocol identifier for the sake of identification with the help of a global counter, which has capability to communicate with the client. When a data packet is transferred from source to destination then slide channel is introduced as interface that is based on the sequence number of TCP connection. The way in which the global internet protocol identification counters the side-channel is specific to the clients operating system, which is very common compared to other procedures of side channel that are used[5].

Here the next sequence number avoids the global internet protocol identification that is related to learning attack which legitimate behavior versions of browsers. The modern browsers use add instances where the defense systems are stored, which logins along with the browser to restrict such attacks. This TCP injection technique is independent of victims operating on the systems[6].

TCP injection allow many attacks, in particular we show the circumvent of basic browsers some origin policy defense and inject spoofed objects such as scripts and web-pages to a connection with a victim website, we also show how attacker can force these objects into the clients cache and form a persistent cross-site scripting / web –spoofing attacks. Malware spreads through TCP/IP by exploiting security vulnerability. Authentication Techniques are implemented on packets in rest or in transit for enhancing the security concerns. The Message Authentication Code (MAC) is also called Tag, which is implemented for computational security that is to protect against attacks. Digital Securities also used for both computational security and unconditional security, where data protection should be done from phishing attacks[7].

2. Related Work

2.1 Spoofing Attacks

It is an attack when a malicious party used to pretend to attack the other devices and uses across network against the data theft or spread of unknown malware to control by command that exist different mechanisms that detect and defense the system through different attacks. Some mechanisms such as diverting the traffic address that include spoofing attacks are Internet Protocol Address Spoofing attacks, Address Resolution Protocol Spoofing Attacks, Domain Name System Spoofing Attacks.

2.2 IP Address Spoofing Attacks

In this mechanism the attacker uses the false source address by masking the actual address by pretending with address, so the attack overloads the networks and destroys the congestion control system. The legitimate IP address will be identified by the intruder and spam internet protocol address will be masked with the legitimate IP address and by implementing through the searching algorithms the spam IP will be available to the user instead of legitimate.

2.3 ARP Spoofing Attacks

In order to transmit data, we require using a protocol to resolve IP address to Media Access Control Address. Address Resolution Protocol Address Threat sends by the malicious party with respect to the ARP Spoofed messages across a LAN in order to link attack's with hardware identification protocol address and hardware device address of a legitimate members of the network environment.

2.4 Man – In Middle Attacks

The mechanism used in this Attack, where the attackers' gets access to retrieve, insert and update messages that place between two communicating particulars in the obscene of the two parties by compromising the link between them. To successfully carryout by intruder can passively observe messages between two users.

2.5 TCP-Session Hijacking

Transmission Control Protocol Session Hijacking mainly concentrates on the Packets that are approaching us the

authorized person of the session by retrieving an already established TCP session and injecting packets into the stream that are Under receivers' session. Here a TCP session is identified by the client IP Address, client port number, server IP Address and Server port number. Any packet hat come across with the alone identifier is considered to be part of existing session. If attackers can spoof these items, they can pass TCP packets to the client or server and have those packets processed as coming from other machine[8].

2.6 Advanced Persistent Threat (APT)

It is a definite design implemented as a provision until it reaches the target and creates backdoor so that it can in and out as per the requirements for future Interference, as the starting it is a passive attack later converts to an active attack where is to steal data rather than cause damage or destruction to the cloud storage environment[9].

These are crafted targeted attacks that are basically uses the intelligence gathering to retrieve the data from cloud computing where the basic determination of this mechanism is to place convention malicious code on one or multiple data centers for specific task and to remain undetected for the longest possible period. There are many different malware variations that are extremely challenging cloud environment, as security is the major factor for survival of the cloud[10].

Malware spreads into organization by Social Engineering methods or by exploiting security vulnerability. When a victim open's email attachment or downloads the files from emails or websites, malware automatically installs without any notice. Even malware attacks when victim clicks on uniform resource locator links provided by emails or websites, where the major task is detecting phishing URLs[11].

3. Mathematical Analysis

Researchers proposed many authentication schemes and mechanisms to protect different Protocols from injection Attacks and many other attacks. These mechanisms are used to detect the malicious packets injected in networks; even alerts can be provided by the system[12].

The Authentication Mechanism on the TCP/IP is not only to identify the malicious packet injects on network it also protects the Protocol and it is a defense system with different stages such as key generation, key distribution and authentication tag which is also known as message authentication code[13].

3.1 Key Generation

The Trusted authority randomly generates the polynomials and these polynomials are of degree k-1, and we denote them by

$$P_i(x) = a_{i,0} + a_{i,1}x + a_{i,2}x^2 + a_{i,3}x^3 + \ldots + a_{i,k-1}x^{k-1}$$

Where i = 0,…..,M

The total number of polynomials generated is M+1 that is $P_0(x)$ ……, $P_M(x)$

3.2 Key Distribution

The trusted authority gives a private key to the source S and the M+1 polynomials $(P_0(x_i),\ldots\ldots,P_M(x_i))$ where i = 1,….V.

The values of $x_1, \ldots\ldots, x_v$ are made public the keys can be given to the nodes when they sign-up for a service protected by the scheme.

3.3 Authentication Tag

When the data sent in the form of packets from source to destination different attackers will try to attack the network system using different techniques, where we use the Authentication Tag is to protect the data packets. Let Source sent n data messages that is from $S_1,\ldots\ldots\ldots S_n$ belongs to a polynomial Set, which forms the authentication tag of each S_i where i = 1,…..n. The packets X_i to be actually sent by the source are of the form

$$As_i(x) = P_0(x) + s_i P_1(x) + s_i^q P_2(x) \ldots + S_i^{q^{(M-1)}} P_M(x)$$

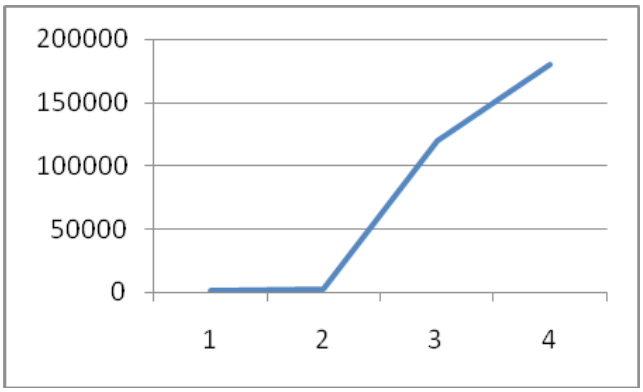
4. Statistical Analysis

Digital Securities plays a great role in protecting confidential and sensitive data in networking environment, Authentication and Authorization are the security credentials to defend different threats and attacks. Regarding security process for the defense, tags are formed over the IP based Network, the messages are communicated from source to destination in the form of packets where the tags are used for authentication. At destinations users can download file only with proper authentication[14].

Transmission Control Protocol over Internet Protocol based network messages M starting the file to be circulated

Table 1. Variable sizes for distribution of files

File Size	Message Length	Nb*LJ* of IP packets	M X L bytes –Message Authentication
18 MB	1500	1	1200
72 MB	3000	2	2400
1.8 GB	15 K	10	120000
4.05 GB	22.5 K	15	180000



Graph 1. Distribution of message authentication.

that can be communicated by the source to destinations in the form of packets, where they are authenticated by use of a key. One tag will be appended with an IP packet then it is considered as J IP packets as one message[15].

In the Table 1, the distribution over the content of Internet Protocol network with our mechanism at most M messages forming the file to be distributed, where one tag for IP Packet, so it is mentioned as J IP packets as one message and authenticated as Message Authentication. The graph obtained by analysis of authentication of message is given as following

5. Experimental Analysis

As we know that Digital Securities are protected confidante of sensitive data in networking environment, authentication and authorization to defend different threats and attacks.

The trusted authority gives a Trinity keys to sources S and M + 1 polynomials, here we can implement the concept of handshaking signals, where the transmission of messages takes place between source and destination with major security to protect packets from attacks.

The Command are injected through sql injections and other means of hacking tools for a successful hijack or attack by an attacker, who indeed need to first of all desynchronize the session which a part of client and server communication between the source and destination when the data is in transit. Intrusion detection and protection system tires to detect the TCP session between client and server, where as the attacker escaping from the IDS and other monitoring tools tries to predict or estimate the sequence number that given chance to be used by client where the attacker tries to accesses the data packet using networking packet sniffer, where the packets belonging to the TCP session and even intruder tires for acknowledgement packet exchange. As this Acknowledge packet will most likely because of a sequence number that is not expected by it, the original client will attempt to re-synchronize with the server by sending it an Acknowledge packet with the sequence number that it is predicted. This acknowledges packet will in turn hold a sequence number that the server is not predicting and so the server will resend its last acknowledge packet[16].

The conditional probability is used to calculate the success rate of attackers' hijacks at TCP Session. When the attacker successfully hijacks the TCP session and injects own spoofed data packets then that server will acknowledge the receipt of the data packets to original client by sending it an acknowledge packets[17].

This mechanism becomes a cycle that will remain continuous process and the fast transient back and forth of the recognized packets which creates the Transmission Control Protocol acknowledge storm. As the Intruder injects more and more data packets, the size of the acknowledge storm increases drastically and immediately brings down performance of the networking. After a certain number of un-successful attempts, the original client eventually gets tired and closes the connection with the server.

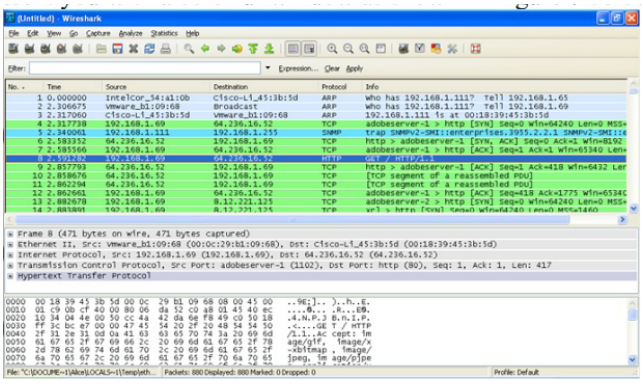


Figure 1. Penetration Testing Tool to analyze and troubleshoot the flow TCP Stream of packets.

Wireshark is a Packet Analyzer used for the network analyzing and troubleshooting. It is also used for the communication protocol development. It is compacted with the network interface controllers such as tcpdump and libpcap. In-spite of absolute sequence number mechanism tcpdump maintains all the connections and generates a relative sequence numbers. It also works as filter and the mechanism used is to captures packets and sends the captured packets to a machine through Wireshark using TaZmen Sniffer Protocol.

Implementation of Defense System is possible with a mechanism of continuous monitoring the network environment and it is possible to detect and defend the TCP Injection and other attacks. Penetration Testing is implemented by using Wireshark with flow TCP Stream, for vulnerability scanning and deploying a defending mechanism to identify the MAC Address of the Intruder of the network flow analysis.

Wireshark is very easy to install and gainful solution set that Identifies and overcomes the vulnerabilities, it is the ultimate elucidation for scanning in-depth positions in Penetration Testing. The packet loss is the most common problem faced by the network of the TCP traffic due to the TCP hijacks. The appropriate solution for this problem is to enable the internal and external scans for a successful defense system implementation[19].

6. Conclusion and Future Work

To defend network from the TCP Injection, a defender has to implement the security measures from the least level to a high sophisticated top level configuration systems with defense in depth that is the onion layer architecture, but majorly concentrated on the application layer and the network layer.

We make use of Transmission Control Protocol which is very important transport protocol over the Internet. Here we also implement the Authentication Mechanism on the TCP/IP which is not only to identify the malicious packet injects on network but it also protects the Protocol and it is a defense system with different stages such as key generation, key distribution and authentication tag which is also known as message authentication code. We use the Authentication Tag to protect the data packets from different attackers on network systems. These tags are created for the purpose of protection over the IP based network, that is at the destinations of users can download file only with proper authentication. In this paper the Digital Securities also plays a great role in protecting confidential and sensitive data in networking environment. In depth analytics and mechanisms are given regarding the threats in transit and TCP Session Hijacking.

Future work is regarding improving the TCP security to protect on path attacks and injection attacks. TCP Supports Multipath so there are more possibilities for an attacker to intrude with in short intervals. The attacker can throughput of unauthorized paths. Data and information security mechanisms and measures are the evergreen updating of solution to the risks, threats and attacks. The other major tasks are congestion control, avoid packet loss and counter measures for network delay. We concentrate that these attacks are not specific to a particular execution, but directly outcome from the design objectives of Multi Path TCP. As a conclusion, we maintain that these attacks are primary and important to Multi Path TCP and may establish a barrier to its wide-scale adoption.

7. References

1. Zhuang Q, Jiang J , Xiong T. An Intelligent Anti-phishing Strategy Model for Phishing Website Detection, 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW). Macau. 2012. p. 51–6.
2. Bennett CH , Gacs P , Li M , Vitanyi PMB, Zurek WH. Information distance. IEEE Transactions on Information Theory.1998; 44(4):1407–23.
3. ALmomani AB, Gupta B, Wan TC, Altaher A, Manickam S . Phishing dynamic evolving neural Fuzzy framework for online detection "Zero-day" phishing email. Indian Journal of Science and Technology. 2013; 6(1):122–6 .
4. Zeydan HZ, Selamat A , Salleh M . Survey of anti-phishing tools with detection capabilities. International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur. 2014. p. 214–9.
5. Chandra JV, Challa N, Pasupuleti S. Intelligence based defense system to protect from advanced persistent threat by means of social engineering on social cloud platform., Indian Journal of Science and Technology. 2015; 8(28):1–9.
6. Chandra JV, Challa N, Hussain MA . Data and information storage security from advanced persistent attack in cloud computing. International Journal of Applied Engineering Research. 2014; 9 (20): 7755–68 .
7. Chen TC, Stepan T, Dick S, Miller J. An Anti-phishing system employing diffused information. ACM Transactions on Information and System Security (TISSEC). 2014; 16(4):12–4.
8. Bilge L, Sen S, Balzarotti D, Kirda E, Kruegel C. Exposure: A passive dns analysis service to detect and report malicious

domains. ACM Transactions on Information and System Security (TISSEC). 2014; 16(4):14.
9. Chandra JV, Challa N, Pasupuleti S, Thirupathi RK, Krishna RV. Numerical formulation and simulation of social networks using graph theory on social cloud platform. Global Journal of Pure and Applied Mathematics. 2015; 11(2):1253–64 .
10. Li B , Sun R, Fang X, Luo X, Chang WH. Emergent challenges and IPDS for Anti-phishing attack. International Conference on IT Convergence and Security (ICITCS): Beijing: 2014. p. 1–4.
11. Zhou Y, Zhang Y, Xiao J, Wang Y, Lin W . Visual similarity based Anti-phishing with the combination of local and global features. IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom): Beijing; 2014. p. 189–196.
12. Singh P, Maravi YPS, Sharma S. Phishing websites detection through supervised learning networks. International Conference on Computing and Communications Technologies (ICCCT): Chennai; 2015. p. 61–5.
13. Basnet RB, Doleck T . Towards developing a tool to detect phishing URLs: A machine learning approach. IEEE International Conference on Computational Intelligence and Communication Technology (CICT): Ghaziabad: 2015.p. 220–3.
14. Lakhita S, Yadav B, Bohra B, Pooja P. A review on recent phishing attacks in Internet. International Conference on Green Computing and Internet of Things (ICGCIoT); Noida: 2015. p. 1312–15.
15. Reddy VKB, Rao T. Reddy LSS, Sai Kiran P . Research Issues in Cloud Computing. Global Journal of Computer Science and Technology. 2011; 11(11):70–6 .
16. Chandra MSS, Raghava Rao K , Hussain MA . An efficient scheme for facilitating secure data sharing in decentralized disruption tolerant networks. Indian Journal of Science and Technology. 2016; 9(5):1–13.
17. Chandra JV, Challa N, Pasupuleti SK. Advanced persistent threat defense system using self-destructive mechanism for cloud security. 2016 IEEE International Conference on Engineering and Technology (ICETECH). Coimbatore: 2016. p. 7–11.
18. Chandra JV, Challa N, Pasupuleti SK. A practical approach to E-mail spam filters to protect data from advanced persistent threat. 2016. International Conference on Circuit, Power and Computing Technologies (ICCPCT); Nagercoil: 2016.p. 1–5.
19. Marri M , Reddy R, Yalla P, Chandra JV. Design and implementation of integrated testing tool based on metrics and quality assurance. International Journal of Applied Engineering Research. 9(21):10463–72.