THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Detection of Attack on Integrity Using Hybrid Techniques

Manoj Kumawat[1] Neha Bagga[2] Rituraj Shekhar[3]

[1,2,3]School of Computer Science and Engineering, Lovely Professional University, Punjab, India

Abstract

Cyber crime is increasing at an alarming rate, to keep our data secure from intruders during transmission over the internet safety measures have to be taken. In this paper a system has been proposed having three different GUI for client, server and hacker. System will ensure the integrity of the data is maintained during transmission and any changes made to the data would be detected with difference in the checksum calculated at sender's and receiver's side. When intruder is able to intercept the file and make changes, modifications can be detected at the client side when it calculates the checksum using SHA256, implementation is done using C#.

Keywords: Data Integrity, Checksum, Intruder, Encoding

1. Introduction

Since the advent of the internet, there has been a surge in the areas in which it is being used. This feat can be contributed to the ease of availability of the internet and its ever-decreasing cost, throughout the world. Gone are those days when only the big and powerful companies used computers and internet for their functionality. Nowadays even micro, small, and medium scale enterprises depend greatly on the computer and its functionality.[3] It has made their functioning less prone to errors and frauds while simultaneously increasing their rate and quality of production. Not only the industries/institution use these services but also a common man in his day-today life.

These exploitations are generally ill intentioned and could cause harms in great magnitude. It could lead to loss of money and important information. What is even more worrying is that these ill intended people don't even need a physical access to such devices. One can sit in opposite side of the globe and can still cause a great damage. This has led scientific community to come up with ways to tackle it.[2,5] Some attacks like Packet Spoofing has major impact on the target systems as the attacker is really hard to trace in between those massive number of requests. As the server-client communication works in designed way of the developer and if the hacker or a malicious user try to mirror the IP address with someone else's IP address then also it is not easy to detect him. [6]

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

2. Related Work

P. Ogale[1], in his work on ensuring integrity of data, worked on setting checkpoints which would check all the traffic passing for any destructive data that could act as a threat for the receiver and to identify the checkpoints IBC(Integrity Breach Conditions) were used. It worked on checking any malicious code inserted in a program from people working within the organization and if any violation of integrity was identified the packets were dropped. J. Lin[2] used integrity checks for smooth running of traffic in Transportation Based Cyber Systems, to ensure hacker is not able to make changes to real time communication happening in the system. The alterations of the messages had serious impact on system, resulting in traffic bottleneck, and increase in average transmission time and ineffective utilization of resources. On detecting manipulated traffic from an intruder FDF(Forged Data Filtering) was used to remove those packets from the network

To improvise the performance of service providing protocols, Hui Xu [3] and protect against Man in the middle attacks, technique of symmetric encryption was used. Deffie Hellman Encryption was used to ensure integrity in both data uploading and downloading phases. For securing building cyber physical systems, Caezarina Marie Calimbahin[4] used sensors to check integrity violation inserted by intruders into the system. Denoising autoencoders (DAE) were used to make the system secure from attacks on integrity and availability. Jin Wei[5] designed a system which secures a system built for monitoring real time data, by using a collection of nodes, out of which one nodes act as the master and receives messages from all other nodes. Deep leaning is used to detect the frequency and place of occurrence of the attacks. S. Kumar[6] tested a Smart Electric Meter in an environment prone to cyber attacks and checking the integrity of the data collected. The collected data can be used to secure an organization or an institution from intruders which can cause fatal damage to resources and data.

3. Proposed System

This project can be used by any organization to keep track of IP packets. In this project there are three modes of controlling Client, Server and Hacker mode. From the client side the files are received when it requests to the server to send the files. File will be in encrypted mode which encoded by various algorithm that used in this project. From hacker side window, the victim system's IP is used to gain the access for the file which is downloading from the server side window. We have the one clicks button that will perform the attack and behind the attack are to change the file or changing the file integrity and user will receive the file as it modified by malicious user.

3.1 System Design

To detect the malicious user over the network it is important that we the destination and source IP addresses from which the data is passes through, as we know that data is send in form of the packets over the internet, the packet header contain the IP address information. Our project can

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

take long time to detect malicious user over the network due to resource limitations. So, in order to get malicious user detection, we have a GUI machine which is safe and flexible user friendly.

To trace the malicious user, we have to check the location of IP address. By this software project the IP address can be detected that is trying to make connection or we can say checking the IP address.

There are lots of methods to identifying IP addresses like using Netstat or other tracing tools. If the user gets the IP address of any machine then the use can get the trace route of that IP address by executing tracert command. Other ways of tracing a malicious user over the internet is through Domain Name Server. DNS are the active running machines that keep the list or log of connected machine's IP address. It can take the string name of host/machine then get the its equivalent IP and search the entry with its IP address location

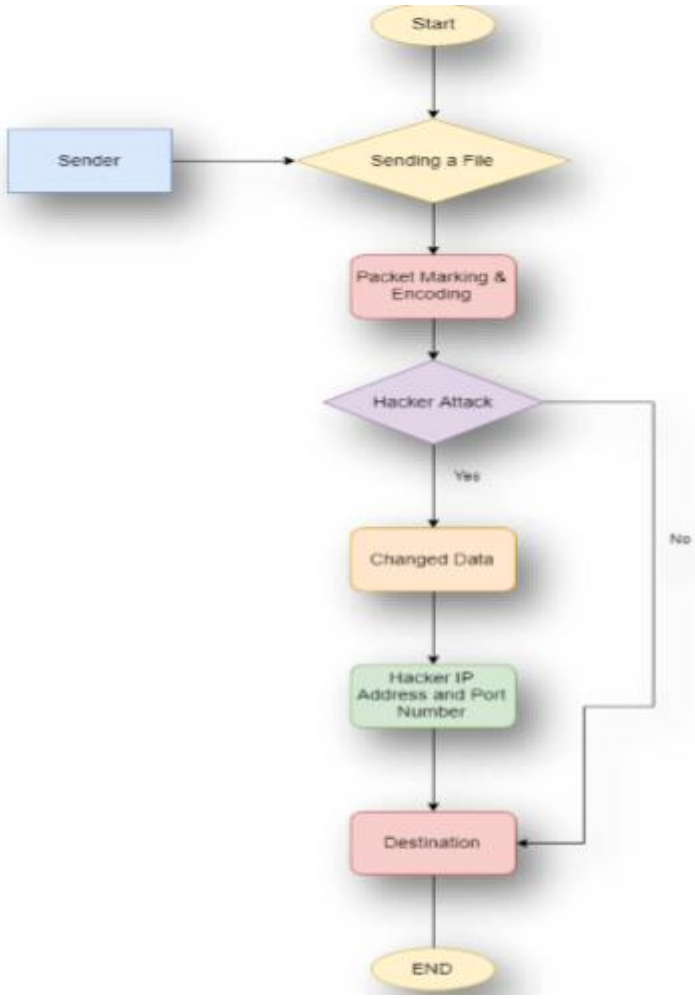

Figure 1: Flow Diagram of the System

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Client GUI:

Step1: Get the IP address to connect with the network.
Step2: Set the receiving location for the file. (default location drive is: E)
Step3: Receive the incoming file from the server machine.
Step4: Calculate the new checksum value of the received file.
Step5: Compare the both checksum value of the received file and checksum value of the server-side machine.

Step5.1: If the checksum values are different then show the zero as checksum value for wrong file received

Step5.1.1: If checksum values are not same then do not show the file receiving message or the indication.

Step5.2: If the checksum values are same then show the new calculated checksum value on receiving right file.

Step5.2.1: If the checksum values are same then show the file receiving written message with open port number.

Step6: Exit**.**

Figure 2: Client GUI

Hacker GUI:

Step1: Set client IP address from the active network.
Step2: Start capturing the packets sent by server machine to the client machine.

Step2.1: If packet capturing is successful then modify the packet and sent to the client machine.

Step2.2: If packet capturing is unsuccessful then keep continuously trying to capture data packets.

Step3: Indicate the message for the start attacking along with victim's IP address.
Step4: Exit**.**

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Figure3: Hacker GUI

Server GUI:

Step1: Brows the valid file with supported file types from the visible location.
Step2: Calculate the checksum value of the selected file.
Step2.1: Display pop window for checksum calculation error if selected file content is none or file is deleted from active location.
Step2.2: In case of file with content show the checksum value on the server machine's checksum field box.
Step3: Set the client machine IP address in destination field of server machine.
Step3.1: If IP address of client machine is not reachable then show the output as IP address is out of range or is not in active network.
Step4: If connection to the client machine is successful.
Step4.1: Proceed with the original file to the client machine.
Step4.2: If server machine unable to make a connection to the client machine then show message file sending fail.
Step5: Exit**.**

Figure 4:Server GUI

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

4. Conclusion

In this paper we have described the working of a system, which will ensure the integrity of data during communication. When file would be transmitted between server and client, it can be intercepted by an intruder. Hacker can modify the content and send the fabricated message to the client which can have serious impact. To overcome this, file can be verified for no alteration by calculating the checksum and verifying it with the calculation made by the server.

References

[1] G.Qiu, Y. Wang, "Integrity Measurement Model Based on Trusted Virtual Platform," International Conference on Genetic and Evolutionary Computing vol.4, pp. 526-529, 2010

[2] C. Calimbahin, S. Pancho-Festin, J. Pedrasa, "Mitigating Data Integrity Attacks in Building Automation Systems using Denoising Autoencoders," pp. 391-395, ICUFN 2019.

[3] J.Wei, "A Data-Driven Cyber-Physical Detection and Defense Strategy Against Data Integrity Attacks in Smart Grid Systems," Symposium on Signal and Information Processing for Optimizing Future Energy Systems, pp. 667-671, 2015.

[4] S.Kumar, H. Kumar, G. Gunnam, "Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack," International Conference on Data Intelligence and Security vol.2, pp. 9-13, 2019

[5] P. Ogale, M. Shin, S. Abeysinghe, "Identifying Security Spots for Data Integrity," IEEE International Conference on Computer Software & Applications vol. 42, pp. 462-467, 2018

[6] J. Lin, W.Yu, N.Zhang, X. Yang, L. Ge, "Data Integrity Attacks Against Dynamic Route Guidance in Transportation-Based Cyber-Physical Systems: Modeling, Analysis, and Defense," IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY VOL. 67, pp. 8738-8752, Sep. 2018.

[7] H.Xu, R. Jiang, "ATTACKSAND IMPROVEMENTS ONDATA INTEGRITYAS A SERVICEPROTOCOLS ," Proceedings of IC-NIDC, pp. 242-246, 2012.

[8] W.Tong, B.Jiang, F.Xu, Q.Li, S.Zhong, "Privacy- Preserving Data Integrity Verification in Mobile Edge Computing," IEEE Conference on Distributed Computing System Vol. 39, pp. 1007-1018, 2019.

[9]S.Kumar, C.Krishna, A.K.Solanki, "A Technique to Resolve Data Integrity and Confidentiality Issues in a Wireless Sensor Network," International Conference on Cloud Computing, Data Science & Engineering vol.8, pp. 183-188, 2018.

[10] C. Schlesinger, K. Pattabiraman, N.Swamy, "Modular Protections against Non-control Data Attacks," Computer Security Foundations Symposium vol.24, pp. 131-145, 2011.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

[11] M. Castro, M. Costa, and T. L. Harris, "Securing software byenforcing data-flow integrity," OSDI. USENIX, pp. 234- 239, 2006.

[12] S.Chen, J.Xu, E.C. Sezer, P. Gauriar, and R. K. Iyer, "Non-control-data attacks are realistic threats,". Usenix Security pp. 53-58 2005.