Department Of Computer Engineering

Marathwada Mitra Mandal's College of Engineering

Karvenagar, Pune-411052

Name: Atharv Rajkumar Nalwade

Class: T.E.1

Roll No: TC-146

Topic: Effective algorithm to detect steeping stone intrusion by removing outliers of packet RTT

Guidance By-

Prof. Shubadha Mone

Introduction

A network intrusion is an unauthorized penetration of a computer in your enterprise or an address in your assigned domain. It can be active or passive. Some intrusions are simply meant to let you know the intruder was there, defacing your Web site with various kinds of messages or crude images. Others are more malicious, seeking to extract critical information on either a one-time basis or as an ongoing parasitic relationship that will continue to siphon off data until it's discovered. Attackers on the Internet often launch network intrusions through compromised hosts, called stepping-stones, in order to reduce the chance of being detected. In a stepping-stone attack, an intruder uses a chain of hosts on the Internet as relay machines and remotely log in these hosts using tools such as telnet, rlogin, or SSH. A benefit of using stepping-stones to launch attacks is that intruders can be hidden by a long interactive session and knowing the actual origin of the attack is hard to determine.

MOTIVATION

In the 21st century where we are surrounded with an invisible web of internet care should be taken that one does not access your any sorts of private data without your authorization that's where the concept of security clears its picture in the field of computer networks**.** Any illicit behavior on a digital network is known as a network intrusion. Any of the following can be considered an intrusion −

- Malware, sometimes known as ransomware, is a type of computer virus.
- Attempts to obtain unauthorized access to a system
- DDOS (Distributed Denial of Service) attacks
- Destruction of cyber-enabled equipment
- Employee security breaches that are unintentional (like moving a secure file into a shared folder)
- Untrustworthy users, both within and external to your company
- Phishing campaigns and other methods of deceiving consumers with ostensibly genuine communication are examples of social engineering assaults.

One such intrusion is stepping stone intrusion where the attacker uses a long chain of compromised hosts to gain access to a remote host which can be prevented effectively up to 85% using the algorithm described in the paper.

Problem Statement:

To detect steeping-stone intrusion in a computer networks system using a effective algorithms by removing outliers of packet RTT.

SCOPE:

The algorithms suggested by the author in the research paper titled "Effective Algorithms to Detect Stepping-Stone Intrusion by Removing Outliers of Packet RTTs" by Lixin Wang, Jianhua Yang, Michael Workman, and Pengjun Wan propose an efficient way to eliminate most of the possible RTT outliers of the packets captured in the Internet environment. Then an efficient SSI detection algorithmis used by mining network traffic using an improved version of k-Means clustering. The proposed detection algorithm for SSI is accurate, effective, and efficient in the context of the Internet. Effective rate of our proposed SSI detection algorithm is higher than 85.7% in the context of the Internet.

METHODOLOGY:

1. Here the author presents an efficient algorithm for removing the outliers in the packet RTTs captured in the Internet environment

   Input: a TXT file with two columns (including packet timestamps and the packet type) obtained from the packets captured in the Internet environment **Output**: a TXT file output.txt containing the packet RTTs with most of the RTT outliers removed

   1: for each of the first five Echo packets, compute the time difference between the Echo packet and its immediate prior Send packet; write this time difference to the file output.txt for each of these five Echo packets

   2: compute the average of all the RTTs in the file output.txt and store the value in the variable average

   3: for the 6th Echo packet, compute the time differences between this Echo packet and its prior five Send packets; assume these Send packets are represented by Send1, Send2, Send3, Send4, and Send5, respectively

   (a) let timediff1 denote the difference between this Echo packet and Send1. Write timediff1 to the file output.txt if timediff1 is less than 10 average; recompute the average of all the RTTs in output.txt and then update the value of average /* if the time difference is larger than or equal to tenfold the average, then the RTT value is most likely an outlier and will not be written into the output file. Here, the tenfold criterion is based on observation*/

   (b) let timediff2 denote the difference between this Echo packet and Send2. Perform the same process for timediff2 as done in the above Step 3(a)

   (c) let timediff3 denote the difference between this Echo packet and Send3. Perform the same process for timediff3 as done in the above Step 3(a)

   (d) let timediff4 denote the difference between this Echo packet and Send4. Perform the same process for timediff4 as done in the above Step 3(a)

   (e) let timediff5 denote the difference between this Echo packet and Send5. Perform the same process for timediff5 as done in the above Step 3(a)

   4: repeat Step 3 for each of the remaining Echo packets in the input file until all the Echo packets are processed

2. We present an effective algorithm to detect SSI by mining network traffic using an improved version of the k-Means clustering approach

   Input: dataset-1, dataset-2, and dataset-3

   Output: The connection chain(s) that are sessions possibly manipulated by malicious hackers

   1: call the 2-Means clustering algorithm on dataset-1. Assume 1 represents the standard derivation

outputted based on Eq. (2) using the two clusters obtained at the end of the 2-Means clustering algorithm execution

2: call the 2-Means clustering algorithm on dataset-2. Assume 2 represents the standard derivation outputted based on Eq. (2) using the two clusters obtained at the end of the 2-Means clustering algorithm execution

3: call the 2-Means clustering algorithm on dataset-3. Assume 3 represents the standard derivation outputted based on Eq. (2) using the two clusters obtained at the end of the 2-Means clustering algorithm execution

4: if $б_1$=min($б_1$, $б_2$, $б_3$); dataset-2 and dataset-3 are sessions possibly manipulated by malicious hackers

5: if $б_2$ = min($б_1$, $б_2$, $б_3$);, dataset-1 and dataset-3 are sessions possibly manipulated by malicious hackers

6: if $б_3$ = min($б_1$, $б_2$, $б_3$), dataset-1 and dataset-2 are sessions possibly manipulated by malicious hacker

Software/Hardware: NONE

REFRENCES:

1. "Watch Your Step! Detecting Stepping Stones in Programmable .." ieeexplore.org/Xplore/home.jsp. . https://ieeexplore.ieee.org/document/8761731 (accessed: Aug. 19, 2022).

2. "Sniffing and Chaffing Network Traffic in Stepping-Stone Intrusion .." https://ieeexplore.ieee.org. https://ieeexplore.ieee.org/document/8418122 (accessed: Aug. 19, 2022).

3. "Modeling Stepping Stone Attacks with Constraints in Cyber .." https://ieeexplore.ieee.org. https://ieeexplore.ieee.org/document/9014266/ (accessed: Aug. 19, 2022).

4." Analysis of Stepping-Stone Attacks in Internet of Things Using .." https://ieeexplore.ieee.org. h https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119593386.ch12 (accessed: Aug. 19, 2022).

5. "A research survey in stepping-stone intrusion detection | EURASIP .." http://paper.ijcsns.org/. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-018-1303-2 (accessed: Aug. 19, 2022).

6. "A research survey in stepping-stone intrusion detection | EURASIP .." http:// paper.ijcsns.org/. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-018-1303-2 (accessed: Aug. 19, 2022).

7. "Mining Network Traffic with the k -Means Clustering Algorithm for .." https://ieeexplore.ieee.org.

https://www.hindawi.com/journals/wcmc/2021/6632671/ (accessed: Aug. 19, 2022).

8. Marco Gamarra; Sachin Shetty; Oscar Gonzalez; David M. Nicol; Charles A. Kamhoua; Laurent L. Njilla, "Analysis of Stepping-Stone Attacks in Internet of Things Using Dynamic Vulnerability Graphs," in *Modeling and Design of Secure Internet of Things* , IEEE, 2020, pp.273-294, doi: 10.1002/9781119593386.ch12

9. Zhang, Yin and Vern Paxson. "Detecting Stepping Stones." *USENIX Security Symposium* (2000).

10. "Detection of Interactive Stepping Stones: Algorithms and Confidence .." http://intelli-sec.cs.berkeley.edu/papers/stepstone.pdf (accessed: Aug. 19, 2022).