Detection of a Real-time Cyber-attack using Locator Agent Algorithm (C006)

Isah, Abdulkadir Onivehu[1]
Idris, Ismail[3]
(1, 3) Department of Cyber Security Science
Federal University of Technology Minna,
Minna, Nigeria
ao.isah@futminna.edu.ng1
ismi.idris@futminna.edu.ng3

Alhassan, John Kolo[2]
Adebayo, Olawale Surajudeen[4]
(2, 4) Department of Cyber Security Science
Federal University of Technology Minna,
Minna, Nigeria
jkalhassan@futminna.edu.ng2
waleadebayo@futminna.edu.ng4

Abstract— **This paper presents a preliminary result of an ongoing research work on attack prevention and location of attacks on the cyberspace. The methodology combines the preventive encryption and locative algorithms. This paper in particular, present the reviews and methodology used in achieving the first objective of the said ongoing research. The existing systems duels on methodologies that attempt mostly postmortem solutions. Whereas, this research uses advanced encryption standard as prevention against compromising confidentiality. The methodology and objective obtained so far present a promising solution of unified model algorithm for real time solution of the ongoing research problem.**

Keywords- Realtime; Cyberspace; Locator agent; Detection

- Introduction

As cyberspace based technologies are being utilized by different individuals, there is a propensity that they would be exposed to increasingly security dangers. Since network systems are utilized by various individuals, there are expanding number of security issues and security of data on transition [1] which required the improvement of various intrusion detection frameworks; such attacks are DOS attacks. SYNflood, smurf, and User Datagram Protocol (UDP) storm assaults [13]. IP traceback [14] is a strategy that is very effective to absolve attacks

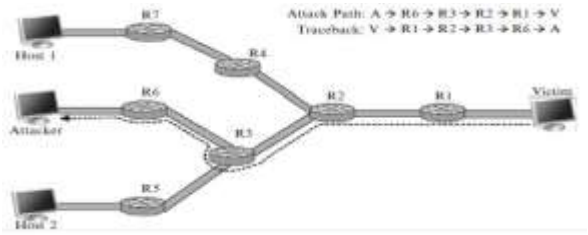

Fig. I IP Traceback Mechanism [14]

and to examine and attribute the attacks during the post-mortem analysis. The traceback system is shown in Fig. I IP traceback issue is characterized as distinguishing the real source of traffics sent over the Internet [14].

The attacks cannot be prevented or mitigated by the techniques of IP traceback. However, in this paper, other network security measures such as

public key cryptosystems, and feedback alert system are to be combined to form a hybrid system that is able to prevent, mitigate and reveal the source of attack.

- Related Work

For malicious programs or malicious packets to be detected, proper monitoring of particular activities is undertaking [8]. Anomaly detection is part of active monitoring techniques [3], detection of signature scan [10], intrusion detection systems [15], access control list [12], and honeypots [13]. Anomaly detection techniques can be utilized to create the behavior of users' pattern and network resources. Any behaviour that moves away from these particular patterns (traffic patterns that are irregular) is malicious [3]. Signature scan method is utilized to keep the mark of the activities in a database. A passive checking is performed on the system activity [10] for informal sample recognition. If the sample matches including the saved signature, it is regarded malicious. It is generally done because of recognized attacks within the network. Intrusion detection systems commonly discover intrusion based totally of pattern matching or statistical anomaly [6]. However, statistical violation identifies malicious activities based totally concerning deviations from the usual utilization pattern. The usual utilization pattern is normally established firstly before deciding a deviation within the network activities. Access control list is utilized to recognize malicious activity by coordinating packets headers with pre-characterized rules [12]. Honeypot is a trap put to screen and keep interlopers from going into secured zone of the system [10]. Honeypot is a camouflage that recreates to secure server and instigates intruders to cooperate. Along these lines, an assault is identified by checking unapproved examining of open ports in the honeypot. The authors are basically concerned with detection and not proactive in the location of the source of attack.

Identification of the source of packets within a particular network is called traceback or IP traceback [7]. It is utilized to detect origin of packets that are being generated by identifying attacks [2]. Traceback is a proper NFT used to detect packets sources by checking the path of attacks especially for DDoS and IP spoofing attacks [10]. Due to botnet, Traceback is significantly more [11] and DDoS attacks [4, 5] that are seen in various distributed systems of network. Distributed systems of network which work together with Internet give likely atmosphere and pull in bot-master for network attacks [9]. To beat these assaults, it is important to keep the system framework anchored by consolidating different traceback systems in an effective way. Although, the improvements made by the various research works are commendable, none is able to effect real-time detection of position of intrusion or attacks; it is rather a post-mortem approach. This is what the ongoing research work seeks to achieve, although, this paper covers the first objective of the research.

- Methodology

The method employed by this paper is formulation of the mathematical relationships which involves functions and variables required in the achievement of the very objective under consideration. The algorithms arising from the mathematical considerations shall be stated and the model shall be drawn out of the final unified algorithm.

  - *Mathematical Considerations*

Logically, the operations and the activations of any of the algorithm is discretely represented. The positive S_{pc} is the Systems positive communication while S_{nc} is the Systems negative communication.

$S_{pc} = 1$…….. (1)

$S_{nc} = 0$…… (2)

The unified model algorithm U_{ma} proposed is achieved by the combination of Encryption algorithm E_a and Locator agent algorithm L_{aa} where the encryption type is the AES.

$E_a + L_{aa} = U_{ma}$……. (3)

But

For equation (i),

$E_a = M_s = V_s = 1$……... (4)

$L_{aa} = M_s = V_s = 1$…….. (5)

M_s is the malicious system and the victim system is V_s

For equation (ii),

$U_{ma} = 0$…… (6)

- *General AES Algorithm*

AES algorithm is traditionally known as encrypting algorithm but it can be adapted to a wide range of data security solutions.

START

SELECT FILE

ENTER AES ENCRYPTION PASSWORD

GENERATE CIPHER USING PASSWORD

READ IN FILE

FIGURE OUT FULL SIZE OF FILE

ENCRYPT FILE DATA

WRITE ENCRYPTED DATA TO NEW FILE

STOP

- *Locator Algorithm*

The algorithm below is the locator algorithm that serves as the locator agent within the cyberspace.

START

INPUT:

ACTIVATE MALICIOUS SYSTEM

VICTIM SYSTEM:

ACCESS SYSTEM CONFIGURATIONS

MALICIOUS:

MALICIOUS AND VICTIM SYSTEMS CONFIGURATION COMMUNICATION LINK

IF ACTIVE

LOCATOR AGENT ACCESS GPS API

SEND LOCATION TO ADMIN

END

- *Algorithm of unified model that can prevent and locate attacks position A*

The algorithm below captures the objective of having a unified solution that is realtime and can be implemented by the programming language that is employed in the ongoing research as stated above.

START

INPUT:

VICTIM SYSTEM FILES

ENCRYPT VICTIM SYSTEM FILES

IF MALICIOUS SYSTEM ACTIVATE

THEN ACTIVATE VICTIM SYSTEM CONFIGURATIONS

ACTIVATE MALICIOUS AND VICTIM CONFIGURATION LINK

IF COMMUNICATION LINK ACTIVE

LOCATOR AGENT ACCESS MALCIOUS SYSTEM

LOCATOR AGENT ACCESS API GPS OF MALICIOUS SYSTEM

LOCATOR AGENT SENDS REPORT TO ADMIN

END

- *Algorithm of unified model that can prevent and locate attacks position A*

Fig. II 2 show the proposed model of the preventive and attack location system, the model shows the communications between each sector of the model with the cyberspace as indicated by the arrows.

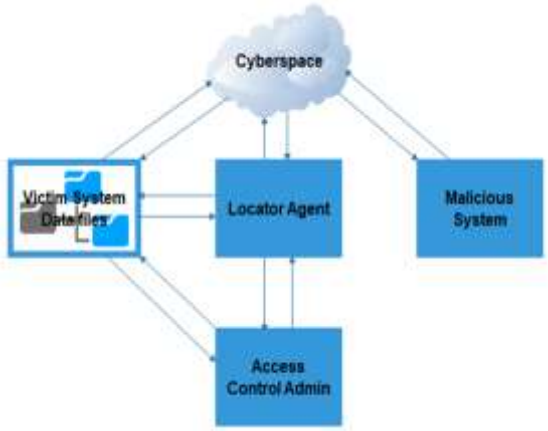

Fig. II Proposed unified model that can prevent and locate attacks position.

- Discusion

The general attacking pattern of cybercriminals as illustrated in fig. I, is by routing through network systems on the cyberspace to get to particular would be victim systems, gain access, maintain access and then get to particular data of interest. There are several tactics employed by cybercriminals and several activities ensues before and during attacks as shown by the mathematical relations.

Gaining of access by unauthorized entity is premised on equations 1 and 2, equation 3 defines the unified algorithm which is active when equation 1 is true and it is not active when equation 2 is true. Equation 3 will readily perform its functions and achieve the mentioned objective when equations 4 and 5 equals discrete value 1 respectively. Equation 6 is non active when equation 2 equals discrete value 0.

The algorithms of *B*, *C* and *D* represent the general AES algorithm, Locator algorithm and algorithm of a unified model that can prevent and locate attacks position respectively. The algorithms of *C* and *D* are the algorithms of interest as they are combined to form the unified model to achieve the objective of the ongoing research as mentioned earlier.

In fig. II, the host system otherwise known as the Victim system, that host the data files of interest, the locator agent and access control admin systems are all communication with the cyberspace. Although the malicious systems used by cybercriminals to access the victim system is not normally in direct communication with the host systems, They also have access to the cyber space from any location across the globe, this makes the victim system accessible to the malicious system. In the proposed solution, the data file on the host system is encrypted against any attack coming from the malicious system, the locator agent monitors the activities of the host system and the location of potential malicious systems since the locator agent is also interacting with the cyber space which is the channel through which the malicious activities can pass through to the host system.

- Conclusion

This paper has been able to achieve the objective which is to design a unified model of detection and locative solutions of the ongoing research work on the problem of malicious attacks. It is hereby recommended that the objective achieved as presented in this paper, is to be considered with

other objectives of the ongoing research work for the desired data security.

REFERENCES

A. O. Isah, J. K. Alhassan, S. S. Olanrewaju, and E. F. Aminu, ''Enhancing AES with Time-Bound and Feedback Artificial Agent Algorithms for Security and Tracking of Multimedia Data on Transition,'' International Journal of Cyber-Security and Digital Forensics, 6(4), 162-179, 2017.

T. Akyuz, and I. Sogukpinar, ''Packet marking with distance based probabilities for IP traceback,'' Networks and Communications, First International Conference on pp. 433-438, December, 2009, IEEE.

V. Chandola, A. Banerjee, and V. Kumar, ''Anomaly detection: A survey,'' ACM computing surveys, 41(3), 15, 2009.

S. Chen, Y. Tang, and W. Du, ''Stateful DDoS attacks and targeted filtering,'' Journal of network and computer applications, 30(3), 823-840, 2007.

W. Dou, Q. Chen, and J. Chen, ''A confidence-based filtering method for DDoS attack defense in cloud environment,'' Future Generation Computer Systems, 29(7), 1838-1850, 2012.

V. M. Igure, and R. D. Williams, ''Taxonomies of attacks and vulnerabilities in computer systems,'' IEEE Communications Surveys & Tutorials, 10(1), 2008.

S. Khan, E. Ahmad, M. Shiraz, A. Gani, A. W. A Wahab, and M. A. Bagiwa, ''Forensic challenges in mobile cloud computing,'' International Conference on Computer, Communications, and Control Technology, pp. 343-347, 2014, IEEE.

S. Khan, M. Shiraz, A. W. Wahab, A. Gani, Q. Han, and Z. B. A. Rahman, ''A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing,'' The Scientific World Journal, 2016.

J. Kok, and B. Kurz, ''Analysis of the botnet ecosystem. 10th Conference of Telecommunication, Media and Internet Techno-Economics, pp. 1-10, 2011, VDE.

P. Li, M. Salour, and X. Su, ''A survey of internet worm detection and containment. IEEE Communications Surveys & Tutorials, 10(1), 2008.

S. Mizoguchi, K. Takemori, Y. Miyake, Y. Hori, and K. Sakurai, ''Traceback framework against botmaster by sharing network communication pattern information,'' International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, (pp. 639-644), 2011, IEEE.

B. Yu, and R. Wang, ''Research of access control list in enterprise network management,'' Informatics and Management Science VI (pp. 121-129), 2013, Springer.

F. N. Ogwueleka and M. N. Okoye, ''Hybrid Incident Response Digital traceback technique in network-based intrusion source detection,'' IUP, 2016.

R.C. Joshi, E.S. Pilli, ''Fundamentals of network forensics, computer communications and networks,'' DOI 10.1007/978-1-4471-7299-4_7 Springer-Verlag London, 2016.

H. J. Liao, C. H. Richard, Y. C. Lin, K. Y. Tung, ''Intrusion detection system: A comprehensive review,'' Journal of Network and Computer Applications, 36, 16–24, 2013.