Design Issues in Stepping Stone Detection

Rajesh Kumar Goutam
Department of Computer Science
University of Lucknow

ABSTRACT
In the rapid changing inter-connected environment, cyber criminals are opting sophisticated tools to hide their identities and locations. Stepping stones are now popular among the miscreants and making the situations worse. The paper details the role of stepping stones in hiding the cyber criminals and highlights it as challenge to differentiate the stepping stones from legitimate computers in the network. The paper details the various issues in stepping stones detection and explains four parameters that are playing a crucial role to identify the stepping stones in this inter-connected digital infrastructure.

Keywords
Stepping stones, Cybercrime, IP Forging

1. INTRODUCTION
In this digital era, organizations are still failure to define the term attribution in the field of information security. The attribution refers to the activity to find the origin of cybercriminal [1]. Attribution not only deals with the original source of cybercrime but it also concerns with the intermediary through which the cybercrime is committed. The desired source may be particular individual, an account, a machine or similar information belongs to a person [1]. The origin may include geographic origin or virtual origin such as IP address or Ethernet address. David A. Wheeler et al. [1] define the attribution as determining the identity or location of an attacker or its related intermediary. It is essential for ideal attribution to locate the original attacker. Cyber criminals are now being more professional; they hide themselves behind the digital infrastructure and its shield of anonymity that provide misleading information about their locations. However, the route of cybercrime is also equally important.

The use of internet by cybercriminals and terrorists presents a higher risk for cyberspace and inter-connected environment. We still need an intelligent monitoring system that can monitor, inspect and analyze the activities being performed over virtual and borderless cyberspace. It should also be capable to differentiate cybercriminals and terrorists activities from normal traffic and can store the logs of each session with a chain of evidences that can be used in support during diplomatic, military and legal action. It is also desirable to incorporate the impact assessment system also.

2. WHY THE ORIGIN OF CYBERCRIME IS NOT OFTEN DETECTED
During the formation of Internet, it was never assumed that miscreants can use it for having financial gain so the policy of cybercrime and its origin detection had completely been neglected [5]. We still do not have any adequate technique that can detect the origin of cybercrime. The major problem in the process of source detection in the cybercrime is involved 'stepping stones'.

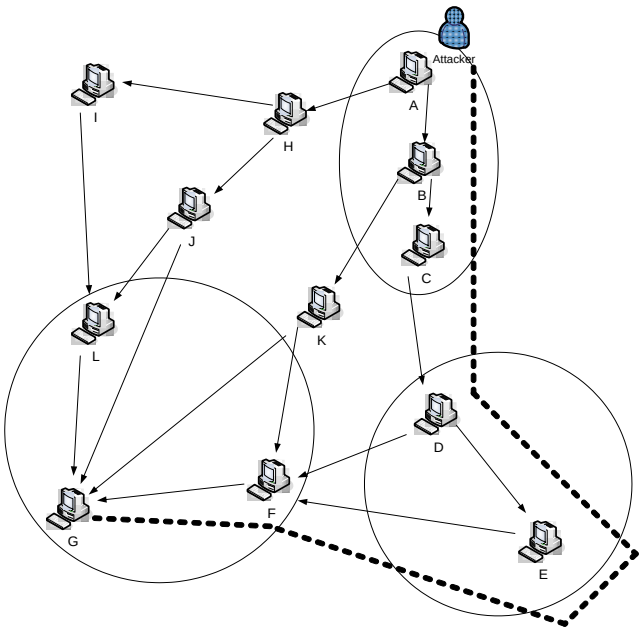

Fig 1. Stepping Stones

Stepping stones are the middleware and compromised systems between the cybercriminals and target systems. In the above fig.1 system A is used by the cybercriminal to attack on the system G. there are various routes possible shown by the solid lines in the fig 1. suppose the cybercriminal use the middleware systems <B,C,D,E,F> then all these systems are called stepping stones. The series of compromised computers need to function in specific order and organized manner to target any system and provide anonymity for cybercriminals to avoid detection. The series of compromised computers is known as 'chained connections'.

Unfortunately, the cyber criminals have more skilled hands and applying almost new techniques every day to hide the source of cybercrime. David A. Wheeler et al. [1] detail some common approaches that are often used to make attribution difficult.

1. Normal internet users do not care for source of information. The information they want to get is the primary concerned regardless how they are retrieving the information or getting services. The cybercriminals often make changes in sender's identity or make forge sender's identities and communicates with users as authentic source or service provider called 'Spoofing' [7]. In more common word, when the changes are made to message to forge sender's identity, we call 'spoofing' [7].
2. Cyber criminals often use ' Reflector host' that are capable to send forges massages to large number of computers which are victims of cyber attacks, often employed to hide the location of cybercriminal [4] .

Cyber criminals use the reflector host that sends the bulk massages to target system and pretends that these messages are being sent form different computers to divert the victim's attention on original cyber criminal. In other words, the reflector host creates fake attackers. Each fake attacker pretends as original attacker and tries to pull victims attention. In this way victim often get confuse and fails frequently to apply security mechanism over networked infrastructure and digital environment.

3. Sometimes, cyber attacks are triggered with a forged computer by setting their IP address for a temporary time. The majority of cyber criminals prefer this type of internet connection to launch cyber attack. The cyber criminal can use the public internet connection for a short period of time by creating a forged IP address there after he never use this ID again. Whenever the victim computer replies to this computer it becomes unable to find its destination.
4. The cybercriminals also use 'step- stone' method for cyber attack. In this method, the cyber criminals include innocent networked computers for attack [2, 3]. The cyber criminals log with intermediate step-stone host and launch the attack [2, 3]. In such a way, the traceback method will not lead to attacker directly but the stepping stone host will be identified as accused.
5. Cyber attacks are now more sophisticated, few attacks leave its impact later by a period of time. The laundering host [4,8] also termed as 'zombie' intentionally inserts some delay for a cyber attack to be active. The cyber criminal gets ample opportunity to escape from the scene.
6. It is our general perception that when cyber attack is triggered, it will cover all the damages that are possible through it in once but few attacks leave its impacts in parts. For example an attack is triggered today it leaves its first impact after 10 hours, may leave its second impacts two days later and third one after few days and so on. In this way, it is converted in continuous ongoing process and prevents the users to guess how dangerous the attack is?

3. FORGING IP ADDRESS

Our intention with traceback system is to determine the computer system through which the attack has been launched. As we have discussed earlier, that step-stone attack may include intermediate hosts to launched attack so determining the intermediate, innocent system would not be an idle traceback [4,5] system. Instead, it is the system that will identify the original system which is responsible for cyber attack. To analyze the traceback problem it is essential to know how the attackers hide their identity.

IP address is used by the internet to transfer data packets from sender to receiver. Each data packet has two addresses. One is sending node's address while other is destination address to which data packet is directed. If the receiver end does not want to establish the connection for further communication then it becomes easy for cyber criminals to attack on receiver system. The network shown in fig. 2 represents this type of communication where the receiving end becomes always unable to judge either the packets are coming from trusted source or not. It becomes difficult to attack on two way communication network. In this type of network, the receiver end sends an acknowledgement to sender host address which is often known by receiving end in advance. In this two way communication system the attackers first occupies the IP of authentic sender and make its own. Thereafter, the connection between authentic sender and receiver is broken so that the acknowledgement from receiving end may divert towards the attackers as shown in fig. 5. Susan C. Lee et al. [6,7] described how forging of IP is usually done with the help of reflector and laundering host.

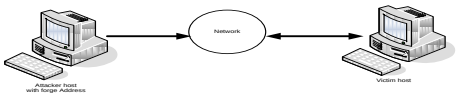

Fig 2. Forging IP

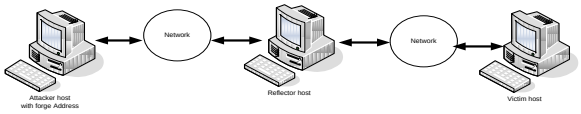

Fig 3. Forging IP with Reflector

Fig 4. Forging IP with laundering Host

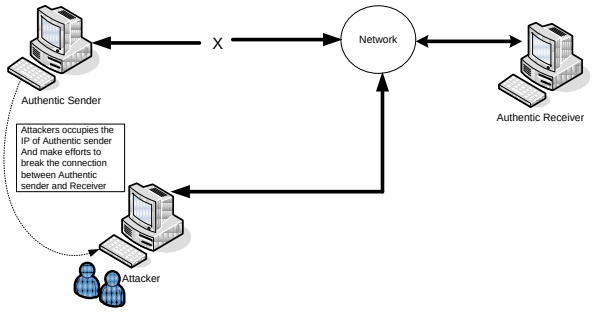

Fig 5. Forging IP in two way Communication

The person sending information would essentially require acknowledgement from receiving end So if an unauthorized person receive the information which is directed for some other system, needs to be pretended as authentic receiver and must send an acknowledgement in manipulating its source address to the sending end. This is bit easy when sending end does not require any information from other end but if the sending end requires some information form other end then it becomes difficult.

3.1 Forging IP with Reflector

Cyber criminal often includes the number of innocent systems between the source of attack and victim system [4]. A reflector is a system that takes the data packets from the cyber criminal with the victim IP address as a source address and response to source address (victim IP address). In this way, victim directly finds the IP of reflector and accuse directly for attack.

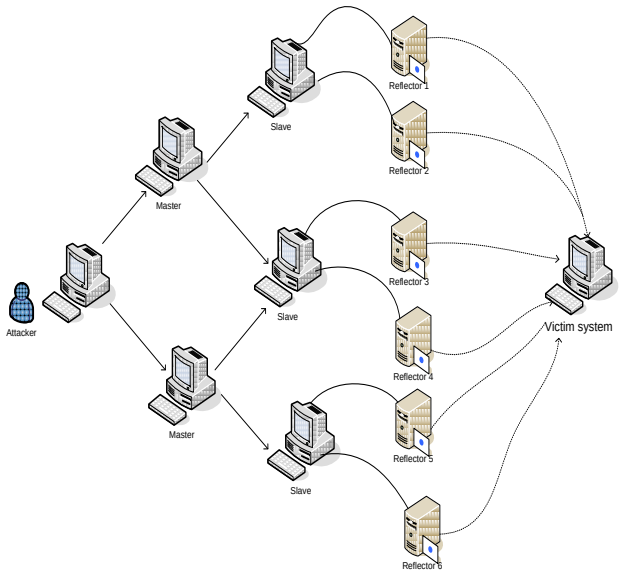

Fig 6. Forging IP with Multiple Reflector

The person who is unauthorized to receive information will grasp the information before it reaches to its authorized hands. The intruder will pretend as authentic receiver and will certainly hide its address. For this reason, attackers can manipulate the response packet's source address (either given the address of another computer or even a nonexistent computer). This response from attacker will be treated as response from authentic receiver with forge receiving node address.

4. ISSUES IN STEPPING STONE DETECTION

We call two computers as connection pair if both computers are the part of same chain connection. The connection pair provides the smooth route to data traffic. Stepping stones are those systems in which legal users are also unaware about their vulnerability. When a cyber criminal launches attack with the help of compromised computer its normal traffic becomes overload, about which the legal user of system becomes unaware. The intrusion code mix-up with the normal traffic in the network and reach to another system in network. So, finding the particular system through which the cybercriminal is making the entry in network is crucial. It can be easily understood if we block activities at the same computer where the cyber criminal makes entry then the chances of intrusion in whole network reduces we can implement our security mechanism at most suitable place.

In this section, we discuss the various considerations we kept in mind during the framework design for stepping stones. There are two types of connection pair, first one is stepping stone connection pair and randomly picked connection pair [2]. In stepping connection pair, all the system in this connection chain must have some invariant values means all these system must be somehow correlated. On the other hand, in randomly picked connection pair the both picked system will be correlated instead of all in the connection chain. The general approach we use here for the design of stepping stone detection framework is correlated traffic characteristics. In the whole process we identify the data traffic characteristics that are invariant in nature.

4.1 Data traffic measurement Parameters

There are few parameters on the basis of which we can measure the symmetry of data flow between two computers connected to Ethernet. These parameters are connection content, inter-packet spacing, ON/OFF patterns of activity, data traffic rate/ volume [2]. In the internet, the node may be in the form data communication equipments like modem, hub, bridge or switch. The node may also be the form of data terminal equipments like digital telephone handset, server or router. The connection content refers to the amount of data transferred between two computers successively. If there is high degree of content symmetry between two computers then chances of perturbation in the network reduces. The connection content of any particular system becomes the sum of amount of connection content on the preceding computer and user's data on the preceding computer. The data packet is the smallest unit of data transferred from one computer to another computer. Inter-packet spacing refers minimum pause between two data packets. There is certain amount of time a packet takes to move from one computer to another computer and this time duration ideally should be same for all the data packets. If there is any variation in this time duration between packets movement then caution should be taken as the activity indicates about the intrusion. The third parameter that is used to know the symmetry in the network is the ON/OFF pattern activity. If there is no data traffic exists on a flow for T_{idle} seconds, then it is assumed that connection is in OFF mode. Whenever a packet appears with non-empty payloads then the OFF mode turns into ON mode [2,3]. This ON mode continues until the non-empty payload is detected. During the intrusion detection, the OFF and ON mode is very important as the same duration of ON and OFF mode is measured across the whole connection chain.

5. CONCLUSIONS

The study shows that stepping stones are hiding the cybercriminals behind a digital infrastructure and must be identified to apply security mechanism. The paper presents six techniques by which miscreants often cheat legitimate internet users, control their computers remotely and use it as intermediary to launch the cyber attack. The paper details four parameters named connection content, inter-packet spacing, ON/OFF patterns of activity and data traffic rate/ volume. We have finished with a discussion that how these parameters are effective in identifying the stepping stones and with the help of these four parameters, how a stepping stone detection framework can be designed.

6. REFERENCES

[1] David A. Wheeler, Gregory N. Larsen and Task Leader, "Techniques for Cyber Attack Attribution", Institute for Defense Analyses, October 2003.

[2] Yin Zhang and Vern Paxson, "Detecting Stepping Stones", in Proc. Of the 9th USENIX Security Symposium Denver, Colorado, USA, August 2000 pp.171-184.

[3] Giovanni Di Crescenzo, Abhrajit Ghosh, Abhinay Kampasi, Rajesh Talpade and Yin Zhang, "Detecting Anomalies in Active Insider Stepping Stone Attacks", Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications, Vol. 2 number , 2011, pp 103-120.

[4] Rajesh Kumar Goutam, "The Problem of Attribution in Cyber Security", International journal of Computer Application, Foundation of computer science, Vol. 131, No. 7, NY, USA, December 2015 pp.34-36.

[5] H.F Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues", Carnegie Mellon Software Engineering Institute, Pittsburgh, November 2002

[6] Susan C. Lee and Clay Shields, "Technical, Legal, and Societal Challenges to Automated Attack Trace back", IT Pro, June 2002.

[7] S. M. Bellovin, "Security problems in the TCP/IP protocol suite" ACM SIGCOMM Computer Communications Review, vol. 19, issue 02, April 1989.

[8] Steven J. Templeton, Karl E. Levitt, "Detecting Spoofed Packets", available at http://seclab.cs.ucdavis.edu/papers/DetectingSpoofed-DISCEX.pdf on 20/04/2017.