The Problem of Attribution in Cyber Security

Rajesh Kumar Goutam
Computer Science Department
University of Lucknow
Lucknow

ABSTRACT

The basic objective for the construction of internet was to provide a common platform to researchers and students to share information among them. It was not constructed to track and trace the behavior of cyber criminals. Due to this reason, it is difficult to locate the origin of cybercrime. The paper defines cybercrime with treat and vulnerability and suggests a number of different techniques which are often used by the cybercriminals to Spoofing the IP. The purpose of this paper is not only to detail about why the attribution of cybercrime is difficult but also to present TTL and step stone logic which are now being heavily used in cybercrime.

Keywords

Cybercrime, Attribution, IP forging.

1. INTRODUCTION

The development of computers and internet made it possible to interchange the information quickly and with minimum cost. Internet has provided a single platform on which people can share their ideas and grow their business. It is open and accessible to all and this is the main drawback of this interconnected environment. It is worldwide accessible virtual place in which everyone can upload their information so it has been grown as huge repository for various types of data and information [9]. As it is clear that information available on web not only becomes relevant for educated community but also for criminals as well. Cybercrime denotes to all those illegal activities that deals with computers, internet and networking [1, 2]. In other words the criminal offences that are facilitated by the use of electronic communications means called cybercrime. The term cybercrime is still used in same context. It does not still have any universal accepted definition. It can include theft of government or corporate secrets through illegal remote access to victims systems worldwide. In can also involve downloading of various kinds of illegal files to stealing million of dollars from online banking frauds [2]. Cybercrime not only incorporate monetary activities but also include non-monetary activities like posting of confidential business information over the server. Sexual harassment and pornography using the internet also fall in the category of cyber crime [2].

2. TREAT AND VULNERBILITY

A threat can be defined as an agent who certainly wants to harm the organization and its networked systems [1]. Threats become responsible for organized crime may include spywares, malwares, adware companies and unsatisfied employees [1]. Worms and virus also fall in treats category because they can cause serious harm to particular organization without any human direction [1]. A threat is something that can share a particular system with strangers, may also prevent authorized users from their access. In other words, treat is a cause of worry by which cybercriminal can grab our soft assets. Vulnerability is a mechanism through which treats can be activated. Vulnerability refers some loopholes in our networked environment by using which cybercriminal makes entry in our environment can cause serious damage for our organization [1]. These loopholes can exist anywhere in our environment like system design and hardware. Most of the loopholes are found in installed software and poor networking configuration [1]. Fig 1. Shows how vulnerability skips the role of vulnerability protection unit and compromise the system for remote access for stranger [5].

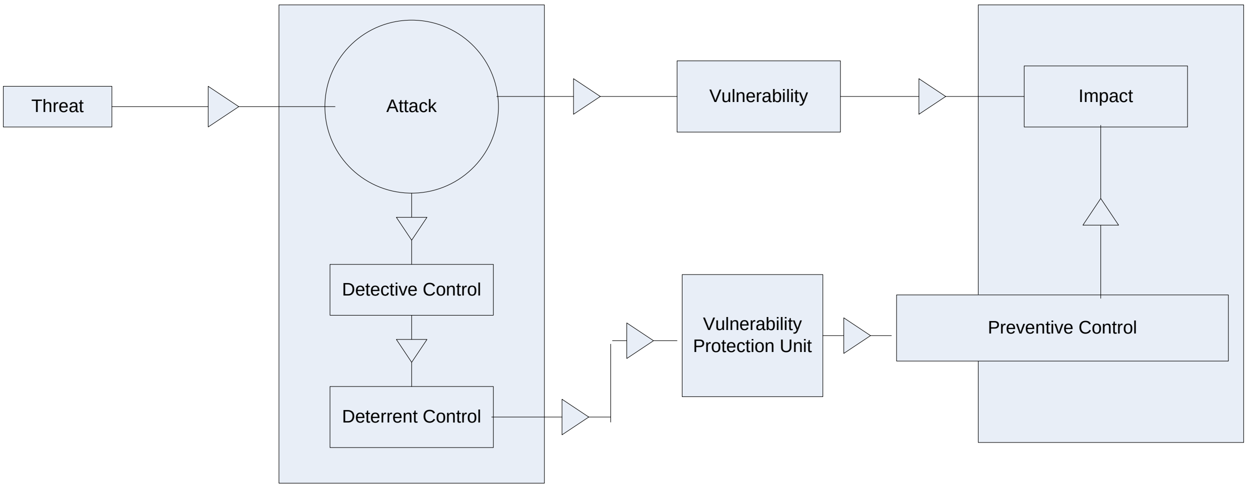

Fig. 1: Treat & Vulnerability Protection Unit

3. ORIGIN OF CYBERCRIME

During early period of computers, Electronic Numeric Integrator and Computer (ENIAC), Binary Automatic Computer (BINAC) and other punch card tabulation machines were beneficial from security prospective as these machines were standalone, large and expensive and access of these computers was very difficult [3]. In 1960 Programmed data processor (PDP-1) computers were introduced, which were available for companies and individuals on the basis of time duration. Same machines were being accessed by multiple users. Someone's data stored on disk was available for other one. Such type of working mechanism made the system venerable. In other words, PDP-1 emergence opened the door of hackers[3]. The first group of hackers was identified from Massachusetts Institute of Technology (MIT) in 1961 after the emergence of PDP-1 [3]. During the period of 1970s, telephones were well established in rich society but the phone calls were costly. A group of people, known as phreak, has given idea for making free phone calls through manipulation in telephone network. Stewart Nelson from MIT developed a software enabled the phreaks to make call free of cost [3].

4. ATTRIBUTION IN CYBER SECURITY

There is no universally accepted definition for attribution but few researchers define the attribution as a process to identify the location of an attacker on geographical area [8]. The attribution not only deals with the original attackers but also deals with the identification of intermediary nodes that acts as bridge for original cybercriminals to conduct cybercrime [8]. Location of cybercriminals may be physical and virtual. The virtual location may include the identification of IP address or Ethernet address [8]. As the technology being sharp, more sophisticated cyber attacks are being triggered. The chances of direct cyber attacks have been reduced. The original cyber criminals make often use normal citizens' systems as intermediary to conduct the cybercrime. Normal citizens often become unknown about the their involvement in cybercrime and indirectly helps the cybercriminals. An ideal attribution [4, 8] process should locate the original attacker's location. Attribution process should work on global context without any political boundary with the help of international cyber Laws, Policies and technology.

4.1 Why Cyber attribution is difficult

Internet was not designed to track and trace the behavior of user instead it was designed to provide a common platform to students and researchers for knowledge sharing [9]. In this paper we refer an adversary as a cyber attacker that is targeting a system or a group of systems with the help of internet or computer network. As a defender, we must ensure that the attacker in intelligent, resourceful and technically skilled person [8]. On the other hand, the individual person and organization which suffers from cyber attacks are the victims or defender that always becomes interested to identify to original attackers [8]. The victim must have an idea about the source so that he can apply their security techniques at appropriate place.

Unfortunately, the cyber criminals have more skilled hands and applying almost new techniques every day to hide the source of cybercrime origin. David A. Wheeler et. al.[8] 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' [5,6,8]. In more common word, when the changes are made to message to forge sender's identity, we call 'spoofing' [5,6].
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 [8].
3. Sometimes, cyber attacks are triggered with a forged computer by setting their IP address for a temporary time. In other words, their 'time to live' (TTL) value is kept too low [8]. 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. The cyber criminal logs with intermediate step-stone host and launches the attack [8]. 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 leaves its impact later by a period of time. The laundering host also termed as 'zombie' intentionally inserts some delay for a cyber attack to be active [8]. 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 [8]. In this way, it is converted in continuous ongoing process and prevents the users to guess how dangerous the attack is?

5. FORGING IP ADDRESS

Our intention with traceback system is to determine the computer systems through which the attack has been launched. As we have discussed earlier, that step-stone attack may include intermediate hosts to launch attack so determining the intermediate, innocent system would not be an idle traceback system [7,8]. 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 [7,8]. 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 [7,8]. The network shown in fig. 1 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 [7]. 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. [7] described how forging of IP is usually done with the help of reflector and laundering host.

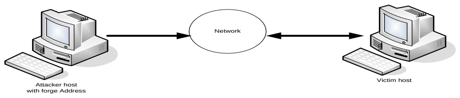

Fig 2. Forging IP

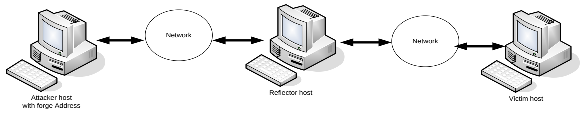

Fig 3. Forging IP with Reflector

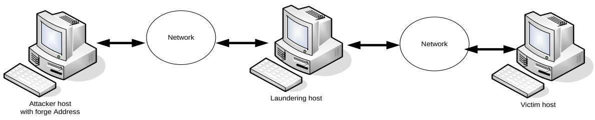

Fig 4. Forging IP with laundering Host

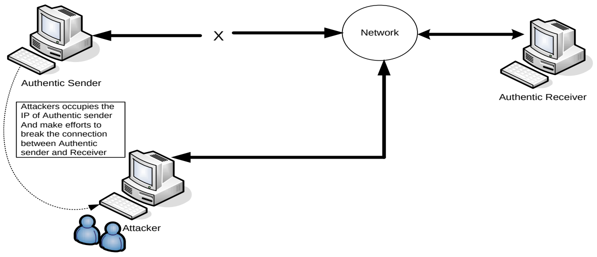
X
Network
Authentic Sender
Authentic Receiver
Attackers occupies the IP of Authentic sender And make efforts to break the connection between Authentic sender and Receiver
Attacker

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 [7]. 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.

5.1 Forging IP with Reflector

Cyber criminal often includes the number of innocent systems between the source of attack and victim system [7,8]. 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) [7]. In this way, victim directly finds the IP of reflector and accuse directly for attack.

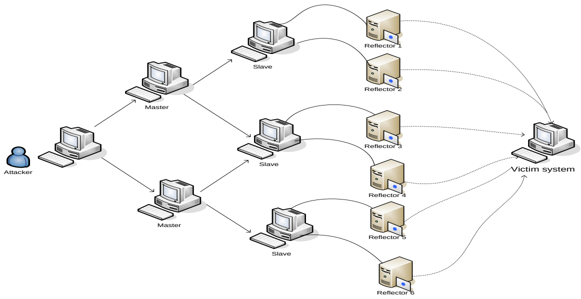

Fig 6. Forging IP with Multiple Reflector

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) [7]. This response from attacker will be treated as response from authentic receiver with forge receiving node address.

6. CONCLUSION

The paper details how the cybercrime, treat and vulnerability are central concern in this highly computing digital environment. Attribution of cyber attack is very difficult due to anonymity feature of cybercrime. The paper examines different techniques that are commonly adopted by the cybercriminals to hide the origin of cyber attack and detail how the cybercriminals use the reflector host and laundering host to spoof the IP of some system. TTL logic and step-stone method have also been emphasized which are often used to create disturbance in identifying the origin of cyber attack.

7. REFERENCES

[1] A Report available at http://www.pen-tests.com/difference-between-threat-vulnerability-and-risk.html.

[2] A Report "Cybercrimes", National crime presentation council, USA, September 2012.

[3] Nilkund Aseef, Pamela Davis, Manish Mittal, Khaled Sedky and Ahmed Tolba, "Cyber-Criminal Activity and Analysis", A White paper report, 2005 available at http://courses.cs.washington.edu/courses/csep590/05au/ whitepaper_turnin/team2-whitepaper.pdf

[4] Jeffrey Hunker, Robert Hutchinson and Jonathan Margulies, "Attribution of Cyber attacks on process control systems", IFIP International Federation for Information Processing, Volume 290; Critical Infrastructure Protection II, pp. 87–99, 2008.

[5] AReportavailableathttp://www.infocean.com/solutions/threatvulnerability-management/. On 05/11/2015.

[6] Bellovin, Steve, "Security Problems in TCP/IP Protocol suite", ACM Computer Communications Review, 1989, pp. 32-48.

[7] Susan C. Lee and Clay Shields, "Technical, Legal and Societal Challenges to Automated Attack Traceback", A Report from IT Pro, June 2002.

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

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