TRACKING OF INTRUDERS ON GEOGRAPHICAL MAP USING IDS ALERT

Manish Kumar[1], M. Hanumanthappa[2], T.V. Suresh Kumar[3]
[1]Asst. Professor, Dept. of Master of Computer Applications, M. S. Ramaiah Institute of Technology, Bangalore-560 054, India
[2]Dept. of Computer Science and Applications, Jnana Bharathi Campus, Bangalore University, Bangalore -560 056, India
[3]Professor & Head, Dept. of Master of Computer Applications, M. S. Ramaiah Institute of Technology, Bangalore-560 054, India

ABSTRACT
Intrusion Detection System (IDS) is the most powerful system that can handle the intrusions of the computer environments by triggering alerts to make the analysts take actions to stop this intrusion. Knowing from where an intrusion originated or where a spammer or suspect intruder is located is key information to identify security threats to your system and confidential information. In this paper we are discussing the method which tracks the intruders on the geographical map. The technique is based on the source IP address of Intruders. In current Internet communication world, validity of the source of IP packet is an important issue. The problems of IP spoofing alarm legitimate users of the Internet. IP spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. This paper also discusses some of the technique to defense the IP spoofing problem.

KEYWORDS: *Intrusion Detection, Geolocation, IP Spoofing.*

I. INTRODUCTION

A computer intrusion is, "An intentional event where an intruder gains access that compromises the confidentiality, integrity, or the availability of computers, networks, or the data residing on them." The amount of damage done by an intruder to a system can vary greatly. Some intruders are malicious in nature and others are just curious and want to explore what is on a local network. Computer users must protect themselves from intrusion. While there are no 100% effective methods of eliminating intruders completely, some methods must be used to reduce intrusions. In the event that an intrusion has taken place the last line of defense is an intrusion detection system. An intrusion detection system can alert the system administrator in the event that the system has been breeched. Once the intrusion detection system has detected an event, an intrusion investigation should be conducted to note the extent of the intrusion and any damages that may have occurred and to locate the source of the attack.

While intrusion prevention, detection and tolerance all play an important role in solving the problem of today's network-based intrusion, they are all passive and not adequate to solve the intrusion problem [22]. One fundamental problem with existing intrusion prevention, detection and tolerance is that they do not effectively eliminate or deter network-based intrusions. The best they can do is to avoid being victims of network-based intrusions temporarily. Because they do not address the root cause of intrusions – intruders, those intruders can always explore new system vulnerabilities, find new accomplices – potentially insiders, and launch new attacks from different places. Because intrusion prevention, detection and tolerance do not effectively address the problem of compromised

system recovery, intruders can use those compromised system as new base for further intrusion. What we need is an effective way to hold network-based intruders accountable for their intrusions.
So far most computer security research regarding network-based intrusions has focused on prevention and detection. Intrusion response has been an afterthought and is generally limited to logging, notification and disconnection at local host. Any further response usually involves manual interactions such as off-line analysis, reporting incidents to CERT and installing fixes. Given today's high-speed network, many network-based intrusions can be very fast and short across wide areas of networks. Current ad hoc and manual intrusion response process neither provides the needed real-time intrusion response nor scales with network. Furthermore, because current automated intrusion responses are passive and lack network-wide response, they do not, however, eliminate or even effectively deter network-based intrusions.
In this paper, we propose Tracing-the intruders on geographical map using the log report IP address to address the problem of network-based intrusions. It differs from existing intrusion defense approaches in that it addresses the intrusion problem by targeting the root cause of the problem: intruders. It collaborates with IDS and will trigger automatically when intrusions are detected. By actively tracing intrusions at real-time, it helps to apprehend the intruders on the spot and hold them accountable for the intrusions. Therefore it is likely a more effective deterrent against further intrusion attempts.

II. INTRUSION DETECTION SYSTEM IN PRACTICE

IDS have historically been categorized as network, host, anomaly or misuse (signature) based. This simple categorization is, however, no longer adequate. IDS can also be distributed or centralized, can be passive or reactive, can be application-specific or general-purpose, can focus on real time or after-the-event analysis [9] [14]. The five IDS described later are not intended to be exemplifiers of these or other various categories, but are presented as an indication of how major trends have developed. Almost all IDS will output a small summary line about each detected attack [15]. This summary line typically contains the information fields shown below.
1. Time/date;
2. Sensor IP address;
3. Vendor specific attack name;
4. Standard attack name (if one exists);
5. Source and destination IP address;
6. Source and destination port numbers;
7. Network protocol used by attack.

Other more general information is also often provided; information such as a textual description of the attack, identification of the software attacked, information that identifies the patches required to fix the vulnerability, and advisories regarding the attack.
Attacks on systems and networks have increased as rapidly changing technology, systems integration, global networks, information warfare and hacker boredom have become prevalent. For a long time, enterprises have relied upon solutions like intrusion detection to alert them of potential attacks. As the Internet and e-business have evolved, so has the need for a more proactive solution. In this paper we are discussing the techniques for detecting the intrusion, tracking the intruders IP address and showing the intruders location on geographical map
The most challenge part is to track the intruders IP address. Many time intruders use the spoofed IP address to hide their identity. We need to first track the correct IP address of the intruders. The following section discusses the various techniques for tracking the intruders IP address.

III. METHODS OF IP TRACEBACK

The purpose of IP traceback is to identify the true IP address of a host originating attack packets [21]. Normally, we can do this by checking the source IP address field of an IP packet. Because a sender can easily forge this information, however, it can hide its identity. If we can identify the true IP address of the attack host, we can also get information about the organization, such as its name and the network administrator's e-mail address, from which the attack originated. With IP traceback technology, which traces an IP packet's path through the network, we can find the true IP address of

the host originating the packet. To implement IP traceback in a system, a network administrator updates the firmware on the existing routers to the traceback support version, or deploys special tracing equipment at some point in the network. Existing IP traceback methods can be categorized as proactive or reactive tracing.

3.1 Proactive Tracing

Proactive tracing prepares information for tracing when packets are in transit. If packet tracing is required, the attack victim (or target) can refer to this information to identify the attack source. Two proactive tracing methods — packet marking and messaging is explained.

Packet Marking: - In packet marking, packets store information about each router they pass as they travel through the network. The recipient of the marked packet can use this router information to follow the packet's path to its source. Routers must be able to mark packets, however, without disturbing normal packet processing.

With IP's record route option, for example, the IP packet can store router addresses in its option field. In another proposed approach, the router writes its identifier probabilistically in the packet's IP header identification field. Each marked packet contains information in its identification field about only one or two routers on the attack path. In a flooding-style attack, however, the target network receives many attack packets and can collect enough information to identify the attack path. The identification field is used to reassemble fragmented packets. Because few fragments are created on the Internet, however, modifying the identification field rarely affects normal packet processing.

Messaging: In messaging approaches, routers create and send messages containing information about the forwarding nodes a packet travels through. The Internet Engineering Task Force's proposed method, the Internet control message protocol (ICMP) traceback message. A router creates an ICMP traceback message, which contains part of a traversing IP packet, and sends the message to the packet's destination. We can identify the traversed router by looking for the corresponding ICMP traceback message and checking its source IP address. Because creating an ICMP traceback message for every packet increases network traffic, however, each router creates ICMP traceback messages for the packets it forwards with a probability of 1/20,000. If an attacker sends many packets (for example, in a flooding-style attack), the target network can collect enough ICMP traceback messages to identify its attack path.

3.2 Reactive Tracing

Reactive tracing starts tracing after an attack is detected. Most of the methods trace the attack path from the target back to its origin. The challenges are to develop effective traceback algorithms and packet-matching techniques. Various proposals attempt to solve these problems.

3.3 Hop-by-hop tracing.

In hop-by-hop tracing, a tracing program, such as MCI's DoS Tracker, logs into the router closest to the attacked host and monitors incoming packets. If the program detects the spoofed packet (by comparing the packet's source IP address with its routing table information), it logs into the upstream routers and monitors packets. If the spoofed flooding attack is still occurring, the program can detect the spoofed packet again on one of the upstream routers. This procedure is repeated recursively on the upstream routers until the program reaches the attack's actual source.

3.4 Hop-by-hop tracing with an overlay network.

In hop-by-hop tracing, the more hops there are, the more tracing processes will likely be required. As a result, a packet will take longer to trace, and necessary tracing information might be lost before the process is complete. To decrease the number of hops required for tracing, one approach builds an overlay network by establishing IP tunnels between edge routers and special tracking routers and then reroutes IP packets to the tracking routers via the tunnels. Hop-by-hop tracing is then performed over the overlay network.

3.5 IPsec authentication.

Another proposed reactive tracing technique is based on existing IP security protocols. With this method, when the IDS detects an attack, the Internet key exchange (IKE) protocol establishes IPsec

security associations (SAs) between the target host and some routers in the administrative domain (for example, autonomous system boundary routers). Routers at the SA ends add an IPsec header and a tunnel IP header containing the router's IP address to traversing packets. If the attack continues and one of the established SAs authenticates a subsequent attack packet, the attack must come from a network beyond the corresponding router. The receiver checks the source IP address of the tunnel IP header to find out which routers the attack packet traversed. Repeating this process recursively, the receiver finally reaches the attack source.

Because this technique uses existing IPsec and IKE protocols, implementing a new protocol for tracing within an administrative domain is unnecessary. To trace beyond the administrative domain, however, a special collaboration protocol is needed. The IETF Intrusion Detection working group (IDWG) is discussing such a protocol. Traffic Pattern Matching. A fourth proposed technique traces an attack path by comparing traffic patterns observed at the entry and exit points of the network with the network map.

IV. CURRENT ACTIVE RESEARCH ON IP TRACEBACK

Two network tracing problems are currently being studied: IP traceback and traceback across stepping-stones (or a connection chain). IP traceback is to identify the origins of sequences IP packets (e.g., identify the origin of DDOS packets) when the source IP addresses of these packets are spoofed. IP traceback is usually performed at the network layer, with the help of routers and gateways. Traceback across stepping-stones is to identify the origin of an attacker through a chain of connections (e.g., connections established with telnet, rlogin, or ssh), which an attacker may use to hide his/her true origin when he/she interacts with a victim host. Traceback across stepping-stones is beyond the network layer, since at each intermediate host the data is transmitted to application layer in one connection, and then resent to the network in the next connection.

Research on IP trace back has been rather active since the late 1999 DDOS attacks [17,24,18]. Several approaches have been proposed to trace IP packets to their origins. The IP marking approaches enable routers to probabilistically mark packets with partial path information and try to reconstruct the complete path from the packets that contain the marking [10,16,4]. DECIDUOUS uses IPSec security associations and authentication headers to deploy secure authentication tunnels dynamically and trace back to the attacks' origins [19,1]. ICMP traceback (iTrace) proposes to introduce a new message "ICMP trace back" (or an iTrace message) so that routers can generate iTrace messages to help the victim or its upstream ISP to identify the source of spoofed IP packets [2]. An intention-driven iTrace is also introduced to reduce unnecessary iTrace messages and thus improve the performance of iTrace systems [3].

An algebraic approach is proposed to transform the IP traceback problem into a polynomial reconstruction problem, and uses techniques from algebraic coding theory to recover the true origin of spoofed IP packets [13]. An IP overlay network named CenterTrack selectively reroutes interesting IP packets directly from edge routers to special tracing routers, which can easily determine the ingress edge router by observing from which tunnel the packets arrive [12]. A Source Path Isolation Engine (SPIE) has been developed; it stores the message digests of recently received IP packets and can reconstruct the attack paths of given spoofed IP packets [11,7]. There are other techniques and issues related to IP traceback (e.g., approximate traceback [8], legal and societal issues [23], vendors' solutions [5]). An archive of related papers can be found at [20].

Though necessary to make attackers accountable (especially for DDOS attacks where there are a large amount of packets with spoofed source IP addresses), IP traceback has its own limitations. In particular, IP traceback cannot go beyond the hosts that send the spoofed IP packets. Indeed, a typical attacker will use a fair number of steppingstones before he/she finally launches, for example, a DDOS attack. Thus, only identifying the source of IP packets is not sufficient to hold the attackers responsible for their actions.

Similar to IP traceback, there have been active research efforts on tracing intruders across stepping-stones. In general, approaches for traceback across a connection chain can be, based on the source of tracing information, divided into two categories: host-based and network-based. In addition, depending on how the traffic is traced, traceback approaches can be further classified

into either active or passive. Passive approaches monitor and compare all the traffic all the time, and they do not select the traffic to be traced. On the other hand, active approaches dynamically control when, where, what and how the traffic is to be correlated through customized processing. They only trace selected traffic when needed.

V. GEOLOCATION TRACKING OF INTRUDER'S IP ADDRESS

After tracking the IP address of intruders, our next objective is to find the geolocation of the intruders. IP to geolocation tracking is the technique of determining a user's geographic latitude, longitude and, by inference, city, region and nation by comparing the user's public Internet IP address with known locations of other electronically neighboring servers and routers IDS can detect the intrusion. We can find the IP address of intruders but barely having a IP address, it do not give the idea that from which place attack is generated.

5.1 Advantage of Geolocation Tracking

Tracking the intruders IP address and plotting the trace on geogrphical (Figure:- 1) map gives a clear picture that whether the attack is distributed and initiated from multiple country or it is initiated from one specific country our region. This information may be the vital information for the organization to take any further action or any precaution measures.

Figure 1: Intruder's IP address tracking on Map

5.2 System Architecture

The overall system (Figure 2) works on IDS alert analysis. Each alerts generated by IDS is passed to IDS alerts log report. All the alerts from IDS log report is further analyzed for tracking the Intruders source IP address. Once the correct source IP address of the intruders is confirmed, it is passed to the API which map the source IP address on geographical map.

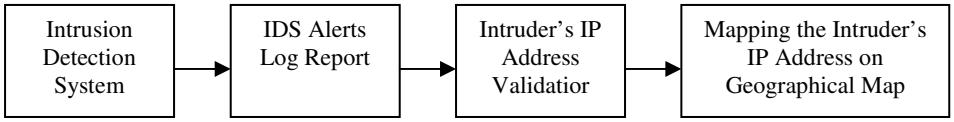

Figure 2: Architecture of Intruders Geographical Location Mapping System

5.3 Implementation Detail

We have implemented the system using Snort and Google API for geolocation mapping of intruders. Snort is the well known open source IDS software which detect the intrusion event. Snort log this report in alert file. The intruders IP address is analyzed and traced back. The traced IP address is passed to Google Geolocation API which enables a web application to:

- Obtain the user's current position, using the `getCurrentPosition` method
- Watch the user's position as it changes over time, using the `watchPosition` method
- Quickly and cheaply obtain the user's last known position, using the `lastPosition` property

The Geolocation API provides the best estimate of the user's position using a number of sources (called location providers). These providers may be onboard (GPS for example) or server-based (a

network location provider). The getCurrentPosition and watchPosition methods support an optional parameter of type PositionOptions which lets you specify which location providers to use.

VI. EVALUATION

Geolocation of intruders are obtained by tracking the IP addresses of intruders using databases that map Internet IP addresses to geographic locations. Google uses MaxMind's database for mapping IP addresses to a geographical location [6]. They claim it is 99% accurate. What is in the fine print, is that it is 99% accurate in determining the country, but pinpointing the exact position is still a challenging issues which need to be addressed.

VII. CONCLUSIONS

Our system is able to trace the intruders geographical map but our whole system is depended on the IP traceback. Traceback has several limitations, such as the problem with tracing beyond corporate firewalls. To accomplish IP traceback, we need to reach the host where the attack originated. Another limitation relates to the deployment of traceback systems. Most traceback techniques require altering the network, including adding router functions and changing packets. To promote traceback approaches, we need to remove any drawbacks to implementing them. Moreover, even if IP traceback reveals an attack's source, the source itself might have been used as a stepping-stone in the attack. IP traceback methods cannot identify the ultimate source behind the stepping-stone; however, techniques to trace attacks exploiting stepping-stones are under study. Some operational issues must also be solved before IP traceback can be widely deployed. To trace an attack packet through different networks, for example, there must be a common policy for traceback. We also need guidelines for dealing with traceback results to avoid infringing on privacy. Furthermore, we need to consider how to use information about an attack source identified by IP traceback. In the future, we will likely need to focus on the authenticity of results from IDSs and IP traceback systems.

REFERENCES

[1] Computer Emergency Response Team. (2000) CERT Advisory CA-2000-01 Denial-of Service Development. http:// www.cert.org/advisories/CA-2000-01.html.
[2] Computer Emergency Response Team. (1999) Results of the Distributed-Systems Intruder Tools Workshop. http://www.cert.org/reports/dsit_workshop.pdf.
[3] Computer Security Institute. Annual CSI/FBI Computer Crime and Security Survey. (2001) http://www.gocsi.com/prelea_000321.htm.
[4] H. Y. Chang, R. Narayan, S.F. Wu, B.M. Vetter, X. Y. Wang et al. (1999) DecIdUouS: Decentralized Source Identification for Network-Based Intrusions, In Proceedings of 6th IFIP/IEEE International Symposium on Integrated Network Management.
[5] H. Jung, et al. Caller Identification System in the Internet Environment. (1993) In Proceedings of 4th USENIX Security Symposium.
[6] http://netsolutions.net.au/web-design/geo-targeting-by-ip-address/ (Accessed on 28/01/2012)
[7] J. D. Howard. (1997) An Analysis of Security Incidents on The Internet 1989 - 1995, PhD Thesis, http://www.cert.org/research/JHThesis/Start.html.
[8] J. Ioannidis and M Blaze. (1993) The Architecture and Implementation of Network-Layer Security under Unix. In Proceedings of 4th USENIX Security Symposium.
[9] K2. *ADMmutate README*. ADMmutate source code distribution. Version 0.8.4. URL: http://www.ktwo.ca/c/ADMmutate-0.8.4.tar.gz (Jan 2002)
[10] K. L. Calvert, S. Bhattacharjee and E. Zegura. (1998) Directions in Active Networks. IEEE Communication Magazine.
[11] L. T. Heberlein, K. Levitt and B. Mukherjee. (1992) Internetwork Security Monitor: An Intrusion-Detection System for Large-Scale Networks. In Proceedings of 15th National Computer Security Conference.
[12] M. B. Greenwald, S. K. Singhal, J. R. Stone and D. R. Cheriton. (1996) Design an Academic Firewall: Policy, Practice and Experience with SURF. Internet Society Symposium on Network and Distributed System Security (NDSS '96).
[13] N.G. Duffield and M. Grossglauser. (2000) Trajectory Sampling for Direct Traffic Observation. Proceedings of the ACM SIGCOMM '2000.
[14] P. Stephenson "The Application of Intrusion Detection Systems in a Forensic Environment", Proceedings of the RAID 2000 Conference, Toulouse, France, 2000.

[15] Peter Sommer "Intrusion Detection Systems as Evidence", Presented in RAID 98 Conference, Louvain-la-Neuve, Belgium.
[16] R. H. Campbell, Z. Liu, M. D. Mickunas, P. Naldurg and S. Yi. (2000) Seraphim: Dynamic Interoperable Security Architecture for Active Networks. In Proceedings of IEEE OPENARCH'2000.
[17] S. M. Bellovin. (2000) ICMP Traceback Messages. Internet Draft: draft-bellovin-itrace-00.txt.
[18] S. Bhattacharjee, K. L. Calvert and E. W. Zegura. (1997) An Architecture for Active Networking. High Performance Networking (HPN'97), White Plans, NY.
[19] S. Staniford-Chen, L. T. Heberlein. (1995) Holding Intruders Accountable on the Internet. In Proceedings of IEEE Symposium on Security and Privacy.
[20] S. Kent, R. Atkinson. (1998) Security Architecture for the Internet Protocol. IETF RFC 2401.
[21] Tatsuya Baba and Shigeyuki Matsuda, "Tracing Network Attacks to Their Sources", IEEE INTERNET COMPUTING, MARCH - APRIL 2002
[22] Wang, X., Reeves, D., & Wu, S. F. (n.d.). Tracing based active intrusion response. Retrieved from http://arqos.csc.ncsu.edu/papers/2001-09-sleepytracing-jiw.pdf
[23] W. Jansen, P. Mell, T. Karygiannis, D. Marks. (1999) Applying Mobile Agents to Intrusion Detection and Response. NIST Interim Report (IR) – 6416.
[24] W. Bender, D. Gruhl, N. Morimoto and A. Lu. (1996) Technique for Data Hiding. IBM Systems Journal, Vol. 35, Nos. 3&4

AUTHORS

Manish Kumar is working as Asst. Professor in Department of Master of Computer Applications, M. S. Ramaiah Institute of Technology, Bangalore, India. His areas of interest are Cryptography and Network Security, Computer Forensic, Mobile Computing and eGovernance. His specialization is in Network and Information Security. He has also worked on the R&D projects relates on theoretical and practical issues about a conceptual framework for E-Mail, Web site and Cell Phone tracking, which could assist in curbing misuse of Information Technology and Cyber Crime. He has published several papers in International and National Conferences and Journals. He has delivered expert lecture in various academic Institutions.

M Hanumanthappa is currently working as a Associate Professor in the Department of Computer Science and Applications, Bangalore University, Bangalore, India. He has over 15 years of teaching (Post Graduate) as well as Industry experience. His areas of interest include mainly Data Structures, Data Base Management System, Data Mining and Programming Languages. Besides, he has conducted a number of training programs and workshops for computer science students/faculty. He is also the member of Board of Studies /Board of Examiners for various Universities in Karnataka, India. He is also guiding the research scholars in the field of Data Mining and Network Security.

T V Suresh Kumar is working as Professor and Head, Department of Master of Computer applications, M S Ramaiah Institute of Technology, Bangalore. He delivered lectures at various organizations like Honeywell, SAP Labs, Wipro Technologies, DRDO, Mphasis, Indian Institute of Science (Proficience), HCL Technologies, L&T Infotech, Nokia and various Universities/Academic Institutions. His areas of interest are Software Performance Engineering, Object Technology and Distributed Systems etc. He has published several research papers in various National and International Conferences and Journals. He has carried out software projects for various organizations. He is life member of ISTE and member of IEEE.