

DETECTING A CYBER-ATTACK SOURCE IN REAL TIME

R. Romanyak¹, A. Sachenko¹, S. Voznyak¹, G. Connolly², G. Markowsky²

Introduction

The ability to determine the source of a cyber-attack is very helpful in stopping such attacks. If this ability were well developed, it would act as a deterrent against such attacks since accurate knowledge of the source of such attacks can be used for legal, criminal, economic or military sanctions [1]. The process of tracing an attack back to its source may also uncover useful details that would help develop effective countermeasures against similar attacks in the future. It might even enable one to interrupt an attack in progress. In most cases, the ability to deter, prevent or interrupt a cyber-attack is of greater value to society than assigning blame and trying to collect damages after an attack has occurred [2].

Current methods for tracing Internet-based attacks are primitive [1]. Sophisticated attacks can be almost impossible to trace to their true source using current tools. Today's cyber-attackers seek to maintain anonymity during their attacks [3].

1. Approaches for localization of remote host in the network

Up to now, three approaches have been developed to locate a computer in physical space: whois, traceroute, and distributed traceroute. The whois database is maintained by Network Solutions to provide information related to a domain name. This might include such information as relevant physical addresses, email addresses and phone numbers. One can also get information about networks, and domain structure [4]. The main database, which includes information about networks, is supported by the InterNic organization. Whois service is available to every internet user and queries can be performed by email. Whois has the limitation that it provides information only about top-level domains, but computers associated with a domain can be widely distributed [3].

Traceroute is a program that displays the route followed by an IP datagram through the Internet from a source host to a destination host. It uses the TTL (Time To Live) field of the IP Header [5]. Each router that handles an IP datagram decrements the TTL field. When the TTL field reaches zero, a router must discard the packet and send an error message to the originator of the datagram. Traceroute uses this feature, initially sending a datagram with the TTL set to one [5]. The first router along the path, upon receiving the datagram decrements the TTL, discards the datagram and sends back an ICMP error message. *Traceroute* records this first IP address (source address of the error message packet) and then sends the next datagram with the TTL set to two [6]. This process continues until the datagram finally reaches the target host, or until the maximum TTL threshold is reached. But using this utility for the geographical localization of a remote computer host has some limitations. The major limitation is that while there are generally several different paths to the target computer, traceroute only uses one path. Using different paths can increase the amount of information available about the physical location of the target computer. Thus, by executing a single trace from a single location one gets results that are geographically biased and insufficient.

¹ Ternopil Academy of the National Economy

² Department of Computer Science, University of Maine

The distributed traceroute approach, using multiple paths through the Internet, was presented in [7]. The basic idea is to run traceroute from several geographically distributed computers to the same target computer. [7] describes the Web Neighborhood Watch project at the University of Maine which seeks to locate computers that host websites created by potentially dangerous individuals. The Whois service complements the distributed traceroute approach very well. By examining the Whois information at each hop, along with information produced by the traceroute display, much information can be obtained regarding the physical location of the target computer. The distributed traceroute approach has limited accuracy when the attacker uses intermediate hosts with software redirectors to make a cyber-attack.

2. The Time Delay Method

An attacking computer (AC) can be directly linked to the victim computer (VC) or it can be attacking through intermediate hosts via redirection software. Our method compares the time delays between the VC and the AC with the time delays from the AC to the VC. We have written a program called *DELAYS* that can perform the calculation. This tool must be initialized with the IP address of the AC, the port number that is being attacked, and the port number of the AC being used for the attack. *DELAYS* will catch the packets that are being sent from the AC to the port on the VC. It also will send packets from the VC to the AC.

The network adapter must first be set to examine only packets that are being sent between the AC and the VC. The key step is to determine the apparent time delays between the sending and receiving of IP-packets. The IP-packet filter follows rules based on initial information entered by the user. The IP-packet filter catches IP-packets addressed to VC automatically. The timer is started when the first packet is received. When the next packet comes, the current timer value is pushed into the array of time delays as its first value. Then, before the third packet comes, the timer is started from the beginning and the process is repeated with consecutive pairs of packets. The filter collects only those packets that are sent to the attacked port on the VC. At the same time, the process of sending packets to the AC is started. The number of packets to send is selected by the user. All packets that return from the AC are collected from the network.

As a result, we end up with an array of time delays from the AC to the VC, as well as an array of time delays from the VC to the AC. If the AC is attacking the VC directly, i.e., without redirection, the times from the AC to the VC and from the VC to the AC will be approximately equal. On the other hand, if the time delays for the packets being sent from the VC to the AC are much smaller than the time delays of the packets coming to the VC from the AC we should be confident that the attack is going through a redirector. The time delay for a packet going from the AC to the VC is calculated by the following formula:

$$T_{total} = \sum_{i=1}^{n+1} t_i,$$

where t_1, \dots, t_{n+1} are the time delays indicated in Figure 1. It is obvious that total time from the AC to the VC is larger than the time it takes for a packet to go from the VC to the last redirector.

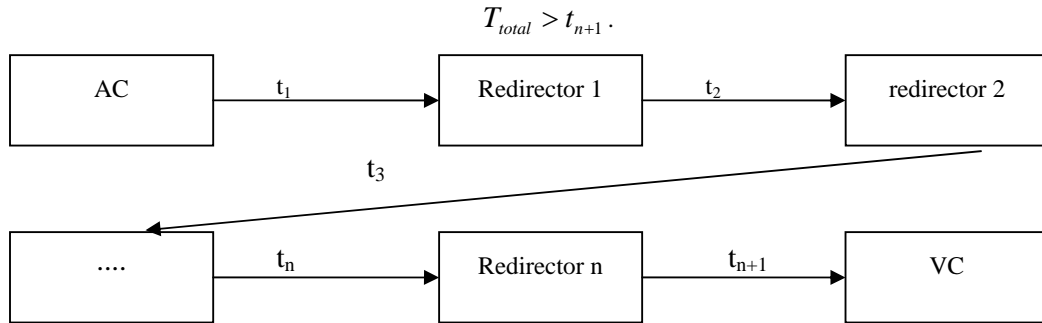


Figure 1. A Cyber-Attack using Redirectors

DELAYS must be fast because these time delays are typically measured in microseconds [8]. Moreover the operations we are interested in are performed in the transport and network levels of the OSI model [6]. To achieve the speed that we need to get we wrote *DELAYS* in C++.

DELAYS performs the following tasks. It examines only the IP-packets that are sent to the attacked port on the VC. It calculates the time delay from packets coming to the VC from the AC. It also sends packets to the AC and determines the delay from the VC to the AC.

DELAYS accuracy module was confirmed experimentally. Experiments were performed using the following servers:

- TANE (Ternopil Academy of the National Economy, Ukraine, 217.196.166.105)
- Kiel University(Germany, 134.245.52.122)
- HTTL (The **H**ome **T**o good service and **T**echnology **L**td, London, England, 217.34.204.1)
-

The time delays between IP-packets between HTTL and TANE with direct connection may be seen in Figures 2 and 3. The time delays between HTTL-srv and TANE-srv using the Kiel-srv software redirector are showed in Figure 4. The time delays shown in Figures 2 and 3 are much smaller than the time delays shown in Figure 4. That's why one can make a conclusion that the link between the two hosts measured in Figure 4 has redirectors in it. In the case of redirectors, the distributed traceroute method will only locate the last redirector. In direct attack situations such as represented by Figures 2 and 3, the distributed traceroute method can geographically locate the AC.

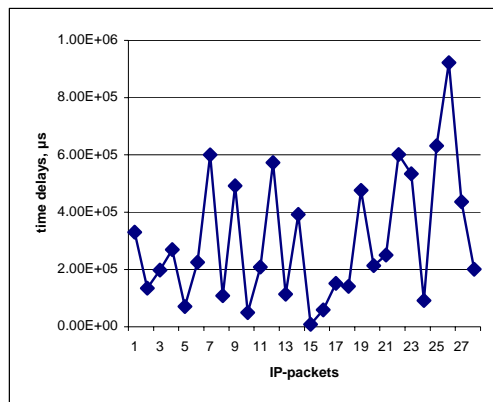


Figure 2. Time Delays from HTTL to TANE (direct connection)

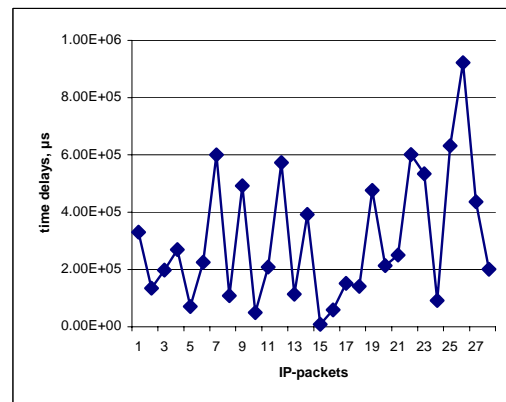


Figure 3. Time Delays from TANE to HTTL (direct connection)

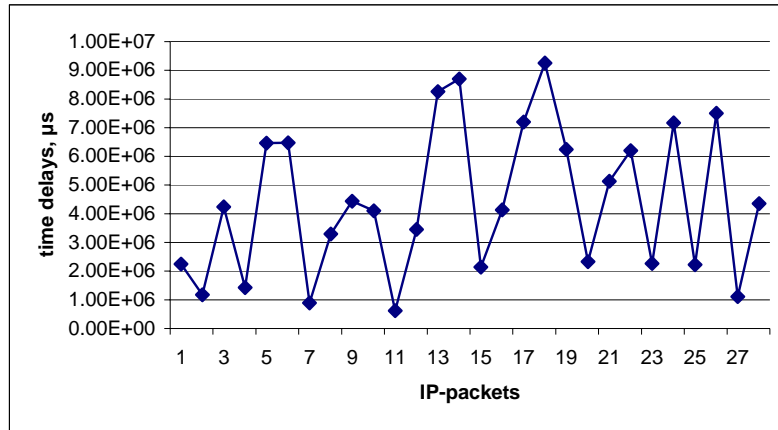


Figure 4. Time Delays from HTTL to TANE using Kiel-redirector

Conclusion

The test results indicate that it is possible to reliably discover that a cyber-attack is going through a redirector. We expect to further develop our methodology to detect the number of redirectors being used in a cyber-attack. This will help to get to an attacker who is hiding behind any number of intermediate hosts running software redirectors.

References

1. Lee H., and Park, K. "On the Effectiveness of Probabilistic Packet Marking for IP Traceroute Under Denial of Service Attack". *Proceedings of IEEE INFOCOM 2001*. Anchorage, Alaska, April 22–26, 2001. New York: IEEE Computer Society Press, 338–347, 2001.
2. Lipson, H. and Fisher, D. "Survivability—A New Technical and Business Perspective on Security," 33–39. *Proceedings of the 1999 New Security Paradigms Workshop*. Caledon Hills, Ontario, Canada, Sept. 22–24, 1999. New York: Association for Computing Machinery, 2000.
3. Savage, S., Wetherall, D., Karlin, A. and Anderson, T. "Practical Network Support for IP Traceroute," 295–306. *Proceedings of ACM SIGCOMM 2000*. Stockholm, Sweden, Aug. 28–Sept. 1, 2000. New York: Association for Computing Machinery, 2000.
4. Fadia A, Ankit P. Getting geographical Information using an IP Address. New York: Association for Computing Machinery, 2000.
5. <http://www.sarangworld.com/TRACEROUTE/>.
6. Nemeth C., Evi D., and Ram P. "GTrace - A Graphical Traceroute Tool." Boston: Addison-Wesley, 2003.
7. Connolly, G., Markowsky, G., and Sachenko, A. "Distributed Traceroute Approach to Geographically Locating IP Devices". *Proceedings of 2003 Spring IEEE Conference on Technologies for Homeland Security*, Boston, USA, May 7-8, 2003.
8. <http://cpp.samara.ws/articles/kir/intro.shtml>