IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 8, Aug 2014, 91-98

TRACE BACK MECHANISM FOR RECTIFIED PROBABILISTIC PACKET MARKING

ANIL V. TURUKMANE & KAILASH D. KHARAT

Assistant Professor, Department of Computer Science, Dr. BAMU University, Aurangabad, Maharashtra, India

ABSTRACT

A new probabilistic packet marking technology (called as P3M) based on path identification to defence serious distributed denial of service attacks and solves complex computation and other problem existed in traditional probabilistic packet marking (PPM) technologies. First contribution is constructing a new payload to carry router address and path identification. The second contribution is designing a new path identification scheme based on router addresses and hash algorithm. P3M is a practical technology to defence DDoS.

KEYWORDS: Structured Network, Secure Data Sharing

INTRODUCTION

The main purpose of system is to describe a technique for tracing anonymous packet flooding attacks in the Internet back towards their source & the proper termination of the trace back procedure with termination packet number (TPN). This work is motivated by the increased frequency and sophistication of denial-of-service attacks and by the difficulty in tracing packets with incorrect, or “spoofed”, source addresses. In this system we describe a general purpose trace back mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs).

The Trace back System proposed in this paper will be implemented with the help of The Probabilistic Packet Marking Algorithm & A Precise Termination Condition of the Probabilistic Packet Marking Algorithm. The main objective of the system is to provide the efficient way to trace back the IP address of attacker over the medium like Internet. The system will mark each & every packet which is to be transfer over the internet according to the contents of the packet & send it over the transfer media. When it reaches to destination at that time the marking is changed of any of the packet then system will capable of tracing the IP address of the attacker.

The proposed system is beneficial in the fields where more importance is given to trace back the IP address while modification in packet is done, such as Cyber Crime, illegal handling of data packets where some important information needs to be transferred.

To propose termination condition of the PPM algorithm, this is missing or is not explicitly defined in the literature. Through the new termination condition, the user of the new algorithm is free to determine the correctness of the constructed graph. The constructed graph is guaranteed to reach the correctness assigned by the user, independent of the marking probability and the structure of the underlying network graph. In this system we proposed a Rectified Probabilistic Packet Marking Algorithm to encode the packet in the routers to detect the attacked packets. To reduce the a constructed graph such that the constructed graph is the same as the attack graph, where an attack graph is the set of paths the attack packets traversed, To construct a graph, is a graph returned by the PPM algorithm. The proposed system that we are going

to develop will be used as the Chief performance system within the different Cyber security or forensics for tracing the IP address of attacker with proper termination method. Therefore, it is expected that the system would perform functionally all the requirements that are specified by the user or any private agency.

INTRUSION DETECTION

Two methods are suggested for the protection of the active packets: fault tolerance techniques and encryption. Encryption refers to the situation where active packets do not consist of clear text code and data. Encryption is usually used for code and data in transit. However, the programs may even be executed in a non-clear text form, which leads to the concept of cryptography. The fault tolerance techniques are replication, persistence, and redirection. Replication means that packets replicate at each node. Persistence means that packets are temporarily stored against node failure so that even if a node crashes, the copy persists in storage. Redirection means that packets may seek alternative routes in case their default route fails. Replication and persistence are unacceptable for the vast majority of network packets because they consume memory and bandwidth, and only very important active packets should be allowed to do this such as packets installing a new version of a routing protocol in all nodes. Redirection and encryption have broader applications in packet protection because they basically consume CPU cycles.

A combination of fault tolerance techniques and encryption may give very good results in the problem of protecting active packets. However, because these techniques are still in their infancy, there is much to be done before definite results are reached. Combining all of the above, when a packet containing executable code arrives at a node, the system must:

- Accept the authenticity of the credentials of the packet
- Identify the sending network element
- Identify the sending user
- Authorize access to appropriate resources based on these identifications and credentials
- Allow execution based on the authorizations and security policy
- Monitor and control access to system resources throughout the execution
- If needed, encrypt the packet to protect its code and data in transit
- To performs connection to access the data
- Send signal to block the connection

If the packet is not identified properly, then it may be allowed to execute the code in a restricted environment or it may not be allowed to execute the code at all.

INTRUSION BLOCKING

The administrator then sends an intrusion blocker directly to the routers connected to vulnerable customer systems. The blocker looks for traffic that matches the attack signature directed at the vulnerable systems— by executing the blocker only on routers where it is necessary and only to prevent specific threats to known vulnerable systems, the overall performance impact is reduced. When an attack is attempted, the blocker drops the offending traffic and no longer allows communication on that connection. This focus allows the blocker to be lightweight, while still allowing valid traffic.

The second intrusion blocker implementation uses the Active Signal Protocol (ASP) Execution Environment, a Java-based EE, also part of the Active Networks program. ASP was chosen because it offers more control over low-level network functions. The new blocker implementation uses adaptive migration— a technique to migrate the blocker based on dynamic network conditions— and also operates on the high-end Intel IXP 1200 network processor. The IXP represents next-generation high-speed network processing systems that could be used for programmable routers.

The second blocker adaptively migrates, based on resource constraints. It can determine when the router where it is executing is under greater network or processing load. Under greater loads, it might not be able to monitor for potentially malicious traffic and still forward unmonitored traffic. When the blocker identifies a potential overload condition, it attempts to migrate to more powerful neighbouring routers, such as an IXP 1200. Another example of adaptive migration would allow protection of a network whose router's security policy does not allow the blocker. When a blocker fails to migrate to such a router, it could run on neighbouring routers instead. The AN-IDR project is concluding by measuring the performance of the Mobile Intrusion Blocker on the ASP platform. This performance testing is intended to determine if the ASP EE is a viable platform and whether the intrusion blocker can perform sufficiently for real world deployment.

AGENT BASED SYSTEM

This agent based system describes a preliminary model we are developing for use in managing network defences in a active manner. It combines an agent-based strategy for investigation and response with an updated version of the HUMMER collaborative intrusion detection system. The original HUMMER system provides for gathering and distributing data across enterprise boundaries, allows for multiple "observation points" of intrusions, and can be used to manage intrusion response for both individual and aggregate sites.

Combined with this framework, we provide for multiple instances of intrusion detection, specific use agents. These agents are sent to network nodes, and may be used to monitor or seek out a specific network or host-based event, or sequences of such events. Agents are classed as "tool agents", "investigation agents", and "defensive agents". We have developed simple instances of both tool and investigation agents, and are working towards a model of defensive agents. Agents are integrated with the collaborative IDS in order to provide them with a wider array of information to use in their response activities. This provides for adaptive defence, while still permitting agents to remain small, and without losing the advantages of a traditional, stationary IDS.

In combination with the agent system above, we are investigating a method for intelligently determining where network attacks are occurring based on techniques. These techniques will be used to aid Investigation by permitting us to predict where to look for intrusions in progress. We divide the agents we dispatch into three categories: "tool agents", "investigation agents", and "defensive agents". Our Tool agents are primarily used to manage data-gathering tools, and they are present primarily to allow roving investigators to perform independently of Hummer (although not, of course, of the agent environment Tahiti). These agents examine log files or look at system features, and they have the advantages of being lightweight and of being activated only when needed for a specific purpose.

Investigation agents are in a sense the "brains" of the Magpie system. These agents control investigations of incidents of misuse; they may dispatch tool or defensive agents, or communicate with the HUMMER system to obtain data. The investigation agents can move between systems, which makes them harder for an attacker to eliminate (future implementations will allow for redundancy of investigation agents).

Defensive agents will be used to provide for system defences. In the long term, defensive agents will be able to directly manage a host (or network)'s defensive posture. At present, our prototype is intended to be far more limited, and

we will allow our defensive agents to work only by influencing the HUMMER perceived level of threat, which HUMMER uses to modify network defences.

PROPOSED SYSTEM

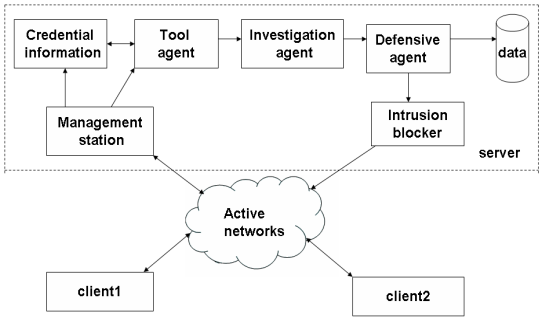

Figure 1

Our proposed system management station provides a signature to the client. The client access data through digital signature. The digital signature and credential information about client are stored in the server in a file. The management station initiates the operation. The agent based system used to collect information, intrusion detection and response. Three types of agents used in this system

Tool agent to collect relevant information and credential information Investigation agent to detect the intrusion based on the detection policy Defensive agent send signal to blocker when detection identified otherwise to make connection to access the data.

The intrusion blocker detects a specific threat by inspecting only for the vulnerable service if it determines an attack is being attempted it blocks the attack and stops future traffic on the connection while allowing subsequent connections. The blocker recognizes the attack signature, drops the attack packet and sets the connection state to drop any remaining traffic. An alert is sent to the management station which enables the administrator to see that an attack was attempted.

SANTS is an active networks EE that provides authentication and authorization services based on digital certificates. SANTS provide strong end to end authentication to enable per-method authorization enforcement. SANTS also provides key and certificate management services. The management station to initiate agent based system. The intrusion detected by the system its information sends to the management station. Then intrusion blocked that information also inform to the management station.

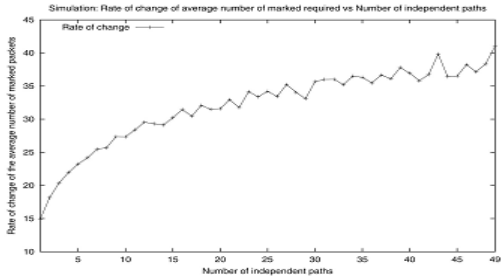

Figure 3: An Increasing Trend in the Rate of Change in the Number of Marked Packets Required

First, one cannot apply the termination condition to complex networks such that the reconstruction of one path is dependent on another. This scenario can be explained in and this presents a multiple-attacker environment. In this graph, the attack packets traversed through eight paths that are identical in structure. However, there are “shared” edges

Among these paths, this implies that the reconstruction of one path is dependent on another. Therefore, one cannot treat (1) as the termination conditions under this scenario and this Restricts the application of the PPM algorithm. Second, although every path in a given network is independent, we have found that the number of marked packets needed to reconstruct the network graph does not have a linear relationship with the number of paths; that is, the claim made is not correct. We have carried out a set of simulations to show our finding and we start the description of our simulation setup from the network depicted in Figure 1. The network contains four paths that are identical in structure and, more importantly, there are no shared edges between any two paths. We name these paths the independent paths.

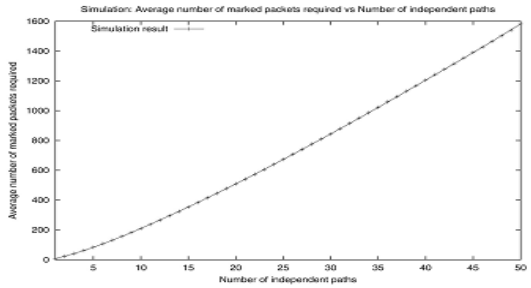

Figure 2: The Relationship Between the Number of Independent paths and the Average Number of Marked Packets Required

We then carry out a simulation to obtain the average number of marked packets required to reconstruct the paths. Next, we repeat this simulation, but this time, we add one more independent path to the network, and there are now five independent paths. Eventually, we perform a series of simulations for one to 50 independent paths. Figure 2 shows the result of this set of simulations. One can observe that the average number of marked packets required to construct a correct constructed graph increases as the number of independent paths increases. In order to show whether the number of required marked packets linearly increases with the number of paths or not, we plot the rate of change in the number of required marked packets in Figure 3. Surprisingly, the graph shows an increasing trend in the rate of change in the number of required marked packets. The claim about the multiple-attacker environment made in is therefore wrong. The or ethically, the packet collecting problem can be transformed into the “coupon-collecting problem with unequal probabilities”. In sum mar y, the first problem of using (1) as the termination condition is that the relationship between the number of attack paths and E ½ X is not known. Therefore, the PPM algorithm cannot guarantee the correctness under the multiple-attacker environment.

Our first requirement is a new payload (called as P3M payload) carrying router address and path identification to avoid influencing the normal running of recombining packets and QoS mechanism.

PATH IDENTIFICATION SCHEME

Our second requirement is a new path identification scheme based on router addresses. The use of path identification makes our probabilistic packet marking technology P3M simple when victim computes DDoS attack paths. And path identification also could be used by other network security equipment. For path identification, we are constructing a graph such that the constructed graph is the same as the attack graph, where an attack graph is the set of paths the attack packets traversed, and a constructed graph is a graph returned by the PPM algorithm. To fulfil this goal, Savage et al. suggested a method for encoding the information of the edges of the attack graph into the attack packets through the cooperation of the routers in the attack graph and the victim site.

ENCODED EDGE RANDOM VARIABLE

By definition, an incoming packet may encode one of the edges of the attack graph, or the incoming packet does not encode any edges of the attack graph. We use a random variable called the encoded edge random variable to represent all possible encodings on an incoming packet. For each value of the encoded edge random variable, there is a corresponding probability for that value and it is called the packet-type probability.

CONCLUSIONS

First contribution is constructing a new payload to carry router address and path identification. The second contribution is designing a new path identification scheme based on router addresses and hash algorithm. P3M is a practical technology to defence DDoS.

ACKNOWLEDGEMENTS

The author is extremely thankful for the respected guide for their encouragement.

REFERENCES

1. Software Engineering – A Practitioners Approach, 7th Edition by Pressman UML User Guide, By Grady Booch, James Rumbaugh and Ivar Jacobsan F. Baker. Requirements for IP Version 4 Routers. RFC 1812, June 1995.
2. S. Savage, D. Wetherill, A. Karl in, and T. Anderson, “Network Support for IP Trace back,” IEEE/ACM Trans. Networking, vol. 9, pp. 226-237, Jun. 2001.
3. D. Song and A. Perrig, “Advanced and Authenticated Marking Schemes for IP trace back,” IEEE INFOCOM 2001, Anchorage, AK.
4. A Year, A. Perrig, and D. Song, “Fast Internet Trace back,” IEEE INFOCOM 2005.
5. T. Peng, C. Leckie and R. Kotagiri, “Adjusted Probabilistic Packet Marking for IP trace back,” Proc. Of Networking, 2002, Pisa, Italy, May 2002.
6. J. Liu, Z. Lee, and Y. Chung, “Efficient dynamic probabilistic packet marking for IP trace back,” the 11th International Conf. Networks (ICON 2003), Sydney, Australia, Sep. 2003.
7. B. Rizvi and E. Fernandez-Gaucherand, “Analysis of adjusted Probabilistic Packet Marking,” IP Operations & Management (IPOM2003), Kansas City, MO, Oct. 2003.
8. M. Adler, “Tradeoffs in Probabilistic Packet Marking for IP Traceback,” Annual ACM Symp. Theory of Computing’02, Quebec, Canada, 2002.
9. H. Aljifri, M. Smets and A. Pons, “IP trace back using header compression,” Computer & Security, vol. 22, pp. 136-151.