CONTROLLING IP FALSIFYING USING REALISTIC SIMULATION

Govindavaram Madhusri [1]

Assistant Professor, Dept. of Informatics
University PG college, Kakatiya University, Warangal
Madhu.gsr@gmail.com
Dr.Chakunta Venkata Guru Rao [2]
Professor & Head, Dept. of Computer Science & Engineering
SR Engineering college, JNTU University, Warangal
Guru_cv_rao@hotmail.com

ABSTRACT

The study of Internet-scale events such as worm proliferation, distributed denial-of-service attacks (DDoS), flash crowds, routing volatilities, and DNS attacks depend on the formation of all the networks that generate or forward valid and malevolent traffic,The Distributed Denial of Services (DDoS) attack is a serious threat to the valid use of the Internet. Forestalling mechanisms are disappointed by the ability of attackers to steal, or spoof, the source addresses in IP packets. IP falsifying is still widespread in network scanning and investigates, as well as denial of service floods.IDPFs can limit the falsifying capability of attackers. Moreover, it works on a small number of candidate networks easily traceable, thus simplifying the reactive IP trace back process. However, this technique does not allow large number of networks, which is a common misapprehension for those unfamiliar with the practice. Current network simulators cannot be used to study Internet-scale events. They are general-purpose, packet-level simulators that reproduce too many details of network communication, which limits scalability. We propose to develop a distributed Internet simulator, with the following novel features. It will provide a built-in Internet model, including the topology, routing, link bandwidths and delays, Instead of being a general-purpose simulator, it will provide a common simulation core for traffic generation and message passing, on top of which we will build separate modules that customize messages and level of simulation details for the event of interest. Customization modules will ensure that all and only the relevant details of the event of interest are simulated, cutting down the simulation time. We will also provide an interface for new module specification, and for existing module modification, this will bring the Internet event simulation at the fingertips of all interested researchers. The simulator will promote research in worm detection and defense, IP falsifying prevention and DDoS defense.

KEYWORDS

IP Falsifying, DDoS, BGP, Network-level Security and Protection, IDPF, Network Simulation Tool.

1 .INTRODUCTION

IP falsifying is most difficult attack in internet like DDos attacks, here the sender sends the information to the receiver, at times attacker may intrude and may hack the information and he acts like proxy and sends the information to receiver for which the sender denies that it was not sent by him. Since a cracker are purely concentrated on bandwidth and resources but does not concentrate on the transactions, rather, they wish to flood many packets to the victim or sender in short duration. To make it effective, they block all the ways by falsifying source IP addresses and also the distributed Dos attack with spoofing quickly blocks the traffic. Here the master sends the

information to the slaver and slaver steals the information sends to the victim. When multiple compromised hosts are participating in the attack, all sending forged traffic; it is very challenging to quickly block traffic. While some of the attacks described above are become old and outdated, such as session hijacking for host-based authentication services, IP falsifying is common network scanner and explorer as well as denial of service floods. Even though they can steal the address, they cannot trace the best path to the destination. Due to this Park and Lee proposed the route-based packet filters as a way of valid or valid IP falsifying.

IDPFs can limit the falsifying capability of attackers. Moreover, it works on a small number of candidate networks easily traceable, thus simplifying the reactive IP trace back process. However, this technique does not allow large number of networks, which is a common misapprehension for those unfamiliar with the practice. Any sort of falsifying beyond simple floods is relatively advanced and used in very specific instance such as avoidance and connection skyjack.

The problems in Inter-scale events have been noticed that they harm the traffic. The dynamics of Internet-scale events such as worm propagation, distributed denial-of-service attacks (DDoS), flash crowds, routing instabilities, and DNS attacks depend on the configuration of all the networks that generate or forward valid and malevolent traffic.

To understand these problems or events researchers need simulation tools to know their occurrence, network, topology in detail. To know these problems researchers need simulation tools that reproduce all the relevant event details and event traffic's interaction with the Internet architecture. Collaborative defenses against Internet-scale attacks have also been proposed. The effectiveness of these defences depends on Internet topology, so high-loyalty Internet simulation is necessary to properly evaluate these defenses.

Now day's network simulators cannot be used to study these Internet-scale events. No simulator is up to the mark. They work only small number of candidate networks. They are general-purpose, packet-level simulators that reproduce too many details of network communication, which limits scalability. Even distributed versions of network simulators such as GTNetS and PDNS, designed for large-scale events, have limited scalability because each packet and its handling are simulated in minute detail. For example, PDNS requires powerful, 100+ CPU clusters, to simulate worm propagation with up to 1.28 M vulnerable hosts. Many researchers do not have an access to such a large cluster.

Another drawback of the existing network simulators is that they lack a built-in Internet model. Researchers who try to simulate Internet-scale events must use their own topology, and determine end-host communication patterns, link bandwidths and routes. The effort required to set up a realistic Internet model from scratch is considerable so many researchers adopt simplified models- assuming infinite bandwidth links, assuming highly symmetric Internet topology etc. which leads to incorrect results.

The idea of packet filters constructed based on the global routing information is encouraged by the work carried out by Zhenhai Duan, Xin Yaun, and Jaideep Chandrashekar who explained that IDPFs rely on BGP update messages exchanged on the Internet to gather the legality of source address of a packet forwarded by a neighbor.

Zhenhai Duan, Xin Yaun, and Jaideep Chandrashekar who explained that the IDPF framework can correctly work without discarding any valid packets have been considered. Here The IDPF

can work within a small number of candidate networks, thus simplifying the reactive IP trace back process.
Wei, Calvin, Jelena and Halefia explained that writing simulator either takes a very long time to be done right or it results in inexperienced approximations that do not match real worm spread conditions and potentially produce invalid results.

Songjie Wei and Jelena Mirkovic showed that the design and implementation of a distributed worm simulator, repeats a realistic Internet environment and its interaction with a simulated worm. This detailed and realistic Internet simulation leads to high fidelity reconstruction of the worm spread events. Researchers can investigate clogging effects of Internet worm spread and its interactions with the background traffic.

The IDPF architecture served as an effective counter measure to the IP falsifying-based DDoS attacks. IDPFs rely on BGP update messages exchanged on the Internet to gather the legality of source address of a packet forwarded by a neighbor.

Here we are minimizing denial of service attacks. For finding possible path we don't need global routing. IDPFs can easily be deployed on the current BGP-based Internet routing architecture. The conditions under which the IDPF framework can correctly work without discarding any valid packets have been studied. IDPFs can limit the falsifying capability of attackers. Moreover, it works on a small number of candidate networks easily traceable, thus simplifying the reactive IP trace back process. However, the technique does not allow large number of networks.

This technique does not allow large number of networks which is a common misapprehension for those unfamiliar with the practice. Any sort of falsifying beyond simple floods is relatively advanced and used in very specific instances such as evasion and connection hijacking.

A worm researcher today must test her hypotheses either by writing a complex simulator from scratch, arranging a proposed system in a real network or repeating a full-packet trace detained from a real network. On the other hand few researchers can initiate the installation of research-grade systems in real networks, or obtain full-packet traces with privacy sensitive data. We concluded from analyzing current worm research that Internet wide solutions must be evaluated with a large-scale, realistic simulation of a worm spread in the Internet environment, while localized solutions require realistic worm and valid traffic conditions in a local network. To support Internet-wide experiments, a scalable, high-fidelity worm spread simulator, was developed and demonstrated through experiments that it can be easily tailored to meet current and future worm researchers' needs.

It may lead to faster prototyping of worm solutions, and easier, more uniform testing. The biggest advantage is an improved realism of worm tests and leveling of worm. The test realism should increase through use of simulator because of its high loyalty in reproducing worm spread events. The leveling of the playing field should occur because it enables tests that previously could only be done by a handful of researchers who either had access to full-packet traces or could install their solutions in real networks.

Database of exploits, worm payloads and valid traffic traces must be enlarged thus increasing diversity of possible tests researchers can perform in simulation framework. The user interface for both tools, to ease their espousal by other researchers must to be improved. These tools should help researchers understand the worm phenomenon and realistically test any defenses they build.

The distributed worm simulator repeats a realistic Internet environment and its interaction with a simulated worm. This detailed and realistic Internet simulation leads to high loyalty construction of the worm spread events. By using the simulator, researchers can investigate clogging effects of Internet worm spread and its interactions with the background traffic.

It supports various user- customizable parameters that can be specified for each simulated host, which facilitates testing of different host and network diversity models, worm scanning strategies and Internet topologies. It also supports for faithful simulation of complex Internet-scale events and validates the correctness of the simulator.

It does not supports for imitation of other Internet-scale events, like distributed denial-of- service (DDoS) attacks, flash-crowd events, botnet recruitment , spam, etc. The Internet model must be improved with more realistic data and dynamics, such as the simulation of the routing dynamics and routing interaction with the clogging events, and the simulation of the time-variable traffic demand and offer between the Autonomous System pairs.

The existing network simulators cannot be used to study Internet-scale events. They are general-purpose, packet-level simulators that reproduce too many details of network communication, which limits scalability. Even distributed versions of network simulators such as GTNetS and PDNS, designed for large-scale events, have limited scalability because each packet and its handling are simulated in minute detail. For example, PDNS requires powerful, 100+ CPU clusters, to simulate worm propagation with up to 1.28 M vulnerable hosts. Many researchers do not have an access to such a large cluster. Another drawback of the current network simulators is that they lack a built-in Internet model. Researchers who try to simulate Internet-scale events must use their own topology, and determine end-host communication patterns, link bandwidths and routes. The effort required to set up a realistic Internet model from scratch is considerable so many researchers adopt simplified models- assuming infinite bandwidth links, assuming highly symmetric Internet topology etc. which leads to incorrect results.

We propose to develop a distributed Internet simulator, with the following novel features, It will provide a built-in Internet model, including the topology, routing, link bandwidths and delays, Instead of being a general-purpose simulator, it will provide a common simulation core for traffic generation and message passing, on top of which we will build separate modules that customize messages and level of simulation details for the event of interest. Customization modules will ensure that all and only the relevant details of the event of interest are simulated, cutting down the simulation time. We will also provide an interface for new module specification, and for existing module modification, this will bring the Internet event simulation at the fingertips of all interested researchers.

It allows us to disturb flows over an IP network helping to study the behavior of applications, devices or services in a disturbed network environment. We will further provide customization modules for simulation of popular worm defenses, distributed denial of service attacks and popular DDoS defenses, and IP falsifying and popular falsifying defenses.

The proposed simulation tool is an IP network simulator software that can generate impairments over IP networks such as: latency, delay, jitter, bandwidth limitation, loss, duplication, falsifying and modification of the packets.

This report is organized into four chapters. The first chapter gives the introduction of the project and tells the objective of the work, it tells the reason and motivation behind this work, theoretical

background necessary to understand the results in simulation tool is reviewed. The IP falsifying-based DDoS attacks and other threats to internet have been explained.. Chapter 2 explains about the comprehensive survey of IDPF, falsifying attacks and simulation tools on internet. It covers problems of existing simulators Chapter 3 explains the existing network simulators demerits and merits and also explains about current network simulators. Chapter 4 summarizes the work done by giving conclusion.

2. LITERATURE SURVEY

Research in time-sharing is provided by a collection of programs whose elaborate and strange design outgrowth of many years of experience with earlier versions. To help develop a secure system, we have continuing competition to devise new way to attack the security of the system (the bad guy) and, at the same time, to device new techniques to resist the new attack (the good guy) . This competition has been in the same vein as the completion of long standing between manufactures of armor plate and those of armor – piercing shells. For this reasons, the description that follows will trace the history of IP falsifying and packet routing rather than just sending a data normally without any encryption in the network.

The greatest threat to servers connected to the internet is TCP hijacking [9] (also known as active sniffing). Although TCP sequence-number prediction and TCP hijacking have many similarities, TCP hijacking differs because the hacker gains access to the network by forcing the network to accept the hackers IP address as a trusted network address rather than forcing the hacker to guess IP addresses until one works. Here, the hacker gains control of computer that links to the hackers target network then disconnects that computer from the network and fools the server into thinking that the hacker has taken the actual hosts place. After the hacker successfully hijacks the trusted computer, the hacker replaces the target computer IP address within each packet with the hackers IP address and spoofs the targets sequence numbers. Security professionals call sequence number simulation IP forging. A component to ITS to improve its scalability using Bloom filters is added. Implementing ITS using Bloom filters is simple, saves a substantial amount of router memory, and does not impose large strain on routers. The basic method to allow for it to be incrementally deployed is shown. The efficiency of the method is demonstrated through simulations by using real world Internet data. For many years the research community has been committed to combating IP forging existing approaches to handle forged IP source addresses, A hierarchical, Inter-domain[10] authenticated source address validation solution named Safe Zone. Safe Zone employs two intelligent designs, lightweight tag replacement and a hierarchical partitioning scheme, each of which helps to ensure that SafeZone can construct trustworthy and hierarchical trust alliances without the negative influences and complex operations on de facto networks. Extensive experiments also indicate that Safe Zone can effectively obtain the design goals of a hierarchical architecture, along with lightweight, loose coupling and “multi-fence support” and as well as an incremental deployment scheme.

The idea of IDPF is motivated by the work carried out by Park and Lee [1], which was the first effort to evaluate the relationship between topology and the effectiveness of route based packet filtering. They showed that packet filters that are constructed based on the global routing information can significantly limit IP spoofing when deployed in just a small number of ASes. In the Network Ingress Filtering proposal described in [2], traffic originating from a network is forwarded only if the source IP in the packets is from the network prefix belonging to the network. Ingress filtering primarily prevents a specific network from being used to attack others. Thus, while there is a collective social benefit in everyone arranging it, individuals does not

receive direct incentives. The main drawback is that the filter nodes require precise knowledge of the routing choices made at all other ASes. Given the decentralized, autonomous nature of inter-domain routing, this requirement is hard to reconcile. We extend this idea in our own work and demonstrate how filters can be constructed using only local routing information. Unicast reverse path forwarding (uRPF)[14], requires that a packet be forwarded only when the interface that the packet arrives on is exactly the same used by the router to reach the source IP (in the packet). If the interface does not match, the packet is dropped. While simple, the scheme is limited given that Internet routing is inherently asymmetric, i.e., the forward and reverse paths between a pair of hosts are often quite different.

Bremler-Barr and Levy proposed a spoofing prevention method (SPM) [5], where packets exchanged between members of the SPM scheme carry an authentication key associated with the source and destination AS domains. Packets arriving at a destination with an invalid authentication key(with respect to the source) are spoofed packets and are discarded. In Hop-Count Filtering (HCF) [11], each end system maintains a mapping between IP address aggregates and valid hop counts from the origin to the end system. Packets that arrive with a different hop count are mistrustful and are therefore discarded or marked for further processing. Bremler-Barr and Levy proposed a spoofing prevention method (SPM) [12], where packets exchanged between members of the SPM scheme carry an authentication key associated with the source and destination AS domains. Packets arriving at a destination with an invalid authentication key(with respect to the source) are spoofed packets and are discardedWorm researchers have also implemented their own worm simulators to examine worm dynamics and to validate various approaches for worm spread detection and defense [3] [4] [5]. Packet level simulation generates a network message for each packet sent to a different simulation node which incurs huge overhead when simulating high-rate worm scans. Instead, these transmissions can be aggregated and sent in a single network message at the end of a simulated time unit. Writing a simulator either takes a very long time to be done right or it results in naive approximations that do not match real worm spread conditions and potentially produce invalid results [6]. A distributed worm simulator repeats a realistic Internet environment and its interaction with a simulated worm. This detailed and realistic Internet simulation leads to high loyalty reconstruction of the worm spread events. Researchers can investigate clogging effects of Internet worm spread and its interactions with the background traffic [7]. These simulators replicate Internet layers in greater detail and simulate each traffic flow and each packet separately. While this is beneficial for small scale simulation, it results in a prohibitively slow and nonscalable simulation of Internet-wide events. With regard to fluid (aggregate) traffic simulation, model flows at coarse time-scales. In their model, each sender and receiver is associated with a variable-rate traffic stream, and the aggregated flow on each link is computed iteratively, hop-by hop, and along the routing path until it converges. It simulates the interaction between some foreground traffic of interest, at the packet level, and the background flows, at the fluid level, using a discrete-event formulation. It also avoids iterative, hop-by-hop, traffic simulation which would prohibitively increase simulation time, while bringing a small gain in accuracy.

Inter-domain packet filter (IDPF) architecture acts as an effective countermeasure to the IP spoofing-based DDoS attacks. IDPFs rely on BGP update messages exchanged on the Internet to infer the validity of source address of a packet forwarded by a neighbor. These can be easily deployed on the current BGP based Internet routing architecture. These conditions were studied under which the IDPF framework can work correctly without discarding any valid packets [8]. Our simulation results showed that, even with partial deployment on the Internet, IDPFs can significantly limit the spoofing capability of attackers. Moreover, they also help pinpoint the true

origin of an attack packet to be within a small number of candidate networks, therefore, simplifying the reactive IP trace back process.

3. PROPOSAL FOR RESEARCH

The study of Internet-scale events such as worm proliferation, distributed denial-of-service attacks (DDoS), flash crowds, routing volatilities, and DNS attacks depend on the configuration of all the networks that generate or forward valid and malevolent traffic. Collabarative defenses against Internet-scale attacks have also been proposed. The effectiveness of these defenses depends on the underlying Internet topology and the deployment locations, so high-loyalty Internet simulation is necessary to properly evaluate these defenses. Researchers that aim to simulate Internet-scale events must themselves assemble the Internet topology, and determine end-host communication patterns, link bandwidths and routes. The effort required to set up a realistic Internet model from scratch is considerable so many researchers adopt simplified models-assuming infinite bandwidth links, assuming highly symmetric Internet topology, which leads to incorrect results. It takes long time to be done right or it results in inexperienced approximations that do not match real worm spread conditions and potentially produce invalid results. The proposed research work tries to overcome them. This detailed and realistic Internet simulation leads to high loyalty reconstruction of the worm spread events. Researchers can investigate clogging effects of Internet worm spread and its interactions with the background traffic.

We propose to develop a distributed Internet simulator, with the following novel features, It will provide a built-in Internet model, including the topology, routing, link bandwidths and delays, Instead of being a general-purpose simulator, it will provide a common simulation core for traffic generation and message passing, on top of which we will build separate modules that customize messages and level of simulation details for the event of interest. Customization modules will ensure that all and only the relevant details of the event of interest are simulated, cutting down the simulation time. We will also provide an interface for new module specification, and for existing module modification, this will bring the Internet event simulation at the fingertips of all interested researchers. The proposed simulation tool is IP network simulator software that can generate impairments over IP networks such as latency, delay, jitter, bandwidth limitation, loss, duplication, falsifying and modification of the packets.

The proposed simulator will create opportunities for teachers, students and researchers to imitate and study Internet behaviour in a variety of settings. It will promote research in worm detection and defence, IP spoofing prevention and DDoS defence. We further expect that the simulator will be extended by interested researchers to add novel event models and thus will expand its customer base. The simulator will be open source, written in C++ following object oriented programming principles and with a modular architecture.

4. CONCLUSION

In this paper we proposed and studied a distributed Internet simulator, as an effective countermeasure to the IP

Falsifying-based DDoS attacks. It will provide a built-in Internet model, including the topology, routing, link bandwidths and delays, Instead of being a general-purpose simulator, it will provide

a common simulation core for traffic generation and message passing, on top of which we will build separate modules that customize messages and level of simulation details for the event of interest. Customization modules will ensure that all and only the relevant details of the event of interest are simulated, cutting down the simulation time. We will also provide an interface for new module specification, and for existing module modification, this will bring the Internet event simulation at the fingertips of all interested researchers. It allows us to disturb flows over an IP network helping to study the behavior of applications, devices or services in a disturbed network environment. We will further provide customization modules for simulation of popular worm defenses, distributed denial of service attacks and popular DDoS defenses, and IP falsifying and popular falsifying defenses.

5. REFERENCES

[1] K. Park and H. Lee. On the effectiveness of route-based packet filtering for distributed DDoS attack prevention in power-law internets. In *Proc.ACM SIGCOMM*, San Diego, CA, August 2001.

[2] P. Ferguson and D. Senie. Network ingress filtering: Defeating denial of service attacks which employ ip source address s poofing. RFC 2267, January 1998

[3] C. C. Zou, W. Gong, and D. Towsley, "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," in Proceedings of ACM CCS Workshop on Rapid Malcode (WORM'03), October 2003.

[4] D. Moore, C. Shannon, G. Voelker, and S. Savage, "Internet Quarantine: Requirement For Containing Self-Propagating Code," in Proceedings of the *IEEE INFOCOM*, April 2003.

[5] N. Weaver, I. Hamadeh, G. Kesidis, and V. Paxson, "Preliminary Results Using Scale Down to Explore Worm Dynamics," in Proceedings of ACM CCS Workshop on Rapid Malcode (WORM'04), October 2004.

[6] Songjie Wei, Calvin ko, Jelena Mirkovic and Alefia Hussain "Tools for Worm Experimentation on the DETER Testbed".

[7] Songjie Wei, Jelena Mirkovic, Martin Swany Distributed Worm Simulation with a Realistic Internet Model.

[8] ZhenhaiDuan,Member,IEEE,XinYuan,Member,IEE,andJaideepchandrashekar,Member, IEEE "Controlling IP Spoofing Through Inter-Domain Packet Filters"*IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING.VOL.5NO.1JANUARY-MARCH 2008.*

[9] Hacker Proof: The Ultimate Guide to Network Security

[10] Safe Zone: A Hierarchical Inter-Domain Authenticated Source Address Validation Solution Jie Lia, Jian-ping, Ke Xu

[11] C. Jin, H. Wang, and K. Shin. Hop-count-filtering: an Effective defense against spoofed DDoS traffic. In *Proceedings of the 10th ACM conference on Computer and communications security*, October 2003.

[12] A. Bremler-Barr and H. Levy. Spoofing prevention method. In *Proc. IEEE INFOCOM*, Florida, March,05.

[13] A Realistic Simulation of InternetScale Events:Songjie Wei and Jelena Mirkovic Department of computer and Information Sciences University of Delaware Newark.

[14] F.Baker, "Requirements for IP Version 4 Routers, "RFC 1812,June 1995.

Authors Biography:

G. Madhu sri received the M.C.A degree in Computer Applications from Alluri Institute of Technology, Warangal, India and M.Tech degree in Comput er Science from JNTUCEH, Hyderabad, India and She is doing Ph.D Informatics in Osmania University, Hyderabad, India. Currently she is an Assistant Professor in the department Computer Science, University Post Graduate College, Warangal, India. Her area of research interests includes Data Mining and Warehousing, Network Security, Software Engineering.

Dr.C.V.Guru Rao was born in India, A.P,. He received his B.Tech degree from Nagarjuna University, MTech degrees from REC, Warangal, M.E form MNREC, Alahabad and ph.D from IIT Khargpur and Know he is working as Prof in Computer Science & Engineering department, SR Engineering College, Warangal. His area of research includes Computer Science & Engineering with specialization in VLSI and Embedded Systems, Software Engineering, Data Mining and Warehousing.