ISSN No. 0976-5697

Volume 4, No. 8, May-June 2013

International Journal of Advanced Research in Computer Science

CASE STUDY AND REPORT

Available Online at www.ijarcs.info

A Survey on Secure Source-Controlled Forwarding Mechanism

Somnath Jagdale[*], Dr. B. B. Meshram[**]

[*,**]Department of Computer Science, Veermata Jijabai Technological Institute, India

somnath.jagadale@gmail.com

Abstract **-** Most of the time we provide security to the our internet by application layer perspective so attacker trying to exploit at network layer by ip snooping and ip spoofing, Man-in-middle attack and ARP spoofing. Previous various researches provided solution for this but all that solution require more effort to implement in real world and all networking node should be designed with fully intelligent capability. In this paper we introducing the secure source routing mechanism in which end user gives control over routing and achieving the flexible communication. The main technique we introducing in this paper is simple crypto graphical constraints on routing entries. We show that it is possible to prevent major attacks on end-host and restrict all types of flooding attacks that are launched on network infrastructure nodes to small constant value.

Index terms **-** internet architecture, routing attacks, security, constraints, network pointers.

I. INTRODUCTION

Originally internet defined with little support for traffic policies and flexibility in packet forwarding but now recognize that present wide area internet does not focused on potential of current deployed architecture in terms of performance and reliability and security .while number of techniques are invented to improve flexibility in routing infrastructure mainly source controlled routing destination path selection improving the flexibility and security in communication. We are here to understand and analyze issues regarding creating scalable, authenticated, policy predicted wide area source routing [1]. We show that it is possible to prevent major attacks on end host and restrict all types of flooding attacks that are launched on network infrastructure nodes to small constant value. Also By use of source routing mechanism we can improve routing performance through path selection policies.

The first will choose same minimal path from source to destination and second will choose from different alternate minimal around round-robin fashion. The evaluation result showing that total forwarding throughput can be doubled for large network[7].Designing infrastructures that give end-hosts control over routing. The flexible control plan of these infrastructures can be exploited to avoid many types of powerful attacks with little effort. Source or destination controls the routing of packets. It provides route information into the identification field of packets That information will takes all forwarding decision. Source controls the routing of packets throughout its gurney. It provides route information into the identification field of packets[2]. That information will takes all forwarding decision. Infrastructure that gives control over routing to user such as end hosts for achieving flexible and efficient communication.

Our traditional IP network is more vulnerable to attack at network layer because most of the security application or protocols are applied to the application layer and transport layer. It's easy for attacker to change routing table entries in the router and divert all traffic through his malicious host.

Several recent proposals have argued for giving third parties and end-users control over routing in the network infrastructure. Some examples of such routing architectures include i3, Data Router, and Network Pointers. Using such control, hosts can achieve many functions that are difficult to achieve in the Internet today (WAN). Examples of such functions include mobility, multicast, content routing, and service composition. While each of these specific functions can be achieved using a specific mechanism.

For example, mobile IP allows host mobility we believe that these *forwarding infrastructures* (FIs) provide architectural simplicity and uniformity in providing several functions. For instance, consider which is a routing system that allows hosts to insert forwarding entries of the form (id,R) , so that all packets addressed to id are forwarded to R. An attacker A can eavesdrop subvert the traffic directed to a victim V by inserting a forwarding entry (idv, A) into its routing table; the attacker can eavesdrop even when it does

II. MODULE DESCRIPTION

We construct a acyclic topology by using node names and their connections. For each node we obtain IP address and port number. We also decide the node hierarchy and determine the paths for each pair of machines. For each path we compute the cost. Node duplication is avoided during the computations [4].

A. Computation phases:

- ***a. Hop login:*** During message transfer, we register hop name, hop password and port number.
- ***b. Encryption:*** We encrypt the message to be transferred using a key. Each router examines the header information and then forwards the message packets. Each router must decrypt the header to verify if it is on the specified path[4].
- ***c. Decryption:*** Decryption is done by each router on the path and also by the destination. A user can change the path value at any time. Therefore it is necessary for the final router and destination to check the cost value[4].

B. SSR Working:

The source of an internet datagram to supply routing information to be used by the gateways or routers in forwarding the datagram to the destination.

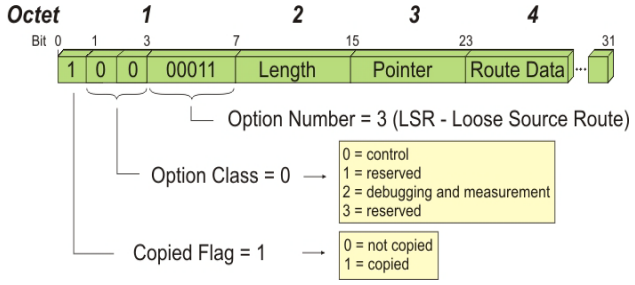

Figure: 2.1 Source Datagram

The Routing header is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination. Loose source routing uses a source routing option in IP to record the set of routers a packet must visit. The destination of the packet is replaced with the next router the packet must visit. By setting the forwarding agent (FA) to one of the routers that the packet must visit, LSR is equivalent to tunneling. If the corresponding node stores the LSR options and reverses it, it is equivalent to the functionality in mobile IPv6[7].

III. ATTACKER THREATS MODEL

We have considered two attacker types:

- ***a. Internal attackers-*** An internal attacker is an adversary who controls some compromised FI nodes or router.
- ***b. External attackers-*** An external attacker does not control any compromised FI node but misuses the flexibility given by the FI. An external attacker can perform only the operations at legitimate host can: insert a forwarding entry and send a packet. An external attacker does not control any compromised FI node but misuses the flexibility given by the FI. Some Attacks,

A. Eveasdroping:

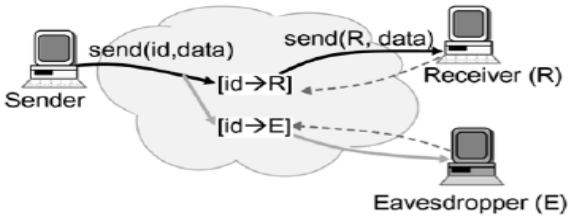

Figure: 3.1 Packet Eavesdropping

Consider an end-host **R** that inserts a pub-lic forwarding entry **[id→R]** (see Figure). An attacker **E** can eavesdrop on packets sent to **R** by inserting a forwarding entry **[id→E]**. All packets that are forwarded via **[id→R]** will be replicated and forwarded via **[id→E]** to **E** as well[5].

B. End host enfloence:

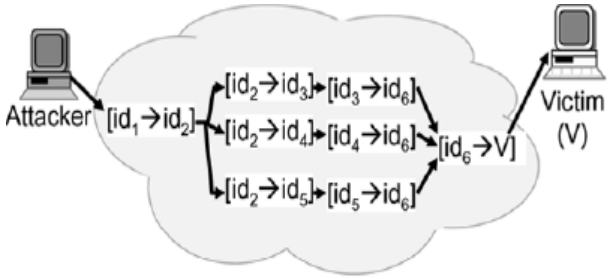

Figure: 3.2 End-host Confluence

By constructing a tree and making the leaves of the tree point to the public identifier of an end-host (see Figure), an attacker can overwhelm the host. Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper. Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression, “One of us (R.B.G.) thanks . . .” Instead, try “R.B.G. thanks”. Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

IV. MODELS OF SSR

A. Identifiers and Forwarding Entries:

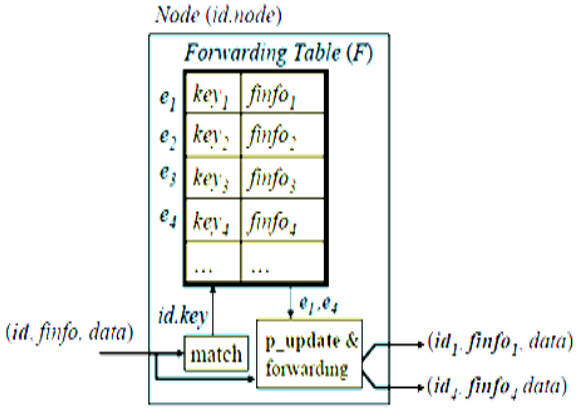

Figure: 4.A Forwarding Entries

Entries are maintained in the FI as soft-state and must be refreshed periodically[7].

B. Packet Routing Functions:

The three steps in routing a packet are:

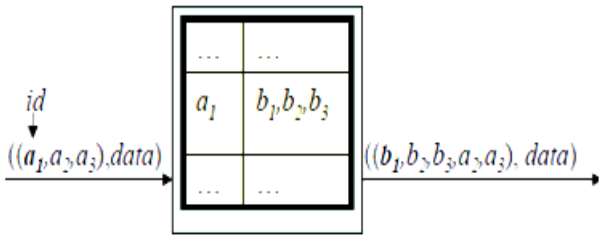

Figure : Packet Matching

- ***a. Packet Matching:*** When a packet arrives at node, the packet identifier is matched against the forwarding table by a matching function match(id,F) → {e1,e2,e3,……..,ek} which takes as input a packet’s *id* and a forwarding table (stored at node *id.node*) and outputs a set of entries, where each entry is a *(id, finfo)* pair[3].
- ***b. Packet Header Update:*** The header and destination of a packet are based only on the incoming packet’s header and the matching entry. If multiple entries are matched, the packet is replicated. The update function

Update(p,e)→p' takes a packet header and an entry and produces a modified packet header[3].
Forwarding the packet to the next hop[3].

C. Source Control Over Forwarding Entries:

FI nodes allow end-hosts to insert and remove entries into and from the forwarding tables at the FI nodes, Insert(n,e)insert entry e into n's forwarding table. Remove(n,e)//remove entry e from n's forwarding table. These IDs differ in their level of "visibility" to end-users a public ID is publicly known, while a private ID is known only to a trusted set of users[1].

D. Properties of a SSR model:

This properties must be satisfied by source routing model to avoid all attacks which are mentioned previously

a. Preventing External Flooding Attacks on End-Hosts:

- ***a) Property 2:*** An external attacker cannot make a single victim end-host receive more packets than the attacker itself sends or receives[1]. This property prevents an external attacker from using the FI to Amplify the traffic it sends to a victim host and A direct traffic meant for other hosts to the victim host.
- ***b) Malicious linking:*** Consider a forwarding entry [id1→X] that receives a large number of packets. An attacker can sign up an end-host R, with an existing public forwarding entry [id→R] , to the high bandwidth traffic stream of the popular entry by inserting the entry [id1→id] .
- ***c) Cycles involving end-hosts:*** Consider two benign hosts R1 and R2 inserting entries [id1→R1] and [id2→R2], respectively. An attacker can create a cycle by inserting entries and. Packets sent to id1and id2 would be indefinitely replicated, thus overwhelming R1 and R2.

b. Limiting External Flooding Attacks on FI :

- ***a) Property 3:*** The forwarding cost is bounded and small[1]. Cycles involving FI nodes: There should fix and bounded time on life time on each packets to avoid loops
- ***b) Dead-ends:*** Frequents updates should be exchanged between routers and hosts to avoid dead end .

c. Limiting Internal Attacks:

- ***a) Property 4:*** An internal attacker should be able to mount only two forms of attacks[1].Drop the packets directed to forwarding entries it is responsible for and A *random* flooding attack, i.e., attacking a host through its forwarding entry *without* knowing the identity of the host.

V. RELATED WORK

In the process of designing security mechanisms for FIs, we have leveraged techniques that have been proposed earlier in the literature. Challenge-response protocols have been used for a long time in diverse areas. The idea of using erasure codes to ensure that uncooperative hosts do not oversubscribe to high-bandwidth streams was proposed recently in the context of multicast [1]. Pushback has been proposed for rate-limiting the traffic of IP aggregates by Mahajan*etal*. [2].

We organize related work into three categories. The rest one references architectures that enable edge systems to control the path of their outgoing trace. The second one references trace back and packet marking schemes, which enable edge systems to identify the paths of their incoming traffic. The third category references addressing protocols that, like WRAP, add path information inside each packet (but do so with different objectives).

A. Route Control:

Route Science Inc. [1] follows an approach similar to ours, in that it involves entities located at the edges of the Internet, which monitor and evaluate multiple paths to each potential destination. Their approach differs from ours, in that a sender does not control the entire path, only the rest ISP. Controlling the rest ISP can sometimes help im prove communication quality and requires no changes to the current Internet architecture. However, it does not always enable a sender to route around failing or undesired regions of the Internet, even if an appropriate route exists. The New Internet Routing Architecture (NIRA) [4] pro- vides similar route control with WRAP, namely enables an edge system to specify the entire domain-level path of its outgoing trace.

B. Traceback and Packet Marking:

An IP traceback mechanism enables an edge system to identify the path followed by its incoming trace. Most mechanisms do that by requiring routers to mark packets; the receiving edge system can then process/combine the marks and reconstruct the path [3,7]. Packet marking can also be used to provide each packet depends on the path followed by the packet. This kind of packet marking may not necessarily enable traceback, but it does enable filtering of packets based on their path [3]. The current Internet architecture does not provide room for packet marking. As a result, traceback and packet marking research has focused on inventing intelligent marking algorithms, which the full path information in lightly utilized IP header fields.

C. Addressing Protocols:

WRAP is similar to the IP-next-layer (IPNL) [9] and IPv4 [2] addressing protocols, in that it (i) is a protocol between the IP and transport layers, (ii) involves an overlay of upgraded routers that relay packets to each other, and (iii) specifies inside each packet's header the set of such routers on the packet's path. However, WRAP-enabled routers map to border routers between administrative do- mains. As a result, and unlike IPNL and IPv4, WRAP enables an edge system to control the full domain-level path of its outgoing and incoming trace.

VI. CONCLUSIONS

We presented a general FI model, analyzed potential security vulnerabilities and willing to present several mechanisms to alleviate attacks. Key defense mechanism, based on lightweight cryptographic constraints, provably prevents a largest of attacks.

Use of simple, light-weight, cryptographic constraints on forwarding entries. The flexible control of these FIs can be exploited to restrict many types of powerful attacks with little effort. It is possible to prevent a large class of attacks

on end-hosts, and Bound the flooding attacks that can be launched on the infrastructure nodes to a small constant value.

We describe a mechanism that provides track policy support for the next-generation Internet. Our mechanism will be enables an edge system to control the domain-level path followed by its track, by adding state in each packet. This datagram" approach provides all the benefits of datagram over virtual circuits, while incurring relatively modest forwarding complication or packet header overhead (the typical costs with datagram). We compared WRAP to the traditional Loose Source Record Route (LSRR) IPv4 option and showed that WRAP provides similar functionality, while avoiding the processing overhead and security problems introduced by traditional LSRR.

VII. ACKNOWLDGMENT

I am grateful to my Thesis guide Dr. B.B. Meshramfor providing me the opportunity to work in an exciting and challenging field of"Source Controlled Routing System". My interactions with him have been of immense help in defining my project goals and in identifying ways to achieve them.

VIII. REFERENCES

[1] T. Anderson, T. Roscoe, and D. Wetherall, "Preventing internet denial-of-service with capabilities," in Proc. Hotnets, 2003.

[2] S. Bellovin, "Security concerns for IPng," RFC 1675, 1994.

[3] K. L. Calvert, J. Griffioen, and S. Wen, "Lightweight network support for scalable end-to-end services," in Proc. ACM SIGCOMM, 2002.

[4] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. S. Wallach,"Secure routing for structured peer-to-peer overlay networks," in Proc.OSDI, Dec. 2002.

[5] D. R. Cheriton and M. Gritter, "TRIAD: A newnext generation internet architecture,"Mar. 2000.

[6] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," Mar. 1999.

[7] D. Dean and A. Stubblefield, "Using client puzzles to protect TLS," in Proc. 10th USENIX Security Symp., 2001.

[8] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in Advances in Cryptolog CRYPTO'92, International Association for Cryptologic Research, ser. LNCS 740, E. Brickell, Ed. Berlin, Germany: Springer-Verlag, 1993, pp. 139–147.

[9] R. Gold, P. Gunningberg, and C. Tschudin, "A virtualized link layer with support for indirection," in Proc. FDNA, 2004.

[10] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel, and A.Rubin, "Working around BGP: An incremental approach to improving security and accuracy in interdomain routing," in Proc. NDSS, Feb. 2003.

Short Bio Data for the Authors

First Author – Somnath J Jagdale, Mtech(Coputer), Department of Computer Technology, Veermata Jijabai Technological Institute, Mumbai, India-400084, somnath.jagadale@gmail.com

Second Author - Department of Computer Technology, Veermata Jijabai Technological Institute, Mumbai, India-400084, bbmeshram@vjti.org.in