Design and Implementation of Transport Relay Translator and its security Mitigations

P. Shanmugaraja [#1], S. Vasanthi [#2], D. Balamurugan[#3], S. Chandrasekar [*4]

[#] Research Scholars, Anna University, India
[1] pshanmugaraja@yahoo.com
[*]Principal, Gnanamani College of Technology, Namakkal, Tamilnadu, India

***Abstract* - The extensive growth of the Internet in the recent years has depleted all the IPv4 address space. It results in scarcity of the IPv4 addresses and leads to design of temporary techniques like NAT. IETF developed IPv6 to overcome this issue. IPv6 is more than 7.9×10^{28} times as many as IPv4. Again, it leads to a new issue of compatibility. IPv6 overcomes the problem of address scarcity but it is incompatible with IPv4 address. So machines configured with IPv4 and machines configured with IPv6 cannot communicate directly. This communication is mandatory because IPv6 cannot replace IPv4 rapidly. It takes time to convert completely from IPv4 infrastructure to IPv6 infrastructure. Until then, both should cooperate. Transition technologies developed to solve this incompatibility. One such technology is Transport Relay Translator. It is based on RFC-3142. A translator located in the transport layer called as transport relay translator. The relay is located somewhere between the communicating hosts and enables IPv6-only hosts to exchange traffic with IPv4-only hosts. A TRT, which runs on a dual-stack node, can use one protocol when communicating with the client and another protocol when communicating with the application server. This paper discusses the implementation of TRT and methods to solve the security issues caused due to this translation.**

1. INTRODUCTION

Recent development in Internet computing leads to new technologies in the field of computer science. One of the important developments in the networking is the IPv6 protocol. IPv6 was developed in the 1990s to overcome the drawbacks of IPv4, which is now currently used[1]. The drawbacks of IPv4 are lack of IP addresses, proprietary IPsec protocol and configuration of nodes using DHCP protocol. To avoid these drawbacks and include some additional features we go for IPv6 protocol. IPv6 protocol has some additional features like extensibility, larger address space, new header format, hierarchical addressing, and built in security[3].

It is not possible to change the entire network to IPv6 overnight. It requires time and cost. Till the time both IPv6 and IPv4 should interoperate. To accomplish the task we have different mechanism[2]. They are

- Dual stack. Hosts and routers run both an IPv4 and IPv6 protocol stack.
- Tunneling. IPv6 packets are tunneled through an IPv4 network.
- Translation. A gateway translates IPv6 packets to IPv4 packets.

The paper is organized as follows. The first section focuses on specifies the operation and design architecture of the Transport Relay Translator (TRT). The second section discusses security threats related to Transport Relay Translator and final section discusses the implementation for securing the threats.

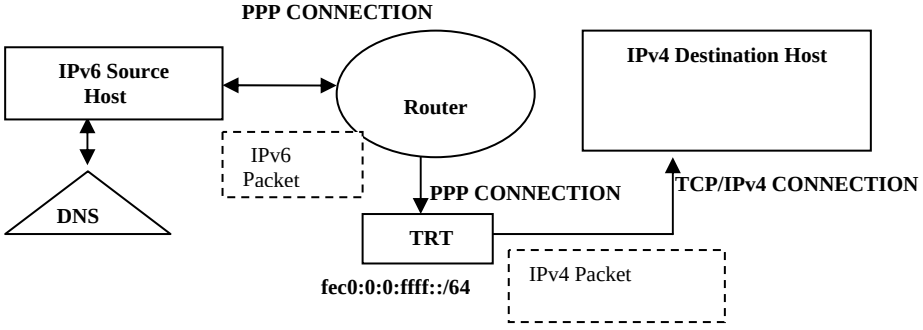

Figure 1. Block Diagram of Transport Relay Translator

II DESIGN ARCHITECTURE FOR TRT

The proposed TRT Project will attempt to overcome some of the drawbacks of existing systems such as NAT unfriendly protocols and UDP.

Terminologies used in block diagram.

1.) IPv6 Source Host:

The System is configured with IPv6 address. And it can communicate only with other IPv6 systems and it cannot communicate with IPv4 systems. Here it sends packets using TCP/IPv6 connection.

2.) DNS (Domain Name System):

IPv6 hosts uses name server to resolve its DNS queries. The IPv6, when asking its name server for the IPv6 (AAAA) record of a IPv4 only host, will receive from DNS an IPv6 address record specially constructed from the IPv4 address(A) instead of an error response telling that no IPv6 address can be found for that host. The constructed address consist of a special network prefix associated with the transport relay and host id(lower 64 bits) that embeds the IPv4 address of the remote host. For small scale installation static mapping is recommended and for large scale installation special DNS server is necessary.

3.) Router:

Router is set up such that packets destined for address with the special network prefix are routed to the TRT relay node.

4.) TRT:

TRT does the translation of IPv6 address to IPv4 address and it makes a TCP/IPv4 connection the destination host. The router routes packets to the TRT. The TRT then intercepts transport sessions and acts towards the client node as a destination end point of an IPv6 session and acts towards the server node as a source for an IPv4 session, copying all data it receives from each session to the other.

5.) IPv4 Destination Host:

The System is configured with IPv4 address. And it can communicate only with other IPv4 systems and it cannot communicate with IPv6 systems.

III FUNCTIONAL ARCHITECTURE

The previous section describes the overall Transport Relay Translator. But the actual functionality lies in the Transport Relay Translator. The Transport Relay Translator performs the conversion from TCP/IPv6 packet to TCP/IPv4 packet. Figure 2. Describes the functional architecture of Transport Relay Translator.

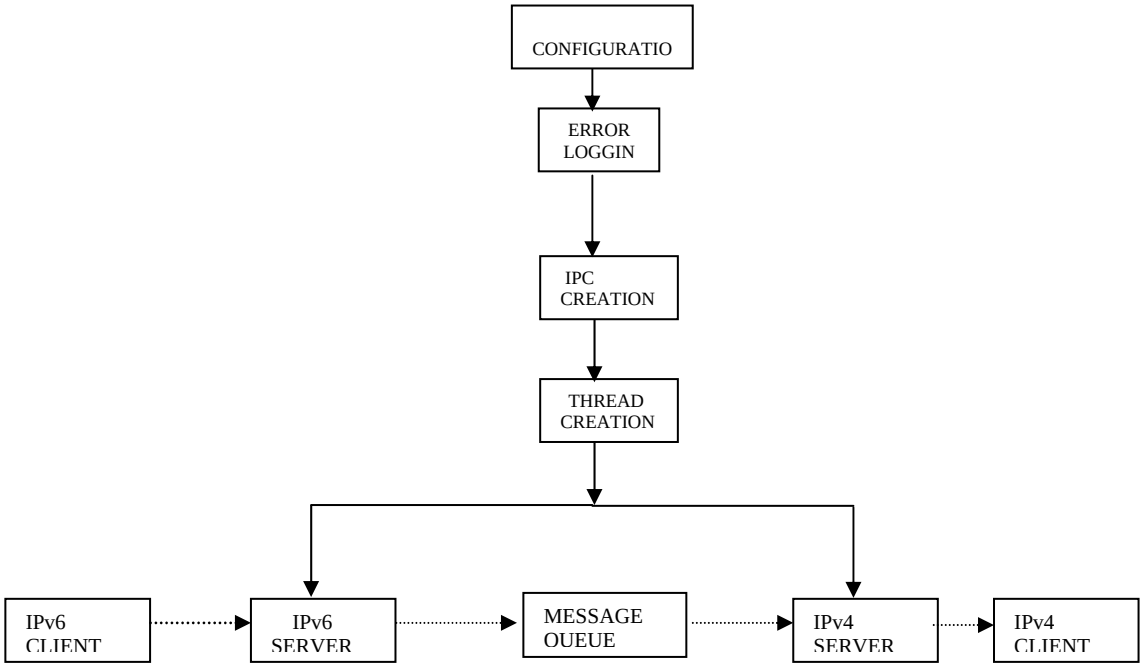

Figure 2. Transport Relay Translator functional architecture**.**

1.) IPC Creation:

It creates a message queue and semaphore. Message queue is used in inter process communication. Semaphore is used to make synchronize the access to the message queue.

2.) THREAD Creation:

Two threads are created. One handles TCP/IPv6 connection and another handles TCP/IPv4 connection.

3.) Configuration

When the system is getting loaded, first it reads a configuration file where the configuration files are stored.

4.) Error logging

It is used to log the errors that occur when the Transport Relay Translator system runs. It stores all the type of errors into a log file. This log file contains the error name and the severity of the error. It will perform graceful shutdown of the system.

5.) IPv6 Server

IPv6 server program runs here. Here the server listens to IPv6 clients. When the data arrives from the IPv6 client, it is sent to the message queue, along with the IPv4 address that the IPv6 client need to send data.

6.) IPv4 Server

IPv4 server program runs here. The server gets the data from the message queue along with the IPv4 address. It makes TCP/IPv4 connection to the destination IPv4 host and sends the data to the IPv4 client.

IV Threats due to Transition Mechanisms

Transition mechanisms open the path for various attacks. This section examines the attacks possible with different mechanisms.

i. Tunneling can be used to evade security measures. It is vulnerable to Denial-of-Service (DoS) attacks, Reflection Denial-Of-Service (DoS) and service theft, in which a malicious node or site or malicious user may make unauthorized use of the service. These attacks are possible because of no preconfigured association between tunneling end points[4]. Tunnel sniffing and eavesdropping on traffic going through tunnel is also possible. If automatic tunneling (6to4, Teredo and ISATAP) is used all receiving nodes must allow decapsulation of packets that can be sourced from anywhere. The problem becomes more serious when IPv6 tunneled over IPv4 encapsulation in UDP, as UDP usually allowed passing through NAT's and Firewalls [6]. Tunnels encapsulating IPv6 in SSL/TLS or IPSec are more dangerous if the datagram payload is encrypted because there is no technique to examine the payload. 6to4 is the most widely used tunneling mechanism in the world for transition between IPv4 to IPv6. 6to4 routers cannot identify whether relays are legitimate [10]. 6to4 is vulnerable to packet laundering. It is subject to administrative abuse, e.g., service theft [9].

ii. Translation technology is affected by threats similar to circumventing ingress filtering or improper use. It is also vulnerable to buffer overflow attack however; this issue depends on the implementation[15]. IPSec cannot be used in Transport Relay Translator because Translation works above the network layer and IPSec in network layer that makes IPv6 vulnerable. The translation system intersects TCP connection between sending and receiving hosts[7]. This is an illegitimate behavior for a communicating node. The Transport Relay Translator must retain state, so it is vulnerable to various DOS attacks [11]. Protocols that base authentication on IP address do not work across TRT [11].

iii. Dual stack technologies drawback is all processes applied for IPv4 duplicates in IPv6 also. A dual stack host will have to face the vulnerabilities of both IPv4 and IPv6. In most cases, Dual stack technology relies on tunneling and translation mechanisms for interoperability for networks that are not dual stack [12]. Unexpected tunneling between the hosts may occur which may violate security policies.

V Security Threats while deploying TRT

Perverts can easily intrude TRT traffic, which is similar to circumventing ingress filtering. Buffer overflow attack can be easily. If TRT is not properly implemented then it may lead to buffer overflow attack. TRT cannot be used in protocols which authenticate the packets based on source address. There is a possibility that Transport layer can monitor the IP packets in TRT. IPv6 cannot be used in TRT which causes a major setback for TRT.

The translation system intersects TCP connection between sending and receiving hosts. This is an illegitimate behavior for a communicating node. The Transport Relay Translator must retain state, so it is vulnerable to various DOS attacks [11]. Protocols that base authentication on IP address do not work across TRT [13].

Transport Relay Translator traffic depends on IPv4 or IPv6 security policies which is enforced before or after translation. Traffic due to IPv6 NAT64 can be restricted by blocking IPv6 natice packets.

VI Techniques to overcome security threats

Security Policies can be locally deployed on a network to protect against security threats to TRT. It can be deployed on Router, Switches or in end computers. This type of technology is simple and does not create any complexity in the network. Deploying this model puts more weight on the switches and routers which are responsible for carrying the packets through out the network[14]. This security model also does not increase network complexity because security is enforced by the hosts rather than network elements like the first-hop switches or routers. The downsides are that this distributed security model makes the network generally harder to manage than one based on a centralized model, and vulnerabilities are nearly impossible to mitigate at the end nodes. The major drawback of this system is single point of failure[8]. If the switch or router fails then entire traffic is shut down. If it is attacked then entire network can be hacked easily. The downsides are that it requires increased intelligence/complexity in the first-hop switch and it clearly introduces a single point of failure; if the first-hop switch is compromised, all protection is gone. The following attacks can be mitigated using this technique. Address spoofing attacks, Layer 2 or 3 and Denial of service attacks.

VII Conclusion

IPv6 protocol will replace IPv4 protocol completely in future. Until then we need translators to make communication between IPv6 and IPv4. Even though IPv6 solves most of the problems of IPv4, it also introduces new network security issues. This paper presents how to implement Transport relay translator and overview of transition mechanisms and their security threats. It mainly focuses on security issues of IPv6 translation technique Transport Relay Translator. The proposed mitigation methods for TRT threats do not mitigate the threats completely and solution that is more effective should be developed to completely prevent the threats. The current Internet growth is massive and new threats emerge every second in this Internet World, which is very difficult to prevent.

REFERENCES

[1] D. Waddington and F. Chang, "Realizing the Transition to IPv6," IEEE Communications Magazine, vol. 40, no. 6, pp. 138–147, June 2002.

[2] Bradner, S., "The End-to-End Security," *IEEESecurity & Privacy*, Mar.-Apr. 2006, pp. 76-79.

[3] Campbell, P.; Calvert, B.; Boswell, S., *Security+Guide to Network Security Fundamental*, Thomson,Canada, 2003.

[4] Carlos E. caicedo, James B.D. Joshi, Summit R. Tuladhar , "IPv6 Security Challenges," *IEEE Internet Computing*, Feb 2009,pp. 36-42.

[5] IPv6 Task Force, "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)," Jan. 2006, US Dept. of Commerce;

[6] S. Convery and D. Miller, "IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)," Mar. 2004; www.seanconvery.com/v6-v4-threats.pdf.

[7] RFC 2460: Internet Protocol, Version 6 (IPv6) Specification.

[8] P. Nikander, J. Kempf, and E. Nordmark, *IPv6 NeighborDiscovery (ND) Trust Models and Threats*, IETF RFC 3756,May 2004; www.rfc-archive.org/getrfc.php?rfc=3756.

[9] P. S. E. Davies, S. Krishnan. (2006, Mar.) IPv6 Transition/Co-existence Security Considerations. IETF Internet draft. -4942. http://www.ietf.org/internet-drafts/draft-ietf-v6ops-security-overview-04.txt

[10] P. Savola,C. Patel, Security considerations for 6to4, IETF RFC 3964, DEC 2004; http://www.ietf.org/rfc/rfc3964.txt

[11] P.Shanmugaraja, S. Chandrasekar," Accessible Methods to Mitigate Security Attacks on IPv4 to IPv6 Transitions" European Journal of Scientific Research Vol.77 No.2 (2012), pp.165-173

[12] F. Baker, P. Savola, Ingress filtering for multi home networks IETF RFC 3704, MAR 2004; http://www.ietf.org/rfc/rfc3704.txt

[13] S. Kent and R. Atkinson, "Security architecture for the internet protocol," RFC 2401 (Proposed Standard), Internet Engineering Task Force, Nov.1998, updated by RFC 3168.

[14] S. Kent and R. Atkinson, "IP encapsulating security payload," RFC 2406(Proposed Standard), Internet Engineering Task Force, Nov. 1998.

[15] P.Shanmugaraja, D. Balamurugan, S. Chandrasekar, "An approach to secure Teredo Tunneling Technology", Vol. 2 Issue 3, March – 2013