Name of Scholar : Ramaswami Radhakrishnan
Name of Supervisors : Dr. Majid Jamil, Professor Moinuddin
Department : Electrical Engineering
Title of the Thesis : Study and possible remedies for security holes in IPv6

ABSTRACT

Present day Internet is based on a technology, which emerged in 1970, has seen unprecedented growth since 1980. The success of this technology based on Internet Protocol version 4 (IPv4) has also brought about its own downfall in terms of performance and security.

The problems with IPv4 are shortage of address space, routing table explosion, difficulty in address configuration, lack of quality of service, ineffectiveness of IPSec and inadequate support for mobility. Inadequacies in present Internet based on IPv4 necessitated development of newer and enhanced version of Internet protocol. The next generation Internet protocol (IP version 6) has many improvements over IPv4. These are: large address space, efficient and hierarchical addressing and routing infrastructure, stateless and stateful address configuration, built-in security, better support for QoS, mobility, new protocol for neighbouring node interaction and extensibility.

Along with the new features are also new security concerns, which need to be addressed. In this thesis security threats arising due to the new features, legacy threats of IPv4 carried forward to IPv6 and other threats relating to firewall and transition from IPv4 to IPv6 are identified. Security threats identified are relating to address auto-configuration, mobility, firewall, IPsec, IKE and transition. Solutions to three threats are proposed in this research work.

Firstly, a proposed solution to address auto-configuration ensures that only authorized nodes are allowed to engage in auto-configuration. The solution is based on the following components:-

- A public key infrastructure (PKI) for IPv6, called UMU-PKIv6
- A Kerberos authentication service.
- Messaging mechanism to authorize Auto-addressing.

A comparative analysis with already existing solutions: IPSec and SeND protocols, shows that the proposed solution is robust and requires lesser computation.

In Mobile IPv6, the packets from a Correspondent Node (CN) can be sent directly to the Mobile Node (MN) without the intervention of Home Agent (HA). This mode is called Route Optimization, which is not properly supported in Mobile IPv4. However, a number of security threats like traffic redirection,

replay attacks, inducing unnecessary binding updates, forcing of non-optimized routing and reflection attacks have been identified. This thesis suggests a solution called Revised Return Routability (RRR) procedure to provide a secured mechanism to ensure that all the players involved in mobility i.e., HAs, MNs and CNs are all verified authenticated nodes and thus leaves almost nil security holes to be exploited by an attacker. The proposed Revised Return Routability procedure consists of following mechanisms:-

- Secured link between HA and MN
- A public key infrastructure (PKI) for IPv6
- Validation of MN and CN

All three players namely the HA, MN and CN are mutually authenticated and tested for routability in a simple and robust manner in RRR procedure compared to other existing solutions namely, Return Routability Procedure, Improved bombing resistant protocol and enhanced CGA based

Current firewall technologies are predominantly based on IPv4 and are still evolving to adapt to new features of IPv6. A mobile IPv6 unaware firewall can be detrimental to route optimization and return routability procedures of IPv6. Mobile node, Home agent and Correspondent node have crucial roles in mobile IPv6 and incorrect filtering of messages exchanged between them by a firewall can seriously affect the mobility functionality. A stateful firewall with deep packet inspection is proposed as a solution. Current stateful firewall implementation supports four connection states, namely, NEW, ESTABLISHED, RELATED and INVALID. A new solution proposes additional states and filtering based on static rules relating to the message pairs sequences at mobile node, home agent and correspondent node. Coloured Petri Nets (CP-nets or CPNs) is used to model and simulate the proposed solution. A hierarchical CPN model implementing the static rules for firewalls of Mobile node, Home agent and Correspondent node has been created and functionality of firewalls have been successfully verified for correctness through simulation of this model using CPN tool.

Solutions to three out of six identified threats are proposed in this research work. Solutions to security issues relating to IPsec, IKE and Transition can be undertaken as future work.