Cynthia Omauzo

SeND

IPv6 TRUST MODELS

The first trust model is that all authenticated nodes trust each other to behave correctly at the IP layer and not send any neighbor/router discovery messages that contain false information. An example of this model is corporate intranet. In the second model, a router is trusted by the other nodes in the network to be a legitimate router that routes packets between the local network and any connected external networks. This router is trusted to behave correctly at the IP layer and not send any neighbor/router discovery messages that contain false information. The clients do not trust each other to behave correctly and believe that any client node can send falsified messages. The third model is where the nodes do not directly trust each other at the IP layer, this is considered suitable where a trusted network operator is not available.

ADDED FEATURES

Neighbor Discovery already has some actions included like:
Router Advertisement Guard which monitors and detects router advertisements and Privacy extensions for stateless address autoconfiguration. **NDPMon** and **Ramond** which are passive monitoring/detection tools and **Cisco First Hop Security** which is Cisco's solution for mitigating IPv6 attacks.

SeND adds three additional features to Neighbor Discovery Protocol; **address ownership proof**, **message protection**, and **router authorization mechanism**. SeND uses Cryptographically Generated Addresses (**CGA**) to prevent address stealing and ensure a node's IP address is bound to its public key. CGAs are generated from the cryptographic hash of a public key and auxiliary parameters. This provides a method for securely associating a cryptographic public key with an IPv6 address in the SeND protocol. The node generating the CGA address must first obtain an RSA key pair and the node then computes the interface identifier part (rightmost 64 bits) and appends the result to the prefix to form the CGA address. CGA address generation is a one-time event. This feature prevents spoofing because the message must be signed with the private key that matches the public key, which only the address owner will have. Replay is also prevented because the signature has a limited lifetime. SeND also includes a nonce in the solicitation message and requires the advertisements to include the nonce.

Authorization Delegation Discovery (ADD) has also been added to validate and authorize routers to act as default gateways and specifies prefixes that a router is allowed to announce on its link. ADD is also used to certify the authority of routers by using a trust anchor. The trust anchor is a third party that the hosts trust and to which the router has a certification path.

SeND adds two new ICMP messages to identify router authorization process. **Certificate Path Solicitation** used to request a certification path between a router and one of the host's trust anchors and **Certificate Path Advertisement** which is sent in reply with certificate path solicitation messages and contains the router's certificate.

ISSUES WITH SeND

- ✗ Most operating systems support NDP but lack support for SeND
- ✗ SeND is not supported on Mac, iOS, Android, HP Networking, and Windows

There are security concerns with SeND as well. CGA cannot provide assurance about the real node's identity. CGAs are not certified so an attacker can create a new valid address from their own public keys and start communication. A certificate authority is necessary to validate the keys.

Works Cited

Hunkeler, Andreas. “IPv6 Secure Neighbor Discovery.” *CSNC*, Jan 2015. Web. 17 Jun 2015.

n.p. “IPv6 Secure Neighbor Discovery.” *Cisco*, n.d. Web. 29 May 2015.