DELVING INTO SECURITY

Cynthia Omauzo
DREU SUMMER 2015

ABSTRACT

The goal of this research is to provide another option for securing Neighbor Discovery in IPv6. ARPsec, a security measure created for ARP succeeded in securing ARP. The plan is to include IPv6 funtionality to this security measure in order to provide an alternative to SeND. The outline of this report will be to cover the foundation of research first. Sections 1 – 7 will cover that. Section 8 - 10 will cover the work done, findings, and conclusions.

1. WHAT IS ARP

ARP (Address Resolution Protocol) found in IPv4, is used to map an IP address to the device's MAC (Media Access Control) address. The simplest way to describe ARP is this: A device needs to know what IP addresses and MAC addresses are associated with each other. If the device already knows, then no problem. If the IP address is not found in the ARP table (a record of the devices' IP and MAC addresses) the device will send out a broadcast message. This broadcast message is sent to a special IP address for that network which allows all devices on that network to receive it. The message “who has IP address ….” should receive a response from the device that owns that IP address. In the response the MAC address for that device will be included in the packets. Here, ARP has *resolved* the address.

2. WHAT IS NEIGHBOR DISCOVERY

In IPv6 ARP is no longer used. It has been replaced by Neighbor Address Resolution. The function of Neighbor Discovery (ND) is for a host to learn the IPv6 addresses of its neighbors and that includes learning about other hosts and routers on the local network. Instead of broadcast messages, IPv6 uses a multicast address and ICMPv6 messages for tracking and discovering other hosts. In order for ND to work, it uses five types of ICMPv6 messages; those are: Neighbor Advertisements, Neighbor Solicitation, Router Advertisement, Router Solicitation, and Redirect.

Nodes will send Neighbor Advertisement (NA) messages periodically to inform neighbors of their presence and send their link-layer addresses to other hosts present on the same network. Neighbor Solicitation (NS) messages are sent so that link-layer addresses of specific

neighbors can be found. NS is used to detect duplicate addresses, verify neighbor reachability, and for Layer 2/3 address resolution. Router Advertisement (RA) messages are sent for every interface as soon as it's configured. In order to inform hosts about prefixes and also to inform that the router is available as a default gateway, RA messages are sent. In Router Solicitation (RS) routers will send RS messages to all multicast address. This occurs without waiting for RA messages.

Duplicate Address Detection is a neighbor solicitation function. When the autoconfiguration is performed the host does not automatically know the address is unique. This could lead to duplicate addresses. The way DAD works is that the host will join the *all nodes multicast address* and *solicited-node multicast address* of the address being checked for uniqueness. The host will send NS messages to the solicited-node address. The address field will be undefined with unspecified address "::". The address being checked is inside the Target Address field. If the host receives any NA responses, it means the address being checked is not unique. In Neighbor Unreachability Detection there are two ways to confirm reachability: a host will send a query to the targeted host's solicited-node multicast address then it is responded with an NA or an RA; when a node is interacting with the targeted host it gets a hint (TCP ACK is one form) from a higher-layer protocol that two-way communication is functioning correctly.

3. WHAT MAKES NDP DIFFERENT FROM ARP

- Router discovery is part of the base IPv6 protocol set.
- IPv6 hosts do not need to snoop the routing protocols to find a router. IPv4 uses ARP, ICMP router discovery, and ICMP redirect for router discovery.
- IPv6 router advertisements carry link-local addresses. No additional packet exchange is needed to resolve the router's link-local address.
- Router advertisements carry site prefixes for a link. A separate mechanism is not needed to configure the netmask, as is the case with IPv4.
- Router advertisements enable address autoconfiguration. Autoconfiguration is not implemented in IPv4.
- Neighbor Discovery enables IPv6 routers to advertise an MTU for hosts to use on the link. All nodes use the same MTU value on links that lack a well-defined MTU. IPv4 hosts on the same network might have different MTUs.
- IPv6 address resolution multicasts are spread over 4 billion (2^32) multicast addresses. Non-IPv6 machines should not be interrupted at all.
- IPv6 redirects contain the link-local address of the new first hop. Separate address resolution is not needed on receiving a redirect.
- Multiple site prefixes can be

associated with the same IPv6 network. By default, hosts learn all local site prefixes from router advertisements. Routers can be configured to omit some or all prefixes from router advertisements. If it is omitted, hosts assume that destinations are on remote networks. Consequently, hosts send the traffic to routers. A router can then issue redirects.

- The recipient of an IPv6 redirect message assumes that the new next-hop is on the local network. In IPv4, a host ignores redirect messages that specify a next-hop that is not on the local network, according to the network mask. The IPv6 redirect mechanism is analogous to the XRedirect facility in IPv4.
- IPv6 neighbor unreachability detection improves packet delivery in the presence of failing routers, partially failing/partitioned links, and when nodes change link-local addresses. IPv4 has no corresponding method for neighbor unreachability detection.
- Neighbor Discovery detects half-link failures by using neighbor unreachability detection. Neighbor Discovery avoids sending traffic to neighbors when two-way connectivity is absent.
- By using link-local addresses to uniquely identify routers, IPv6 hosts can maintain the router associations. IPv4 does not have a comparable method for identifying routers.
- Neighbor Discovery messages have a hop limit of 255 upon receipt, the protocol is immune to spoofing attacks originating from off-link nodes. In contrast, IPv4 off-link nodes can send ICMP redirect messages. IPv4 off-link nodes can also send router advertisement messages.
- By placing address resolution at the ICMP layer, Neighbor Discovery becomes more media independent than ARP. Consequently, standard IP authentication and security mechanisms can be used.

4. VULNERABILITY IN ARP

When it comes to security, no device should be trusted, but during the process of determining a MAC address through broadcast messages there is no method for the ARP protocol to authenticate where the reply came from. Because of this, any device can claim to have the requested information. Most operating systems will accept the first reply or the last response to an ARP request. Linux, for example, always takes the first reply and ignores the others.

This opens the door for ARP spoofing or cache poisoning. The attacker will inject a new MAC/IP binding into the victim's ARP cache by sending a forged ARP request or reply to the victim. The goal is to associate the attacker's MAC address with the IP address of the victim. This will cause traffic meant for the victim to be sent to the attacker instead. ARP Spoofing may allow the attacker to intercept frames on a network, modify the

traffic, or even stop all traffic. Most often this attack is used as an opening for other attacks like denial of service, man in the middle and session hijacking.

5. ARPSEC

ARPsec is a security approach for ARP based on logic and the use of the Trusted Platform Model (TPM) to implement security guarantees. A logic prover reasons about the validity of an ARP reply from the remote machine based on the codified logic rules and the previously stored binding history of the local system. The TPM attestation protocol is implemented to challenge the remote machine if the logic layer fails to determine the trustworthiness.

TPM is a cryptographic chip embedded in motherboards. The TPMs can help determine the true identity of a remote host via Attestaion Identity Key (AIK) verification during the TPM attestation. After creating an AIK pair, the TPM hardware communicates with Privacy Certification Authority using the information embedded within itself to prove its identity and get the AIK credentials.

After all of this, a remote machine can prove its integrity by reporting the values of its Platform Configuration Registers (PCR). This value or measurement is based on the current state of the underlying hardware, BIOS, boot loader and operating system. If the values are different from what is expected, the remote host might be compromised, thus not trustworthy. Unless the TPM hardware is compromised, there is no disclosed method of hacking into the TPM through software and changing the PCR values.

6. VULNERABILITY IN NDP AND EXISITING SECURITY

Just like in ARP, NDP is also vulnerable to attacks. NDP's Neighbor Solicitation/Advertisement messages can be spoofed. The attacker will send a neighbor advertisement with a fake binding of IP address and MAC address. This is similar to ARP spoofing. Node A will now send traffic destined for Node B to an arbitrary MAC address. If there is no response from that MAC address, Node A will eventually perform a Neighbor Unreachability Detection (NUD) and the binding will be flushed from its cache. In order for the attack to be continued, the attacker must respond to the NUD or send another neighbor advertisement.

There is currently a security measure made for Neighbor Discovery, which is SeND. It uses the cryptographic hash of a public key and auxiliary parameters to generate CGAs or Cryptographically Generated Addresses. The node generating a CGA address must first obtain an RSA key pair, then computes the interface identifier part and appends the result to the prefix to form the CGA address.

7. NDPROTECTOR

When a Neighbor Discovery message (ICMPv6 packet) is received or is emitted on/by an interface, a hook set

by ip6tables redirects the packet to the userspace before it goes to the kernel/network card. This extraction is performed by the libnetfilter_queue. The libnetfilter_queue is a userspace library providing an application programming interface to packets that have been queued by the kernel packet filter. A modified version of scapy6, which is a packet manipulation tool for computer networks, dissects each intercepted message and inspects the "important" fields. It decides whether the message needs to modified (add an RSA signature for outgoing packets) or passed (for ingoing packet with a correct signature).

Each assigned address is bound to a Public Key/Private Key. Whenever a message comes from this address, the implementation uses the Private Key and adds an RSA signature option to it.

8. RESEARCH WORK

In the first step of the process, editing the source code of NDP was needed. This will include a new struct to capture the important components of the Neighbor Advertisement and Neighbor Solicitation messages. Once this was complete, the kernel needed to be compiled and be stable with the new features.

With the knowledge of Ndprotector, the software was installed on both machines and a local network was created for them to communicate. Ping6 was often used to ensure successful communication between the two. The next step was to generate public and private key pairs using the openssl command in Ubuntu Linux. This was done for both machines and the host configuration file (found in Ndprotector) was edited to include paths to all keys. Also, Machine A needed to have Machine B's public key stored somewhere that it can access and vice versa. Once Ndprotector was running properly, ping6 needed to be used again to be sure that the machines were still able to communicate.

When using ping, one will notice that the first ping is a little longer than the following pings, this is because there is no IP/MAC binding in the cache, so the host must get the needed information before they can communicate freely.

Since the machines were communicating, wireshark was included to determine which kind of NDP messages were being sent between them. While using wireshark and looking into the contents of the ping, it was seen that Machine A will send a unicast message (like a broadcast in ARP) requesting information about Machine B. Machine B will then respond to the message with a neighbor advertisement. Within that response, the MAC address is sent. While the machines are communicating back and forth, the contents of the messages also include the CGA and RSA signatures.

On the end with Ndprotector, there are messages displayed on the screen, informing the user of the current status. The displayed messages let the user know that they have received either a neighbor advertisement

message or neighbor solicitation message and that it is storing the information found within those messages and signing the response.

9. PERFORMANCE EVALUTATION

In this stage ping6 is the main tool used. It is used to test regular Neighbor Discovery and also with NDprotector. The goal is to use the ping command when no MAC address is known and gather the information (min/max/avg/mdev times), then when the mac address is stored, ping is run again and the values are gathered. When running Ndprotector and with a known MAC address, a neighbor solicitation message is sent out periodically. It is believed that NDprotector might have an internal timer that clears the cache, but it's clearing too fast.

The next step is to run a program that clears the cache after each ping. This program will be used with regular Neighbor Discovery and NDprotector and gather those values. After that has been completed, evaluation is performed for ARPsec when it is configured to include IPv6.

10. CONCLUSION

Once ARPsec daemon has been configured to include IPv6 functionality and evaluated, Neighbor Discovery will then have another security measure option. This security measure will be friendly to many machines, unlike SeND. ARPsec with IPv6 provides a new solution to securing Neighbor Discovery.

11. REFERENCES

Butler, Kevin R., Krishnaswamy, Padma, McDaniel, Patrick D., Tian, Jing. “Securing ARP From the Ground Up.” *University of Oregon*, 2013. Web. 15 Jun 2015.

Cheneau, Tony. “Ndprotector.” *Amnesiak,* n.d. Web 12 Jun 2015.

Lenzer, George H. “What is a Link Local Address.” *Server Fault*, 02 Mar 2010. Web. 02 Jun 2015.

n.p. “Comparison of Neighbor Discovery to ARP and Related IPv4 Protocols.” *Oracle*, n.d. Web. 02 Jun 2015.

n.p. “Internet Control Message Protocol.” *Wikipedia*, 17 May 2015. Web. 07 Jun 2015.

n.p. “IPv6 Address Space Management.” *Oracle*, n.d. Web. 07 June 2015.

n.p. “Prefixes in IPv6.” *Oracle*, n.d. Web. 07 Jun 2015.

n.p. “What is IPv6 Autoconfiguration.” *Opus*, n.d. Web. 07 Jun 2015.

Reifschneider, Sean. “Networking Basics: How ARP Works.” *Tummy*, 02 Mar 2013. Web. 07 Jun 2015.

Rouse, Margaret. “Maximum Transmission Unit.” *Search Networking*, n.d. Web. 03 Jun 2015.

Valter. “NDP - Neighbor Discovery Protocol.” *How Does Internet Work,* 31 Dec 2012. Web. 07 Jun 2015.