IPv6 Security Considerations

CITC Task force 14th Meeting

Nov 2014

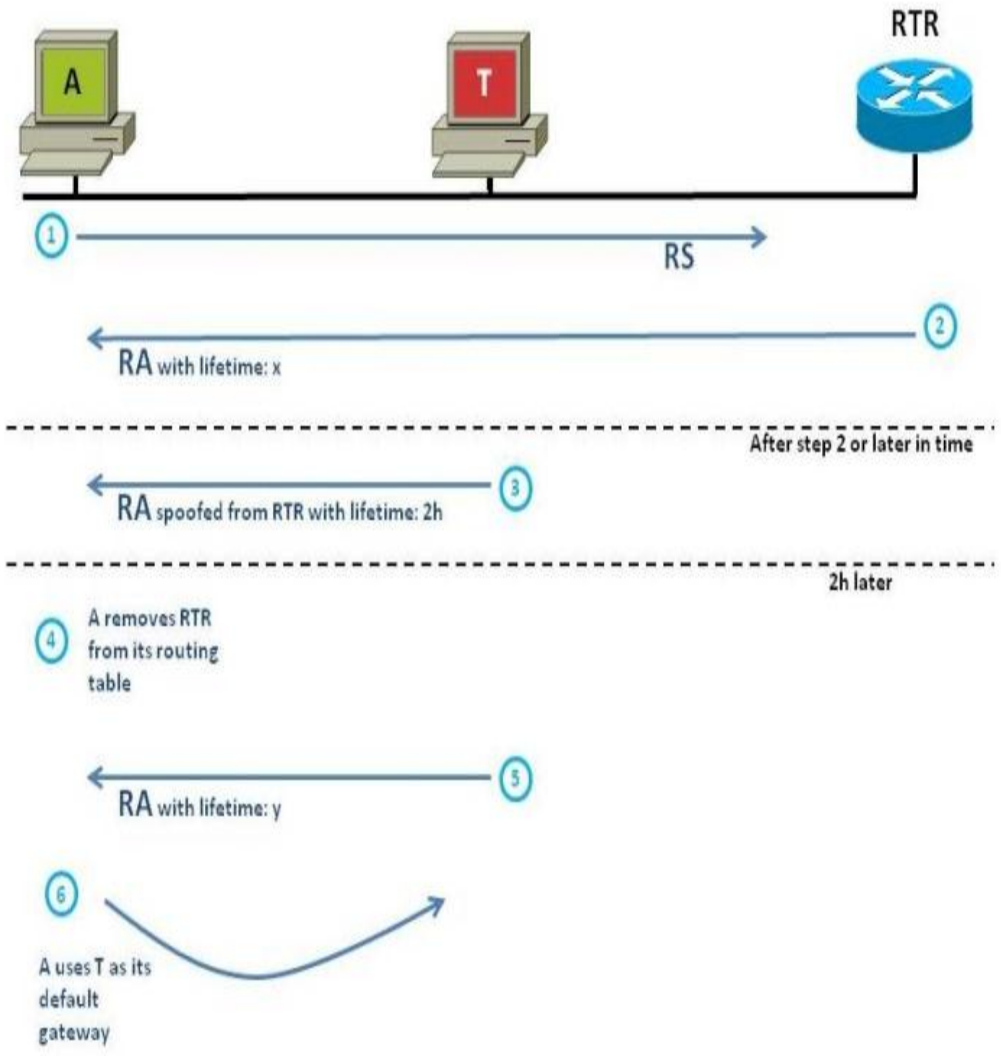
Agenda

- Neighbor Discovery Threats
- Neighbor Discovery Protection
- Best Paractices

Neighbor Discovery Threats

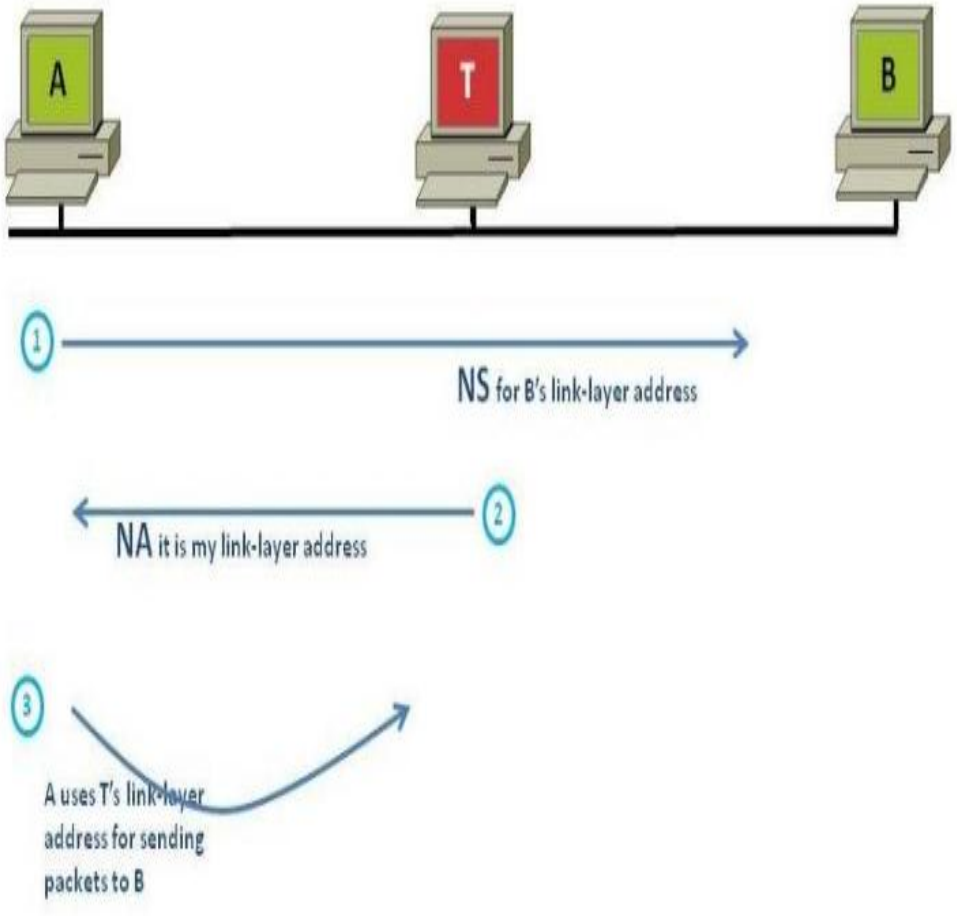
Router Discovery Attack

1. **Host A** sends an ICMPv6 router solicitation message requesting information for the routers in its local link
2. **RTR**, Responds with an ICMPv6 router advertisement for a lifetime x that lets host A know that it is the router in the link
3. **Host A** installs a default route to its routing table that points to RTR for x time.
4. **Host T** could attempt to insert itself as a default router in the routing table of host A
5. If **Host T** succeeds in becoming the default route, it can see all traffic from host A that is using its default route, and may gain additional information or deploy other types of attacks.



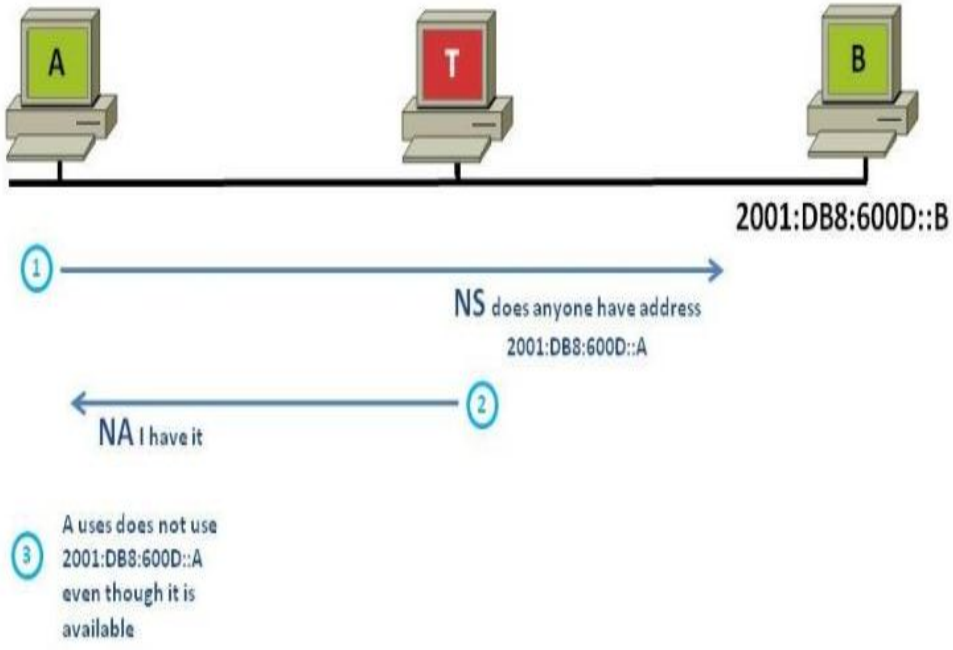
Address Resolution Attack

1. **Host A** sends an ICMPv6 Network solicitation message requesting information for the host in its local link
2. **Host B**, Responds with an ICMPv6 network advertisement for a lifetime x that lets host A know that host B is in the link
3. If **Host T** succeeds in becoming the default route, it can see all traffic from host A that is using its default route, and may gain additional information or deploy other types of attacks.



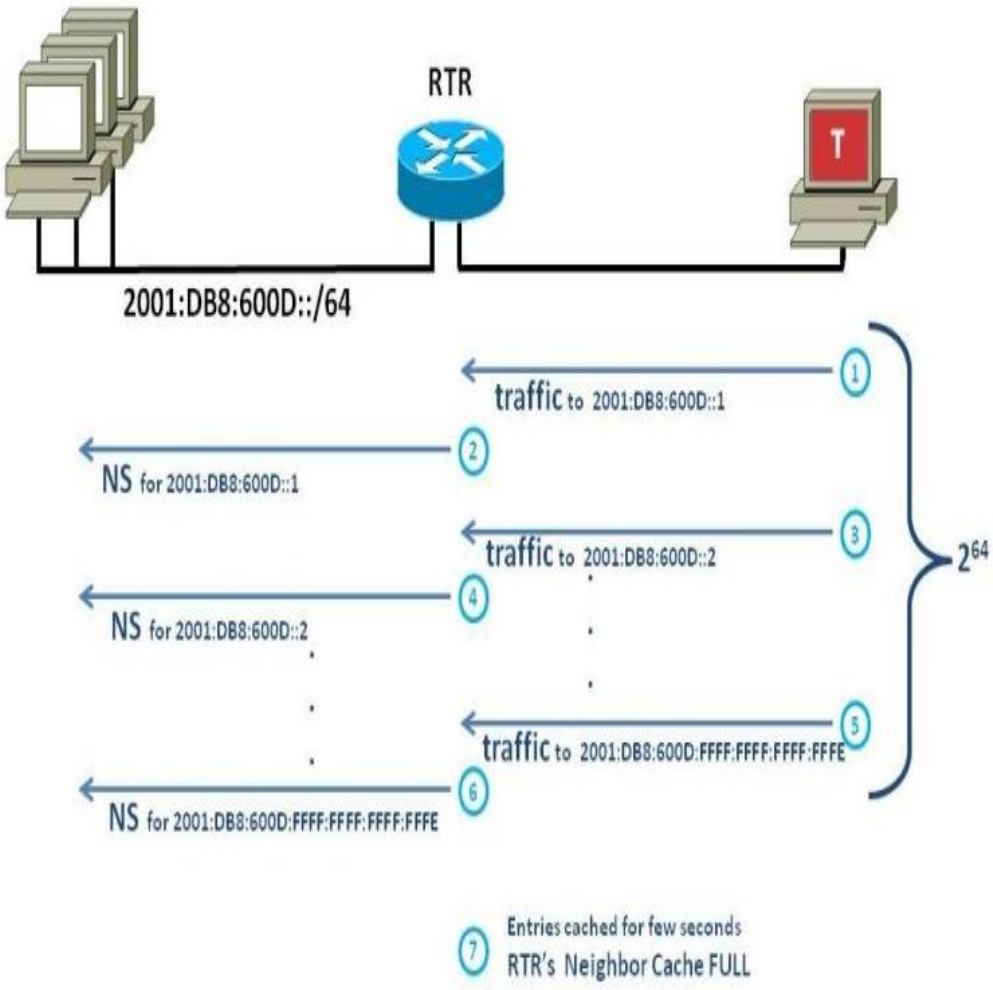
Duplicate Address Detection Attack

1. **Host A** sends an ICMPv6 Network solicitation message requesting information for the host in its local link
2. **Host B**, Responds with an ICMPv6 network advertisement for a lifetime x that lets host A know that host B is in the link
3. **Host T** will impersonate being host B and prevent host A from taking any IP address,



Neighbor Cache Attack

1. Malicious **host T** can attack the neighbor cache of a host or routing device and attempt to fill it or cause a DoS condition
2. **Host T** knows that **RTR** is connected to its link and to a link with hosts in the 2001:DB8:600D::/64 prefix.
3. **Host T** can start scanning 2001:DB8:600D::/64 by sending a packet to the hosts one by one
4. **RTR** will create a cache entry that will be incomplete and remain in the **RTR** neighbor cache for a few seconds until it times out
5. If **Host T** is fast enough it could cause DoS condition

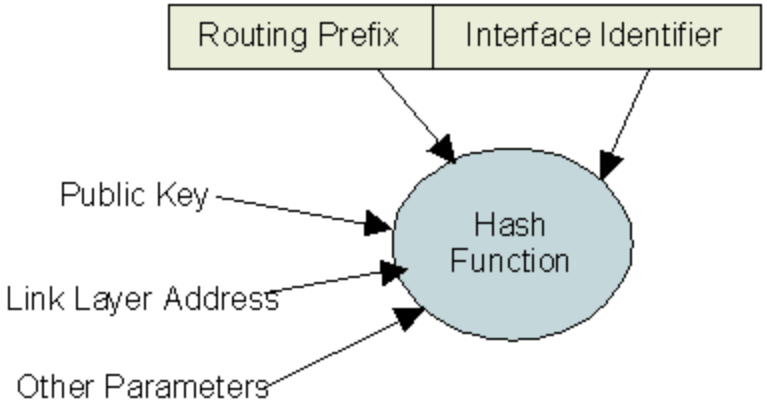


Neighbor Discovery Attacks – The solution

- SeND Protocol
  - Cryptographically Generated Addresses in SeND

    ○ The CGA ensures that the sender of an NDP message is the owner of the claimed address. Before claiming an address, each node generates a public-private key pair and the CGA option verifies this key.

    ○ RSA Signature Option: The public key signatures maintain the integrity of the messages and authenticate the sender identity. The RSA Signature option protects messages by requiring public-key based signatures attached to every NDP message.



  - Authorization Delegation Discovery
    - Authorization delegation discovery is used to certify the authority of routers by using a trust anchor
    - separate certification path solicitation and advertisement messages are used to know the certification path to the trust anchor

Other IPv6 Threats

1. **Reputation-based protection does not yet exist**
   - Many security software vendors use the reputation of IP addresses to filter out malicious websites that are known sources of malware
   - This still does not exist in IPv6.
2. **IPv6 may run by default**
   - All the security measure that you have invested in IPv4 are gone with the wind.
   - You are network is now exposed not secured are more.
   - If you still don't have IPv6 security implemented in your network, make sure to shut down any IPv6 interface in your servers and LAN.
3. **DDoS Attack in IPv6**
   - Hackers use similer tichniqes used in IPv4.
   - Because in IPv6 there is more space attack can be genered from billions of source address to billions of address.
   - Current technologies can't handle that much.
4. **Port Scanning Internal security Audits**
   - One Subnet in IPv6 can have 2^{64} IPv6 addresses.
   - It will take about 50 years to scan one subnet with current technologies.
   - It is recommended to use last /118 of the subnet to make scanning easier.
   - Firewalls has be hardened to protect against external port scanning.

Best Practices

- Use standard, non-obvious static addresses for critical systems
- Ensure adequate filtering capabilities for IPv6
- Filter internal-use IPv6 addresses at border routers
- Block all IPv6 traffic on IPv4-only networks
- Filter unnecessary services at the firewall
- Develop a granular ICMPv6 filtering policy and filter all unnecessary ICMP message types
- Maintain host and application security with a consistent security policy for both IPv4 and IPv6;

Recognized Achievements (1/2)

As part of the strategy of Bayanat/Mobily for IPv6, it has proudly achieved a number of the IPv6 Task Force Strategy Milestones that was developed by CITC in 2008. Showing below the Milestones aligned with Bayanat/Mobily deployment

IPv6 TaskForce Milestones	Contribution and Achievement	Date
IPv6 at ONE FBPs	Announced the connection to a Tier-1 IPv6 International Provider	May 2009
IPv6 Task Force Saudi Arabia	Attendance and Participation of Mobily and Bayanat as one of the first members of Saudi Arabia IPv6 Task Force	Feb 2009
Establish and IPv6 Lab	Deployed a fully service isolated Lab for internal and external awareness and ready for integration with other Labs	Q3 2009
IPv6 National Event	Mobily has hosted one of the IPv6 National meetings for support of awareness and deployment by sharing its own experience with IPv6	May 2009
IPv6 at Multiple FBPs	Partial achievement by support IPv6 service as of Mobily and Bayanat	Since 2009
IPv6 Compliant.SA ccTLD Registry	Partial achievement, by having an IPv6 enabled DNSv6 in the network which can be used for future deployment	Q4 2010
Commercial IPv6 Service Available from 5 ISPs	Partial Achievement, by offering and deploying the first IPv6 transit service with an ISP (Nesma). Also on going pilots are conducted to push the service to end users	Q4 2009

Recognized Achievements (2/2)

IPv6 TaskForce Milestones	Contribution and Achievement	Date
IPv6 Filtering	Successfully demonstrated a working filtering solution for IPv6 and integrated with the commercial IPv6 service offering.	Q1 2012
IPv6 Dual-Stack Network	Successfully build a full dual-stack network for Mobily's International MPLS network.	Q1 2012
IPv6 Native Peering	Native IPv6 peering all major Content providers. (Google, facebook, Yahoo, Akami …)	Q2 2012

Sources

- http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html
- http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html#wp1101791
- http://www.infosec.gov.hk/english/technical/files/ipv6s.pdf
- http://www.esecurityplanet.com/network-security/7-ipv6-security-risks.html
- http://www.ietf.org/rfc/rfc3971.txt
- http://www.ietf.org/rfc/rfc3972.txt

Q & A

Thank You