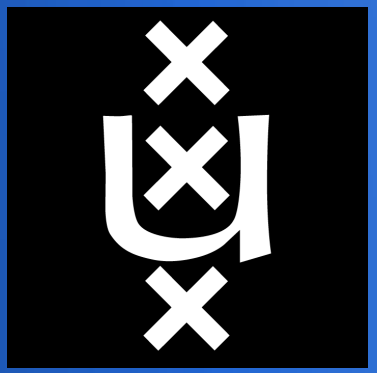
Security of IPv6 and DNSSEC for penetration testers

Vesselin Hadjitodorov

Master education System and Network Engineering

June 30, 2011



Agenda

- Introduction
- DNSSEC security
- IPv6 security
- Conclusion
- Questions

Introduction

- DNSSEC was developed to fix security vulnerabilities of DNS.
  - DNSSEC solves them by introducing signatures
- IPv4 address pool is exhausted.
  - IPv6 has a much larger address space.
- Companies and ISP are switching to Ipv6.
- These protocols are still not fully researched.

Research questions

What are the security issues of IPv6 and DNSSEC and how to perform penetration tests in order to identify them ?

- Are the issues new or were present before ?
- Are there issues during the IPv6 transition period ?
- What tools can be used for performing penetration tests ?
- How to perform tests on the large IPv6 scopes ?

DNSSEC security

DNSSEC security issues

- DNSSEC zone walking
- DNSSEC implementation issues
- DNS DoS amplification attack
  - DNSSEC has larger RRs

DNSSEC zone walking (1/2)

- NSEC RR are used to provide authenticated denial of existence for DNS data.
  - NSEC RR of a domain contain the name of the next domain in the DNS zone.
  - NSEC RR form a chain which can be used to enumerate domains by “walking” the chain.
- NSEC3 RR was developed to fix the problem.
  - NSEC3 uses hashes of the domains in the zone.
  - Hashes can be brute-forced.

DNSSEC zone walking (2/2)

smtp.ipv6.os3.nl. 3600 IN NSEC
sunni.ipv6.os3.nl. AAAA NSEC RRSIG

sunni.ipv6.os3.nl. 3600 IN NSEC
tummi.ipv6.os3.nl. AAAA NSEC RRSIG

tummi.ipv6.os3.nl. 3600 IN NSEC
vpnsmurf.ipv6.os3.nl. AAAA NSEC RRSIG

DNSSEC implementation issues

- Most of the vulnerabilities related to DNSSEC are bugs in the implementations.
  - They can result in:
    - cache poisoning
    - DoS
  - These vulnerabilities can also apply to DNS.

DNSSEC penetration testing tools

DNSSEC penetration testing tools

- Nmap – offers “zone walking” feature
- Nessus – detects implementation specific issues
- OpenVAS – detects implementation specific issues using plugins
- Dig – can query for DNSSEC RRs and validate DNSSEC

IPv6 security

IPv6 security issues

- Neighbor Discovery Protocol
  - NS / NA spoofing – comparable to ARP spoofing in IPv4
  - RS / RA spoofing – comparable to rogue DHCP server on IPv4
  - …
- Routing header type 0
- Implementations
- Transition techniques
- IPv6 smurfing
- Low awareness of IPv6 autoconfiguration

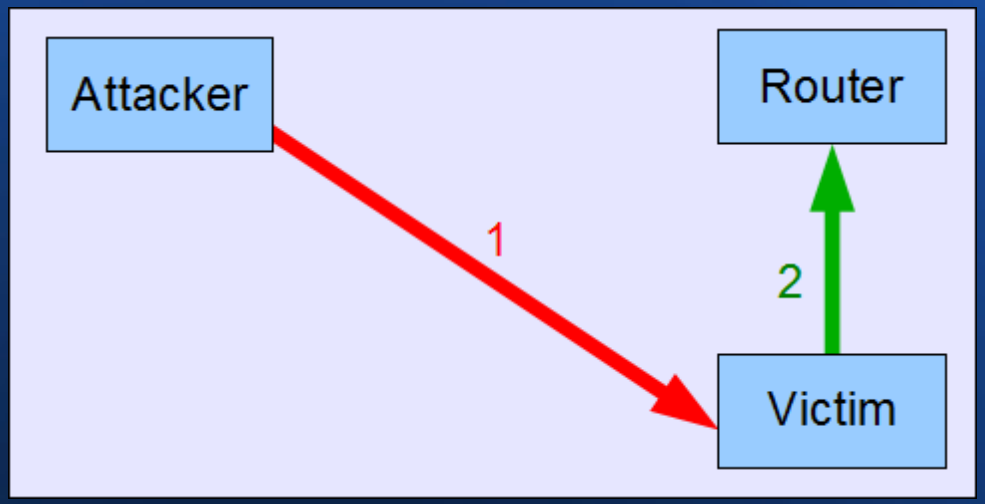
Neighbor Discovery Protocol

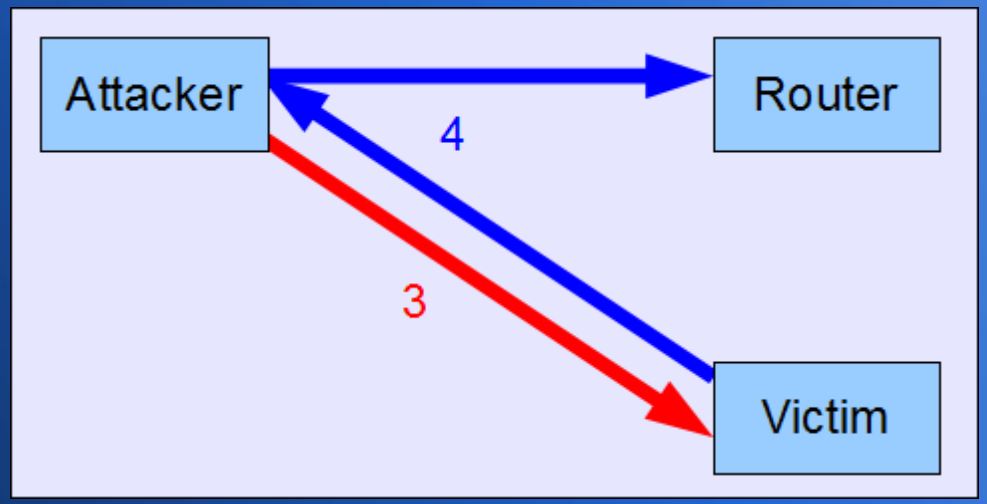
- NDP uses ICMPv6 packets to performs functions similar to ARP in IPv4.
- No authentication mechanism built into ICMPv6, allowing packets to be spoofed.
- Spoofed packets can cause redirection of traffic and DoS.
- These vulnerabilities are limited to the local network.
- Most of the NDP attacks are implemented by Van Hauser in the IPv6 attack toolkit.

NDP host redirection spoofing (1/2)

- Redirection is used by a router to inform a host of a better route to a particular destination.
- The NDP redirect has a security mechanism:
  - A copy of the packet causing the redirection must be included in the NDP redirect message.
- What if the attacker can cause the victim to send a predictable message ?

NDP host redirection spoofing (2/2)





1. The Attacker sends to the Victim an ICMPv6 echo request, with spoofed source address claiming to be originating from the router.
2. The Victim replies to the router with ICMPv6 echo reply.
3. The Attacker knows that the Victim is going to reply and can use the reply message to craft the NDP redirect packet, which advertises the Attacker as a better route to the Router.
4. Now all the traffic which is going from the Victim to the Router goes to the Attacker. The Attacker can sniff the packets and redirect them to the Router in order to stay unnoticed.

Duplicate Address Detection attack

- In IPv6 network it is not allowed the same IP address to be shared by several host.
- A host must verify if an IP is free before using it.
  - The host sends NS and waits for NA message
- An attacker can pretend to use every IP in the network.
  - This will create DoS since the host won't be able to obtain an IP address.

Neighbor Solicitation flooding

- Routers can store limited number of ND cache entries (similar to CAM tables in switches).
- A flood with NS messages can result in:
  - the router might stop learning new entries
  - the router might delete legitimate old entries
  - router crash
- Some hosts might use a “new” IPv6 address for each TCP connection as a security mechanism, resulting in a NS flooding.

Routing header type 0 (RH0)

- RH0 is used to force a packet to follow strictly predefined path between network nodes.
- The same IP address may be included more than once.
- RH0 can be exploited to cause:
  - amplification attack (via packet bouncing)
  - bypassing of firewalls
- RH0 is deprecated since December 2007.

Implementation issues

- Large number of the vulnerabilities in IPv6 are caused by bad implementations.
- They can result in:
  - DoS
  - security policies bypassing
  - buffer overflow
- It is likely that implementations will go better when IPv6 is adopted widely.

Transition techniques issues

Dual-stack networks

- Systems can be subject to attack on both IPv4 and IPv6.
- A firewall may not be enforcing the same policy for IPv4 as for IPv6 traffic due to:
  - Misconfiguration
  - Usage of firewall with limited IPv6 functionality
- This can result in exposing internal services to the Internet.

Tunneled IPv6 over IPv4

- IPv6 address are globally routable, thus allowing hosts behind NAT to be addressed
  - If the hosts were not protected, they will requite installing a firewall before using tunneled IPv6.
- Encapsulated IPv6 traffic could pass unnoticed by the firewall.
- The tunneling programs require opening a port in the firewall that could be used for attacks.

IPv6 penetration testing tools

IPv6 penetration testing tools

- Nmap – partial support of IPv6, still in development
- Nessus – requires the scanning engine to be run under Linux or Mac OS X
- Netcat6 – full support of IPv6
- Metasploit – 19 of 224 payloads are using IPv6
- THC IPv6 attack toolkit – designed for testing IPv6 netwroks

Enumeration of IPv6 hosts

Enumeration of IPv6 hosts

- IPv6 subnets are /64
  - This is 4 294 967 296 times the size of IPv4.
- New approaches have to be used in order to enumerate hosts in IPv6 networks.
  - Reducing the address space
  - DNS

Enumeration of IPv6 host by reducing the address space

- Reducing the address space can be done by analyzing patterns in the address.
- In most cases IPv6 address are not random, but are generated using a system:
  - Consecutive ordered
  - Autoconfiguration
    - hosts with embedded MAC address
    - hosts with embedded IPv4 address

Enumeration of IPv6 host using DNS

- IPv6 address are harder to remember and type.
  - DNS could be more widely used with IPv6
- IPv6 host can be enumerated by:
  - Brute-force
  - Reverse DNS of IPv4
  - Searching the Web for subdomains
  - DNSSEC zone walking

Conclusion

DNSSEC Conclusion

- Are the DNSSEC issues new or were present before ?
  - DNS amplification attack was present before.
  - Implementation vulnerabilities were present also in DNS.
  - DNS zone walking applies only to DNSSEC.
- What tools can be used for performing penetration tests ?
  - DNS querying tools can be used to fetch DNSEC RR.
  - Vulnerability scanners can detect implementation specific issues.

IPv6 Conclusion

- Are the IPv6 issues new or were present before ?
  - Some issues are new and some were present before.
- Are there issues during the IPv6 transition period ?
  - There are issues caused by low awareness and bad implementations of IPv6.
- What tools can be used for performing penetration tests ?
  - Most of the well known penetration testing tools are partially or fully compatible with the IPv6.
- How to perform tests on the large IPv6 scopes ?
  - The IPv6 scopes can be enumerated by analyzing the numbering scheme or by various uses of DNS.

Questions