Development of a Snort IPv6 Plugin
– Detection of Attacks on the Neighbor Discovery Protocol

Martin Schütte, Thomas Scheffler & Bettina Schnor

{mschuette,scheffler}@beuth-hochschule.de, schnor@cs.uni-potsdam.de

IPv6 Security Issues
- Main IPv6 RFCs from 1995/1998, IPv6 has to catch up with 15 years IPv4 security experience
- Many accompanying RFCs and Internet Drafts (IPsec, SEND, RH0 deprecation . . . )
- Few implementations
- Even fewer in deployed end user devices
- Documented attacks against Neighbor Discovery Protocol
- IPv6 implementations (e.g. THC Toolkit)

Snort IDS
- Widely used Open Source NIDS
- Filter/inline mode (Intrusion Prevention System)
- Decoder for common tunnel protocols
- Plugin APIs for processing stages
- Extendable with 3rd party preprocessors, options and rules

Schematic data flow in the Snort IDS

IPv6 Preprocessor
Simple configuration in snort.conf, for example:
```
preprocessor ipv6:
  net_prefix 2001:0db8:1::/64 2001:0db8:2::/64
  router_mac 00:16:76:03:bd:92
```
Added Snort functionality:
- Reads ICMPv6 messages
- Follows network state, i.e. logs (MAC, IP) of:
  - On-link routers
  - On-link hosts
  - Ongoing DADs
- Alerts on new/unknown hosts and routers

IPv6 Preprocessor Alerts
SID: Log Message:
1. RA from new router
2. RA from non-router MAC address
3. RA prefix changed
4. RA flags changed
5. RA for non-local network address prefix
6. RA with lifetime of 0
7. new DAD started
8. new host in network
9. new host with non-allowed MAC address
10. DAD with collision
11. DAD with spoofed collision
12. mismatch in MAC/NDP source link-layer address
13. extension header contains only padding
14. option lengths ≠ extension header length
15. padding option contains data ≠ zero
16. multiple consecutive padding options

New IPv6 Rule Options
- Make all IPv6 fields accessible for Snort signatures:
  - Basic Header, Extension Headers, Neighbor Discovery Options
- Take literal values and comparison operations
- Return match/no_match
- To be used as part of more complex attack signatures

Option: Tests:
- `ipv` IP version
- `ip6_tclass` Traffic Class
- `ip6_flow` Flow Label
- `ip6_exthdr` Extension Header Type
- `ip6_extnum` Number of Extension Headers
- `ip6_option` Destination-/Hop-by-Hop-Option Type
- `ip6_optval` Destination-/Hop-by-Hop-Option Value
- `ip6_rh` Routing Header Type

New Signature Example
```
alert icmp any any -> any any (  
  ipv: 4; itype: 3;  
  msg: "ICMPv4 dest unreachable";  
  sid: 1000002; rev: 1;)
```
```
alert icmp any any -> any any (  
  ipv: 6; itype: 3;  
  msg: "ICMPv6 time exceeded";  
  sid: 1000003; rev: 1;)
```
These Snort signatures use the `ipv` option for IP protocol distinction. A normal Snort configuration provides only the `itype` option and is not able to distinguish these events.

Conclusion
- Successfully tested against our network traffic
- Dynamic library (installs without Snort recompilation)
- Basis for new signatures
- Good performance
- Snort & IPv6-Plugin detects THC attacks

Contact Info
Project Homepage: http://ipv6-ids.de/
Software Repository: http://github.com/mschuett/spp_ipv6

Joint research project of Potsdam University and Beuth University of Applied Sciences Berlin, funded by the German Federal Ministry of Education and Research.