IPv6 Security: Attacks and Countermeasures in a Nutshell

Johanna Ullrich,
SBA Research

Motivation

- Diverse sources for IPv6 security issues
- Collection of issues
- Systematization of Vulnerabilities

https://www.sba-research.org/wp-content/uploads/publications/Johanna%20IPv6.pdf

Classification Attributes

- ***Action:*** assign, flood, insert, listen, send, etc.
- ***Object***
- ***Target***
- ***Unauthorized Result***
- ***Origin*****:** configuration, design, implementation
- ***Type:*** interception, interruption, modification

Classification

- ***Assign:*** set the address for [target] to [object]
- ***Flood:*** emit a high number of [object] to [target]
- ***Insert:*** include [object] into [target]
- ***Listen:*** eavesdrop on the traffic for [object***]***
- ***Scan:*** iterate through the addresses of [target]
- ***Send:*** emit a packet including [object] to [target]
- ***Spoof:*** emit [object] to [target] pretending to be another node

Attacks ...

	ID	Vulnerability	Action	Object	Target	Unauthorized Result	Origin	Type
Security	v01	Fragmentation Header I	send	overlapping fragments		modified header fields	design	modification
	v02	Fragmentation Header II	send	port number in second fragment		middlebox evasion	design	interception
	v03	Fragmentation Header III	flood	fragments		memory shortage	design	interruption
	v04	Fragmentation Header IV	flood	atomic fragments		packet loss	design	interruption
	v05	Routing Header Type 0 I	send	routing header		traffic amplification	design	interruption
	v06	Routing Header Type 0 II	send	routing header		middlebox evasion	design	interception
	v07	Extension Header Options I	send	router alert option		increased workload	design	interruption
	v08	Extension Header Options II	spoof	invalid 10xxxx option	multicast address	multiple responses	design	interruption
	v09	Hop-by-Hop Header	send	hop-by-hop header		increased workload	design	interruption
	v10	New Extension Header	send	unknown extension header		middlebox evasion	design	interception
	v11	New Extension Header	send	unknown extension header		increased workload	design	interruption
	v12	Flow Label I	send	different flow labels		memory shortage	design	interruption
	v13	Flow Label II	send	existing flow label		quality-of-service theft	design	interruption
	v14	Neighbor Advertisement I	spoof	neighbor advertisement		wrongly resolved address	design	interruption
	v15	Neighbor Advertisement II	spoof	neighbor advertisement		traffic redirection	design	modification
	v16	Neighbor Advertisement III	spoof	neighbor advertisement		address assignment prevention	design	interruption
	v17	Router Advertisement I	spoof	router advertisement		new default router	design	modification
	v18	Router Advertisement II	spoof	router advertisement		removed default router	design	modification
	v19	Router Advertisement III	spoof	router advertisement		wrong locally-announced prefix	design	modification
	v20	Router Advertisement IV	flood	router advertisement		multiple address assignment	implementation	interruption
	v21	Router Advertisement V	spoof	router advertisement		prevention of DHCP assignment	design	interruption
	v22	Router Advertisement VI	send	router advertisement		IPv6 activation	implementation	modification
	v23	Redirect I	spoof	redirect		redirected traffic	design	modification
	v24	Redirect II	spoof	redirect		wrong locally-announced node	design	modification
	v25	Echo Request I	spoof	echo request	multicast address	multiple responses	implementation	interruption
	v26	SeND	send	authenticated messages		increased workload	design	interruption
	v27	Tunneling I	send	IPv6 packet as IPv4 payload		middlebox evasion	implementation	interception
	v28	Tunneling II	send	tunnel packet	relay router	cycling packet	implementation	interruption
	v29	Tunneling III	send	tunnel packet		cycling packet	configuration	interruption
	v30	Teredo	send	Teredo bubble	server	cycling packet	design	interruption
	v31	Nesting	insert	packet into packet		packet overhead	configuration	interruption
	v32	Fragmentation Header V	send	packet too big		inclusion of atomic fragments	design	interception
	v33	Neighbor Discovery	scan		subnetwork	memory shortage	implementation	interruption
	v34	Forwarding	send	returning packet		traffic amplification	design	interruption
	v35	Mobile IPv6 I	spoof	binding update	home agent	traffic redirection	design	modification
	v36	Multicast Listener	assign	lowest address	itself	new MDL query router	design	modification

… attacks ...

	ID	Vulnerability	Action	Object	Target	Unauthorized Result	Origin	Type
Privacy	c01	Fragmentation Header VI	send	overlapping fragments		identification	implementation	interception
	c02	Modified EUI Format	scan	interface identifier	networks	tracking	design	interception
	c03	Echo Request II	send	echo request	invalid multicast address	identification of sniffing nodes	implementation	interception
	c04	Mobile IPv6 II	listen	binding update		tracking	design	interception
	c05	DHCP I	listen	DHCP traffic		tracking	design	interception
	c06	DHCP II	send	DHCP information request	DHCP server	tracking	design	interception
	c07	DNS	send	DNS request	DNS server	reconnaissance	design	interception
	c08	Reverse DNS	send	Reverse DNS query		reconnaissance	implementation	interception
	c09	Echo Request III	send	echo request	multicast address	multiple responses	implementation	interception
	c10	Extension Header Options III	send	packet with invalid option	multicast address	multiple responses	design	interception
	c11	Anycast	send		anycast address	response with unicast address	implementation	interception
	c12	Traffic Class	insert	secret information	traffic class field	leaked information	design	interception
	c13	Flow Label	insert	secret information	flow label field	leaked information	design	interception
	c14	Privacy Extension I	insert	secret information	interface identifier	leaked information	design	interception

… and countermeasures

	NDP Mon	Answer with Anycast Address	DHCP	No Forwarding	Fragment Isolation	IPsec	IPsec with Manual Key Configuration	IPv6 Support	Format Deprecation	Multicast Listener Address	No Multiple Edge Routers	No Multiple Tunnels	No Multicast Responses	No Overlapping Fragments	Packet Rate	Physical Protection	Privacy Extension	RA Throttler	No RAs	No Routing Header Type 0	Router Preference	Segmentation	SeND	Subnet Size	Temporary DUID	No Tunneling	Uniform Format	Address Change	Address Checks	Change Field en route	Echo Requests	Hop-by-Hop Options Header	Fragmented Packet Filtering	Invalid Options	Link Layer Access Control	Message Checks	NDP Inspection	RA Guard	RA Filtering	Router Listing	Tunnel Encapsulation Limit Option	Tunnel Ingress and Exit	Unused Addresses
Fragmentation Header I													✓																															
Fragmentation Header II																															✓												
Fragmentation Header III																																											
Fragmentation Header IV					✓																																						
Routing Header Type 0 I																			✓																								
Routing Header Type 0 II																			✓																								
Extension Header Options I																														✓							✓						
Extension Header Options II												✓																		✓	✓												
Hop-by-Hop Header																														✓												
New Extension Header																									✓																		
New Extension Header																									✓																		
Flow Label I																																										
Flow Label II																																										
Neighbor Advertisement I	✓						✓								✓						✓	✓											✓	✓	✓								
Neighbor Advertisement II	✓						✓								✓						✓	✓											✓	✓	✓								
Neighbor Advertisement III	✓						✓								✓						✓	✓											✓	✓	✓								
Router Advertisement I	✓						✓								✓		✓	✓		✓	✓	✓											✓	✓		✓							

Benefits

- Introduction to IPv6 security (for your colleagues ...)
- Overview and common ground for discussion
- Check list, e.g., penetration tests

Challenges (back then)

- Securing the local network (*SeND*)
- Reconnaissance (*maprg*)
- Addressing (*RFC 7217, 4941*)

Challenge (now)

- New privacy legislation in EU in May 2018
- Online identifiers (IP addresses) are considered as personal data (Art. 4)
- Strict data protection rules apply (Art. 5)
- Addresses are stored everywhere ...