IPNG Working Group
Internet Draft
draft-kempf-ipng-netaccess-threats-01.txt
Expires: December, 2002

J. Kempf
E. Nordmark

# Threat Analysis for IPv6 Public Multi-Access Links

## Status of this Memo



## Abstract

The Mobile IP Working Group has been conducting a threat analysis for the purpose of securing specific Mobile IPv6 mechanisms. In the process of conducting the analysis, threats were identified that are not specific to Mobile IP but that are amplified by the nature of mobility. These threats are likely to be more or less of an issue within any Public Multi-Access network, regardless of whether mobility is involved. This document discusses threats associated with Public Multi-Access links in IPv6. The document covers non-Mobile IP specific threats uncovered by the Mobile IPv6 study, threats raised in the IPv6 Neighbor Discovery and Stateless Address Autoconfiguration RFCs that have yet to be adequately addressed, and new threats that have not previously been identified.

## Table of Contents

## 1.0 Introduction

The Mobile IP Working Group has been conducting a threat analysis for securing specific Mobile IPv6 mechanisms [1]. While conducting



---



the analysis, threats were identified that involve host utilization of IPv6 protocols on a Public Multi-Access link, such as 802.11, that were not specific to Mobile IP. Although the initial analysis focused on wireless networks, the identified threats may occur in any Public Multi-Access IPv6 network, such as Ethernet.

Despite the initial impetus given to this study by considering wireless Ethernet, this document is not about link-layer specific security issues, e.g. threats specific to 802.11, but is instead about IP layer threats that are independent of the link layer threats. These threats will remain even for multi-access link layers that are completely secure. One way to think about this is to assume that link layer access is somehow granted securely. This could be done by, for example, granting physical access to an Ethernet plug by some physical security mechanism or by being handed the 802.11 keys necessary to get access to the link layer. The threats that remain after secure link access has been established are the scope of this study.

In this document, threats involved in Neighbor Discovery and Stateless Address Autoconfiguration [2] [5] on a Public Multi-Access link are discussed. The analysis does not recommend any solutions, although it does try to identify what specific part of the IPv6 Neighbor Discovery and Stateless Address Autoconfiguration procedures (e.g. Router Solicitation/Advertisement, Neighbor Solicitation/Advertisement, and Duplicate Address Detection) are impacted by the threats. The analysis in this document explicitly excludes point-to-point links, because the nature of a point-to-point link physically excludes the possibility that a third party could intrude on the activities of a legitimate host. The analysis also excludes any discussion of authentication or authorization of host access, because that work is under the charter of a separate working group.

## 2.0 Previous Work

The RFCs that specify the IPv6 Neighbor Discovery and Address Autoconfiguration protocols [2] [5] contain the required discussion of security in a Security Considerations section. Some of the

threats identified in this document were raised in the original RFCs. The recommended remedy is to include an IPsec AH header [6]. However, this solution is not always possible in a Public Access network. A host attempting to gain access to a Public Access network may or may not have the required IPsec security association set up with the network. In a roaming (but not necessarily mobile) situation, where a user is currently accessing the network through a service provider different from the home provider, it is not likely that the host will have been preconfigured with the proper mutual trust relationship for the foreign provider's network.

Any IPsec security association between the host and the last hop routers or other hosts on the link would need to be completely



---



manually preconfigured, since the Neighbor Discovery and Address Autoconfiguration protocols deal to some extent with how a host obtains initial access to a link. If a security association is required for initial access and the host does not have that association, there is no way that the host can dynamically configure itself with that association, even if it has the necessary minimum prerequisite keying material. This situation could induce administration hardships when events such as re-keying occur.

In addition, Neighbor Discovery and Address Autoconfiguration use a few fixed multicast addresses plus a range of 4 billion "solicited node" multicast addresses. A naive application of pre-configured SAs would require pre-configuring an unmanagable number of SAs on each host and router just in case a given solicited node multicast address is used. Preconfigured SAs are impractical for securing such a large potential address range.

## 3.0 IPv6 Public Multi-Access Link Threat Analysis

There are two general types of threats:

1) Redirect attacks in which a malicious node redirects packets away from the last hop router to another node on the link.

2) Denial of Service (DoS) attacks, in which a malicious node prevents communication between the node under attack and all other nodes, or a specific destination address.

A redirect attack can be used for DoS purposes by having the node to which the packets were redirected drop the packets, either

completely or by selectively forwarding some of them and not others.

The subsections below identify specific threats for IPv6 network access. Redirect threats are included first, DOS attacks second.

### 3.1 Malicious Last Hop Router

This threat was identified in [1], but was classified as a general IPv6 threat and not specific to Mobile IP. It is also identified in [2]. This threat is a redirect attack.

An attacking node on the same subnet as a host attempting to discover a legitimate last hop router could masquerade as an IPv6 last hop router by multicasting legitimate-looking IPv6 Router Advertisements or unicasting Router Advertisements in response to multicast Router Advertisement Solicitations from the entering host. If the entering host selects the attacker as its default router, the attacker has the opportunity to siphon off traffic from the host. The attacker could ensure that the entering host selected itself as the default router by multicasting periodic Router Advertisements for the real last hop router having a lifetime of zero. This



---



essentially spoofs the entering host into believing that the real access router is not willing to take any traffic. Once accepted as a legitimate router, the attacker could send Redirect messages to hosts, then disappear, thus covering its tracks.

This threat involves Router Advertisement and Router Advertisement Solicitation.

### 3.2 Good Router Goes Bad

In this attack, a router that previously was trusted is compromised. The attacks available are the same as those in Section 3.1. This is a redirect attack.

### 3.3 Neighbor Solicitation/Advertisement Spoofing

An attacking node can cause packets for legitimate nodes, both hosts and routers, to be sent to some other link-layer address. This can be done by either sending a Neighbor Solicitation with a different source link-layer address option, or sending a Neighbor Advertisement with a different target link-layer address option.

If the spoofed link-layer address is a valid one, as long as the attacker responds to the unicast Neighbor Solicitation messages sent as part of the Neighbor Unreachability Detection, packets will continue to be redirected. This is a redirect attack.

This mechanism can be used for a DoS attack by specifying an unused link-layer address, however, the attack is of limited duration since after 30-50 seconds (with default timer values) the Neighbor Unreachability Detection mechanism will discard the bad link-layer address and multicast anew to discover the link-layer address. As a consequence, the attacker will need to keep responding with fabricated link layer addresses if it wants to maintain the attack beyond the timeout.

This threat involves Neighbor Solicitation and Neighbor Advertisement messages.

### 3.4 Spoofed Redirect Message

The Redirect message can be used to send packets for a given destination to any link-layer address on the link. The attacker uses the link-local address of the current first-hop router in order to send a Redirect message to a legitimate host. Since the host identifies the message by the link-local address as coming from its first hop router, it accepts the Redirect. As long as the attacker responds to Neighbor Unreachability Detection probes to the link-layer address, the Redirect will remain in effect. This is a redirect attack.

This threat involves Redirect messages.



---



### 3.5 Bogus On-Link Prefix

An attacking node can send a Router Advertisement message specifying that some prefix of arbitrary length is on-link. If a sending host thinks the prefix is on-link, it will never send a packet for that prefix to the router. Instead, the host will try to perform address resolution by sending Neighbor Solicitations, but the Neighbor Solicitations will not result in a response, denying service to the attacked host. This is a DoS attack.

The attacker can use an arbitrary lifetime on the bogus prefix

advertisement. If the lifetime is infinity, the sending host will be denied service until it loses the state in its prefix list e.g. by rebooting, or the same prefix is advertised with a zero lifetime. The attack could also be perpetrated selectively for packets destined to a particular prefix by using 128 bit prefixes, i.e. full addresses.

This threat involves Router Advertisement messages.

### 3.6 Bogus Address Configuration Prefix

An attacking node can send a Router Advertisement message specifying an invalid subnet prefix to be used by a host for address autoconfiguration. A host executing the address autoconfiguration algorithm uses the advertised prefix to construct an address [5], even though that address is not valid for the subnet. As a result, return packets never reach the host because the host's source address is invalid. This is a DoS attack.

This attack has the potential to propagate beyond the immediate attacked host if the attacked host performs a dynamic update to the DNS based on the bogus constructed address. DNS update causes the bogus address to be added to the host's AAAA record in the DNS. Should this occur, applications performing name resolution through the DNS obtain the bogus address and an attempt to contact the host fails. However, well-written applications will fall back and try the other IP address in the AAAA RRset, which may be correct.

This threat involves Router Advertisement messages.

### 3.7 Duplicate Address Detection DoS Attack

In networks where entering hosts obtain their addresses using stateless address autoconfiguration [5], an attacking node could launch a DOS attack by responding to every duplicate address detection attempt by an entering host. If the attacker claims the address, then the host will never be able to obtain an address. This threat was identified in RFC 2462 [5].

This attack involves Neighbor Solicitation/Advertisement.





### 3.8 Neighbor Discovery DoS Attack

In this attack, the attacking node begins fabricating addresses with the subnet prefix and continuously sending packets to them. The last hop router is obligated to resolve these addresses by sending neighbor solicitation packets. A legitimate host attempting to enter the network may not be able to obtain Neighbor Discovery service from the last hop router as it will be already busy with sending other solicitations. This DoS attack is different from the others in that the attacker may be off link. The resource being attacked in this case is the conceptual neighbor cache, which will be filled with attempts to resolve IPv6 addresses having a valid prefix but invalid suffix.

This attack involves Neighbor Advertisement.

### 3.9 Parameter Spoofing

IPv6 Router Advertisements contain a few parameters used by hosts when they send packets and to tell hosts whether or not they should perform stateful address configuration [2]. An attacking node could send out a valid-seeming Router Advertisement that duplicates the Router Advertisement from the legitimate default router, except the included parameters are designed to disrupt legitimate traffic. This is a DoS attack.

Specific attacks include:

1) The attacker includes a Current Hop Limit of one or another small number which the attacker knows will cause legitimate packets to be dropped before they reach their destination.

2) The attacker implements a bogus DHCPv6 server or relay and the 'M' and/or 'O' flag is set, indicating that stateful address configuration and/or stateful configuration of other parameters should be done. The attacker is then in a position to answer the stateful configuration queries of a legitmate host with its own bogus replies.

This attack involves Router Advertisements.

## 4.0 Security Considerations

This document discusses security threats to network access in IPv6. As such, it is concerned entirely with security.

## 5.0 Acknowledgements

Thanks to Alper Yegin, DoCoMo Communications Laboratories USA, for identifying the Neighbor Discovery DOS attack.

## 6.0 References

[1] Mankin, et. al., "Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6," draft-ietf-mobileip-mipv6-scrty-reqts-01.txt, a work in progress.
[2] Narten, T., Nordmark, E., and Simson, W., "Neighbor Discovery for IP Version 6 (IPv6)," RFC 2461, December, 1998.
[3] Blunk, L., and Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)," RFC 2284, March, 1998.
[4] Haskin, D. and Allen, E., "IP Version 6 over PPP," RFC 2472, December, 1998.
[5] Thomas, S., and Narten, T., "IPv6 Stateless Address Autoconfiguration," RFC 2462, December, 1998.
[6] Kent, S., and Atkinson, R., "IP Authentication Header," RFC 2402, November 1998.
[7] Droms, R., editor, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", draft-ietf-dhc-dhcpv6-20.txt, a work in progress.

## 7.0 Author's Addresses

James Kempf
DoCoMo USA Labs
181 Metro Drive, Suite 300 Phone: +1 408 451 4711
San Jose, CA, 95110 Email: kempf@docomolabs-usa.com
USA

Erik Nordmark
Sun Microsystems Laboratories Phone: +33 4 76 18 88 03
29, Chemin du Vieux Chene Fax: +33 4 76 18 88 88
38240 Meylan Email: erik.nordmark@sun.com
France