Network Working Group
Internet-Draft
Expires: October 19, 2006

J. Kempf
DoCoMo USA Labs
C. Vogt
Universitaet Karlsruhe (TH)
April 17, 2006

Security Threats to Network-based Localized Mobility Management
draft-ietf-netlmm-threats-00.txt

Status of this Memo

Copyright Notice

Abstract

This document discusses security threats to NETLMM-based mobility management with a focus on threats on the interface between mobile nodes and access routers. Threats to the NETLMM protocol itself, which runs between the access routers and mobility anchor points, are similar to those faced by other protocols between network entities like routers. These threats are handled in the NETLMM protocol specification. In contrast, threats on the interface between mobile

nodes and access routers are different, because the access routers are presenting the NETLMM domain as a single subnet, in order to allow mobile nodes to continue using the same IP address as they move from one access router to another.

Table of Contents

1. Introduction

The NETLMM architecture supports movement of IPv6 mobile nodes within a localized mobility management domain with minimal involvement on the part of the mobile node itself. In contrast to architectures where there is no localized mobility management support or where localized mobility management support is provided by a host-based solution, in the NETLMM architecture, the mobile node is able to keep its IP address constant within the localized mobility management domain as it moves, avoiding the signaling overhead required to change the address. Software specifically for localized mobility management is not required on the mobile node, though software for IP link movement detection may be needed and of course driver software for link layer movement is always required. More on the localized mobility management problem can be found in [3].

In this document, threats to the protocols involved in implementing the NETLMM architecture are discussed. The document focuses on threats on the mobile node to access router interface. Threats to the NETLMM protocol itself, which runs on the access router to mobility anchor point interface are briefly described, but detailed requirements and solutions for security for the NETLMM protocol are handled in the requirements and NETLMM protocol specification documents [1][4]. While a default IP-based protocol for the interface between mobile nodes and access routers has been specified [2], that interface is the focus of this document because the protocol running across it can potentially be completely handled by the wireless link protocol without any IP involvement. This document is intended to provide guidance to developers linking the NETLMM protocol to such wireless link protocols so that they know what the potential security threats are.

1.1 Terminology

Mobility terminology in this document follows that in [5], with those revisions and additions from [3] and [4].

2. NETLMM Architecture

Figure 1 depicts the NETLMM architecture. A mobility anchor point (MAP) manages routing for packets to mobile nodes as they move through the NETLMM domain. The MAP communicates with a collection of access routers (AR_1 through AR_n in Figure 1). Each access router is connected to a collection of wireless access points (AP_1 through AP_m in Figure 1) that provide wireless access links to mobile nodes.

The access routers handle routing updates to the MAP when a new mobile node moves onto the IP link controlled by the access router. In order for the mobile node to keep its address constant across the NETLMM domain, the access routers must all advertise the same IPv6 subnet prefixes to mobile nodes on their link, and the internal gateway protocol (IGP) used to distribute routes to routers throughout the IGP routing domain must target the MAP as the last hop router for those IPv6 subnet prefixes that span IP links in the NETLMM domain. The MAP tunnels packets to and from the access routers, changing to a new access router when a routing update from a new access router indicates that an mobile node has moved.

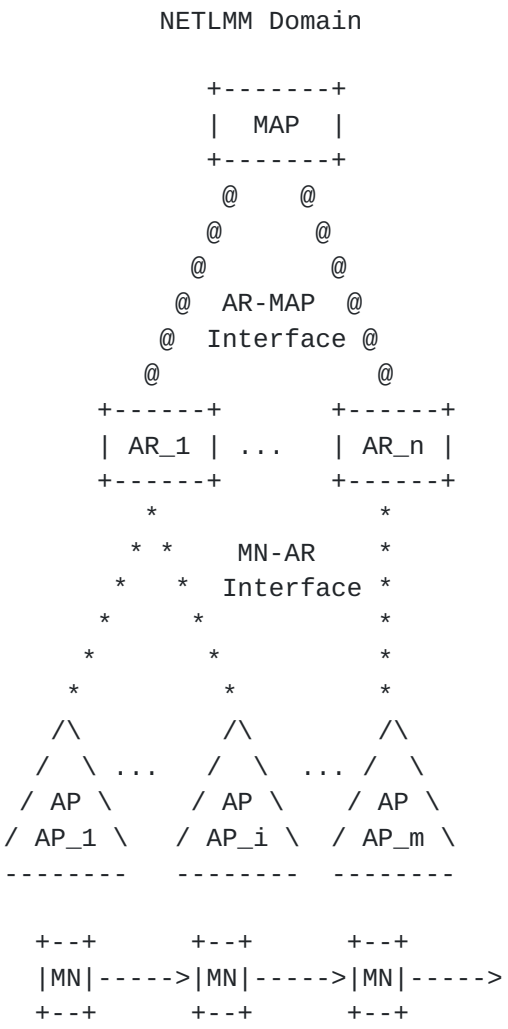

Figure 1: Protocol Interfaces in the NETLMM Architecture

3. Outline of Threats

The threats for the NETLMM architecture break down into two parts:

- Threats on the interface between mobile nodes and access routers.
- Threats on the interface between the access routers and a MAP.

Threats on the interface between mobile nodes and access routers are, in many respects, similar to threats [6] against the IPv6 Neighbor Discovery protocol, except that rather than being confined to a single IP link, the threat potential is distributed across the last hops of the NETLMM domain. The interface between mobile nodes and access routers may run the default IP protocol [2], or it may run a wireless link technology-specific protocol. Threats on this interface are discussed in detail in the following sections.

The threats on the interface between access routers and a MAP are of the same nature as the threats that an IGP for routing faces. Specifically, a rogue MAP or a rouge access router can end up injecting incorrect tunnels or host routes for mobile nodes. This may result in traffic being siphoned off, facilitating impersonation of the mobile node or the mobile node's peer, or in traffic being dropped, resulting in a DoS attack on the mobile node.

Rouge access routers and MAPs can be handled with the same security measures used by IGPs for standard IP routing. Since these threats are specific to the NETLMM protocol, which runs across the interface between the access routers and a MAP, they are discussed in the NETLMM protocol specification [1]. The document also identifies specific security measures for the NETLMM protocol.

Another threat on the interface between access routers and the MAP is DoS against network entities. Here, an attacker manages to obtain a globally routable IP address of an access router, a MAP, or some other network entity, and perpetrates a DoS attack against that IP address. In general, NETLMM-based mobility management is somewhat more resistant to DoS attacks than host-based localized mobility management because nodes within the domain need never obtain a globally routable IP address of any entity within the NETLMM domain. As a consequence, a compromised node cannot pass such an IP address off to an attacker, limiting the ability of an attacker to extract information on the topology of the NETLMM domain. It is still possible for an attacker to perform address scanning if access routers and MAPs have globally routable IP addresses, or for a compromise to happen in another way, but the much larger IPv6 address space makes address scanning considerably more time consuming. Network operators need to take these considerations into account, and ensure that their internal network topologies are sparsely populated.

4. Threats to IPv6 Address to Mobile Node Identifier Mapping

A mobile node identifies itself to the NETLMM domain based on an identifier that is conceptually independent of its IP and link-layer addresses. For packets to be later recognized as coming from the mobile node, the mobile node's identity is tied to its IP address, or possibly to any other identifier which shows up in the packets (e.g., the link-layer address or an IPsec SPI), during the initial authentication procedure. Without lack of generality, it is assumed in the following that the mobile node's IP address is used for this purpose.

Per se, a mapping between the mobile-node identifier and the IP address is insufficient to protect the mobile node against impersonation by a third party. Specifically, the following attacks are conceivable.

4.1 Roaming at a Victim's Costs

Given that regular IP packets do not carry a signature of the mobile node or a comparable proof of origin, an attacker may trick the NETLMM domain into accepting packets, sent by the attacker from the mobile node's IP address, and charging any forwarding services or other due services to the mobile node's account. This allows the attacker to roam across the entire NETLMM domain and communicate at the mobile node's costs.

The attacker not necessarily needs to be a customer of the NETLMM domain since it does not have to authenticate itself to the NETLMM domain. It rather waits for the mobile node to accomplish the authentication procedure. The attacker must also record the mobile node's IP address so that it can later forge packets that appear to be coming from the mobile node. The attack may or may not overlap with a period during which the mobile node itself communicates, and the attacker may or may not be on the same link as the mobile node while the attack proceeds. The duration of the attack depends on how long a refresh interval the NETLMM domain imposes on the mobile node's authentication.

This threat can be eliminated if appropriate per-packet authentication is used for packets that the mobile node sends. The packets can be authenticated either on the link layer or on the IP layer, provided that the IP address, based on which the NETLMM domain identifies the packets as coming from the mobile node, is covered by the protection and securely bound to the authentication context.

A possible mechanism for link-layer authentication is a combination

of IEEE 802.11i technology and a function in the access router that verifies whether or not an inbound packet's IP source address is bound to the link-layer encryption keys. At the IP layer, IPsec AH provides appropriate protection. Note that IPsec ESP is not sufficient as it does not cover a packet's IP header.

A related attack shows the importance of a secure binding between a mobile node's IP address and the keys it uses for per-packet authentication: Failure to provide such a binding allows an attacker, who is itself a customer of the NETLMM domain, to authenticate to the NETLMM domain, obtain the keys for per-packet authentication, and then spoof its IP source address to be the address of some third node. The attacker can thus roam and communicate at its victim's costs.

4.2 Off-Path Eavesdropping

If an attacker can forge a victim's mobile-node identifier or generate packets that appear to originate from the victim, the attacker can siphon off packets meant for the victim and redirect them to its own location. The perpetrator can inspect these packets, effectively waging an "off-path" eavesdropping attack. However, it is impossible for the attacker to forward the packets on to the victim given that the attacker and the victim use the same IP address. The compromised communication session is therefore highly likely to abort before the attack causes significant damage.

The described redirection attack resembles a related man-in-the-middle attack identified in [8]. In that attack, the impersonator manages to redirect packets exchanged between a victim and the victim's peer via itself. Packets thus eventually reach their intended destination, although the attacker can eavesdrop on them or modify them on the fly. The triangular routing becomes possible because the attacker uses a different IP address than its victim. The NETLMM architecture mitigates this attack to some extent in that the attacker cannot redirect a third node's packets unless it somehow duplicates that node's IP address.

4.3 Denial of Service

A similar attack strategy to the one described in Section 4.2 causes denial of service to a victim. Again, the attacker forges the victim's mobile-node identifier or generates packets that appear to originate from the victim, and it thereby redirects the packets meant for the victim to its own location. Any request that the victim sends to nodes located elsewhere than its local link will

consequently solicit responses that the NETLMM domain will route to the attacker's location. As a result, the victim is unable to communicate.

This attack is limited in that the attacker can only redirect the victim's packets to its own location because it must obtain the victim's IP address. This is a natural limitation of the NETLMM architecture because packets are only forwarded to links where the destination node is known (or believed) to be present.

5. Threats to Access Router Functions

An attacker that is able to set up a bogus access router can trick mobile nodes into sending their packets to the attacker. The attacker can thus act as an active or passive man in the middle, possibly forwarding the victim's packets to their actual destination via a path outside the NETLMM domain.

Return packets sent by the victim's peer are likely to be delivered through the NETLMM domain, however. The attacker may hence not be able to manipulate those packets, although it may still read them.

A more sophisticated attacker can impersonate an access router and act as a NAT box at the same time. It tricks a victim into accepting it as its default router and forwards the victim's packets, after manipulation, with an IP source address through which it is itself reachable. Unless the victim's peer expects a particular IP address, it will send any responses "back" to the attacker. The attacker can read and/or manipulate these packets and finally deliver them to the victim.

Essentially, a NETLMM domain is subject to attacks against access routers in the same way as any conventional IPv6 domain. These threats are due to vulnerabilities of the IPv6 Neighbor Discovery protocol, and are as such identified in [6]. In particular, impersonating an access router requires the attacker to send spoofed Router Advertisement messages, which can be precluded, or at least mitigated to a reasonable extent, by SeND [7].

6. Threats to Location Privacy

The location privacy of mobile nodes may be compromised if their identities can somehow be associated to their IP or MAC addresses. This may happen if mobile-node identifiers can be read from the

protocol executed on the interface between mobile nodes and access routers, if the NETLMM protocol run between access routers and the MAP leaks the mobile-node identifiers, or if an attacker manages to steal confidential information from a NETLMM database. Certainly, an attacker may also be able to infer a mobile node's identity from other sources, e.g., from information extracted from application-layer payloads sent or received by the mobile node. But those attacks are not specific to NETLMM and hence outside the scope of this document.

Threats to location privacy that are specific to NETLMM can conceptually be separated into threats that emanate from nodes which are themselves within the NETLMM domain and threats that may also come from nodes outside the NETLMM domain.

6.1 Threats from Nodes within the NETLMM Domain

An attacker within the localized mobility management domain can obtain location information through the usual IPv6 Neighbor Discovery mechanisms. E.g., the attacker can obtain the IP address of a victim within the localized mobility management domain and multicasts a Neighbor Solicitation message to resolve this IP address to the victim's link-layer address. If the attacker receives a Neighbor Advertisement message in response, it knows that the victim is present somewhere in the NETLMM domain.

The obtained location information may be more precise depending on how far beyond the local link IPv6 Neighbor Discovery messages are forwarded by the NETLMM routing fabric. In case such messages are kept link-local, the attacker can even conclude from a received Neighbor Advertisement message that the victim is on the same link.

Likewise, the attacker can use Duplicate Address Detection to determine whether another node is within the localized mobility management domain or on the local link. The attacker multicasts a Neighbor Solicitation message to the solicited-node multicast address for the victim's address. If a Neighbor Advertisement message returns, the attacker knows that the victim is somewhere in the localized mobility management domain or on the local link, depending on whether or not NETLMM routers forward Duplicate Address Detection signaling.

IPv6 Neighbor Discovery messages are normally of link-local scope and as such not forwarded by routers. This is based on the prerequisite that prefix sets of different links are disjunct. However, links within a NETLMM domain all use the same set of prefixes. While this does not necessarily imply that address-resolution messages need to

be distributed across an entire NETLMM domain (link-local redirects may also be feasible), it does imply that messages exchanged for the purpose of Duplicate Address Detection would have to.

More precise location information can only be acquired from a position where the links incoming to and outgoing from the MAP can be monitored. An attacker in this position can listen to the NETLMM protocol traffic between the MAP and the different access routers and thus derive the link where its victim is currently attached to. The attacker may even be able to reasonably track its victim if it has access to only a subset of the links to and from the MAP.

6.2 Threats from Nodes At Any Location

Furthermore, a mobile node's presence within the NETLMM domain is also implied by the prefix of its IP source address. Correspondent nodes can identify the NETLMM domain and coarsely localize the mobile node based on this address, as they could do with any other IP node.

The NETLMM architecture blurs the resolution of such location information to some extent in that the IP source address does not contain information about the link within the NETLMM domain where the mobile node currently is. Tracing tools such as "traceroute" may allow the correspondent node (or any other node with the mobile node's IP address) to obtain the IP addresses of some routers on the path to the mobile node. But since packets are tunneled on the sub-path between the MAP and the mobile node's current access router, the acquired information may not be sufficient to actually locate the mobile node.

The location tracker does not necessarily have to be a correspondent node of its victim. The attacker may also be another node, both outside and within the NETLMM domain, provided that it has somehow obtained the victim's IP address.

This threat can be eliminated by filtering tracing attempts at the NETLMM domain gateways.

7. Security Considerations

This document deals with the security of the NETLMM architecture.

8. Acknowledgment

The authors would like to thank Phil Roberts for his comments and suggestions regarding the initial version of this document.

9. Informative References

[1] "NETLMM Protocol Specification (TBD)", IETF Working Group Item (work in progress).

[2] "NETLMM Mobile-Node Access-Router Protocol Specification (TBD)", IETF Working Group Item (work in progress).

[3] Kempf, J., "Problem Statement for IP Local Mobility", IETF Internet Draft draft-kempf-netlmm-nohost-ps-00.txt (work in progress), June 2005.

[4] Kempf, J., "Requirements and Gap Analysis for IP Local Mobility", IETF Internet Draft draft-kempf-netlmm-nohost-req-00.txt (work in progress), July 2005.

[5] Manner, J. and M. Kojo, "Mobility Related Terminology", IETF Request for Comments 3753, June 2004.

[6] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", IETF Request for Comments 3756, May 2004.

[7] Aura, T., "Cryptographically Generated Addresses (CGA)", IETF Request for Comments 3972, March 2005.

[8] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", IETF Request for Comments 4225, December 2005.

Authors' Addresses

James Kempf
DoCoMo USA Labs
181 Metro Drive, Suite 300
San Jose, CA 95110
USA

Phone: +1 408 451 4711
Email: kempf@docomolabs-usa.com

Christian Vogt
Institute of Telematics
Universitaet Karlsruhe (TH)
P.O. Box 6980
76128 Karlsruhe
Germany

Email: chvogt@tm.uka.de

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.