Network Working Group
Internet-Draft
Expires: January 24, 2007

C. Vogt
Universitaet Karlsruhe (TH)
J. Kempf
DoCoMo USA Labs
July 23, 2006

Security Threats to Network-Based Localized Mobility Management
draft-ietf-netlmm-threats-02.txt

Status of this Memo

Copyright Notice

Abstract

This document discusses security threats to network-based localized mobility management. Threats may occur on two interfaces: the interface between an LMA and a MAG, as well as the interface between a MAG and a mobile node. Threats to the former interface impact the localized mobility management protocol itself.

Table of Contents

1. Introduction

The network-based localized mobility management (NETLMM) architecture [1] supports movement of IPv6 mobile nodes locally within a domain without requiring mobility support in the mobile nodes' network stacks. A mobile node can keep its IP address constant as it moves from link to link, avoiding the signaling overhead and latency associated with changing the IP address. While software specifically for localized mobility management is not required on the mobile node, IP-layer movement detection software may be necessary, and driver software for link-layer mobility is prerequisite.

The IP addresses of mobile nodes have a prefix that routes to a localized mobility anchor (LMA). This LMA maintains an individual route for each mobile node. Any particular mobile node's route terminates at a mobile access gateway (MAG) which the mobile node uses as a default router on its current access link. MAGs are responsible for updating the mobile node's route on the LMA as the mobile node moves. The localized mobility management architecture therefore has two interfaces:

1. The interface between MAGs and the LMA where route update signaling occurs.

2. The interface between mobile nodes and their currently selected MAGs where link-layer handoff signaling and possibly IP-layer movement detection signaling occurs.

The localized mobility management architecture specifies no standardized protocol for a MAG to detect the arrival or departure of mobile nodes on its local link and initiate route update signaling with the LMA. An appropriate mechanism may be entirely implemented at the link layer, such as is common for cellular networks. In that case, the IP layer never detects any movement, even when a mobile node moves from one link to another handled by a different MAG. If the link layer does not provide the necessary functionality, the mobile node must perform active IP-layer movement detection signaling so as to trigger route update signaling at the MAG.

This document discusses security threats on both interfaces of localized mobility management. The discussion is limited to threats specific to localized mobility management; threats to IPv6 in general are documented in [2].

1.1 Terminology

The terminology in this document follows the definitions in [3], with

those revisions and additions from [1]. In addition, the following definition is used:

Network access identity

An identity established for the mobile node during network access authentication that allows the network to unambiguously identify the mobile node for signaling purposes. The network access identity may, e.g., be bound to a link-layer session key, a network access identifier (NAI) [4], or a SEND public key [5].

2. Threats to Interface between LMA and MAG

The localized mobility management protocol executed on the interface between the LMA and a MAG serves to establish, update, and tear down routes for data plane traffic of mobile nodes. Threats to this interface can be separated into compromise or impersonation of a legitimate LMA, compromise or impersonation of a legitimate MAG, man-in-the-middle attacks, and denial-of-service attacks on the LMA.

2.1 LMA Compromise or Impersonation

A compromised LMA can ignore routing updates from a legitimate MAG, or forge routing updates for a victim mobile node in order to redirect or deny the mobile node's traffic. Since data plane traffic for all mobile nodes routes through the LMA, a compromised LMA can also intercept, inspect, modify, redirect, or drop such traffic on a MAG supported by the LMA. The attack can be conducted transiently, to selectively disable traffic for any particular mobile node or MAG at particular times.

Moreover, a compromised LMA may manipulate its routing table such that all packets are directed towards a single MAG. This may result in a DoS attack against that MAG and its attached link.

These threats also emanate from an attacker which tricks a MAG into believing that it is the legitimate LMA. This attacker can cause the MAG to conduct route update signaling with the attacker instead of with the legitimate LMA, enabling it to ignore route updates from the MAG, or forge route updates in order to redirect or deny a victim mobile node's traffic. The attacker does not necessarily have to be on the original control plane path between the legitimate LMA and the MAG, provided that it can somehow make its presence known to the MAG. E.g., the IP address of a mobility anchor point in hierarchical

Mobile IPv6 mobility management [6] may be proliferated across a domain hop by hop in Router Advertisement messages. Failure to properly authenticate a comparable mechanism for localized mobility management would allow an attacker to establish itself as a rouge LMA.

The attacker may further be able to intercept, inspect, modify, redirect, or drop data plane traffic to and from a mobile node. This is obvious if the attacker is on the original data plane path between the legitimate LMA and the mobile node's current MAG, which may happen independent of whether or not the attacker is on the original control plane path. If the attacker is not on this path, it may be able to leverage the localized mobility management protocol to redefine the prefix that the mobile node uses in IP address configuration. The attacker can then specify a prefix that routes to itself. Whether or not outgoing data plane packets sourced by the mobile node can be interfered with by an attacker off the original data plane path depends on the specific data plane forwarding mechanism within the localized mobility management domain. E.g., if IP-in-IP encapsulation or an equivalent per-mobile-node approach is used for outbound data plane packets, the packets will route through the attacker. On the other hand, standard IP routing may cause the packets to be relayed via the legitimate LMA and hence to circumvent the attacker.

2.2 MAG Compromise or Impersonation

A compromised MAG can redirect a victim mobile node's traffic onto its local access link arbitrarily, without authorization from the mobile node. This threat is similar to an attack on a typical routing protocol where a malicious stub router injects a bogus host route for the mobile node. In general, forgery of a subnet prefix in link state or distance vector routing protocols requires support of multiple routers in order to obtain a meaningful change in forwarding behavior. But a bogus host route is likely to take precedence over the routing information advertised by legitimate routers, which is usually less specific, hence the attack should succeed even if the attacker is not supported by other routers. A difference between redirection in a routing protocol and redirection in localized mobility management is that the former impacts the routing tables of multiple routers, whereas the latter involves only the compromised MAG and the LMA.

A compromised MAG can further ignore the presence of a mobile node on its local access link and refrain from registering the mobile node at the LMA. The mobile node then loses its traffic. Attacks that the MAG can mount on its access link interface are common for any regular

IPv6 access router [2].

Moreover, a compromised MAG may be able to cause interruption to a mobile node by deregistering the mobile node at the LMA, pretending that the mobile node has powered down. The mobile node then needs to reinitiate the network access authentication procedure, which the compromised MAG may prevent repeatedly until the mobile node moves to a different MAG. The mobile node should be able to handle this situation, but the recovery process may be lengthy and hence impair ongoing communication sessions to a significant extent.

All of these threats apply not just to a MAG that is compromised, but also to an attacker that manages to counterfeit the identity of an authorized MAG in interacting with both mobile nodes and the LMA. Such an attacker can behave towards mobile nodes like a legitimate MAG and engage the LMA in route update signaling. The attack may be conducted transiently, to selectively disable traffic for any particular mobile node at particular times.

2.3 Man in the Middle Attack

An attacker that manages to interject itself between the legitimate LMA and a legitimate MAG can act as a man in the middle with respect to both control plane signaling and data plane traffic. If the attacker is on the original control plane path, it can forge, modify, or drop route update packets so as to cause the establishment of incorrect routes or the removal of routes that are in active use. Similarly, an attacker on the original data plane path can intercept, inspect, modify, redirect, and drop data plane packets sourced by or destined to a victim mobile node.

A compromised router located between the LMA and a MAG may cause similar damage. Any router on the control plane path can forge, modify, or drop control plane packets, and thereby interfere with route establishment. Any router on the data plane path can intercept, inspect, modify, and drop data plane packets, or rewrite their IP headers so as to divert the packets from their original path.

An attacker between the LMA and a MAG may further impersonate the MAG towards the LMA and vice versa in route update signaling. The attacker can so interfere with route establishment even if it is not on the original control plane path between the LMA and the MAG. An attacker off the original data plane path may undertake the same to cause inbound data plane packets destined to the mobile node to be routed first from the LMA to the attacker, and from there to the mobile node's MAG and finally to the mobile node itself. As

explained in Section 2.1, here, too, it depends on the specific data plane forwarding mechanism within the localized mobility management domain whether or not the attacker can influence the route of outgoing data plane packets sourced by the mobile node.

2.4 Denial of Service Attack on the LMA

An attacker may launch a denial-of-service attack on the LMA by sending packets to arbitrary IP addresses which are potentially in use by mobile nodes within the localized mobility management domain. Like a border router, the LMA is in a topological position through which all data plane traffic goes, so it must process the flooding packets and perform a routing table lookup for each of them. The LMA can discard packets for which the IP destination address is not registered in the routing table. But other packets must be encapsulated and forwarded. A target MAG as well as any mobile nodes attached to its access link are also likely to suffer damage because the unrequested packets must be decapsulated and consume link bandwidth as well as processing capacities on the receivers. This threat is in principle the same as for denial of service on a regular IPv6 border router, but because either the routing table lookup enables the LMA to drop a flooding packet early or, on the contrary, additional tunneling workload is required, the impact of an attack against localized mobility management may be different.

In a related attack, the villain manages to obtain a globally routable IP address of an LMA or a different network entity within the localized mobility management domain and perpetrates a denial-of-service attack against that IP address. Localized mobility management is in general somewhat resistant to such an attack because mobile nodes need never obtain a globally routable IP address of any entity within the localized mobility management domain. A compromised mobile node hence cannot pass such an IP address off to a remote attacker, limiting the feasibility of extracting information on the topology of the localized mobility management domain. It is still possible for an attacker to perform IP address scanning if MAGs and LMAs have globally routable IP addresses, but the much larger IPv6 address space makes scanning considerably more time consuming.

3. Threats to Interface between MAG and Mobile Node

In order to detect the arrival and departure of mobile nodes and accordingly initiate route updates with the LMA, a MAG monitors the mobile nodes' link-layer handoff signaling or IP-layer movement detection signaling. Cellular access technologies utilize only the

signaling at the wireless link layer, and the IP stack never sees any change when the mobile node moves from one MAG to a MAG on a different link. For non-cellular access technologies, such as IEEE 802.11 or wired Ethernet, the link-layer signaling may not hide a handoff from the IP layer. Instead, IP-layer movement detection signaling may have to be performed in response to a notification from the link layer that a change in link-layer attachment has occurred. This signaling may involve extensions [7] for IPv6 Neighbor Discovery [8], DHCPv6 [9], or additional technology-specific functionality at the IP layer. In any case, the security threats on the interface between the MAG and a mobile node are the same. They either pertain to impersonation of the mobile node or to man-in-the-middle attacks.

3.1 Network Access Identity

In order for localized mobility management to be able to definitively and unambiguously identify a mobile node upon handoff, the mobile node must establish a network access identity when it initially connects to the localized mobility managment domain. E.g., the mobile node may authenticate itself to the domain based on its NAI [4] and an AAA-based protocol. The network access identity is conceptually independent of the mobile node's IP or link-layer addresses. For some wireless access technologies, the network access identity must be re-established on every link-layer handoff.

Localized mobility management requires the establishment of a secure binding between the network access identity and either the IP addresses of the mobile node, or any authentication keys associated with these IP addresses. The binding is used by the MAG to deduce that the mobile node has handed over onto the MAG's access link, thereby providing the trigger for route update signaling to the LMA. The binding must be robust to spoofing because it would otherwise facilitate impersonation of the mobile node by a third party or man-in-the-middle attacks.

3.2 Impersonation of Mobile Nodes

An attacker that is able to forge the network access identity of a neighboring victim mobile node can trick its MAG into redirecting the mobile node's packets to itself. Such an on-link attack is common for any regular IPv6 network [2].

However, if handoff signaling cannot definitively be linked back to the legitimate network access identity, an attacker may be capable of fabricating handoff signaling of a victim mobile node that currently attaches to a different link. The attacker can thus trick its MAG

into believing that the mobile node has handed over onto the MAG's access link. The MAG will then initiate route update signaling to the LMA, causing the LMA to redirect inbound data plane packets for the mobile node to the attacker's MAG and finally to the attacker itself. The attacker can so examine the packets that legitimately belong to the mobile node, or discard the packets and deny the mobile node service. This is conceivable both if the attacker and the mobile node are on links that connect to different MAGs, as well as if they are on separate links connecting to the same MAG. In the former case, two MAGs would think they see the mobile node and both would independently perform route update signaling with the LMA. In the latter case, route update signaling is likely to be performed only once, and the redirection of packets from the mobile node to the attacker is internal to the MAG. The mobile node can always recapture its traffic back from the attacker through another run of link-layer handoff signaling and/or IP-layer movement detection signaling. But standard mobile nodes are generally not prepared to counteract this kind of attack, and even where network stacks include suitable functionality, the attack may not be noticeable early enough at the link or IP layer to quickly institute countermeasures. The attack is therefore disruptive at a minimum, and may potentially persist until the mobile node initiates signaling again upon a subsequent handoff.

Off-link impersonation attacks can be prevented at the link layer. E.g., they are not possible with cellular access technologies, where the handoff signaling is completely controlled by the wireless link layer. Here, an attacker must be on the same link as the victim mobile node in order to disrupt the negotiation between the mobile node and the network. Cellular access technologies also provide other cryptographic and non-cryptographic attack barriers at the link layer, which make mounting an impersonation attack, both on-link and off-link, very difficult. For non-cellular access technologies, however, off-link impersonation attacks may be possible.

3.3 Man in the Middle Attack

An attacker which can interpose between a victim mobile node and the MAG during link-layer handoff signaling and/or IP-layer signaling for movement detection, router discovery, and IP address configuration can mount a man-in-the-middle attack on the mobile node, spoofing the mobile node into believing that it has a legitimate connection with the localized mobility management domain. The attacker can thus intercept, inspect, modify, or selectively drop packets sourced by or destined to the mobile node.

4. Security Considerations

This document describes threats to network-based localized mobility management. These may either occur on the interface between the LMA and a MAG, or on the interface between a MAG and a mobile node. Mitigation measures for the threats, as well as the security considerations associated with those measures, are described in the respective protocol specifications [10][11] for the two interfaces.

5. IANA Considerations

This document has no actions for IANA.

6. Acknowledgment

The authors would like to thank the NETLMM working group, especially Jari Arkko, Gregory Daley, Gerardo Giaretta, Wassim Haddad, Julien Laganier, Lakshminath Dondeti, Henrik Levkowetz, Phil Roberts, Vidya Narayanan, and Pekka Savola (in alphabetical order) for valuable comments and suggestions regarding this document.

7. Informative References

[1] Kempf, J., "Problem Statement for Network-based Localized Mobility Management", IETF Internet Draft draft-ietf-netlmm-nohost-ps-04.txt (work in progress), June 2006.

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

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

[4] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", IETF Request for Comments 4282, December 2005.

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

[6] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", IETF Request for Comments 4140, August 2005.

[7] Kempf, J., Narayanan, S., Nordmark, E., Pentland, B., and JH. Choi, "Detecting Network Attachment in IPv6 Networks (DNAv6)", IETF Internet Draft draft-ietf-dna-protocol-01.txt (work in progress), June 2006.

[8] Narten, T., "Neighbor Discovery for IP version 6 (IPv6)", IETF Internet Draft draft-ietf-ipv6-2461bis-07.txt (work in progress), May 2006.

[9] Droms, R., Bound, J., Volz, B., Lemon, T., E., C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", IETF Request for Comments 3315, July 2003.

[10] Giaretta, G., "NetLMM Protocol", IETF Internet Draft draft-giaretta-netlmm-dt-protocol-00.txt (work in progress), June 2006.

[11] Laganier, J., Narayanan, S., and F. Templin, "Network-based Localized Mobility Management Interface between Mobile Node and Access Router", IETF Internet Draft draft-ietf-netlmm-mn-ar-if-01.txt (work in progress), June 2006.

Authors' Addresses

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

Email: chvogt@tm.uka.de

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

Appendix A. Change Log

The following is a list of technical changes that were made from version 01 to version 02 of the document. Editorial revisions are not explicitly identified.

- Section 2.1: Included DoS/flooding attack against MAG. Also clarified how a malicious node off the control plane path between the authorized LMA and one or multiple target MAGs could impersonate the authorized LMA against the MAGs. Such an attacker could use various means to interfer with data plane traffic even if it is off the original data plane path between the legitimate LMA and the MAGs.

- Section 2.2: Malicious MAG may deregister an actively communicating mobile node, without consent of the mobile node.

- Section 2.3: Included related threats pertaining to MITM between LMA and MAG, which were formerly described in other sections.

- Section 2.4: Included description of DoS/flooding attack against LMA, including its impact on the target MAGs, their links, and the target mobile nodes.

- Section 3: Revised the structure of this section. Threats are now divided into attacks against a mobile node's network access identity; impersonation of a mobile node, both from the mobile node's link and from off link; as well as man-in-the-middle attacks.

- Section 3.1: The binding with the network access identity may be with the authentication keys associated with the mobile node's IP address, not necessarily with the IP addresses themselves.

- Section 3.2: Off-link attack may be mounted from a link that connects to a different MAG than the victim mobile node's MAG.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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