Network Working Group
Internet-Draft
Expires: December 25, 2006

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

Security Threats to Network-based Localized Mobility Management
draft-ietf-netlmm-threats-01.txt

Status of this Memo

Copyright Notice

Abstract

This document discusses security threats to NETLMM mobility management. Threats to NETLMM occur on two interfaces: the access router/localized mobility anchor interface and the access router/ mobile node interface. Threats to the access router/localized mobility anchor interface are threats to the NETLMM protocol itself. This document discusses threats on these two interfaces.

Table of Contents

1. Introduction 3
1.1 Terminology 4
2. Threats to the AR/LMA Interface 4
2.1 Unauthorized AR 4
2.2 Unauthorized LMA 5
2.3 Man in the Middle Attack 5
2.4 Denial of Service Attack on the LMA 5
3. Threats to the MN-AR Interface 6
3.1 Mobile Node Identity 6
3.2 Impersonation on Handover 7
3.3 Off-Link Attacks 7
4. Security Considerations 8
5. Acknowledgment 8
6. Informative References 9
Authors' Addresses 10
Intellectual Property and Copyright Statements 11

1. Introduction

The NETLMM architecture supports movement of IPv6 mobile nodes within a localized mobility management domain with no specialized support on the mobile node for localized mobility management. 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 movement detection may be needed and, of course, driver software for link-layer movement is always required. More on the network-based localized mobility management architecture can be found in [1].

In the NETLMM architecture, a localized mobility anchor (LMA) maintains routes for mobile nodes. Packets to and from mobile nodes (MNs) on the last hop wireless links are routed through the LMA. When a MN moves from one access router (AR) to another, the route for the mobile node on the LMA is updated by the ARs. The NETLMM architecture therefore has two interfaces:

1. The AR to LMA interface where route update signaling occurs.

2. The MN to AR interface where movement detection and IP handover signaling occurs.

The NETLMM architecture specifies no standardized protocol on the MN/AR interface. The network must be informed when a mobile node having an IP address moves from one access router to another, but how that occurs is not part of the NETLMM protocol. The mechanism can be entirely implemented by the wireless link protocol, such as is common for cellular networks. In that case, the IP layer never detects any movement, even though the mobile node may be moving from one link to another handled by a different access router. If the wireless link protocol does not handle movement detection and IP handover, however, support at the IP level is required. In that case, the mobile node must perform IP signaling for active movement detection. The access router uses this signaling to infer mobile node movement. More about IP level movement detection and NETLMM can be found in the NETLMM MN-AR interface document [2].

The NETLMM protocol itself is defined on the AR/LMA interface, and is specified in [3].

This document discusses threats to security on the NETLMM interfaces.

The discussion in this document focuses only on NETLMM signaling traffic, both for the NETLMM protocol itself and for signaling on the MN/AR interface that signals mobile node movement to the network. Details on how the threats are handled by the NETLMM protocol and the IP MN/AR interface are discussed in [3] and [2] respectively.

1.1 Terminology

Mobility terminology in this document follows that in [4], with those revisions and additions from [1] and [5]. In addition, the following definition is used:

Network access identity

> A identity established for the mobile node with the network during network access authentication that allows the network to unambiguously identify the mobile node for signaling purposes. For example, a wireless link session key established by the wireless link layer, the Network Access Identifier (NAI) [6], or the SEND public key [7] may serve as the identifier associated with the network access identity.

2. Threats to the AR/LMA Interface

In this section, threats to the AR/LMA interface are discussed. Since the information propagated between the AR and LMA is routing updates, the threats on this interface are similar to the threats experienced by two routers exchanging routing information with a routing protocol. One difference is that the AR and LMA need not be separated by a single hop, whereas routing updates are usually propagated by flooding, so two routers exchanging routing information are usually separated by a single hop.

2.1 Unauthorized AR

An AR that is not authorized to propagate NETLMM routing updates can result in serious damage to the security of a localized mobility management domain. The AR can redirect traffic from MNs on the AR's lst hop link arbitrarily, without authorization from the MN. The AR can ignore routing updates from the LMA so that the victim MNs lose their traffic. An unauthorized AR can also intercept, inspect, and redirect data plane traffic for mobile nodes on its last hop interface, but this threat is common for any last hop router.

Note that this threat applies not just to an AR that is compromised, but also to an off-path attacker that manages to forge the identity of an authorized AR, and thereby spoof the LMA into conducting NETLMM protocol signaling as if the attacker were legitimate. Such an attack could be conducted transiently, to selectively disable traffic for particular mobile nodes at particular times.

2.2 Unauthorized LMA

An unauthorized LMA can ignore routing updates from legitimate ARs, or forge routing updates for MNs in order to redirect or deny traffic to victims. Since data plane traffic for mobile nodes routes through the LMA, a rogue LMA can also intercept, inspect, and redirect data plane traffic for mobile nodes on ARs supported by the LMA. A piece of malware might further manipulate the LMA's routing table such that all packets are directed towards a single AR, resulting in a DoS attack against that AR and its attached link. Again, these are the same threats experienced by any intermediate router in the network.

Note that these threats apply not just to a LMA that is compromised, but also to an off-path attacker that manages to forge the identity of an authorized LMA, and thereby spoof the ARs in a localized mobility domain into conducting NETLMM protocol signaling as if the attacker were legitimate. Such an attack could be conducted transiently, to selectively disable traffic for particular mobile nodes or ARs at particular times.

2.3 Man in the Middle Attack

An unauthorized intermediate router or other node that manages to interject itself between the AR and LMA is in a position to intercept, inspect, and redirect NETLMM protocol signaling traffic between an authorized LMA and authorized ARs handling mobility management for the localized mobility management domain. If the attacker can masquerade as an AR to the LMA and as the LMA to the ARs, it may be in a position to spoof both sides into believing that they have a secure link. The attacker can then utilize the information derived from the NETLMM protocol signaling for various purposes.

2.4 Denial of Service Attack on the LMA

An attacker could launch a denial-of-service attack on the LMA by sending packets to arbitrary IP addresses with a prefix from the NETLMM domain. The LMA is in a topological position through which

all data-plane traffic goes, so it would have to process the flooding packets and perform a routing table lookup for each of them. The LMA could discard packets for which the destination IP address is not registered in the routing table. But other packets would have to be encapsulated and forwarded. There would also be some damage to the target AR and its link.

In a related attack, the attacker manages to obtain a globally routable IP address of an LMA or a different network entity within the NETLMM domain, 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 unauthorized attacker to extract information on the topology of the NETLMM domain. It is still possible for an attacker to perform address scanning if ARs and LMAs 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.

3. Threats to the MN-AR Interface

In order to detect IP level handovers of mobile nodes, NETLMM access routers utilize handover signaling between the mobile node and the access router. For cellular-type interfaces, such signaling occurs at the wireless link layer, and the IP stack never sees any change when the mobile node moves from one AR to an AR on a different link. For non-cellular interfaces, such as 802.11 or wired Ethernet-type interfaces, link layer signaling may not hide IP handover from the IP stack. The IP stack may need to perform movement detection in response to some kind of link layer hint that a change in access point has occurred. This signaling may involve extensions of IPv6 Neighbor Discovery [8] or it may involve DHCP [9] or it may involve some link-specific IP level mechanism. In any case, the security threats to the handover signaling that triggers NETLMM routing updates are the same, and are described in this section.

3.1 Mobile Node Identity

In order for NETLMM to be able to definitively identify a mobile node upon handover, the mobile node must establish a network access identity when it initially enters the network. For example, a mobile node may initially authenticate itself to the NETLMM domain based on

its NAI and an AAA-based protocol. This identifier is conceptually independent of the mobile node's IP or link-layer addresses. In some wireless networks, the network access identity must be re-established on every handover between access points.

NETLMM requires that the access network establish a binding between the network access identity and the IP addresses that the mobile node self-configures (if address auto-configuration is used) or that it is assigned (if stateful address configuration is used). This binding is used by the AR to definitively and unambiguously deduce that a mobile node has handed over into the AR's last hop subnet, thereby providing the trigger for NETLMM route update signaling to the LMA. The binding between the initial mobile-node authentication and the IPv6 addresses must be robust to spoofing, for it would otherwise facilitate impersonation of the mobile node by a third party. Lacking this binding, the following attacks are conceivable.

3.2 Impersonation on Handover

An attacker that is able to forge an MN's network access identity can use this capability to fabricate handover signaling, thereby tricking the AR into believing that the victim has handed over into the AR's last hop subnet. The AR will then perform route update signaling with the LMA, causing the LMA to redirect traffic to the attacker. The attacker can utilize this capability to examine and discard traffic that legitimately belongs to the MN, as a means of denying the MN service or to snoop the MN's traffic. If the attacker can interpose between the MN and the network during router discovery and address configuration, the attacker can mount a man in the middle attack on the MN, spoofing the MN into believing it has a legitimate connection with the network.

3.3 Off-Link Attacks

Depending on the exact nature of the handover signaling, an impersonation attack could be mounted from off link. Off-link attacks are possible in cases where the NETLMM domain consists of multiple access routers serving multiple last hop links. If the security on network access identity establishment is weak, or the IP level movement detection signaling is unprotected so that the network cannot definitively link the signaling back to the legitimate mobile node network access identity, then an attacker from another link could spoof IP level movement detection signaling for a victim mobile node and thereby steal the mobile node's traffic.

Off-link attacks can be prevented at the link-layer. E.g., they are

not possible with cellular-style protocols, where the handover signaling is completely controlled by the wireless link layer, because an attacker must be on the same link with the MN in order to disrupt the negotiation with the network. Cellular-style protocols also have other cryptographic and noncryptographic barriers to attack at the link layer, which make mounting an impersonation attack, both on-link and off-link, very difficult. For non-cellular-style protocols, however, it may be possible for an off-link attacker to mount an impersonation attack.

4. Security Considerations

The document describes threats to the NETLMM protocol [3] and to the MN-AR interface functions necessary to support network-based mobility management [2]. Mitigation measures for these threats, and the security considerations associated with those measures, are described in the respective drafts that discuss the NETLMM protocol and the MN-AR interface.

5. Acknowledgment

The authors would like to thank Gregory Daley, Gerardo Giaretta, Julien Laganier, Phil Roberts, and Vidya Narayanan for their comments and suggestions regarding this document.

6. Informative References

[1] Kempf, J., "Problem Statement for IP Local Mobility", IETF Internet Draft draft-ietf-netlmm-nohost-ps-01.txt (work in progress), April 2006.

[2] Laganier, J. and S. Narayanan, "Network-based Localized Mobility Management Interface between Mobile Node and Access Router", IETF Internet Draft draft-ietf-netlmm-mn-ar-if-00.txt (work in progress), April 2006.

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

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

[5] Kempf, J., "Goals for Network-based Localized Mobility Management (NETLMM)", IETF Internet Draft draft-ietf-netlmm-nohost-req-01.txt (work in progress), April 2006.

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

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

[8] 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-00.txt (work in progress), February 2006.

[9] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", IETF Internet Draft draft-ietf-dna-protocol-00.txt (work in progress), February 2006.

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

[11] 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

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

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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