Network Working Group
Request for Comments: 4832
Category: Informational

C. Vogt
Universitaet Karlsruhe (TH)
J. Kempf
DoCoMo USA Labs

April 2007

Security Threats to Network-Based Localized Mobility Management (NETLMM)

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document discusses security threats to network-based localized mobility management. Threats may occur on two interfaces: the interface between a localized mobility anchor and a mobile access gateway, as well as the interface between a mobile access gateway 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. Software specifically for localized mobility management is not required on the mobile node, whereas 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) [3]. The LMA maintains an individual route for each registered mobile node. Any particular mobile node's route terminates at a mobile access gateway (MAG) [3], to which the mobile node attaches at its current access link. MAGs are responsible for updating the mobile node's route on the LMA as the mobile node moves. A MAG detects the arrival of a mobile node on its local access link based on handoff signaling that the mobile node pursues. The MAG may additionally monitor connectivity of the mobile node in order to recognize when the mobile node has left the local access link. The localized mobility management architecture therefore has two interfaces:

1. The interface between a MAG and an LMA where route update signaling occurs.

2. The interface between a mobile node and its current MAG where handoff signaling and other link maintenance signaling occur.

The localized mobility management architecture demands no specific protocol for a MAG to detect the arrival or departure of mobile nodes to and from its local access link and accordingly initiate route update signaling with an 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 IP-layer movement detection and auto-configuration signaling, thereby providing the trigger for the MAG to update its route on the LMA. A mobile node identity, established by the localized mobility management domain when the mobile node initially connects and authenticates, enables the MAG to ascribe the decisive link- or IP-layer signaling to the correct mobile node. Some wireless access technologies may require the mobile node identity to be reestablished on every link-layer handoff.

Vulnerabilities in either interface of the localized mobility management architecture may entail new security threats that go beyond those that already exist in IPv6. Potential attack objectives may be to consume network services at the cost of a legitimate mobile node, interpose in a mobile node's communications and possibly impersonate the mobile node from a position off-link, operate under the disguise of a false or non-existing identity, or cause denial of service to a mobile node or to the localized mobility management domain as a whole. This document identifies and discusses security threats on both interfaces of the localized mobility management architecture. It is limited to threats that are peculiar to localized mobility management; threats to IPv6 in general are documented in [4].

1.1. Terminology

The terminology in this document follows the definitions in [2], with those revisions and additions from [1]. In addition, the following definition is used:

Mobile Node Identity

> An identity established for the mobile node when initially connecting to the localized mobility management domain. It allows the localized mobility management domain to definitively and unambiguously identify the mobile node upon handoff for route update signaling purposes. The mobile node identity is conceptually independent of the mobile node's IP or link-layer addresses, but it must be securely bound to the mobile node's handoff signaling.

2. Threats to Interface between LMA and MAG

The localized mobility management protocol executed on the interface between an 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, and man-in-the-middle attacks.

2.1. LMA Compromise or Impersonation

A compromised LMA can ignore route updates from a legitimate MAG in order to deny service to a mobile node. It may also be able to trick a legitimate MAG into creating a new, incorrect route, thereby preparing the MAG to receive redirected traffic of a mobile node; it may cause the traffic forwarded by a MAG to be redirected to a different LMA; or it may simply have the MAG drop an existing route

in order to deny the mobile node service. Since data plane traffic for mobile nodes routes through the LMA, a compromised LMA can also intercept, inspect, modify, or drop such traffic, or redirect it to a destination in collusion with the attacker. 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 denial-of-service attack against that MAG and its attached access link.

These threats also emanate from an attacker which tricks a MAG into believing that it is a 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 induce incorrect route changes at the MAG as described above, in order to redirect or deny a 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. Failure to mutually authenticate when establishing an association between an LMA and a MAG would allow an attacker to establish itself as a rogue LMA.

The attacker may further be able to intercept, inspect, modify, drop, or redirect 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 independently of whether 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. For example, if IP-in-IP encapsulation or an equivalent approach is used for outbound data plane packets, the packets can be forced to be routed through the attacker. On the other hand, standard IP routing may cause the packets to be relayed via a legitimate LMA and hence to circumvent the attacker.

2.2. MAG Compromise or Impersonation

A compromised MAG can redirect a 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 an LMA.

Moreover, a compromised MAG can ignore the presence of a mobile node on its local access link and refrain from registering the mobile node at an LMA. The mobile node then loses its traffic. The compromised MAG may further be able to cause interruption to a mobile node by deregistering the mobile node at the serving 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.

Denial of service against an LMA is another threat of MAG subversion. The compromised MAG can trick an LMA into believing that a high number of mobile nodes have attached to the MAG. The LMA will then establish a routing table entry for each of the non-existing mobile nodes. The unexpected growth of the routing table may eventually cause the LMA to reject legitimate route update requests. It may also decrease the forwarding speed for data plane packets due to higher route lookup latencies, and it may, for the same reason, slow down the responsiveness to control plane packets. Another adverse side effect of a high number of routing table entries is that the LMA, and hence the localized mobility management domain as a whole, becomes more susceptible to flooding packets from external attackers (see Section 4). The high number of superfluous routes increase the probability that a flooding packet, sent to a random IP address within the localized mobility management domain, matches an existing routing table entry at the LMA and gets tunneled to a MAG, which in turn performs address resolution on the local access link. At the same time, fewer flooding packets can be dropped directly at the LMA on the basis of a nonexistent routing table entry.

All of these threats apply not just to a compromised MAG, but also to an attacker that manages to counterfeit the identity of a legitimate MAG in interacting with both mobile nodes and an LMA. Such an

attacker can behave towards mobile nodes like an authorized MAG and engage an LMA in route update signaling. In a related attack, the perpetrator eavesdrops on signaling packets exchanged between a legitimate MAG and an LMA, and replays these packets at a later time. These attacks 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 a 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, drop, and redirect data plane packets sourced by or destined to a mobile node.

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

An attacker between an LMA and a MAG may further impersonate the MAG towards the LMA, and vice versa in route update signaling. The attacker can interfere with a 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, then 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.

3. Threats to Interface between MAG and Mobile Node

A MAG monitors the arrival and departure of mobile nodes to and from its local access link based on link- or IP-layer mechanisms. Whatever signaling on the access link is thereby decisive must be securely bound to the mobile node identity. A MAG uses this binding to ascribe the signaling to the mobile node and accordingly initiate route update signaling with an LMA. The binding must be robust to

spoofing because it would otherwise facilitate impersonation of the mobile node by a third party, denial of service, or man-in-the-middle attacks.

3.1. Mobile Node Compromise or Impersonation

An attacker that is able to forge the mobile node identity of a mobile node can trick a MAG into redirecting data plane packets for the mobile node to the attacker. The attacker can launch such an impersonation attack against a mobile node that resides on the same link as the attacker, or against a mobile node on a different link. If the attack is on-link, the redirection of packets from the mobile node to the attacker is internal to the MAG, and it involves no route update signaling between the MAG and an LMA. On-link attacks are possible in a regular IPv6 network [4] that does not use Secure Neighbor Discovery [5].

Off-link impersonation requires the attacker to fabricate handoff signaling of the mobile node and thus trick the MAG into believing that the mobile node has handed over onto the MAG's access link. The attack is conceivable both if the attacker and the mobile node are on separate links that connect to different MAGs, as well as if they are on separate, possibly virtual per-mobile-node links that connect 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 handoff 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.

Impersonation attacks can be prevented at the link layer, particularly with cellular technologies where the handoff signaling between the mobile node and the network must be authenticated and is completely controlled by the wireless link layer. Cellular access technologies provide a variety of cryptographic and non-cryptographic attack barriers at the link layer, which makes mounting an impersonation attack, both on-link and off-link, very difficult. However, for non-cellular technologies that do not require link-layer authentication and authorization during handoff, impersonation attacks may be possible.

An attacker that can forge handoff signaling may also cause denial of service against the localized mobility management domain. The attacker can trick a MAG into believing that a large number of mobile nodes have attached to the local access link and thus induce it to initiate route update signaling with an LMA for each mobile node assumed on link. The result of such an attack is both superfluous signaling overhead on the control plane as well as a high number of needless entries in the LMA's and MAG's routing tables. The unexpected growth of the routing tables may eventually cause the LMA to reject legitimate route update requests, and it may cause the MAG to ignore handoffs of legitimate mobile nodes onto its local access link. It may also decrease the LMA's and MAG's forwarding speed for inbound and outbound data plane packets due to higher route lookup latencies, and it may for the same reason slow down their responsiveness to control plane packets. An adverse side effect of this attack is that the LMA, and hence the localized mobility management domain as a whole, becomes more susceptible to flooding packets from external attackers (see Section 4). The high number of superfluous routes increases the probability that a flooding packet, sent to a random IP address within the localized mobility management domain, matches an existing routing table entry at the LMA and gets tunneled to a MAG, which in turn performs address resolution on the local access link. At the same time, fewer flooding packets can be dropped directly at the LMA on the basis of a nonexistent routing table entry.

A threat related to the ones identified above, but not limited to handoff signaling, is IP spoofing [6]. Attackers use IP spoofing mostly for reflection attacks or to hide their identities. The threat can be reasonably contained by a wide deployment of network ingress filtering [7] in routers, especially within access networks. This technique prevents IP spoofing to the extent that it ensures topological correctness of IP source address prefixes in to-be-forwarded packets. Where the technique is deployed in an access router, packets are forwarded only if the prefix of their IP source address is valid on the router's local access link. An attacker can still use a false interface identifier in combination with an on-link prefix. But since reflection attacks typically aim at off-link targets, and the enforcement of topologically correct IP address prefixes also limits the effectiveness of identity concealment, network ingress filtering has proven adequate so far. On the other hand, prefixes are not limited to a specific link in a localized mobility management domain, so merely ensuring topological correctness through ingress filtering becomes insufficient. An additional mechanism for IP address ownership verification is necessary to prevent an attacker from sending packets with an off-link IP source address.

3.2. Man-in-the-Middle Attack

An attacker that can interpose between a mobile node and a MAG during link- and/or IP-layer handoff signaling may be able to 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 drop data plane packets sourced by or destined to the mobile node.

4. Threats from the Internet

A localized mobility management domain uses individual host routes for data plane traffic of different mobile nodes, each between an LMA and a MAG. Creation, maintenance, and deletion of these routes cause control traffic within the localized mobility management domain. These characteristics are transparent to mobile nodes as well as external correspondent nodes, but the functional differences within the domain may influence the impact that a denial-of-service attack from the outside world can have on the domain.

A denial-of-service attack on an LMA may be launched by sending packets to arbitrary IP addresses that 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 a substantial amount of 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 its routing table. But other packets must be encapsulated and forwarded. A target MAG as well as any mobile nodes attached to that MAG's local 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 the routing table lookups may enable the LMA to drop part of the flooding packets early on or, on the contrary, additional tunneling workload is required for packets that cannot be dropped, the impact of an attack against localized mobility management may be different.

In a related attack, the attacker 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. Hence, a compromised mobile node 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.

5. Security Considerations

This document describes threats to network-based localized mobility management. These may either occur on the interface between an 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 [3][8] for the two interfaces.

6. Acknowledgments

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

7. References

7.1. Normative References

[1] Kempf, J., Ed., "Problem Statement for Network-Based Localized Mobility Management", RFC 4830, April 2007.

[2] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

7.2. Informative References

[3] Levkowetz, H., Ed., "The NetLMM Protocol", Work in Progress, October 2006.

[4] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[5] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[6] CERT Coordination Center, "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks", September 1996.

[7] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[8] Laganier, J., Narayanan, S., and F. Templin, "Network-based Localized Mobility Management Interface between Mobile Node and Access Router", 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
3240 Hillview Avenue
Palo Alto, CA 94304
USA

EMail: kempf@docomolabs-usa.com

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

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