INTERNET DRAFT
Category: Informational
Document: draft-mutaf-paging-security-requirements-00.txt
Date: May, 2001

P. Mutaf
C. Castelluccia
INRIA

IP Paging Security Requirements

Status of This Memo

Abstract

This document contains a risk assessment of IP paging. The described risks are probably independent of any underlying functional architecture and mobility protocol.

Accordingly, several security requirements are defined. These requirements are to be supported by an IP paging protocol in order to completely defeat or not to encourage the relevant attacks.

Table of Contents

1.0 Introduction

"Paging" is one of the main components of mobility management in wireless networks. Combined with "registration", paging is an optimization method for reducing (i) the signaling costs due to location tracking and (ii) the power consumption of battery powered mobile nodes in dormant mode.

However, an IP paging protocol may introduce security issues. These may include some new security problems which will affect the operation of the Internet and/or some threats against the proper operation of the IP paging protocol itself.

This document describes the risks of paging and defines several requirements to be supported by an IP paging protocol.

2.0 Terminology

Please see [STAT,PREQ] for definition of terms used in this document.

3.0 Assumptions

We assume that all IPsec functionalities are available to the functional entities of IP paging [IPSEC]. These entities are described in [PREQ]. In particular, we assume that any kind

of location registration is authenticated and immune to replay attacks. Otherwise the protocol will be vulnerable as described in [MIP,MIP6].

4.0 Risks of Paging

4.1 DoS Amplification

A DoS (Denial-of-Service) or DDoS (Distributed DoS) attack generally consists of flooding a target network with bogus IP packets in order to cause degraded network performance at victim nodes and/or routers. Performance can be degraded to the point that the network cannot be used. Currently, there is no preventive solution against these attacks, and the impacts can be very important.

In general a DoS attacker profits from a so-called "amplifier" in order to increase the damage caused by his attack. Paging can serve for an attacker as a DoS amplifier.

An attacker (a malicious correspondent node) can send large numbers of packets pretending to be sent from different (bogus) correspondent nodes and destined for large numbers of mobile nodes in inactive and dormant modes. This attack, in turn, will be amplified by the paging agent which wide casts paging messages over paging areas, resulting in several networks being flooded. Clearly, the damage can be more important in wireless networks which already suffer from scarce radio bandwidth.

Alternatively, an attacker can sort out a mobile node which:

(i) sends periodic messages declaring that it is in dormant mode,

(ii) never replies to paging requests.

Such a node may be the attacker's node itself, or a second node participating in the attack.

That node is never in inactive mode because of (i). In this case, the attacker can send large numbers of packets destined for that mobile node which periodically declares that it is in dormant mode but never replies to paging messages. The impact will be the same as above however in this case the attack will be amplified indefinitely.

4.2 Selective DoS against Mobile Nodes

The following vulnerabilities may already exist in the absence of paging. However, they are included here since they can affect the correct operation of the IP paging protocol.

These vulnerabilities can be exploited by an attacker in order to eliminate one or more particular mobile nodes. This, in turn, can be used as a stepping stone to launch other attacks.

4.2.1 Forced Battery Consumption

An attacker can frequently send packets to a mobile node in order to prevent that mobile node from switching to dormant mode. As a result the mobile node may quickly run out of battery, hence become inaccessible.

4.2.2 Paging Queue Overflow

For reliability reasons, the paging protocol may need to make provisions for a "paging queue" where a paging request is buffered until the requested mobile node replies by sending a location registration message.

An attacker can exploit that by sending large numbers of packets having different (bogus) correspondent node addresses and destined for one or more inactive mobile nodes. These packets will be buffered in the paging queue. However, since the mobile nodes are inactive, the paging queue may quickly overflow, blocking the incoming traffic from legitimate correspondent nodes. As a result, all registered dormant mobile nodes may be inaccessible for a while. The attacker can re-launch the attack in a continuous fashion.

4.2.3 Bogus Paging Areas

An attacker can periodically emit malicious packets in order to confuse one or more mobile nodes about their actual locations. Currently, there is no efficient way to authenticate such packets.

In the case of IP paging, these packets may also contain bogus paging area information. Upon receipt of such a packet, a mobile node may move and send a location registration message pointing to a non-existing or wrong paging area. The functional entities of the IP paging protocol may loose contact with the mobile node. Depending on the paging strategy, additional harm can be caused.

This attack can also serve for sorting out a mobile node which shows the behaviors (i) and (ii) described in Section 4.1.

4.3 Attacks against the Functional Entities

According to [PREQ] the monitoring, tracking and paging agents can be separate network elements or combined into a single network element. In the former case an attacker can spoof the traffic between these entities.

The impacts can range from DoS amplification to loss of contact

with one or more mobile nodes.

5.0 IP Paging Security Requirements

The following security requirements are to be supported by the IP paging protocol.

5.1 General Requirements

- The IP paging protocol MUST be able to handle large numbers of paging requests without denying access to any legitimate IP node nor degrading its performance.

- If the tracking, monitoring and paging agents are separate network elements, any traffic between these entities MUST be authenticated.

- The IP paging protocol SHOULD depend on provisions for "authorization" in order to prevent a malicious mobile node from registering its address with the functional entities of the IP paging protocol.

- The security of the IP paging protocol MUST NOT call for additional power consumption on mobile nodes, excessive message exchanges in wired and/or wireless links, nor excessive paging delays.

5.2 IPsec Requirements [IPSEC]

A mobile node may have security associations (SAs) with some of the correspondent nodes. Mobile nodes must be able to decide security policies just like any other node of the Internet.

- The IP paging protocol MUST NOT impose any limitations on mobile nodes' security policies.

- The IP paging protocol MUST NOT break the end-to-end properties of the IPsec protocols.

These requirements mandate that the functional entities of the IP paging protocol do not have any knowledge about what kind of SAs a mobile node have with which correspondent nodes, nor the intervening IPsec keys.

For clarity, these requirements also mandate that a dormant mobile node MAY NOT reply to a correspondent node if its security policies dictate to do so.

5.3 Attack-Specific Requirements

5.3.1 Detection of Inactive Mobile Nodes

According to [PREQ], the protocol SHOULD provide a mechanism to allow a mobile node to declare its transition to inactive mode. In this case, the inactive mode will not be unnecessarily paged

when it is completely unreachable.

Due to many factors, a mobile node may not be capable of signaling its transition to inactive mode. For example, the mobile node may be out of range of a radio access point, run out of battery, etc. The mobile node may also have a pathological behavior due to an implementation error, hence may not behave as expected. This might victimize many other nodes in the case of an attack. Furthermore, a mobile node itself may be malicious, hence not respect the requirements.

- The IP paging protocol SHOULD make provisions for detecting inactive mobile nodes without denying service to any legitimate node.

This requirement helps defend against the attacks described in Sections 4.1 and 4.2.2.

5.3.2 Detection of Bogus Correspondent Nodes

- The IP paging protocol SHOULD make provisions for detecting and ignoring bogus correspondent nodes.

- A bogus correspondent node SHOULD be detected and ignored before any paging message is wide cast on behalf of that correspondent node.

These requirements help defend against the attacks described in Sections 4.1, 4.2.1 and 4.2.2.

5.3.3 Authenticity of Paging Areas

- The IP paging protocol SHOULD make provisions for preventing or detecting the propagation of bogus paging area and location information.

This requirement helps defend against the attacks described in Sections 4.2.3 and 4.1.

6.0 Security Considerations

This document discussed some security risks and requirements relevant to IP paging.

References

[IPSEC] Kent, S., and Atkinson R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[MIP] Perkins, C., ed., "IP Mobility Support," RFC 2002, October,

1996.

[MIP6] Johnson, D., and Perkins, C., "Mobility Support in IPv6," draft-ietf-mobileIP-ipv6-13.txt, work in progress.

[PREQ] Kempf, J. et al, "Requirements and Functional Architecture for an IP Host Alerting Protocol", draft-ietf-seamoby-paging-requirements-01.txt, work in progress.

[STAT] Kempf, J., "Sending IP Traffic to Dormant Mobile Devices: Problem Statement," draft-ietf-seamoby-paging-problem-statement-02.txt, work in progress.

Authors' Addresses

Pars Mutaf
INRIA Rhone-Alpes
655 avenue de l'Europe
38330 Montbonnot Saint-Martin
FRANCE

email: pars.mutaf@inria.fr
phone: +33 4 76 61 55 07
fax: +33 4 76 61 52 52

Claude Castelluccia
INRIA Rhone-Alpes
655 avenue de l'Europe
38330 Montbonnot Saint-Martin
FRANCE
email: claude.castelluccia@inria.fr
phone: +33 4 76 61 52 15
fax: +33 4 76 61 52 52