MIP6 WG
Internet-Draft
Expires: August 5, 2004

X. Chen
Orange PCS Ltd.
M. Watson
Nortel Networks
M. Harris
Orange PCS Ltd.
February 5, 2004

Problem Statement for MIPv6 Interactions with GPRS/UMTS Packet Filtering
draft-chen-mip6-gprs-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 5, 2004.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This document provides an analysis of certain inter-working problems between IPv6 nodes running Mobile IPv6, at least one of which is connected to a GPRS/UMTS network. The inter-working problems are caused by some specific packet filtering operations at the edge of the GPRS/UMTS network which are applied to control access to the GPRS/UMTS services and network resources. However, we believe that other scenarios may exist in which similar packet filtering operations may be applied and that similar problems would arise in these, more general, scenarios.

The GGSN checks the source address or the destination address in the basic IPv6 header of incoming or outgoing IP datagrams against a set of packet filtering information established during the GPRS/UMTS session set-up. The packet filtering information remains stable during the sessions and independent of Mobile IP. When MIPv6 is activated by either end of the IPv6 mobile nodes, the packet filtering will fail to perform properly and subsequently block the traffic due to the mismatch between the packet filters and the current source address or destination address in the basic IPv6 header of the IP datagrams to and from the IPv6 mobile nodes.

Table of Contents

1. Introduction

Mobile IPv6 [1] allows a mobile node to maintain its IP connectivity regardless of its network attachment point. Packets sent to the mobile node may still use its home address, or the care-of address of the mobile node as the destination address. The mobile node may continue to communicate with its existing communication peers (stationary or mobile) by using its topologically correct IP addresses. An important and highly desirable feature of mobile IP based mobility is that the control is transparent to transport and higher-layer protocols and applications, i.e. the higher layer protocols and applications function as if the mobile node is "stationary".

Packet filtering in GPRS/UMTS is used for differentiating GPRS/UMTS connections and QoS, and protecting the network resources and services against Theft of Service attacks. It is achieved by checking the header information of the incoming and outgoing IP datagrams against a set of packet filtering information. The packet filtering information is defined or authorised by the application layer entities during the set-up of the GPRS/UMTS and IP Multimedia Subsystem sessions and operates independently of Mobile IP. This pre-defined packet filtering information is then used by the GGSN to check the header of incoming or outgoing IP datagrams so as to select the appropriate GPRS/UMTS sessions with QoS or control the access to network resources and IMS services based on the operator defined local policies. For example, the Service-based Local Policy control (SBLP) in UMTS IP Multimedia Subsystems (IMS) enables the GGSN to check the destination address for outgoing IP datagrams according to policy information authorised by the Policy Decision Function during the IMS session establishment.

When Mobile IPv6 is activated, an IPv6 node sends IP datagrams using Care-of Address as either the destination address or source address while its home address is carried in the extension headers. The change of source address or destination address in the basic IPv6 header from the mobile node's home address to its care-of address or from one care-of address to another during a session leads to a mismatch with the header information such as the source address or destination address in the set of parameters for packet filtering information and, as a result, the discard of incoming or outgoing IP datagrams by the GGSN.

In the following sections, the basic packet filtering operations in GPRS/UMTS are described and followed by the analysis of the failure of those operations when Mobile IPv6 is activated.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED","SHALL","SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [4].

3. Packet Filtering in GPRS

The following sections list some packet filtering operations in GPRS/ UMTS. It is not intended to exhaust all the possible application scenarios for packet filtering operations in 3G networks such as those used by Firewalls.

3.1 Mobile Terminal Defined Packet Filtering

To support multimedia services with differentiated QoS, GPRS/UMTS networks support multiple simultaneous sessions as typically represented by multiple secondary PDP (Packet Data Protocol) Contexts [5]. Each GPRS/UMTS session may be assigned specific QoS with the necessary network resources (including radio resources). An incoming IP datagram from the external public data network such as Internet will be checked by the GGSN, to decide if there is an existing GPRS/UMTS session to deliver the datagram through the network to the mobile terminal. The basic IPv6 header as well as some higher layer information such as the ports is checked against a Traffic Flow Template (TFT) [6] that contains the packet filtering information such as the IPv4/IPv6 Source Addresses, Protocol Identifier, Source/Destination Ports, etc.

The TFT is generated by the mobile node and recorded by the GGSN upon a successful establishment of a GPRS/UMTS session for the mobile node. The GGSN will use at least one of those packet filter parameters, primarily the Source Address, to check if an appropriate GPRS/UMTS session has been set up for incoming traffic. The GGSN searches for a GPRS/UMTS session with the TFT that contains the parameter values matching those carried in the datagram. For example, the Source IP Address field of each existing TFT will be compared with the source address carried in the basic IPv6 header of an IPv6 datagram. If no matching TFT is found, the datagram may be discarded.

3.2 Network Service Defined Packet Filtering

The IP Multimedia Subsystem (IMS) [7] is defined by 3GPP to provide SIP-based IP multimedia services. In IMS, Service-based Local Policy control(SBLP) [8][9] is enforced by the GGSN to authorise and control the access to the IMS services and the GPRS/UMTS network resources based on operator defined local policies.

An IMS service request, a GPRS/UMTS session set-up request and the subsequent data packets originated by the mobile terminal will be checked by the GGSN against a set of policy control information parameters such as Destination Address, Destination Port Number, Transport Protocol ID, etc. The policy control information is issued as an authorisation from the upper layer (the IMS/Policy Decision Function -PDF). An IP datagram carrying a IMS service request or user data will be blocked by the GGSN if mismatch is found between the authorised policy information and those carried by the IP datagram. For example, an IMS service request or a VoIP packet will be blocked by the GGSN if the destination address carried by the IP datagram does not match that authorised by the Policy Decision Function. This is designed for protecting GPRS/UMTS and IMS against ToS attacks.

4. Problem statement

The problem is stated in terms of an IPv6 node, A, communicating with a second IPv6 node, B. B is connected to the GPRS/UMTS network. We consider in turn the cases in which the GPRS node, B, is acting either as a Correspondent Node or as a Mobile Node.

For each case, we consider sub-cases related to terminal defined filters (i.e. TFTs) and network defined filters (i.e. SBLP).

Further, for each sub-case, we further consider the use of Home Agent tunnelling and Route Optimisation by the Mobile Node.

4.1 GPRS node, B, acting as Correspondent Node

This is the case where A is a Mobile Node having live multimedia sessions with a Correspondent Node, B. B is connected to a GPRS/UMTS network. The sessions are set up when A is connected to its home network link.

4.1.1 Mobile Terminal defined Packet Filtering (TFTs)

Upon an successful establishment of multimedia sessions between A and B, each session is associated with a TFT packet filter(s) defined by B which have A's home address as the source address for IP datagrams sent from A to B. The GGSN uses these packet filters to decide which PDP Context to use to deliver an incoming IP datagram to B.

4.1.1.1 Home Agent Tunnelling

The IP datagrams sent from A to B use the (reverse) tunnel from AÆs current CoA to its HA. IP datagrams exit the tunnel at AÆs home agent and transmit to B using AÆs home address as the source address. Upon

arriving at the GGSN, the IP datagramsÆ source address matches the IPv6 source address (AÆs home address) recorded in one of the TFT filters and, if other filtering parameters are matched as well, the IP datagrams will be delivered to B through the PDP Context corresponding to the TFT. No specific issues are identified for this case.

4.1.1.2 Route Optimisation

When A moves away from its home network link and connects to a foreign network link and attempts the Mobile IPv6 binding update procedures, it starts sending IP datagrams to B directly using its CoA address as the Source Address and carrying its Home Address in the Home Address Destination Type 2.

When such an IP datagram sent from A arrives at the GGSN, it does not match the TFT packet filters containing AÆs home address as the IPv6 source address. As result, two possible decisions can be made by the GGSN; If there happens to be a different PDP Context with a TFT which does match AÆs CoA or a PDP Context without an associated TFT, the GGSN will decide to use it to deliver the IP datagram to B. But in this case it may not receive the correct Quality of Service treatment.Additionally, the PDP Context with the Quality of Service appropriate for delivering the IP datagram is left unused.

The following diagram shows an example of two GPRS sessions that are distinguished by GGSN using TFT packet filters, TFT1 and TFT2, respectively.

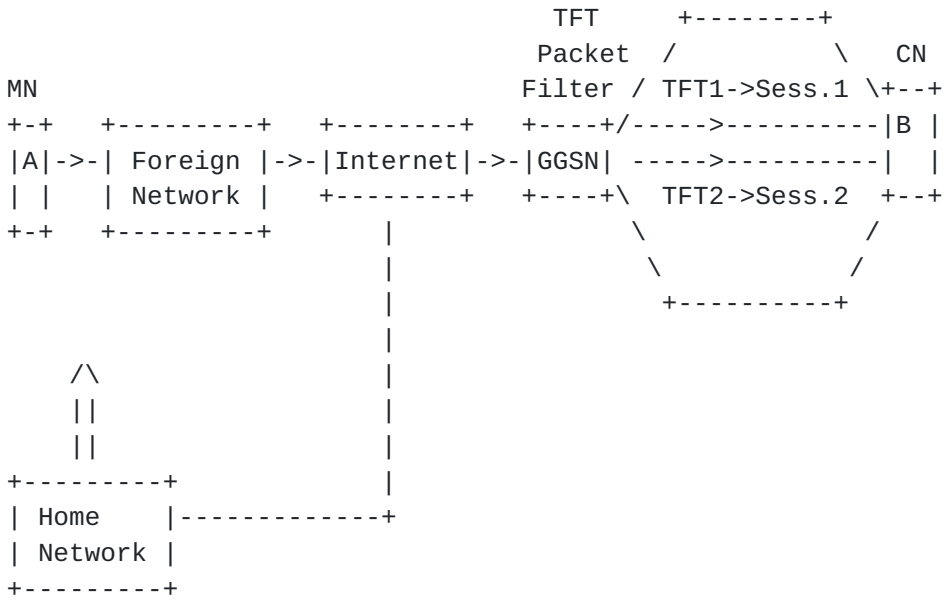

Figure 1

Alternatively the GGSN will discard the IP datagram if all sessions have TFTÆs and none of them match the incoming packet.

The first such IP datagram sent by A will carry the æCare Of Test InitÆ message of the Return Routability Procedure. If this message is dropped, then Route Optimisation will not complete, and IP datagrams from A to B will continue to be routed via the Home Agent instead (see Section 4.1.1.1).

If, instead, this message is delivered to B by the GGSN, the Return Routability procedure may complete and subsequent datagrams will be routed in the same way as the Care Of Test Init. The session with optimized route from A to B will therefore continue.

The major problem is then that the IP datagrams will not receive the correct Quality of Service treatment. Since UMTS Quality of Service can involve small constant bit-rate bandwidth reservations, this can cause a complete loss of service, if the incorrect QoS treatment involves a path with too low a bandwidth or no bandwidth guarantee at all.

In addition, extra complexity or even difficulties will be incurred in the system with respect to PDP Contexts and network resources, especially, the radio resources, that remain unused but are being paid for by the user.

4.1.2 Network Service defined Packet Filtering (SBLP)

4.1.2.1 Home Agent tunneling

We have not identified any issues with this case, for the same reason as discussed in Section 4.1.1.1.

4.1.2.2 Route Optimization

When IMS multimedia sessions are set up between A and B, the SBLP Policy Control authorizes IP datagrams to be sent from B to AÆs home address using assigned GPRS/UMTS network resources and the associated QoS. When A moves away from its home network link and connects to foreign network link, Mobile IPv6 Route Optimisation may be used to allow B to continue sending IP datagrams to A by using AÆs CoA.

Upon arrival at the GGSN, they will not match the SBLP filter for the session which is authorized only for destination equal to AÆs home address. SBLP filters are associated with the particular UMTS QoS reservation (PDP Context) for the session. If B continues to use

this QoS reservation for these packets, the GGSN will drop them as they do not match the filter.

The following diagram shows an example of SBLP packet filtering for IP datagrams sent from B through IMS sessions, 1 and 2, to A.

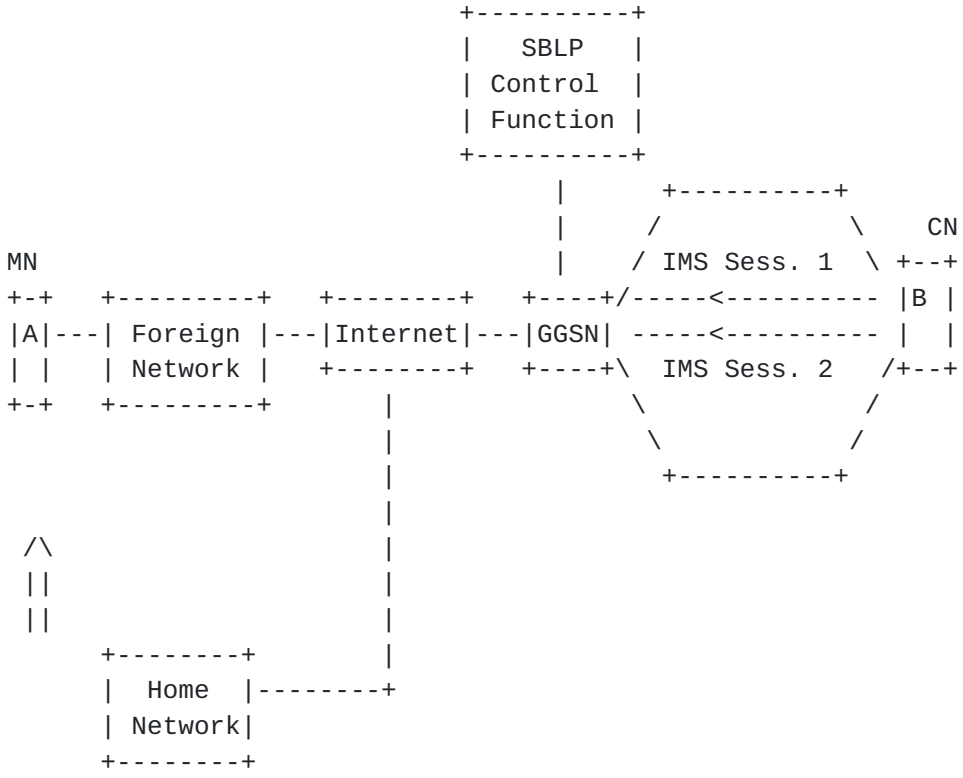

Figure 2

In practice, as discussed in Section 4.1.1.2, the Return Routability procedure requires that there is a route for the Care Of Test Init message from A to B. A route from B to A for the Care Of Test itself is also required.

The means by which outgoing MIP control packets are allocated to QoS reservation on the GPRS link by the UE are undefined in 3GPP, but we note that such a message would not pass the SBLP filters (as described above).

If the message is routed (i.e. on a different QoS reservation), then Route Optimisation can be established with the consequences as described above.

Similar considerations to those of Section 4.1.1.2 apply to IP datagrams sent from A to B.

4.2 GPRS node, B, acting as Mobile Node

This is the case where the GPRS node ,B, is acting as MIPv6 Mobile Node and has a live session such as VoIP with a Correspondent Node, A. The MN, B, connects to the GPRS network after leaving either a GPRS network or non-GPRS network. Therefore, the current GPRS link is NOT taken to be B's Home link but a foreign link.

4.2.1 Mobile Terminal defined Packet Filtering (TFTs)

4.2.1.1 Home Agent Tunnelling

When B moves away from its home network link and connects to GPRS network link, a PDP Context is set up and associated with a TFT filter containing A's address as the Source Address for IP datagrams sent from A to B. This will occur when the GPRS session control on BÆs terminal is not MIP-aware and the IP stack is not QoS/ GPRS-aware.

The following diagram shows an example of two GPRS sessions, 1 and 2, that are distinguished by GGSN using TFT filters, TFT1 and TFT2, for incoming IP datagrams to be delivered to B.

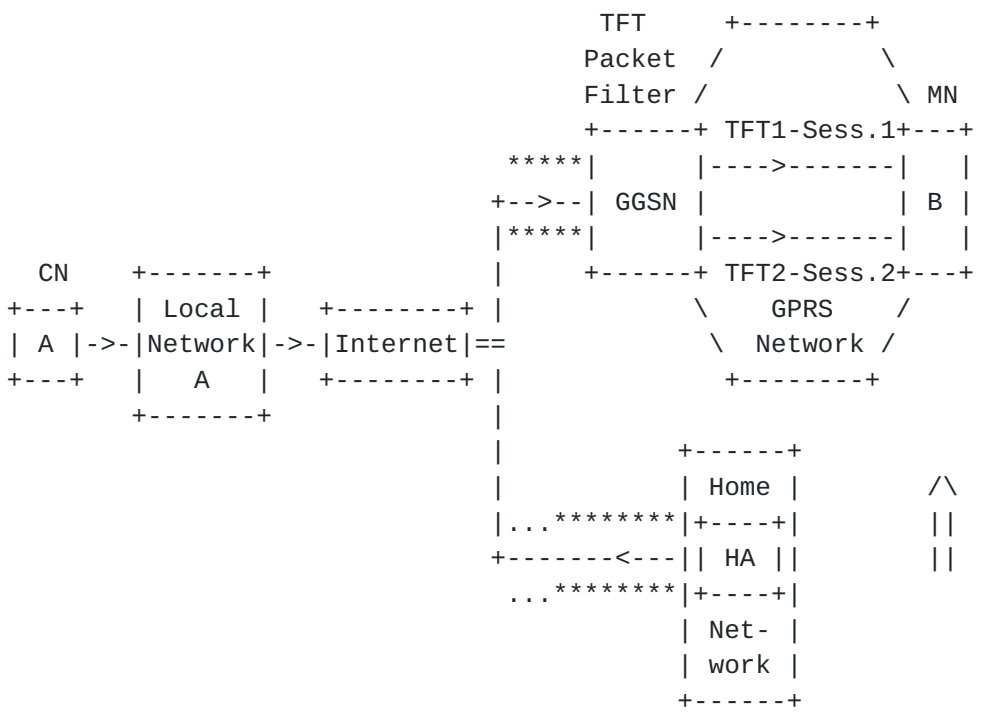

Figure 3

The IP datagrams sent from A to B may use Home Agent Tunneling from B's Home Agent to its current CoA. The IP datagrams tunneled from B's Home Agent to B's CoA have the Home Agent address as the source address in the outer header, while the TFT filter associated with the existing session has A's address as the Source Address. When the IP datagrams arrive at the GGSN, the source address in the outer header does not match the Source Address in the TFT template associated with the session. As a result, the IP datagrams may be discarded by the GGSN or provided with incorrect QoS treatment.

4.2.1.2 Route Optimisation

For the Return Routability Procedure to complete, there needs to be a route from HA to B to deliver the Home Test messages. If no matching TFT is found by the GGSN for the tunneled Home Test Messages and the GGSN chooses to drop the message, the Return Routability procedure will fail and, as a result, the Route Optimisation will not take place.

If tunnelled packets are routed at all from the Home Agent to B, then the Return Routability procedure can complete successfully.

Packets from A are then sent directly to B's Care Of Address. These will be correctly filtered by the TFTs and then delivered through the corresponding PDP Context to B

4.2.2 Network Service defined packet filtering (SBLP)

4.2.2.1 Home Agent Tunnelling

When B moves away from its home network link and connects to a GPRS network, it requests and acquires an IMS session with terminal A with authorised SBLP information containing A's address as the Destination Address for IP datagrams sent from B to A.

When Home Agent Tunnellling operation mode is used, B uses a (reverse) tunnel from its CoA to its Home Agent to send IP datagrams to A. In the reverse tunnel, the IP datagrams tunneled from B carry its Home Agent address as the destination.

The following diagram shows an example of two IMS sessions, each of which is associated with a SBLP filter, SBLP1 and SBLP2, for IP datagrams to be sent to the authorised destination, i.e. AÆs address.

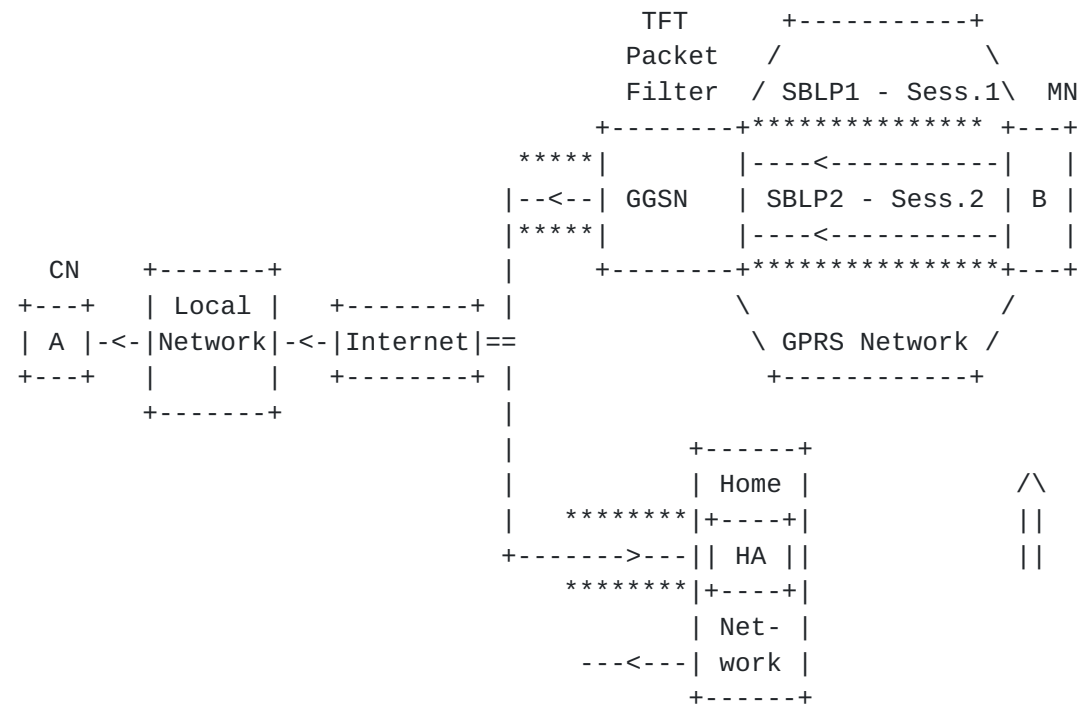

Figure 4

When the IP datagrams in an IPinIP tunnel arrive at the GGSN, GGSN will find no authorised SBLP matching the destination indicated by the outer header of the tunnelled IP datagrams, and it will block and drop them.

4.2.2.2 Route Optimisation

When Route Optimisation is used, IP datagrams from A to B (and B to A) use B's Care of Address as destination (resp. source) and therefore will not match any of the established SBLP filters. This is because the pre-established SBLP filters authorise IP datagrams sent to BÆs Home Address to enter the GPRS/UMTS network. These will either be blocked or carried with inappropriate QoS treatment.

The following diagram shows an example of filtering IP datagrams sent from A directly to B using route optimization passing an SBLP filter SBLP1 or SBLP2. Both authorize the use of IMS sessions and associated network resources to deliver IP datagrams to BÆs home address.

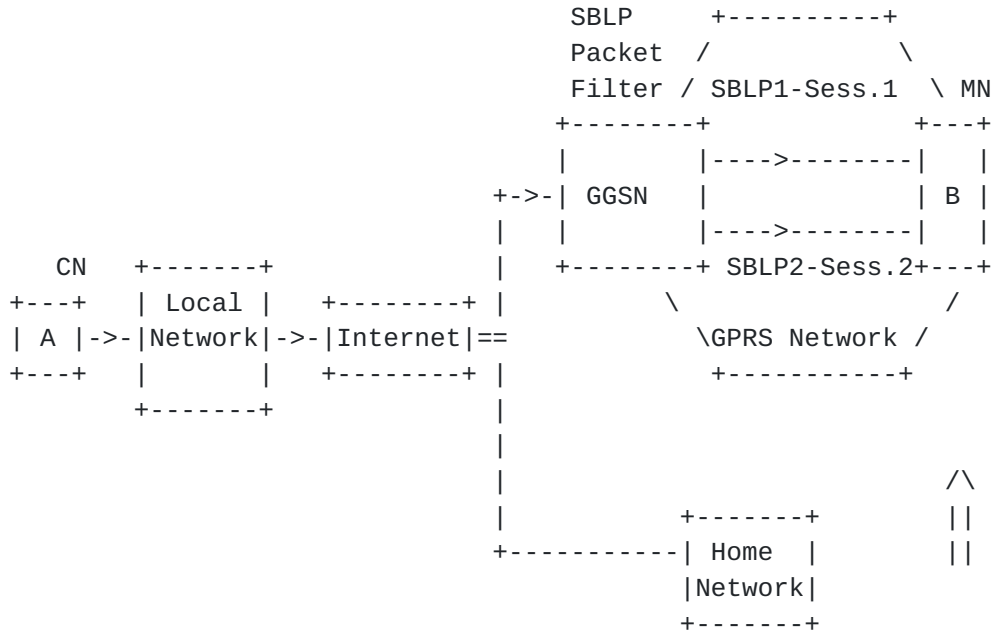

Figure 5

Depending on the policy applied to packets which do not match the SBLP filters, the Return Routability procedure may not complete. This is because the SBLP filters, SBLP1 and SBLP2, authorize IP datagrams sent to BÆs Home Address for accessing GPRS network resources and IMS services. The ôCare of Testö message in response to the ôCare of Test Initö message from B uses BÆs Care-of Address as the destination address.

5. Problem generalization

Although the description above is presented in terms of GPRS-specific mechanisms for installing packet filters in the network. More general situations may exist in which such filters are installed. This may give rise to similar problems.

In the analysis above, we classify the filters as æmobile terminal definedÆ and ænetwork service definedÆ. This represents the source of the information within the filters.

An example of a æterminal definedÆ filter in the network is a filter

installed as a result of RSVP (or in future NSIS protocols). Such filters determine the QoS treatment that will be applied to packets according to the userÆs request and are therefore very similar to Traffic Flow Templates.

An example of a ænetwork service defined Æ filter would be one installed through policy mechanisms. In this case it is in order to apply appropriate network policy that packets filtered.

6. Security Considerations

6.1 User security considerations

No user security issues have been identified.

6.2 Network security considerations

In the case of network service defined filters (e.g. Service Based Local Policy), the purpose of the filters is to ensure that appropriate network policy for controlling access to network resources and services is applied to the packets.

The problems described in this paper do not themselves represent security issues for the network (for example users circumventing the networkÆs policy). Indeed, the problems arise largely because the policies cause packets to be dropped, or treated according to a different policy which explicitly allows those packets to pass.

However, care must be taken in considering solutions to these problems which cause modification of the networkÆs policies. Such modification will necessarily be caused by the mobility event at one or other user. These events can easily be faked by users.

For example, IP address spoofing could be used to convince the network that a user has moved when in fact they have not. Collaborating users could convince the network that a user has moved, when in fact the new address belongs to a different host.

7. Acknowledgments

The authors would like to thank Paul Reynolds, Ric Bailey, Ronan Le Bras, Graham Fisher, Stuart Shutt, Steve Blythe and Rob Allan for their constant and valuable support for the work.

References

[1] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24 (work in progress), July

2003.

[2] 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.

[3] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Services (GPRS); Service Description; Stage 2", 3GPP TS 23.060.

[6] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile Radio Interface Layer 3 Specifications; Core Network Protocols - Stage 3", 3GPP TS 23.008.

[7] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2", 3GPP TS 23.228.

[8] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; End-to-end Quality of Service; Concept and Architecture", 3GPP TS 23.207.

[9] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Core Network; Policy Control over Go Interface", 3GPP TS 29.207.

Authors' Addresses

Xiaobao Chen
Orange PCS Ltd.
Keypoint
St. James Court, Almondsbury Park
Bradley Stoke
Bristol BS32 4QJ
UK

Phone: +44 7989 477679
EMail: xiaobao.chen@orange.co.uk

Mark Watson
Nortel Networks
Maidenhead Office Park
Westacott Way
Maidenhead, BERKS SL6 3QH
UK

Phone: +44 1628 434456
EMail: mwatson@nortelnetworks.com

Martin Harris
Orange PCS Ltd.
Keypoint
St. James Court, Almondsbury Park
Bradley Stoke
Bristol BS32 4QJ
UK

Phone: +44 7974 365080
EMail: martin.harris@orange.co.uk

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgment

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