Sun Qian, Mu Lei, Henrik Petander, Kun-chan Lan, Mahbub Hassan, On securing dynamic home agent address discovery of on-board mobile router in mobile IPv6 networks, in Proceedings of the 12th International Conference on Telecommunications (ICT 2005), Capetown, South Africa, 03-06 May 2005.

On securing dynamic home agent address discovery of on-board mobile router in mobile IPv6 networks

Sun Qian* Mu Lei*
*School of Computer Science and Engineering
University of New South Wales
Sydney, NSW 2052, Australia

Henrik Petander†,‡
‡Department of Computer Science
Helsinki University of Technology, Finland

Kun-chan Lan† Mahbub Hassan*,†
†National ICT Australia Ltd
Bay 15, Australian Technology Park
Eveleigh NSW 1430, Australia

***Abstract*— In on-board mobile networks, users are connected to a local network that attaches to the Internet via a mobile router and a wireless link. The mobile router has a central role in servicing the mobile network, which makes the security of the mobile router crucial. The security of mobility management protocols used by mobile router, such as Mobile IPv6, have been studied thoroughly. However, the security of configuration protocols for mobile routers has received very little attention. In this paper, we focus on the security of dynamic home agent address discovery (DHAAD) protocol, a protocol that allows mobile router to automatically configure its home agent. We first present some vulnerabilities in the DHAAD protocol which can be exploited by attackers to launch denial of service attacks (DOS) against the mobile router. Next, we present a secure version of the DHAAD protocol. Finally, we provide an analysis of the effectiveness and overhead of our protocol extension.**

***Index Terms*— DHAAD, Security, Mobile IPv6, On-board network, NEMO, Network mobility**

I. Introduction

There is a growing interest in introducing broadband Internet services to public transport passengers by deploying high-speed local area networks (LANs) on-board public transport vehicles. These on-board LANs are connected to the Internet via on-board mobile routers (MR). Figure 1 shows a typical on-board architecture, which consists of a high-speed mobile LAN and a mobile router that provides connectivity to the Internet through a wireless link (e.g. cellular or satellite). Passengers can simply connect their devices to the on-board LAN and start enjoying Internet services. The mobility of the on-board LAN is handled transparently by the MR with a mobility management protocol such as NEMO [6] to hide the mobility from the devices connected to the on-board LAN.

NEMO is an IETF standardized network mobility management protocol for on-board mobile networks, which is based on an extension of the Mobile IPv6 protocol [13]. The NEMO architecture consists of three main components: a high-speed mobile LAN (MLAN), a mobile router (MR), and a home agent (HA) which provide a mobility management service to the MLAN. The MLAN provides a local high-speed connectivity to the on-board passengers. The MR facilitates communication between the MLAN and the Internet through a wireless access network and routes the traffic of the MLAN through the HA. The MR and HA utilize NEMO protocol to hide the mobility of the MLAN from the devices connected to it and to maintain the reachability of the devices to the Internet.

The use of Mobile IPv6 and NEMO requires the configuration of a number of settings in the MR. While these settings can be pre-configured, it may be preferable to dynamically configure as many of these settings as possible. Currently, there exist three standardized protocols used for configuring the necessary information for NEMO in MR: the Mobile Prefix Discovery protocol (MPD) [13], Dynamic Home Agent Address discovery protocol (DHAAD) [13] and prefix delegation with Dynamic Host Configuration Protocol (DHCP PD) [23]. The MPD protocol allows a MR to configure new addresses from the home link. The DHAAD protocol allows MR to discover a new HA on its home link. The DHCP PD protocol allows MR to acquire new prefixes for the MLAN. Together these three protocols allow MR to dynamically configure the information required for running NEMO with a minimal amount of pre-configured information.

The use of Mobile IP or NEMO is not possible without a successful configuration of the mobile router. While the security of Mobile IPv6 protocol has been studied thoroughly [2], [21], the security of configuration protocols and their interactions with Mobile IPv6 and NEMO has received only very little attention. Any vulnerabilities in the configuration protocol could prevent MR from servicing MLAN, which is a serious issue in an on-board mobile network because the failure of the mobile router will impact a large number of user devices. Furthermore, the use of Mobile IPv6 and NEMO on insecure links (i.e. links with insufficient physical and cryptographic security measures) such as most 802.11 networks [4] and GSM/GPRS cellular phone networks [3] makes it easy for a determined attacker within range to exploit any vulnerabilities in the configuration protocols. Given the

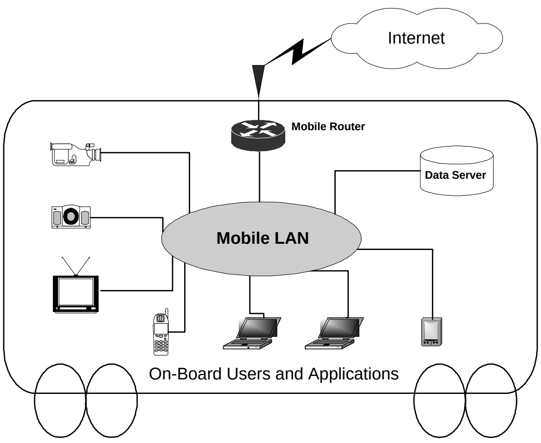


Fig. 1. On-board communication architecture.

easy exploitability of potential vulnerabilities and the large impact of a successful attack on MR, it is important to secure the configuration protocols used by MR.

Currently, among the three standardized configuration protocols described previously, the Mobile Prefix Discovery protocol is protected with IPsec [14]–[16], a protocol suite for securing IP datagrams, and can be considered as secured. Similarly, DHCP PD, when used between MR and HA, can also be protected with IPsec. This leaves only DHAAD without security.

DHAAD is already present in most available Mobile IPv6 implementations [8]. Although there also exist alternative methods to DHAAD for configuring HA information in MR, such as the work proposed by Ohba et al. [20], the availability and mature status of DHAAD make its future use in operational networks highly probable. For example, the availability of DHAAD has resulted that the 3GPP2 partnership is standardizing the use of DHAAD in their next generation cellular network infrastructure [17]. Based on this observation, it seems probable to us that DHAAD will be deployed on a large scale in the near future, and thus any vulnerabilities in DHAAD may become crucial for mobile network security.

For the reasons above, we focus our work in this paper on the security of the dynamic home agent address discovery protocol (DHAAD) which MR uses for automatic configuration of home agent. We first present some vulnerabilities in the DHAAD protocol which can be exploited by attackers to launch denial of service attacks (DOS) against the mobile router (Section II). Next, we present a secure version of the DHAAD protocol (Section IV). Finally, we analyze the security of our improved protocol(Section V).

II. Security analysis of the DHAAD protocol

DHAAD protocol allows a MR to dynamically discover the home agents on its home link. A MR is typically required to perform DHAAD in the following two cases. First, a MR starting up without a preconfigured HA address needs to find a suitable HA. Second, a MR needs to perform an address discovery, if its HA becomes unreachable or unable to serve the MR. In this section we first describe the DHAAD protocol and then point out several security problems in DHAAD.

A. The DHAAD protocol

The MR initiates DHAAD by sending a DHAAD request (an ICMP message) to the anycast address of Home Agents on its home network with a flag set to indicate that it wants to know about the ability of the HAs to service a MR. Any HA which receives such a request sends a ICMP DHAAD reply to the MR consisting of a list of all the NEMO capable HAs on the home link ordered by their preference to act as a HA.

Operation of the DHAAD protocol for MR is shown in Figure 2. MR first sends the request to HA and includes a 16-bit identifier in the request. When MR receives a reply from HA, the MR compares the identifier in the reply with the one it sent in the request. Reply packets with incorrect identifiers or failed ICMP checksums are dropped by the MR. In addition, the MR employs a resending timer to cope with packets lost due to network problems. The request is resent if the MR does not receive the reply before a timeout.

As shown in Figure 3 the operation of HA in the DHAAD protocol is stateless. HA merely verifies that the DHAAD request has a correct checksum. HA builds the reply from its home agents list and the 16-bit identifier from the received request. The reply is then sent back to the address from which HA received the request.

Each HA maintains a home agents list for building DHAAD replies by listening to router advertisements (RAs) sent by other HAs on the home link. RAs contain the information about the preference of the sending router to serve as a HA and the router's capability to support network mobility. RAs are by default not authenticated in any way.

The protocol message flow is shown in Figure 4. Note that the DHAAD protocol as specified in the Mobile IPv6 specification [13] is unauthenticated.

B. Analysis of the vulnerabilities in the protocol

An attacker located on the same shared access wireless network link (e.g. a 802.11b WLAN) as MR can hear all the unencrypted traffic sent by MR, including the DHAAD request. Even if the link is encrypted, an attacker may be

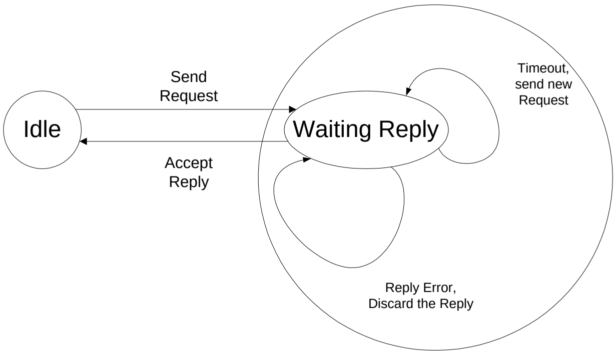


Fig. 2. MR state machine.

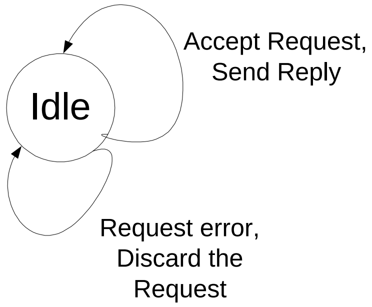


Fig. 3. HA state machine.

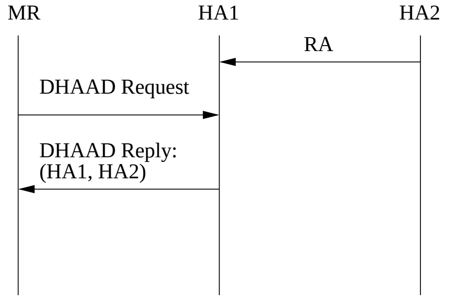


Fig. 4. DHAAD Protocol

able to access the traffic by first breaking the encryption. For example the mechanisms used for protecting 802.11b [4], CDPD [10] and GSM [3] networks have been broken recently.

Since the DHAAD request is unauthenticated, an attacker can pose as the HA and send an unauthorized DHAAD reply containing invalid HA addresses to MR, thus preventing MR from registering with a real HA. While the attacker may not be able to intercept and block the authentic DHAAD messages from reaching MR and HA, due to his proximity to MR, the attacker can respond to the message quicker than the genuine HA. Thus, when the real DHAAD reply arrives, MR will discard it as a duplicate.

A variation of the above mentioned attack can also be used to attack the MR: The attacker first intercepts the DHAAD request sent by MR and then forwards the message onward with the Mobile Router flag set to zero. As a result, any HA receiving the modified DHAAD request message will not add the capability of the HAs to its DHAAD reply. Thus, the MR is fooled into believing that there is no NEMO-capable HA on the home link. Note that this attack requires that the attacker is capable of performing a man-in-the-middle attack and blocking the original DHAAD request. The blocking requirement limits the applicability of this attack, since on radio networks it is harder to block traffic than to overhear it.

Additionally, an attacker can utilize the lack of authentication in the DHAAD protocol to explore HA information on the home link : An attacker can send a DHAAD request to find out the home addresses of HAs on a specific home link, since a HA cannot distinguish the requests coming from authentic MRs from attackers. The ability to learn addresses of HAs may prove to be useful for attackers, as brute-force scanning of the address space is not practical with IPv6. The leakage of such information may be used as a stepping stone to make subsequent attacks (such as distributed denial of service attacks [5], [19]) against the home network easier. Note that an attacker may learn the HA addresses also through eavesdropping valid DHAAD messages, or through eavesdropping the addresses of the packets used in Mobile IPv6 signaling.

Finally, the backend protocol used for building the HA list also has a vulnerability. The current Mobile IPv6 standard does not mandate RA messages to be protected. Therefore, an attacker located on the home link of the MR can easily pose as a number of HAs by sending fake RAs. Additionally, the attacker can send the fake RAs with a higher value for HA preference. Once the attacker floods the home link with fake RAs, all DHAAD reply packets received by MR will contain only bogus information, since the size of the DHAAD reply packet is limited and the list of HAs in the reply is ordered according to the preference [13]. As a result, any MR trying to configure itself with a HA would end up registering only with invalid addresses.

III. Related Work

DHAAD uses anycast addressing to deliver the DHAAD request to the HA closest to MR. In an anycast paradigm, a client communicates with a group of anycast servers, so that any one server can reply to the request of the client. Securing anycast protocols requires that the client can authenticate the received reply comes from an authorized server and the server can authenticate that the received request comes from an authorized client. In this section, we describe some prior work in securing anycast communications.

Previously, Dondeti et al. analyzed the problem of securing the anycast communications and securing anycast group membership [7]. They discussed some general requirements for secure anycast communications. They argued that securing anycast communications can be done using either source or content authentication. However, in the case of DHAAD, content authentication does not offer real benefits due to the fact that the HA sending the reply is also the creator of the content (i.e. the list of HAs).

Source authentication for IPv6 network protocols can be done with the IPsec protocols [14]–[16], which provide strong authentication of source along with integrity and confidentiality protection. Internet Key Exchange protocol (IKE) [11] has been commonly used for key establishment for IPsec. However, previous study [12] showed that dynamic keying with Internet Key Exchange protocol is not possible for anycast communications. This limits the applicability of IPsec to be used for DHAAD.

IV. Securing the DHAAD protocol

The vulnerabilities presented in section II-B are a result of that the messages in DHAAD and its backend protocol are not authenticated and their integrity is not protected.

To secure the DHAAD protocol, DHAAD request, DHAAD reply and RAs on the home link should be protected. In addition, to make the DHAAD protocol usable over low bandwidth wireless links, the message sizes of DHAAD request and reply should remain small. In the rest of the paper, we assume that MR and HAs share a secret key. The key may be either pre-configured or established on-demand as part of the bootstrapping procedure of MR. For example, such an on-demand key can be established by using DHCP and the Authentication Authorization and Accounting (AAA) infrastructure [17]. In this section, we present a secure version of DHAAD and describe how to protect its backend protocol.

A. Extensions to the DHAAD protocol

To secure the DHAAD protocol, we introduce two new options to the DHAAD protocol. In addition, to provide protection against replayed messages, we extend the identifier field to 24 bits by utilizing 8 bits of the reserved field in the messages. The motivation for extending the identifier field is described more in detail in section V. The new message formats for DHAAD request and reply are shown in Figure 5(a) and Figure 5(b) respectively.

To authenticate the sender of DHAAD messages and to protect their integrity, we introduce a new authenticator option containing a message authentication code (MAC) created from the message and a secret key. The authenticator option contains an 8-bit type field, an 8-bit length field in addition to the a 96-bit MAC. The MAC is created with a key shared by MR and all the HAs on the home link using HMAC SHA-1, a one way cryptographic hash function [9], [18].

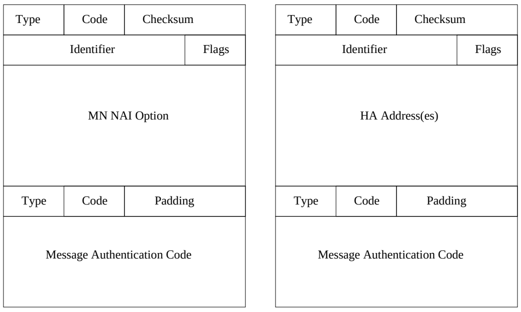
We also introduce the use of the mobile node identifier option [22] (MN-NAI Option), which was originally designed to be used with Mobile IPv6 mobility management signaling messages. When the MR initiates a DHAAD session, the DHAAD request message, as shown in Figure 5(a)), includes mobile node identifier option containing the identity of MR. The MR may use its permanent home address as the identity in the MN-NAI Option.

When processing the DHAAD request, HA can use the identity of MR to look up the correct key for authenticating the DHAAD request and to look up the key for creating the authenticator for the DHAAD reply.

The operation of our extended DHAAD protocol is similar to the basic DHAAD protocol, and can be described using the state machines shown in Figure 2 and Figure 3. The difference between our extension and the original version is that only correctly authenticated messages can change state or result in a response in MR or HA.

B. Securing the DHAAD backend protocol

The attacks on the backend protocol can be prevented with the use of secure neighbor discovery (SEND) protocol. SEND protects RA messages using public key cryptography [1]. RAs protected with SEND include a digital signature created by the router using its public key. Nodes receiving the RA can retrieve a certificate from a trusted certificate authority and certify if the public key of the sender of the RA belongs to an authorized router.



(a) DHAAD request (b) DHAAD reply

Fig. 5. DHAAD message format

The inclusion of the signature in RAs allows the receiver to verify the integrity of the messages and also provides strong authentication of the sender. Finally, SEND can be used with no modifications to protect the building of the HA list, provided that all the authorized routers on the home link are also authorized to act as HAs.

V. ANALYSIS OF THE DHAAD PROTOCOL EXTENSION

In this section, we present an informal analysis of the security of our extended protocol and the additional overhead it introduces.

A. The security and limitations of the DHAAD protocol extension

Authentication of the DHAAD request and reply protects MR and HA against all attacks against the protocol, in which an attacker impersonates HA or MR, as described in Section II. The authentication of the messages also provides integrity protection, thus preventing an attacker from changing the messages in transit.

If the freshness of the DHAAD reply is not protected, even with strong authentication of DHAAD messages, an attacker can still disrupt the protocol by re-using an old reply from HA. By continuously listening and recording DHAAD traffic, an attacker can send an outdated reply to MR in response to its new request, assuming that the outdated reply has the same identifier as the new request from MR. In our extension, the freshness of the DHAAD reply is ensured through the use of a 24-bit random number in the DHAAD request identity field, which is then copied by HA to the reply. The probability of a collision for the 24-bit identifier is extremely low, which consequently makes such a traffic-replay attack hard to realize.

The use of SEND for RAs protects against all attacks against the DHAAD backend protocol. Note that we assume that none of the routers on home links is compromised, in which case all protocols and transactions in which the router participates are considered secured. Further analysis of the security of SEND was discussed by Arkko et al in their work [1].

Note that, while the authentication of the DHAAD request can prevent an attacker from actively querying the HA addresses on the home link, a determined attacker can still learn these addresses by passively listening to the contents and the source addresses of the DHAAD replies. We do not consider blocking such a passive attack in our extended protocol. The blocking of the passive attacks would expectedly incur a larger overhead, especially hiding addresses in IPv6 packets would significantly complicate the DHAAD, Mobile IPv6 and NEMO protocols.

B. The overhead of the DHAAD protocol extension

Our extended DHAAD protocol increases the sizes of DHAAD and RAs messages and also requires more computing power for the processing and creation of these messages. In this section, we analyze the incurred overhead due to our extension.

Our extended protocol increases the size of DHAAD request from 48 bytes (40 bytes for IPv6 header + 8 bytes for DHAAD Request) to 85 bytes (48 bytes for original DHAAD size + 19 byte for MN NAI option + 14 bytes for authenticator option). The DHAAD reply size increases from a minimum of 64 bytes (40 bytes for IPv6 header + 24 bytes for DHAAD reply with one IPv6 address) to 78 bytes (IPv6 + DHAAD reply + authenticator). Although the ratio of increase in message size is significant, the total size of the request/reply messages still remains small. The computing overhead in creating and verifying the authenticator is comparable to the overhead of authenticating the Mobile IPv6 binding updates and acknowledgments using IPsec ESP or AH. Such an overhead is not significant in our opinion.

The downside of using SEND is the additional overhead due to the increased size of RAs and creation and processing of RA message. The increase in the size of RA messages can be significant, depending on the public key cryptography algorithm used with SEND, typically several hundred bytes. The communications overhead might limit the use of SEND to home links that have sufficient bandwidth to handle the large RAs. The communications overhead should not limit the use of SEND between HAs though, assuming the HAs have sufficient processing power or even dedicated hardware to offload public key cryptography operations.

VI. Conclusions

In this paper we pointed out several vulnerabilities in the DHAAD protocol used in Mobile IPv6 for configuration of home agent address. The threats associated with these vulnerabilities are important for an on-board mobile router connected to the infrastructure through a wireless access network, due to the large impact of an attack and easy exploitability of the vulnerabilities. We presented a simple extension for securing DHAAD protocol by leveraging a pre-existing trust relationship between MR and HAs. Our extension secures the protocol effectively with little overhead, which makes it also suitable for narrow-band wireless networks. We also presented a simple way of securing the DHAAD backend protocol.

VII. Acknowledgements

We would like to thank the people who participated on the discussion about the security problems in DHAAD, especially Alexandru Petrescu, Vijay Devarapalli, James Kempf and Jari Arkko.

References

[1] J. Arkko, J. Kempf, B. Sommerfeld, B. Zill, and P. Nikander. ”SEcure Neighbor Discovery (SEND)”. INTERNET-DRAFT, Jul 2004. Work in Progress.

[2] Tuomas Aura. Mobile ipv6 security. In *Proc. Security Protocols, 10th International Workshop*, LNCS, Cambridge, UK, April 2002. Springer.

[3] Eli Biham, Elad Barkan, and Nathan Keller. Instant Ciphertext-only cryptanalysis of GSM encrypted communications. In *Proceedings of Advances in Cryptology - Crypto 2003*, volume 2729 of *Lecture Notes in Computer Science*, Santa Barbara, California, USA, 2003. Springer.

[4] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting mobile communications: The insecurity of 802.11. `http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html`, 2001.

[5] D. Moore and G. Voelker and S. Savage”. Inferring Internet Denial-of-Service Activity. In *Proceedings of USENIX Security Symposium 2001*, pages 9–22, 2001.

[6] J. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. ”Network Mobility (NEMO) basic support protocol”. INTERNET-DRAFT, June 2004. Work in progress.

[7] L. Dondeti, T. Hardjono, and B. Haberman. ”Security Requirements of IPv6 Anycast”. INTERNET DRAFT, Jun 2001. Work in Progress.

[8] M. Dunmore and C. Edwards. ”Survey and Evaluation of MIPv6 Implementations”. Technical report, 6NET Project, 2002.

[9] D. Eastlake, 3rd, and P. Jones. US Secure Hash Algorithm 1 (SHA1). RFC 3174, IETF, September 2001.

[10] Y. Frankel, A. Herzberg, P. Karger, H. Krawczyk, C. Kunzinger, and M. Yung. Security Issues in a CDPD Wireless Network. *IEEE Personal Communications*, 1995.

[11] D. Harkins and D. Carrel. The Internet Key Exchange (IKE). RFC 2409, IETF, November 1998.

[12] J. Itojun and K. Ettikan. ”An analysis of IPv6 anycast”, Oct 2000. Work in Progress.

[13] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. RFC 3775, IETF, July 2004.

[14] S. Kent and R. Atkinson. IP Authentication Header. RFC 2402, IETF, November 1998.

[15] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). RFC 2406, IETF, November 1998.

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

[17] B. Kidwell. cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Services. Technical report, 3rd generation partnership project 2, 2004.

[18] C. Madson and R. Glenn. The Use of HMAC-SHA-1-96 within ESP and AH. RFC 2404, IETF, November 1998.

[19] R. Mahajan, S. Bellovin, S. Floyd, J. Vern, and P. Scott. Controlling high bandwidth aggregates in the network, 2001.

[20] Y. Ohba, R. Lopez, M. Yanagiya, H. Ohnishi, and K. Chowhdury. Mobile IPv6 Bootstrapping Architecture Using DHCP. INTERNET DRAFT, Oct 2004. Work in Progress.

[21] G. O’Shea and M. Roe. Child-proof authentication for MIPv6 (CAM). *SIGCOMM Comput. Commun. Rev.*, 31(2):4–8, 2001.

[22] A. Patel, K. Leung, M. Khalil, H. Akhtar, and K. Chowdhury. ”Mobile Node Identifier Option for Mobile IPv6”. INTERNET-DRAFT, Dec 2004. Work in Progress.

[23] O. Troan and R. Droms. IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6. RFC 3633, IETF, December 2003.