James Kempf
DoCoMo Labs USA
Rajeev Koodli
Nokia-Siemens
Research
Center

Internet Draft
Document: draft-ietf-mipshop-handover-key-03.txt
Intended Status: Proposed Standard

Expires: May, 2008

November, 2007

Distributing a Symmetric FMIPv6 Handover Key using SEND (draft-ietf-mipshop-handover-key-03.txt)

Status of this Memo

Abstract

Fast Mobile IPv6 requires that a Fast Binding Update is secured using a security association shared between an Access Router and a Mobile Node in order to avoid certain attacks. In this document, a method for provisioning a shared key from the Access Router to the Mobile Node is defined to protect this signaling. The Mobile Node generates a public/private key pair using the same public key algorithm as for SEND (RFC 3971). The Mobile Node sends the public key to the Access Router. The Access Router encrypts a shared handover key using the public key and sends it back to the Mobile Node. The Mobile Node decrypts the shared handover key using the matching private key, and the handover key is then available for generating an authenticator on a Fast Binding Update. The Mobile Node and Access Router use the Router Solicitation for Proxy

Advertisement and Proxy Router Advertisement from Fast Mobile IPv6
for the key exchange. The key exchange messages are required to

have SEND security; that is, the source address is a Cryptographically Generated Address and the messages are signed using the CGA private key of the sending node. This allows the Access Router, prior to providing the shared handover key, to verify the authorization of the Mobile Node to claim the address so that the previous care-of CGA in the Fast Binding Update can act as the name of the key.

Table of Contents

1.0 Introduction

In Fast Mobile IPv6 (FMIPv6) [FMIP], a Fast Binding Update (FBU) is sent from a Mobile Node (MN), undergoing IP handover, to the previous Access Router (AR). The FBU causes a routing change so traffic sent to the MN's previous care-of address on the previous AR's link is tunneled to the new care-of address on the new AR's link. Only a MN authorized to claim the address should be able to change the routing for the previous care-of address. If such authorization is not established, an attacker can redirect a victim MN's traffic at will.

In this document, a lightweight mechanism is defined by which a shared handover key for securing FMIP can be provisioned on the MN by the AR. The mechanism utilizes SEND [SEND] and an additional public/private key pair, generated on the MN using the same public key algorithm as SEND, to encrypt/decrypt a shared handover key sent from the AR to the MN. The key provisioning occurs at some arbitrary time prior to handover, thereby relieving any performance overhead on the handover process. The message exchange between the MN and AR to provision the handover key is required to be protected by SEND; that is, the source address for the key provisioning messages must be a CGA and the messages must be signed with the CGA private key. This allows the AR to establish the MN's

authorization to operate on the CGA. The AR uses the CGA to name the handover key. The SEND key pair is, however, independent from the handover encryption/decryption key pair and from the actual

handover key. Once the shared handover key has been established, when the MN undergoes IP handover, the MN generates an authorization MAC on the FBU. The previous care-of CGA included in the FBU is used by the AR to find the right handover key for checking the authorization.

Handover keys are an instantiation of the purpose built key architectural principle [PBK].

1.1 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 [RFC2119].

In addition, the following terminology is used:

CGA public key

Public key used to generate the CGA according to RFC 3972 [CGA].

CGA private key

Private key corresponding to the CGA public key.

Handover key encryption public key

Public key generated by the MN and sent to the current AR to encrypt the shared handover key

Handover key encryption private key

Private key corresponding to handover key encryption public key, held by the MN

2.0 Overview of the Protocol

2.1 Brief Review of SEND

SEND protects against a variety of threats to local link address resolution (also known as Neighbor Discovery) and last hop router (AR) discovery in IPv6 [RFC3756]. These threats are not exclusive to wireless networks, but they generally are easier to mount on certain wireless networks because the link between the access point and MN can't be physically secured.

SEND utilizes CGAs in order to secure Neighbor Discovery signaling

[CGA]. Briefly, a CGA is formed by hashing together the IPv6 subnet prefix for a node's subnet, a random nonce, and an RSA public key, called the CGA public key. The CGA private key is used to sign a Neighbor Advertisement (NA) message sent to resolve the

link layer address to the IPv6 address. The combination of the CGA and the signature on the NA proves to a receiving node the sender's authorization to claim the address. The node may opportunistically generate one or several keys specifically for SEND, or it may use a certified key that it distributes more widely.

2.2 Protocol Overview

The protocol utilizes the SEND secured Router Solicitation for Proxy Advertisement (RtSolPr)/Proxy Router Advertisement (PrRtAdv) [FMIP] exchange between the MN and the AR to transport an encrypted, shared handover key from the AR to the MN. First, the MN generates the necessary key pair and associated CGA addresses so that the MN can employ SEND. Then the MN generates a public/private key pair for encrypting/decrypting the shared handover key, using the same public key algorithm as was used for SEND. The MN then sends a RtSolPr message with a Handover Key Request Option containing the handover key encryption public key. The source address of the RtSolPr message is the MN's care-of CGA on the AR's link, the RtSolPr message is signed with the MN's CGA key, and contains the CGA Parameters option, in accordance with RFC 3971 [SEND]. The AR verifies the message using SEND, then utilizes the handover key encryption public key to encrypt a shared handover key, which is included with the PrRtAdv in the Handover Key Reply Option. The MN decrypts the shared handover key and uses it to establish an authorization MAC when it sends an FBU to the previous AR.

3.0 Handover Key Provisioning and Use

3.1 Sending Router Solicitations for Proxy Advertisement

At some time prior to handover, the MN MUST generate a handover key encryption public/private key pair, using exactly the same public key algorithm with exactly the same parameters (key size, etc.) as for SEND [SEND]. The MN can reuse the key pair on different access routers but MUST NOT use the key pair for any other encryption or for signature operation. In order to prevent cryptanalysis, the key pair SHOULD be discarded after either a duration of HKEPK-LIFETIME or HKEPK-HANDOVERS number of handovers, whichever occurs first. See Section 3.7 for definitions of protocol constants.

The MN MUST send a Router Solicitation for Proxy Advertisement (RtSolPr) containing a Handover Key Request Option with the handover encryption public key. A CGA for the MN MUST be the source address on the packet, and the MN MUST include the SEND CGA Option and SEND Signature Option with the packet, as specified in

[SEND]. The SEND signature covers all fields in the RtSolPr, including the 128 bit source and destination addresses and ICMP checksum as described in RFC 3971, except for the Signature Option itself. The MN also sets the handover authentication Algorithm Type (AT) extension field in the Handover Key Request Option to

the MN's preferred FBU authentication algorithm. The SEND Nonce MUST also be included for anti-replay protection.

3.2 Receiving Router Solicitations for Proxy Advertisement and Sending Proxy Router Advertisements

When an FMIPv6 capable AR with SEND receives a RtSolPr from a MN protected with SEND and including a Handover Key Request Option, the AR MUST first validate the RtSolPr using SEND as described in RFC 3971. If the RtSolPr can not be validated, the AR MUST NOT include a Handover Key Reply Option in the reply. The AR also MUST NOT change any existing key record for the address, since the message may be an attempt by an attacker to disrupt communications for a legitimate MN. The AR SHOULD respond to the RtSolPr but MUST NOT perform handover key provisioning.

If the RtSolPr can be validated, the AR MUST then determine whether the CGA is already associated with a shared handover key. If the CGA is associated with an existing handover key, the AR MUST return the existing handover key to the MN. If the CGA does not have a shared handover key, the AR MUST construct a shared handover key as described in Section 3.6. The AR MUST encrypt the handover key with the handover key encryption public key included in the Handover Key Request Option. The AR MUST insert the encrypted handover key into a Handover Key Reply Option and MUST attach the Handover Key Reply Option to the PrRtAdv. The lifetime of the key, HK-LIFETIME, MUST also be included in the Handover Key Reply Option. The AR SHOULD set the AT field of the Handover Key Option to the MN's preferred algorithm type indicated in the AT field of the Handover Key Request Option, if it is supported; otherwise, the AR MUST select an authentication algorithm which is of equivalent strength or stronger and set the field to that. The AR MUST also include the SEND nonce from the RtSolPr for anti-replay protection. The AR MUST use the CGA constructed from its certified key as the source address for the PrRtAdv and include a SEND CGA Option and a SEND Signature Option with the SEND signature of the message. The SEND signature covers all fields in the PrRtAdv, including the 128 bit source and destination addresses and ICMP checksum as described in RFC 3971, except for the Signature Option itself. The PrRtAdv is then unicast back to the MN at the MN's care-of CGA that was the source address on the RtSolPr. The handover key MUST be stored by the AR for future use, indexed by the CGA, and the authentication algorithm type (i.e., the resolution of the AT field processing) and HK-LIFETIME MUST be recorded with the key.

3.3 Receiving Proxy Router Advertisements

Upon receipt of one or more PrRtAdvs secured with SEND and having

the Handover Key Reply Option, the MN MUST first validate the PrRtAdvs as described in RFC 3971. Normally the MN will have obtained the router's certification path to validate an RA prior to sending the PrRtSol and the MN MUST check to ensure that the key used to sign the PrRtAdv is the router's certified public key.

If the MN does not have the router's certification path cached, it MUST use the SEND CPS/CPA messages to obtain the certification path to validate the key. If a certified key from the router was not used to sign the message, the message MUST be dropped.

From the messages that validate, the MN SHOULD choose one with an AT flag in the Handover Key Reply Option indicating an authentication algorithm that the MN supports. From that message, the MN MUST determine which handover key encryption public key to use in the event the MN has more than one. The MN finds the right public key to use by matching the SEND nonce from the RtSolPr. If no such match occurs, the MN MUST drop the PrRtAdv. The MN MUST use the matching private key to decrypt the handover key using its handover key encryption private key, and store the handover key for later use, named with the AR's CGA, along with the algorithm type and HK-LIFETIME. The MN MUST use the returned algorithm type indicated in the PrRtAdv. The MN MUST index the handover keys with the AR's IPv6 address, to which the MN later sends the FBU, and the MN's CGA to which the handover key applies. This allows the MN to select the proper key when communicating with a previous AR. Prior to HK-LIFETIME expiring, the MN MUST request a new key from the AR if FMIPv6 service is still required from the router.

If more than one router responds to the RtSolPr, the MN MAY keep track of all such keys. If none of the PrRtAdvs contains an algorithm type indicator corresponding to an algorithm the MN supports, the MN MAY re-send the RtSolPr requesting a different algorithm, but to prevent bidding down attacks from compromised routers, the MN SHOULD NOT request an algorithm that is weaker than its original request.

3.4 Sending FBUs

When the MN needs to signal the Previous AR (PAR) using an FMIPv6 FBU, the MN MUST utilize the handover key and the corresponding authentication algorithm to generate an authenticator for the message. The MN MUST select the appropriate key for the PAR using the PAR's CGA and the MN's previous care-of CGA on the PAR's link. As defined by the FMIPv6 [FMIP], the MN MUST generate the authentication MAC using the handover key and the appropriate algorithm and MUST include the MAC in the FBU message. As specified by FMIPv6, the MN MUST include the old care-of CGA in a Home Address Option. The FMIPv6 document provides more detail about the construction of the authenticator on the FBU.

3.5 Receiving FBUs

When the PAR receives an FBU message containing an authenticator, the PAR MUST find the corresponding handover key using the MN's

care-of CGA in the Home Address Option as the index. If a handover key is found, the PAR MUST utilize the handover key and the appropriate algorithm to verify the authenticator. If the handover key is not found, the PAR MUST NOT change forwarding for the care-

of CGA. The FMIPv6 document [FMIP] provides more detail on how the AR processes an FBU containing an authenticator.

3.6 Key Generation and Lifetime

The AR MUST randomly generate a key having sufficient strength to match the authentication algorithm. Some authentication algorithms specify a required key size. The AR MUST generate a unique key for each CGA public key, and SHOULD take care that the key generation is uncorrelated between handover keys, and between handover keys and CGA keys. The actual algorithm used to generate the key is not important for interoperability since only the AR generates the key; the MN simply uses it.

A PAR SHOULD NOT discard the handover key immediately after use if it is still valid. It is possible that the MN may undergo rapid movement to another AR prior to the completion of Mobile IPv6 binding update on the PAR, and the MN MAY as a consequence initialize another, subsequent handover optimization to move traffic from the PAR to another new AR. The default time for keeping the key valid corresponds to the default time during which forwarding from the PAR to the new AR is performed for FMIP. The FMIPv6 document [FMIP] provides more detail about the FMIP forwarding time default.

If the MN returns to a PAR prior to the expiration of the handover key, the PAR MAY send and the MN MAY receive the same handover key as was previously returned, if the MN generates the same CGA for its care-of address. However, the MN MUST NOT assume that it can continue to use the old key without actually receiving the handover key again from the PAR. The MN SHOULD discard the handover key after MIPv6 binding update is complete on the new AR. The PAR MUST discard the key after FMIPv6 forwarding for the previous care-of address times out or when HK-LIFETIME expires.

3.7 Protocol Constants

The following are protocol constants with suggested defaults:

HKEPK-LIFETIME: The maximum lifetime for the handover key encryption public key. Default is 12 hours.

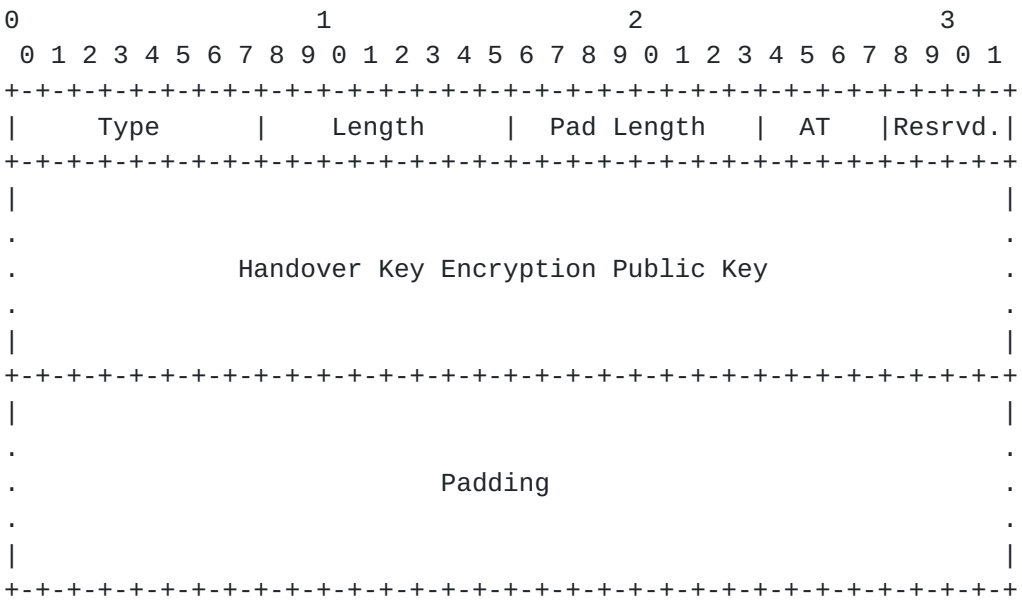
HKEPK-HANDOVERS: The maximum number of handovers for which the handover key encryption public key should be reused. Default is 10.

HK-LIFETIME: The maximum lifetime for the handover key. Default is 12 hours (43200 seconds).

4.0 Message Formats

4.1 Handover Key Request Option

The Handover Key Request Option is a standard IPv6 Neighbor Discovery [RFC2461] option in TLV format. The Handover Key Request Option is included in the RtSolPr message along with the SEND CGA Option, RSA Signature Option, and Nonce Option.



Fields:

Type: To be assigned by IANA.

Length: The length of the option in units of 8 octets, including the Type and Length fields. The value 0 is invalid. The receiver MUST discard a message that contains this value.

Pad Length: The number of padding octets beyond the end of the Handover Key Encryption Public Key field but within the length specified by the Length field. Padding octets MUST be set to zero by senders and ignored by receivers.

AT: A 4-bit algorithm type field describing the algorithm used by FMIPv6 to calculate the authenticator. See [FMIP] for details.

Resrvd.: A 4-bit field reserved for future use. The value MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Handover Key Encryption Public Key:

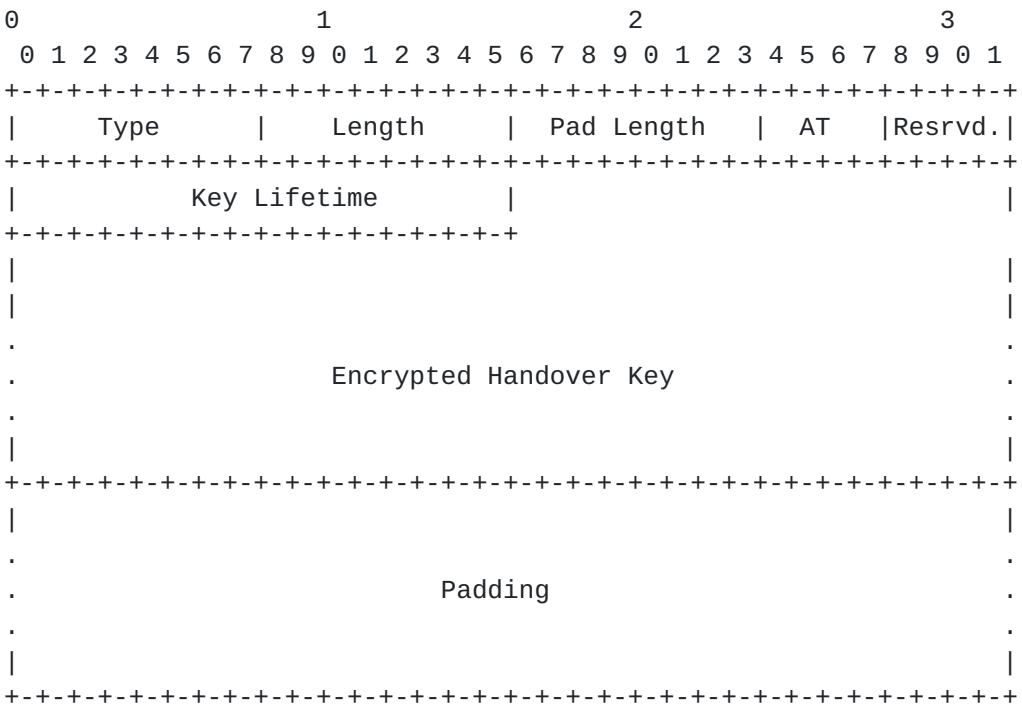
The handover key encryption public key. The key

MUST be formatted according to the same specification as the CGA key in the CGA Parameters Option [CGA] of the message, and MUST have the same parameters as the CGA key.

Padding: A variable-length field making the option length a multiple of 8, containing as many octets as specified in the Pad Length field.

4.2 Handover Key Reply Option

The Handover Key Reply Option is a standard IPv6 Neighbor Discovery [RFC2461] option in TLV format. The Handover Key Reply Option is included in the PrRtAdv message along with the SEND CGA Option, RSA Signature Option, and Nonce Option.



Fields:

Type: To be assigned by IANA.

Length: The length of the option in units of 8 octets, including the Type and Length fields. The value 0 is invalid. The receiver MUST discard a message that contains this value.

Pad Length: The number of padding octets beyond the end of the Encrypted Handover Key field but within the length specified by the Length field. Padding octets MUST be set to zero by senders and ignored by receivers.

AT: A 4-bit algorithm type field describing the algorithm used by FMIPv6 to calculate the authenticator. See [FMIP] for details.

Resrvd.: A 4-bit field reserved for future use. The value MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Key Lifetime: Lifetime of the handover key, HK-LIFETIME, in seconds.

Encrypted Handover Key:

The shared handover key, encrypted with the MN's handover key encryption public key, using the RSAES-PKCS1-v1_5 format [RFC3447].

Padding: A variable-length field making the option length a multiple of 8, containing as many octets as specified in the Pad Length field.

5.0 Security Considerations

This document describes a shared key provisioning protocol for the FMIPv6 handover optimization protocol. The key provisioning protocol utilizes a public key generated with the same public key algorithm as SEND to bootstrap a shared key for authorizing changes due to handover associated with the MN's former address on the PAR. General security considerations involving CGAs apply to the protocol described in this document, see [CGA] for a discussion of security considerations around CGAs. This protocol is subject to the same risks from replay attacks and DoS attacks using the RtSolPr as the SEND protocol [SEND] for RS. The measures recommended in RFC 3971 for mitigating replay attacks and DoS attacks apply here as well. An additional consideration involves when to generate the handover key on the AR. To avoid state depletion attacks, the handover key SHOULD NOT be generated prior to SEND processing that verifies the originator of RtSolPr. State depletion attacks can be addressed by techniques such as rate limiting RtSolPr, restricting the amount of state reserved for unresolved solicitations, and clever cache management. These techniques are the same as used in implementing Neighbor Discovery.

For other FMIPv6 security considerations, please see the FMIPv6 document [FMIP].

6.0 IANA Considerations

Two new IPv6 Neighbor Discovery options, the Handover Key Request Option and Handover Key Reply Option, are defined, and require a IPv6 Neighbor Discovery option type code from IANA.

7.0 Normative References

[FMIP] Koodli, R., editor, "Fast Handovers for Mobile IPv6", Internet Draft, Work in Progress.

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

[CGA] Aura, T., "Cryptographically Generated Addresses", RFC 3972, March 2005.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[RFC2461] Narten, T., and Nordmark, E., "Neighbor Discovery for IP version 6 (IPv6)", RFC 2461, December 1998.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

8.0 Informative References

[RFC3756] Nikander, P., editor, Kempf, J., and Nordmark, E., " IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[PBK] Bradner, S., Mankin, A., and Schiller, J., "A Framework for Purpose-Built Keys (PBK)", Internet Draft, work in progress.

9.0 Author Information

James Kempf
DoCoMo Labs USA
3240 Hillview Avenue
Palo Alto, CA
94303
USA
Phone: +1 650 496 4711
Email: kempf@docomolabs-usa.com

Rajeev Koodli
Nokia-Siemens Research Center
313 Fairchild Drive
Mountain View, CA
94043
USA
Phone: +1 650 625 2359
Fax: +1 650 625 2502
Email: Rajeev.Koodli@nokia.com

10.0 IPR Statements

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.

11.0 Disclaimer of Validity

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.

12.0 Copyright Statement

13.0 Acknowledgments

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

The authors would like to thank John C. Mitchell and Arnab Roy, of Stanford University, for their review of the design and suggestions for improving it.