Singapore Management University
Institutional Knowledge at Singapore Management University

Research Collection School Of Information Systems

School of Information Systems

9-2005

Security Analysis and Improvement of Return Routability Protocol

Ying QIU
Institute for Infocomm Research, Singapore

Jianying ZHOU
Institute for Infocomm Research, Singapore

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

DOI: https://doi.org/10.1007/11801412_16

Citation

QIU, Ying; ZHOU, Jianying; and DENG, Robert H.. Security Analysis and Improvement of Return Routability Protocol. (2005). *Secure Mobile Ad-hoc Networks and Sensors: First International Workshop, MADNES 2005, Singapore, September 20-22, 2005: Revised Selected Papers*. 4074, 174-181. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/566

Published in International Workshop on Secure Mobile Ad-hoc Networks and Sensors, MADNES 2005, September 20-22
http://dx.doi.org/10.1007/11801412_16

Security Analysis and Improvement of Return Routability Protocol

Ying Qiu[1], Jianying Zhou[1], and Robert Deng[2]

[1] Institute for Infocomm Research (I^{2}R) 21, Heng Mui Keng Terrace,
Singapore, 119613
{qiuying, jyzhou}@i2r.a-star.edu.sg
[2] Singapore Management University (SMU) 80 Stamford Road, Singapore 178902
robertdeng@smu.edu.sg

Abstract. Mobile communication plays a more and more important role in computer networks. How to authenticate a new connecting address belonging to a said mobile node is one of the key issues in mobile networks. This paper analyzes the Return Routability (RR) protocol and proposes an improved security solution for the RR protocol without changing its architecture. With the improvement, three types of redirect attacks can be prevented.

Keywords: Authentication, Redirect Attacks, Security, MIPv6.

1 Introduction

Mobile networking technologies, along with the proliferation of numerous portable and wireless devices, promise to change people's perceptions of the Internet. In true mobile networking, communications activities are not disrupted when a user changes his/her device's point of attachment to the Internet - all the network reconnections occur automatically and transparently to the user. The IETF RFC 3775 [1] supports mobile networking by allowing a mobile node to be addressed by two IP addresses, a home address and a care-of address. The former is an IP address assigned to the mobile node within its subnet prefix on its home subnet and the latter is a temporary address acquired by the mobile node while visiting a foreign subnet. The dual address mechanism in Mobile IP network allows packets to be routed to the mobile node regardless of its current point of attachment and the movement of the mobile node away from its home subnet is transparent to transport and higher-layer protocols. Fig 1 shows the basic operation in mobile IPv6.

One of the major features in Mobile IPv6 is the support for "Route Optimization" as a built-in fundamental part of the Mobile IPv6 protocol. The integration of route optimization functionality allows direct routing from any correspondent node (CN) to any mobile node (MN), without needing to pass through the mobile node's home sub-net and be forwarded by its home agent (HA), and thus eliminates the problem of "triangle routing". Route optimization in Mobile IPv6 requires that the MN, HA and the CNs maintain a Binding Cache. A binding

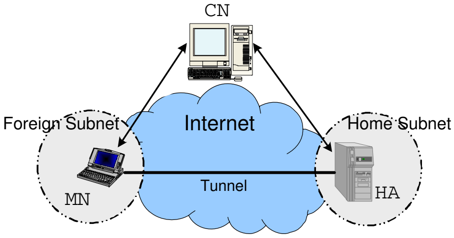


Fig. 1. Basic operation in mobile IPv6

is the association of a MN's home address (HoA) with a care-of address (CoA) for that mobile node, along with the remaining lifetime of that association. A mobile node uses Binding Update (BU) messages to notify its CNs or its HA of its current binding. Unfortunately, unauthenticated binding update messages provide intruders with an easy means to launch "Redirect Attacks", i.e., malicious acts which redirect traffic from the correspondent nodes to destinations chosen by intruders. Therefore, security of the binding update messages is of para-mount importance for Mobile IPv6 to meet its basic security requirements.

In IETF RFC 3775 [1], the Return Routability protocol (RR) is deployed to secure binding updates from MN to CNs. The basic RR mechanism consists of two checks, a home address check and a care-of-address check.

In the paper, we will analyze the RR mechanism and point out three attacks to the RR protocol, and finally propose a solution without changing the RR architecture.

The notations used throughout this paper are listed below:

h( ) a one-way hash function, such as SHA1 [2].
prf(k, m) a keyed pseudo random function - often a keyed hash function [3]. It accepts a secret key k and a message m, and generates a pseudo random output. This function is used for both message authentication and cryptographic key derivations.
e(k ,m) encryption of message m with a secret key k.
m|n concatenation of two messages m and n.
MN mobile node HA home agent of a mobile node.
CN correspondent node of a mobile node.
CNA IP address of CN.
HoA home address of a mobile node.
CoA MN's care-of address when it visits a foreign network.

2 Brief Review of RR Protocol

In RFC 3775's Return Routability (RR) protocol [1], a CN keeps a secret key k_{CN} and generates a nonce at regular intervals, say every few minutes. CN uses the same key k_{CN} and nonce with all the mobile nodes it is in communication with, so that it does not need to generate and store a new nonce when a new mobile node contacts it. Each nonce is identified by a nonce index. When a new nonce is generated, it must be associated with a new nonce index, e.g., j. CN keeps both the current value of N_j and a small set of previous nonce values, $N_{j-1}, N_{j-2},.$ Older values are discarded, and messages using them will be rejected as replays. Message exchanges in the RR protocol are shown in Fig 2, where the $HoTI$ (Home Test Init) and $CoTI$ (Care-of Test Init) messages are sent to CN by a mobile node MN simultaneously. The HoT (Home Test) and CoT (Care-of Test) are replies from CN. All RR protocol messages are sent as IPv6 "Mobility Header" in IPv6 packets. In the representation of a protocol message, we will use the first two fields to denote source IP address and destination IP address, respectively. We will use CNA to denote the IP address of the correspondent node CN.

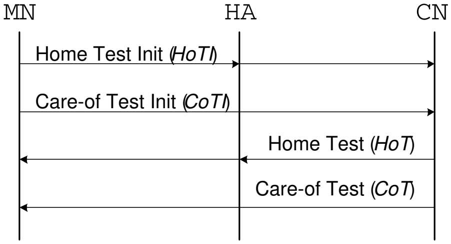


Fig. 2. Return Routability protocol

When MN wants to perform route optimization, it sends

$$HoTI = \{HoA, CNA, r_H\}$$

and

$$CoTI = \{CoA, CNA, r_C\}$$

to CN, where r_H and r_C are random values used to match responses with requests. $HoTI$ tells MN's home address HoA to CN. It is reverse tunneled through the home agent HA, while $CoTI$ informs MN's care-of address CoA and is sent directly to CN.

When CN receives $HoTI$, it takes the source IP address of $HoTI$ as input and generates a home keygen token

$$KT_H = prf(k_{CN}, HoA|N_j|0)$$

and replies MN with

$$HoT = \{CNA, HoA, r_H, KT_H, j\},$$

where | denotes concatenation and the final "0" inside the pseudo random function is a single zero octet, used to distinguish home and care-of cookies from each other. The index j is carried along to allow CN later efficiently finding the nonce value N_j that it used in creating the token KT_H. Similarly, when CN receives $CoTI$, it takes the source IP address of $CoTI$ as input and generates a care-of keygen token

$$KT_C = prf(k_{CN}, CoA|N_i|1)$$

and sends

$$CoT = \{CNA, CoA, r_C, KT_C, i\}$$

to MN, where the final "1" inside the pseudo random function is a single octet "0x01". Note that HoT is sent via MN's home agent HA while CoT is delivered directly to MN.

When MN receives both HoT and CoT, it hashes together the two tokens to form a session key

$$k_{BU} = h(KT_H|KT_C),$$

which is then used to authenticate the correspondent binding update message to CN:

$$BU = \{CoA, CNA, HoA, Seq\#, i, j, MAC_{BU}\},$$

where $Seq\#$ is a sequence number used to detect replay attack and

$$MAC_{BU} = prf(k_{BU}, CoA|CNA|HoA|Seq\#|i|j)$$

is a message authentication code (MAC) protected by the session key k_{BU}. MAC_{BU} is used to ensure that BU was sent by the same node which received both HoT and CoT. The message BU contains j and i, so that CN knows which nonce values N_j and N_i to use to first recompute KT_H and KT_C and then the session key k_{BU}. Note that CN is stateless until it receives BU and verifies MAC. If MAC is verified positive, CN may reply with a binding acknowledgement message

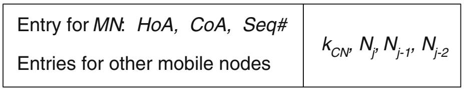
$$BA = \{CNA, CoA, HoA, Seq\#, MAC_{BA}\},$$

where $Seq\#$ is copied from the BU_{CN} message and

$$MAC_{BA} = prf(k_{BU}, CNA|CoA|HoA|Seq\#)$$

is a MAC generated using k_{BU} to authenticate the BA message. CN then creates a binding cache entry for the mobile node MN. The binding cache entry binds HoA with CoA which allows future packets to MN be sent to CoA directly.

An example implementation of the binding cache at CN is shown in Fig 3, where HoA is used as an index for searching the binding cache, the sequence number $Seq\#$ is used by CN to check the freshness of binding updates. Each binding update sent by MN must use a $Seq\#$ greater than (modulo 2^{16}) the one sent in the previous binding update with the same HoA. It is not required, however, that the sequence number value strictly increase by 1 with each new binding update sent or received [1]. Note that the session key k_{BU} is not kept in the cache entry. When CN receives a binding update message, based on the



Entry for *MN*: *HoA, CoA, Seq#*	$k_{CN}, N_j, N_{j-1}, N_{j-2}$
Entries for other mobile nodes	

Fig. 3. A binding cache implementation at CN in the RR protocol

nonce indexes i and j in the message, it recomputes the session key using k_{CN} and the list of the most recent nonce values, say $\{N_j, N_{j-1}, N_{j-2}\}$, and then verifies BU using the newly computed session key.

The mobile node MN maintains a Binding Update List for each binding update message sent by it, for which the lifetime has not yet expired. A binding update list for a correspondent node CN consists of CNA, MN's HoA and CoA, the remaining lifetime of the binding, the maximum value of the sequence number sent in previous binding updates to CN and the session key k_{BU}.

3 Redirect Attacks to RR Protocol

Obviously, the RR protocol protects binding updates against intruders who are unable to monitor the HA-CN path and the MN-CN path simultaneously. However, one has no reason to assume that an intruder will monitor one link and not the other, especially when the intruder knows that monitoring a given link is particularly effective to expedite its attack. Even worse, we demonstrate that the RR protocol can be attacked under its original assumption of no simultaneous monitor of both the HA-CN path and the MN-CN path.

3.1 Session Hijacking Attacks

Let's consider the scenarios showed in Fig 4, a mobile node MN_1 is communicating with a correspondent node CN. An intruder sends a forged binding update message (or replays an old binding update message) to CN, claiming that MN_1 has moved to a new care-of-address belonging to a node MN_2. If CN accepts the fake binding update, it will redirect to MN_2 all packets that are intended to MN_1. This attack allows the intruder to hijack ongoing connections between MN_1 and CN or start new connections with CN pretending to be MN_1. This is an "outsider" attack since the intruder tries to redirect other nodes' traffic. Such an attack may result in information leakage, impersonation of the mobile node MN_1 or flooding of MN_2.

This attack is serious because MN_1, MN_2, CN and the intruder can be any nodes anywhere on the Internet. All the intruder needs to know is the IP addresses of MN_1 and CN. Since there is no structural difference between a mobile node home address and a stationary IP address, the attack works as well against stationary Internet nodes as against mobile nodes. The deployment of a binding update protocol without security could result in breakdown of the entire Internet [4].

In the case of the static IPv6 without mobility (which is equivalent to the mobile node MN at its home subnet in Mobile IPv6), to succeed in the attack, the intruder must be constantly present on the CN-HA path. In order to redirect CN's traffic intended for MN to a malicious node, the intruder most likely has to get control of a router or a switch along the CN-HA path. Furthermore, after taking over the session from MN, if the malicious node wants to continue the session with CN while pretending to be MN, the malicious node and the router need to collaborate throughout the session. For example, the router tunnels CN's traffic to the malicious node and vise versa.

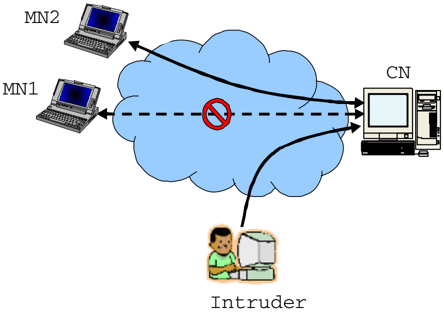


Fig. 4. Session hijacking attacks

In the case of Mobile IPv6, the effort committed to break the RR protocol to launch a session hijacking attack could be considerably lesser. Assume that MN_1 and CN are having an on-going communication session and the intruder wants to redirect CN's traffic to his collaborator MN_2. The intruder monitors the CN-HA path (i.e., anywhere from MN_1's home network to CN's network) to obtain HoT, extracts the home keygen token KT_H and sends it to MN_2.

Upon receiving KT_H, MN_2 sends a $CoTI$ to CN and CN will reply with a care-of keygen token KT_C. MN_2 simply hashes the two keygen tokens to obtain a valid binding key, and uses the key to send a binding update message to CN on behalf of MN_1. The binding update will be accepted by CN which will in turn direct its traffic to MN_2.

3.2 Movement Halting Attacks

Another related attack is when a mobile node MN rapidly moves from one care-of ad-dress CoA to another CoA'. Since MN runs the RR protocol whenever it moves to a new location, an intruder can intercept the care-of keygen token KT_C in the current RR session and the home keygen token KT_H in the next RR session, hash the two keygen tokens to get a valid binding key, and then send a binding update message with the CoA in the current session to the correspondent node. The correspondent node will still send its traffic back to CoA. Hence, MN, which has moved to CoA', will not receive data from the correspondent node. Note that in this attack the attacker does not have to intercept the two keygen tokens at the "same time".

3.3 Traffic Permutation Attacks

The RR protocol is also subject to a "traffic permutation" attack. Consider a correspondent node which provides on-line services to many mobile clients (Fig 5). An intruder can simply eavesdrop on the RR protocol messages to collect keygen tokens on the border between the correspondent node and the Internet. The intruder then hashes random pairs of keygen tokens to form binding keys, and sends binding update messages to the correspondent node.

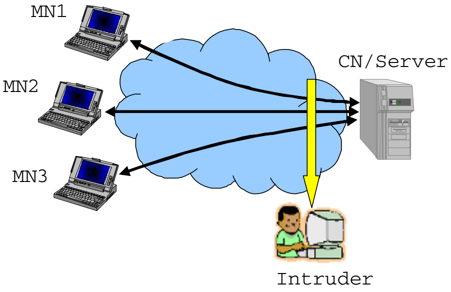


Fig. 5. Intruder attacks an on-line server

Such a forged binding update message will be accepted by the correspondent node with probability 1/4. This will cause redirection of traffic to randomly selected mobile clients and eventually bring down the services of the correspondent node.

4 Improvement of RR Protocol

The attacks outlined in the above section are due to the decoupling of HoA and CoA in RR messages. In the original RR protocol, the home keygen token

$$KT_H = prf(k_{CN}, HoA|N_j|0)$$

and the care-of keygen token

$$KT_C = prf(k_{CN}, CoA|N_i|1)$$

are delivered without any stated relationship. Any pair of home keygen token and care-of keygen token can generate a valid binding key

$$k_{BU} = h(KT_H|KT_C)$$

as long as the indexes, i and j, are still valid.

However, the attacks described in the above section can be prevented by modifying the RR protocol to include both CoA and HoA in the generation of home keygen token and care-of keygen token, respectively. In the improved RR protocol, HoA and CoA are bound together. (The modified parts are underscored.) A mobile node sends

$$HoTI' = \{HoA, CNA, CoA, r_H\}$$

and

$$CoTI' = \{CoA, CNA, HoA, r_C\}$$

to a CN, which replies with the home keygen token

$$KT'_H = prf(k_{CN}, HoA|N_j|CoA|0)$$

and the care-of keygen token

$$KT'_C = prf(k_{CN}, CoA|N_i|HoA|1).$$

Then the new binding key

$$k'_{BU} = h(KT'_H|KT'_C)$$

is valid only for the pair of HoA and its claimed CoA. Therefore the misuse of keygen tokens can be avoided.

5 Conclusion

In this paper, we first reviewed the Return Routability protocol in RFC 3775, then demonstrated three redirect attacks: Session Hijacking Attacks, Movement Halting Attacks and Traffic Permutation Attacks. We further pointed out that the attacks are due to the decoupling of HoA and CoA in RR messages. We also proposed an improved solution that provides much stronger security than the original RR protocol without changing its architecture.

References

1. D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", IETF RFC 3775, June 2004.
2. NIST, "Secure Hash Standard", NIST FIPS PUB 180, May 1993.
3. H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Messaging Authentication", IETF RFC 2104, February 1997.
4. T. Aura, "Mobile IPv6 Security", Proceedings of the 10th International Workshop on Security Protocols, LNCS 2467, Cambridge, UK, April 2002.