Mobile IP WG
INTERNET-DRAFT
Date: 23 February 2001
Expires: 23 August 2001

Franck Le
Stefano M. Faccin
Basavaraj Patil
Nokia Research Center

Challenge-Response Authentication Request
<draft-le-mobileip-authreq-00.txt>

Status of This Memo

Abstract

A mobile IP node may share a security association with its home AAA server to allow the mobile node to be authenticated when roaming to different visited domains. The Mobile IP framework has defined some extensions enabling challenge response based authentication mechanisms. Currently, the challenge used for the authentication is generated by the visited domain and broadcasted in Router Advertisements messages. The mobile node uses this challenge to compute authentication data when it wants to register to the network. In order to allow for an easy deployment of Mobile IP for cellular networks, the security of Mobile IP should be enhanced at least to match the level of security available nowadays in cellular networks.

For this reason, the home domain need the ability to ask a user to provide authentication information anytime during a session, and thus to decide whether the session can be continued or has to be terminated according to the result of the authentication. In addition, the visited domain should be able as well to to ask a user to provide authentication information anytime during a session, thus allowing the visited domain more control on the roaming. In the same way, the mobile node should also be able to authenticate the network at any time. This document specifies extensions to Mobile IP messages to enable the home domain and the visited domain at any time during a session to ask a mobile node to provide authentication credentials. This document also defines the extensions to enable the mobile node to perform network authentication at any time during a session.

1. Introduction

A mobile IP node may share a security association with its home AAA server to allow the mobile node to be authenticated when roaming to different visited domains. The Mobile IP framework has defined some extensions [1], [2] enabling challenge response based authentication mechanisms. Currently, the challenge used for the authentication is generated by the visited domain and broadcasted e.g. in Router Advertisements messages. The mobile node uses this challenge to compute authentication data when it wants to register to the network.

As indicated above, the home and visited domain need the ability to ask a user to provide authentication information anytime during a session, and thus to decide whether the session can be continued or has to be terminated according to the result of the authentication. This is needed in order to limit frauds, e.g. to avoid that a fraudulent mobile node impersonates a legitimate mobile node and accesses the resources of the visited domain. Possible triggers for a network initiated user authentication procedure include, e.g., a periodic timer time-out, the presence of the mobile node in a high-fraud area, a mobile node "marked" as possibly fraudulent by the home domain, or an authorization request from the mobile node for certain resources causing the network to require user re-authentication etc.

Challenge-response based authentication mechanisms provide strong entity authentication, thus the network should be able at any time to challenge the mobile node by sending an Authentication Request message carrying a random number (the challenge) and requesting the mobile node to authenticate.

Differently from the current challenge-response mechanisms, where the challenge used for the authentication is generated by the visited domain and broadcasted in Router Advertisements messages, this mechanism proposed in this document is user specific. In fact, the challenge generated by the network is directed to a particular MN (rather than to all MNs able to receive the broadcasted information,

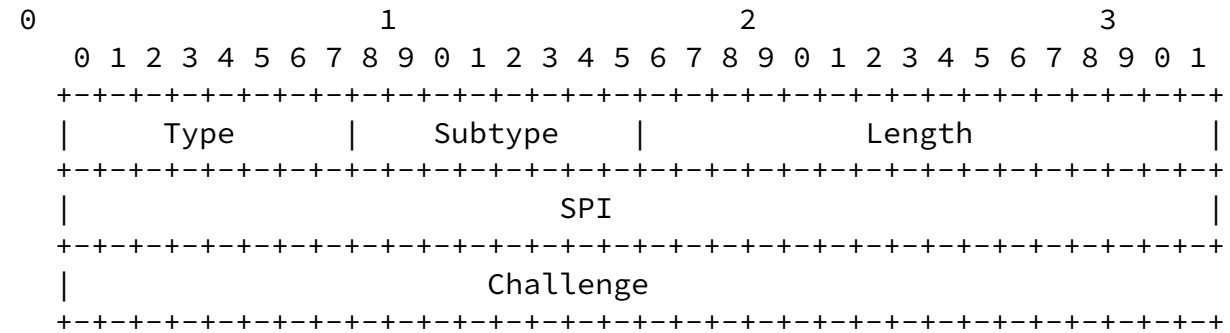
as it is currently defined). Since the random number for the challenge is changed for each operation, the proposed authentication mechanism provides a much more secure user authentication. Whether the first authentication procedure succeeded or failed, the user specific challenge authentication can serve as a double check on the authenticity of the MN.

In the same way, the mobile node should also be able to authenticate the network by generating a challenge at any time during a session and sending it to the network.

2. Mobile IP Authentication Request Extension

The Authentication Request destination option is used to request a mobile node or the network to authenticate. As a destination option, the Authentication Request MAY be sent in a packet by itself or MAY be included in any existing packet being sent to the mobile node when initiated by the network or by the mobile node when iniated by the mobile node. A packet containing a Authentication Request option is sent in the same way as any packet to the receiving end point. When a mobile node or the network receives a packet containing an Authentication Request option, it SHOULD return an Authentication Response to the source of the Authentication Request.

The Authentication Request option is encoded the format as follows:



Type TBD

Subtype	a number assigned to identify the way in which the Challenge is to be used
Length	4 plus the number of bytes in the Subtype Data; SHOULD be at least 20.
SPI	Security Parameters Index
Challenge	The Challenge to be used to compute the Authentication data

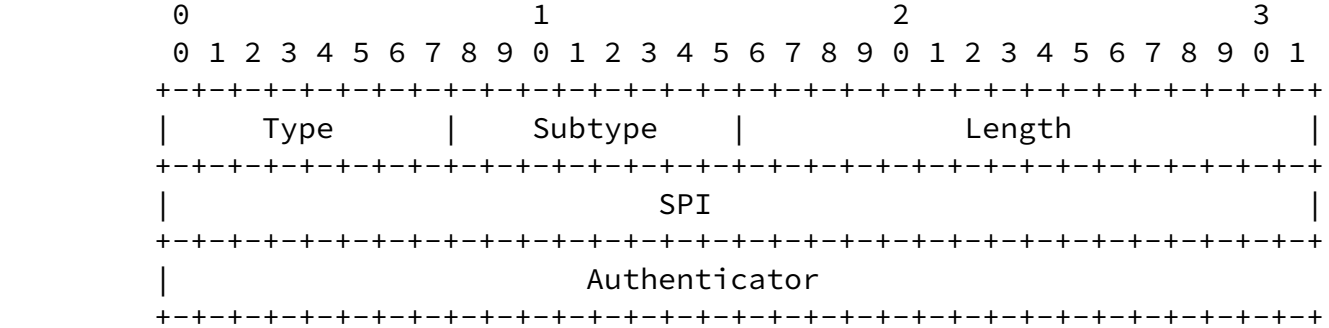
3. Mobile IP Authentication Response Extension

The Authentication Response destination option is sent in response to an Authentication Request option sent by the mobile node or the

network respectively to the network or the mobile node in order to provide the authentication data.

Authentication Response destination option MAY be sent in a packet by itself or MAY be included in any existing packet being sent to the mobile node by the network or by the mobile node to the network. A packet containing a Authentication Response option is sent in the same way as any packet to the receiving end point.

The Authentication Response option is encoded the format as follows:



Type	TBD
Subtype	a number assigned to identify the way in which the Challenge is used
Length	4 plus the number of bytes in the Subtype Data; SHOULD be at least 20.
SPI	Security Parameters Index
Authenticator	The variable length Authenticator field

4. Request-Response matching scheme

It is possible that the Home/Visited network or the MN sends an authentication request respectively to the MN or the Home/Visited network and, after a few seconds, it sends another authentication request which has a different challenge encoded in it. The receiving end point may never receive the first authentication request (e.g. a message is lost on the access link) and receive only the second authentication request. In this situation, when an authentication response is sent back to the Home/Visited network or the MN (i.e. the

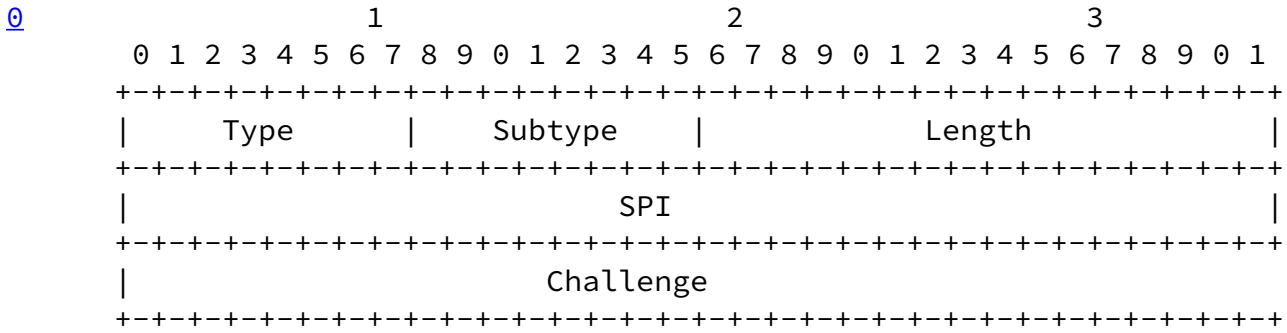
entity initiating the authentication procedure), the Home/Visited network or the MN needs to know which authentication request the the authentication response was received for in order to perform the correct validation of the authentication data received.

Two options are possible: the entity receiving the authentication request includes the challenge received in the authentication request in the authentication response message, or the entity initiating the authentication procedure includes a Challenge_Identifier in the Authentication Request extension and the entity receiving the authentication request includes the Challenge_Identifier in the authentication response.

4.1. Basic Request-Response matching scheme

In this first option, the entity receiving the authentication request includes the challenge received in the authentication request in the authentication response message.

Consistently to [1], the additional destination option containing the challenge used for the authentication is added to the message containing the authentication response and has the following format.



4.2. Optimized Request-Response Matching Scheme

There may be some cases where there is the need to optimize the information used for authentication over the access link, e.g. wireless links where the radio resources are limited. In such cases, including the Challenge in the authentication response may make the header too large. A solution for this case is that the entity initiating the authentication procedure includes a Challenge_Identifier in the Authentication Request extension, e.g. in the format of a timestamp or a counter, and the entity receiving the

authentication request includes this Challenge_Identifier in the authentication response for the authenticator can know which challenge the response corresponds to.

5. Applicability to Mobile IPv4

The extensions defined in this document are specific to Mobile IPv6

but similar extensions can be defined for Mobile IPv4 enabling any entity to request authentication at any time. The same concept can therefore apply to Mobile IPv4.

6. Security Considerations

This document specifies extensions to Mobile IP messages to carry the parameters to perform either user specific or network challenge response based authentication mechanism, but does not define the algorithms to use to process the authentication data.

7. References

[1] C. Perkins and P. Calhoun. Mobile IPv4 Challenge/Response Extensions. Request for Comments 3012, Internet Engineering Task Force, November 2000.

[2] N. Asokan, Patrik Flykt, Charles E. Perkins and Thomas Eklund AAA for IPv6 Network Access. Internet Draft, Internet Engineering Task Force, January 2000.

8. Authors' Addresses

Franck Le
Nokia Research Center
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972 374-1256
E-mail: franck.le@nokia.com

Stefano M. Faccin
Nokia Research Center
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972 894-4994
E-mail: stefano.faccin@nokia.com

Basavaraj Patil
Nokia Corporation
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972-894-6709
E-Mail: Raj.Patil@nokia.com

Table of Contents