IETF
Internet-Draft
Intended status: Standards Track
Expires: August 7, 2008

B. Wallis
Mavenir Systems

February 4, 2008

Hypertext Transfer Protocol (HTTP) Digest Authentication using Global System for Mobile Communications (GSM) A3 and A8 draft-ietf-http-digest-auth-a3a8-01

Status of this Memo

Copyright Notice

Abstract

This memo specifies a one-time password generation mechanism for Hypertext Transfer Protocol (HTTP) Digest access authentication based on Global System for Mobile Communications (GSM) authentication and key generation functions A3 and A8. The HTTP Authentication Framework includes two authentication schemes: Basic and Digest. Both schemes employ a shared secret based mechanism for access authentication. The A3-A8 mechanism performs user authentication and

session key distribution in GSM and Universal Mobile Telecommunications System (UMTS) networks. A3-A8 is a challenge-response based mechanism that uses symmetric cryptography.

Table of Contents

1. Introduction and Motivation

The Hypertext Transfer Protocol (HTTP) Authentication Framework, described in RFC 2617 [1], includes two authentication schemes: Basic and Digest. Both schemes employ a shared secret based mechanism for access authentication. The Basic scheme is inherently insecure in that it transmits user credentials in plain text. The Digest scheme improves security by hiding user credentials with cryptographic hashes, and additionally by providing limited message integrity.

The GSM A3 and A8 functions [2] perform authentication and session key distribution in Global System for Mobile Communication (GSM) and Universal Mobile Telecommunications System (UMTS) networks. A3-A8 is a challenge- response based mechanism that uses summetric cryptography. A3-A8 is typically run in a GSM Services Identity Module (SIM), which resides on a smart card like device that also provices tamper resistant storage of shared secrets. The Authentication and Key Agreement (AKA) mechanism is most closely associated with UMTS; however, mobile operators commonly distribute GSM SIMs with UMTS mobile phones, resulting in the use of GSM A3-A8 in place of AKA.

This document specifies a mapping of A3-A8 parameters onto HTTP Digest authentication. In essence, this mapping enables the usage of A3-A8 as a one-time password generation mechanism for Digest authentication.

As the Session Initiation Protocol (SIP) [3] Authentication Framework closely follows the HTTP Authentication Framework, Digest A3-A8 is directly applicable to SIP as well as any other embodiment of HTTP Digest. This in turn allows A3-A8 authentication and key generation within the 3GPP IP Multimedia Subsystem (IMS) or other SIP-based core networks. This is of particular use for GSM mobile operators who wish to deploy IMS or other SIP-based core networks while providing support for existing deployed SIMs, which could number in the tens of millions.

This document is based heavily on [5] which specified a mapping of Authentication and Key Agreement (AKA) onto HTTP Digest authentication.

1.1. Terminology

This section explains the terminology used in this document.

AuC	Authentication Center.
GSM	Global System for Mobile Communication.
IMS	IP Multimedia Subsystem.
ISIM	IP Multimedia Services Identity Module. IMS counterpart to SIM.
Kc	Cypher Key.
Ki	Subscriber Key.
RAND	Random Challenge. Generated by the AuC.
SIM	Subscriber Identity Module.
SRES	Signed Authentication Response. Generated by the SIM.
UMTS	Universal Mobile Telecommunications System.
USIM	Universal Mobile Telecommunications System. UMTS counterpart to SIM.

1.2. Requirements Language

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 [1].

2. A3-A8 Mechanism Overview

This chapter describes the GSM A3-A8 operation in detail:

1. A shared secret Ki is established beforehand between the SIM and the Authentication Center (AuC). The secret is stored in the SIM, which resides on a smart card like, tamper resistant device.

2. The AuC of the home network produces an authentication vector AV, based on the shared secret Ki. The authentication vector contains a random challenge RAND, an expected authentication result, and a session key for ciphering Kc.

3. The authentication vector is downloaded to a server. Optionally, the server can also download a batch of AVs, containing more than one authentication vector.

4. The server creates an authentication request, which contains the random challenge RAND.

5. The authentication request is delivered to the client.

6. The client produces a signed authentication response SRES, using the shared secret Ki and the random challenge RAND.

7. The authentication response SRES is delivered to the server.

8. The server compares the authentication response SRES with the expected response. If the two match, the user has been successfully authenticated, and the session key Kc can be used for protecting further communication between the client and the server.

3. Specification of Digest A3-A8

In general, the Digest A3-A8 operation is identical to the Digest operation in RFC 2617 [1]. This chapter specifies the parts in which Digest A3-A8 extends the Digest operation. The notation used in the Augmented BNF definitions for the new and modified syntax elements in this section is as used in SIP [3], and any elements not defined in this section are as defined in SIP and the documents to which it refers.

3.1. Algorithm Directive

In order to direct the client to use A3-A8 for authentication instead of the standard password system, the RFC 2617 defined algorithm directive specifies Digest A3A8.

```
algorithm        = "algorithm" EQUAL ( a3a8-namespace
                   / algorithm-value )
a3a8-namespace   = "A3-A8" "-" algorithm-value
algorithm-value  = ( "MD5" / "MD5-sess" / token )
```

algorithm
A string indicating the algorithm used in producing the digest and the checksum. If the directive is not understood, the nonce SHOULD be ignored, and another challenge (if one is present) should be used instead.

Reuse of the same SRES value in authenticating subsequent requests and responses is NOT RECOMMENDED. An SRES value SHOULD only be used as a one-time password, and algorithms such as "MD5-sess", which limit the amount of material hashed with a single

key, by producing a session key for authentication, SHOULD NOT be used.

3.2. Creating a Challenge

In order to deliver the A3-A8 authentication challenge to the client in Digest Ae-A8, the nonce directive defined in [2] is extended:

```
nonce             = "nonce" EQUAL ( a3a8-nonce / nonce-value )
a3a8-nonce        = LDQUOT a3a8-nonce-value RDQUOT
a3a8-value-value  = <base64 encoding of RAND>
```

nonce
A parameter which is populated with the Base64 [4] encoding of the A3-A8 authentication random challenge RAND.

3.3. Client Authentication

When a client receives a Digest A3-A8 authentication challenge, it extracts the RAND from the "nonce" parameter an druns the A3-A8 algorithms with the RAND challenge and shared secret Ki.

The resulting A3-A8 SRES parameter is treated as a "password" when calculating the response directive of [2]. Due to the fact that that the SRES parameter is 32 bits and the response directive of [2] is defined as 32 hex digits, SRES is encoded in the low order (i.e. rightmost) 32 bits of "response", padded with leading zeroes.

Example:

response="00000000000000000000000007018d8a1"

3.4. Server Authentication

With Digest A3-A8, the server uses the expected response received in the authentication vector as "password" when calculating the "response-auth" of the "Authentication-Info" header defined in [2].

4. Example Digest A3-A8 Operation

Figure 2 below describes a message flow describing a Digest A3-A8 process of authenticating a SIP request, namely the SIP REGISTER request.

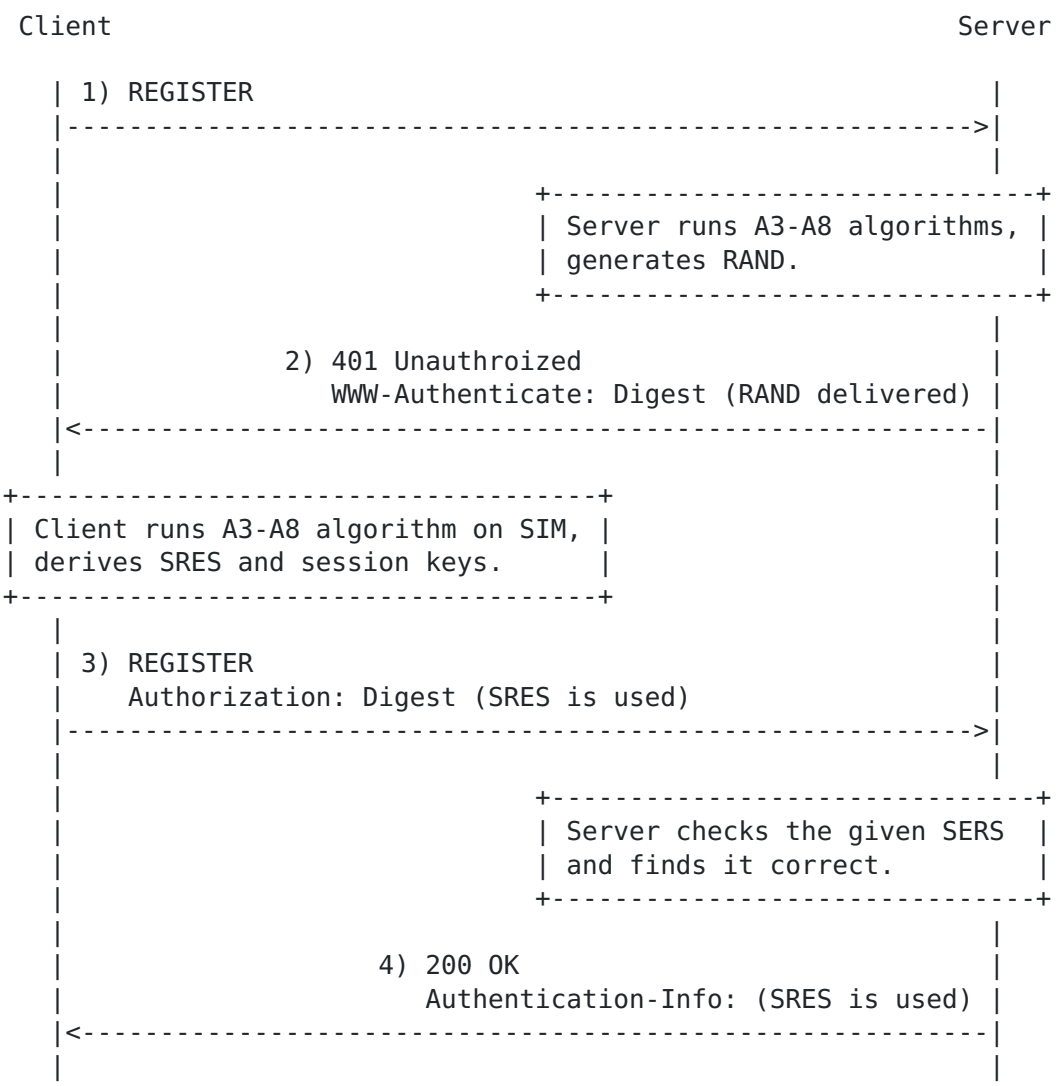

Figure 1: Message flow representing a successful authentication

1) Initial request

```
REGISTER sip:home.mobile.example.com SIP/2.0
```

2) Response containing a challenge

```
SIP/2.0 401 Unauthorized
WWW-Authenticate: Digest
        realm="RoamingUsers@example.com",
        nonce="I1U8vpY3pJ0hiuZNrke/NQ==",
        qop="auth,auth-int",
        opaque="6dae728da9089dab9112373c9f0a9731",
        algorithm=A3-A8-MD5
```

3) Request containing credentials

```
REGISTER sip:home.mobile.example.com SIP/2.0
Authorization: Digest
        username="adam.smith@example.com",
        realm="RoamingUsers@example.com",
        nonce="I1U8vpY3pJ0hiuZNrke/NQ==",
        qop=auth-int,
        nc=00000001,
        cnonce="0b8f29d6",
        response="00000000000000000000000046f8416a",
        opaque="6dae728da9089dab9112373c9f0a9731"
```

4) Successful response

```
SIP/2.0 200 OK
Authentication-Info:
        qop=auth-int,
        rspauth="00000000000000000000000046f8416a",
        cnonce="0b8f29d6",
        nc=00000001
```

5. Security Considerations

In general, Digest A3-A8 is vulnerable to the same security threats as HTTP authentication [2]. This chapter discusses the relevant exceptions.

5.1. Authentication of Clients using Digest A3-A8

A3-A8 is typically -- though this isn't a theoretical limitation -- run on a SIM application that usually resides in a tamper resistant smart card. Interfaces to the SIM exist, which enable the host device to request authentication to be performed on the card. However, these interfaces do not allow access to the long-term secret outside the SIM, and the authentication can only be performed if the device accessing the SIM has knowledge of a PIN code, shared between the user and the SIM. Such PIN codes are typically obtained from user input, and are usually required when the device is powered on.

The use of tamper resistant cards with secure interfaces implies that Digest A3-A8 is typically more secure than regular Digest implementations, as neither possession of the host device nor Trojan Horses in the software give access to the long-term secret. Where a PIN scheme is used, the user is also authenticated when the device is powered on. However, there may be a difference in the resulting

security of Digest A3-A8, compared to traditional Digest implementations, depending on whether those implementations cache/ store passwords that are received from the user.

5.2. Limited Use of Nonce Values

The Digest scheme uses server-specified nonce values to seed the generation of the request-digest value. The server is free to construct the nonce in such a way that it may only be used from a particular client, for a particular resource, for a limited period of time or number or uses, or any other restrictions. Doing so strengthens the protection provided against, for example, replay attacks.

Digest A3-A8 limits the applicability of a nonce value to a particular SIM. Typically, the SIM is accessible only to one client device at a time. However, the nonce values are strong and secure even though limited to a particular SIM. Additionally, this requires that the server is provided with the client identity before an authentication challenge can be generated. If a client identity is not available, an additional round trip is needed to acquire it.

5.3. Multiple Authentication Schemes and Algorithms

In HTTP authentication, a user agent MUST choose the strongest authentication scheme it understands and request credentials from the user, based upon that challenge.

In general, using passwords generated by Digest A3-A8 with other HTTP authentication schemes is not recommended even though the realm values or protection domains would coincide. In these cases, a password should be requested from the end-user instead. Digest A3-A8 passwords MUST NOT be re-used with such HTTP authentication schemes, which send the password in the clear. In particular, A3-A8 passwords must not be re-used with HTTP Basic.

The same principle must be applied within a scheme if several algorithms are supported. A client receiving an HTTP Digest challenge with several available algorithms MUST choose the strongest algorithm it understands. For example, Digest with "A3-A8-MD5" would be stronger than Digest with "MD5".

5.4. Online Dictionary Attacks

Since user-selected passwords are typically quite simple, it has been proposed that servers should not accept passwords for HTTP Digest which are in the dictionary [2]. This potential threat does not exist in HTTP Digest A3-A8 because the algorithm will use SIM

originated passwords. However, the end-user must still be careful with PIN codes. Even though HTTP Digest A3-A8 password requests are never displayed to the end-user, she will be authenticated to the SIM via a PIN code. Commonly known initial PIN codes are typically installed to the SIM during manufacturing and if the end-users do not change them, there is a danger than an unauthorized user may be able to use the device. Naturally this requirse that the unauthorized user has access to the physical device, and that the end-user has not changed the initial PIN code. For this reason, end-users are strongly encouraged to change their PIN codes when they receive a SIM.

5.5. Session Protection

Digest A3-A8 is able to generate an additional session key for integrity (Kc) protection. Even though this document does not specify the use of these additional keys, they may be used for creating additional security within HTTP authentication or some other security mechanisms.

5.6. Replay Protection

5.7. Improvements to A3-A8 Security

Even though A3-A8 is perceived as a secure mechanism, Digest A3-A8 is able to improve it. More specifically, the A3-A8 parameters carried between the client and the server during authentication may be protected along with other parts of the message by using Digest A3-A8. This is not possible with plain A3-A8.

5.8. AKA Securityy

Evolutions of GSM networks, specifically Universal Mobile Telecommunications System (UMTS) and IP Multimedia System (IMS) networks, use an enhanced shared secret based mechanism for authentication known as Authentication and Key Agreement (AKA). In these networks, AKA is typically run in a UMTS Services Identity Module (USIM) or IP Multimedia Services Identity Module (ISIM). GSM phones can also be equipped with a USIM, in which case AKA is used for authentication as opposed to A3-A8.

6. IANA Considerations

This memo includes no request to IANA.

7. References

7.1. Normative References

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

[2] Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A.,, Stewart, L., "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999

[3] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[4] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

7.2. Informative References

[5] Niemi, A. and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, September 2002.

[6] 3rd Generation Partnership Project, "Specification of the GSM-MILENAGE algorithms (Release 7)", TS 55.205, June 2007

Appendix A. Acknowledgements

This template was derived from an initial version written by Pekka Savola and contributed by him to the xml2rfc project.

Author's Address

Brett Wallis
Mavenir Systems
1651 N. Glenville Dr., Ste #201
Richardson, TX 75081
US

Phone: +1 469 916 4393 x5048
Email: brett@mavenir.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).