3GPP TSG SA WG3 Security **S3-030370**

15th – 18th July, 2003

San Francisco, CA, USA

Agenda Item:

Source: Ericsson

Title: HTTP Digest AKAv2 status and SQN issues

Document for: Information

1. Introduction

This document reports the progress of HTTP Digest AKAv2 in IETF. It also draws SA3 attention to one new feature of AKAv2 that may help in solving potential SQN synchronization failure issues when AKA is re-used with several applications.

The latest version of the draft is attached to this contribution.

2. Progress in IETF

The first version of [akav2] has been published in IETF I-D directory. The draft does not belong to any specific WG, and it is supposed to proceed as individual submission. The draft has been announced to SIPPING mailing list in order to receive comments.

After the previous SA3 meeting, Nokia has reviewed and commented the draft directly to Ericsson. The major comment was related to the scope of the draft, and on how closely AKAv2 should be tied to the use of TLS. The current understanding is that the since the use of any algorithm in the HTTP authentication framework with TLS includes the Man-in-the-middle problem, IETF should solve the general problem in some other work item. For this reason, Ericsson is not planning to change the current scope of the draft.

The plan is to update the draft, and make the final submission to IANA as soon as possible. Currently, there seems to be one major change, i.e. adding a one-way hash function to AKAv2 password generation procedure. IANA will put the draft to Expert Review, and may also ask comments from SIPPING WG. Registration of new HTTP Digest AKA algorithm version number is expected within the next six months.

3. Re-use of AKAv2 passwords

Re-use of AKA authentication credentials with several applications may be problematic because of potential synchronization failure problem. In practice, AKA authentication challenges need to arrive to USIM at specific order [TS 33.102]. Otherwise, USIM will consider the challenge old, and it will generate a synchronization failure message.

There are several ways to overcome the problem, e.g. reserving different SQN spaces for different applications, trying to minimize the number of new interface towards HSS, or limiting the frequency of authentication.

Ericsson would like to draft SA3 attention to one specific feature of HTTP Digest AKAv2 that may partly be used for solving the problem. That is, HTTP Digest password generated with AKAv2 is not limited to one time use only. The length of the passwords is significantly longer and has more entropy in AKAv2 than what is included in HTTP Digest AKAv1.

[akav2] does not directly specify how the passwords are re-used in practice. However, according to HTTP authentication framework the passwords are not tied to the used algorithm, instead they are tied to the “username” and “realm” parameters. For this reason, SA3 could assume the following functionality from the UE:

- If the UE is challenged with HTTP Digest AKAv2, it should temporarily store the new password to be later used with the same “realm” and “username” later.

- If the UE is challenged with normal HTTP Digest challenge using some ordinary algorithm, such as MD5, the UE should start using the “username” and password generated with HTTP Digest AKA for the same “realm”.
- If the UE is re-challenged by HTTP Digest AKAv2, it will automatically generate a new password, and does not re-use the existing one.

It should also be noted that it would be very easy to define some 3GPP specific functionality for AKAv2 if needed. For example, AKAv2 could be used to assign the newly generated HTTP Digest passwords to a new “realm”. Using the similar principle, AKAv2 could be used to generate temporary end-user identity to the new “realm”.

4. Conclusions

This document reported the progress of HTTP Digest AKAv2 in IETF. The work has progressed well, and in the next step the authors will initiate the registration process in IANA. Ericsson is not aware of any reason why the work would not progress well in the future as well.

SA3 attention is also drawn to a feature of HTTP Digest AKAv2 of being able to re-use the passwords. This feature may help when the SQN synchronization failure problem is solved.

5. References

[akav2] Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2, IETF, draft-torvinen-http-digest-aka-v2-00.txt.

[TS 33.102] 3GPP, 3G Security; Security Architecture.

Network Working Group
Internet-Draft
Expires: December 15, 2003

V. Torvinen
J. Arkko
Ericsson
June 16, 2003

Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2

draft-torvinen-http-digest-aka-v2-00.txt

Status of this Memo

Copyright Notice

Abstract

HTTP Digest is known to be vulnerable to man-in-the-middle attacks, even when run inside TLS, if the same passwords are used for authentication in some other context without TLS. This is a general problem that affects not just HTTP digest but also other IETF protocols. However, for a class of strong algorithms the attack is avoidable. This document defines version 2 of the HTTP Digest AKA algorithm. Unlike previous versions of HTTP Digest such as MD5 or AKAv1, this algorithm is immune to the man-in-the-middle attack.

Table of Contents

1. Requirements notation 3
2. Introduction 4
2.1 Terminology 5
3. Digest password generation in AKAv2 7
4. Example Digest AKAv2 Operation 8
5. Security Considerations 9
5.1 Multiple Authentication Schemes and Algorithms 9
5.2 Session Protection 9
5.3 Man-in-the-middle attacks 9
5.4 Entropy 11
6. IANA Considerations 12
6.1 Registration Information 12
Normative References 13
Informative References 14
Authors' Addresses 14
Intellectual Property and Copyright Statements 15

1. Requirements notation

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 [RFC2119].

2. Introduction

The Hypertext Transfer Protocol (HTTP) Digest Authentication, described in [RFC2617], has been extended in [RFC3310] to support Authentication and Key Agreement (AKA) mechanism [AKA-REF]. AKA mechanism performs authentication and session key distribution in Universal Mobile Telecommunications System (UMTS) networks. HTTP Digest AKA enables the usage of AKA as a one-time password generation mechanism for Digest authentication.

HTTP Digest is known to be vulnerable to man-in-the-middle attacks, even when run inside TLS, if the same HTTP Digest authentication credentials are used in some other context without TLS. The attacker may initiate a TLS session with a server, and when the server challenges the attacker with HTTP Digest, the attacker masquerades the server to the victim. If the victim responds to the challenge, the attacker is able to use this response towards the server in HTTP Digest. Note that this attack is an instance of general attack that affects a number of IETF protocols such as PIC. The general problem is discussed in [Asokan-Niemi-Nyberg] and [Puthenkulam-binding-draft].

Because of the previous vulnerability, the use of HTTP Digest "AKAv1" should be limited to the situations where the client is able to demonstrate that in addition to AKA response, it possess the AKA session keys. This is possible, for example, if the underlying security protocol uses the AKA generated session keys to protect the authentication response. This is the case for example in the 3GPP IP Multimedia Core Network Subsystem (IMS) where HTTP Digest "AKAv1" is currently applied. However, HTTP Digest "AKAv1" should not be used with tunnelled security protocols that do not utilize the AKA session keys. For example, the use of HTTP Digest "AKAv1" is not necessarily secure with TLS if the server side is authenticated using certificates and the client side is authenticated using HTTP Digest AKA.

There are at least four potential solutions to the problem:

1. The use of the authentication credentials is limited to one application only. However, this would increase the total number of authentication credentials for an end-user, and would cause scalability problems in the server side.

2. The keys used in the underlying security protocols are somehow bind to the keys used in the tunneled authentication protocol. However, this would cause problems with the current implementations of underlying security protocols. For example, it is not possible to use the session keys from TLS at application

layer. Furthermore, this solution would only solve the problem when HTTP Digest is used over one hop, and leave the problem of using HTTP Digest via multiple hops, e.g. via proxy servers, unsolved.

3. Authentication credentials are used in cryptographically different way for each media and/or access network. However, it may be difficult to know which underlying media is used below the application.

4. Authentication credentials are used in cryptographically different way for each application.

This document specifies a new algorithm version for HTTP Digest AKA, i.e. "AKAv2". "AKAv2" specifies a cryptographically different way to use AKA credentials in applications that are based either on HTTP Digest authentication or UMTS authentication (cf. approach 4 above). The only difference to "AKAv1" is that in addition to AKA response RES the AKA related session keys, IK and CK, are also used as the password for HTTP Digest. AKAv2 is immune to man-in-the-middle attack described above. However, if AKAv2 is used in some environment both with and without some underlying security, such as TLS, the problem still exists.

New HTTP Digest AKA algorithm versions can be registered in IANA based on Expert Review. Documentation of new algorithm versions is not mandated as RFCs. However, "AKAv2" is documented as an RFC because the use of different AKA algorithm versions includes security implications that the implementators should be aware of. The extension version and security implications are presented in this document.

2.1 Terminology

This chapter explains the terminology used in this document.

AKA

Authentication and Key Agreement.

AKA is a challenge-response based mechanism that uses symmetric cryptography. AKA can be run in a UMTS IM Services Identity Module (ISIM) or in UMTS Subscriber Identity Module (USIM), which reside on a smart card like device that also provides tamper resistant storage of shared secrets.

CK

Cipher Key. An AKA session key for encryption.

IK

Integrity Key. An AKA session key for integrity check.

ISIM

IP Multimedia Services Identity Module. Sometimes ISIM is implemented using USIM.

RES

Authentication Response. Generated by the ISIM.

SIM

Subscriber Identity Module. GSM counter part for ISIM and USIM.

UMTS

Universal Mobile Telecommunications System.

USIM

UMTS Subscriber Identity Module. UMTS counter part for ISIM and SIM.

XRES

Expected Authentication Response. In a successful authentication this is equal to RES.

3. Digest password generation in AKAv2

In general, the Digest AKAv2 operation is identical to the Digest AKAv1 operation described in [RFC3310]. This chapter specifies the parts in which Digest AKAv2 is different from Digest AKAv1 operation. The notation used in the Augmented BNF definitions for the new and modified syntax elements in this section is as used in SIP [RFC3261], and any elements not defined in this section are as defined in [RFC3310].

In order to direct the client into using AKAv2 for authentication instead of other AKA versions or other HTTP Digest algorithms, the AKA version directive of [RFC3310] shall have the following new value:

```
aka-version        =  "AKAv2"
```

The AKA version directive is used as a part of the algorithm field as defined in [RFC3310].

```
Example:  algorithm=AKAv2-MD5
```

The client shall use the concatenated AKA parameters (RES||IK||CK) as a "password" when calculating the HTTP Digest response directive for AKAv2.

The server shall use the concatenated AKA parameters (XRES||IK||CK) as a "password" when checking the HTTP Digest response or when calculating the "response-auth" of the "Authentication-Info" header.

4. Example Digest AKAv2 Operation

This document does not introduce any changes to the operations of HTTP Digest or HTTP Digest AKA. Examples defined in [RFC3310] applies directly to AKAv2 with the following two exceptions:

1. The algorithm directive has a prefix "AKAv2" instead of "AKAv1".

2. The HTTP Digest password is derived from (RES||IK||CK) or (XRES||IK||CK) instead of (RES) or (XRES) respectively.

5. Security Considerations

5.1 Multiple Authentication Schemes and Algorithms

The rules for an user agent for choosing among multiple authentication schemes and algorithms are as defined in [RFC3310] except that the user agent MUST choose "AKAv2" if both "AKAv1" and "AKAv2" are present.

Since HTTP Digest is known to be vulnerable for bidding-down attack in environments where multiple authentication schemes and/or algorithms are used, the system implementators should pay special attention for scenarios where both "AKAv1" and "AKAv2" are used. Especially if the AKA generated sessions keys or some other additional security measures to authenticate the clients, such as client certificates, are not used, the use of both AKA algorithm versions should be avoided.

5.2 Session Protection

Even though "AKAv2" uses the additional integrity (IK) and confidentiality (CK) keys as a part of HTTP Digest AKA password, these session keys may still be used for creating additional security within HTTP authentication or some other security mechanism. This recommendation is based on the assumption that algorithms used in HTTP Digest, such as MD5, are sufficiently strong one-way functions, and consequently HTTP Digest responses leak no or very little computational information about IK and CK.

5.3 Man-in-the-middle attacks

[Asokan-Niemi-Nyberg] describe a "man-in-the-middle" attack related to tunnelled authentication protocols. [Asokan-Niemi-Nyberg] discuss the attack mostly in EAP context; however, it can exist in any similar contexts where tunnelled authentication is used and where the same authentication credentials are used without protection in some other context or the client fails to authenticate the server.

For example, the use of TLS with HTTP Digest authentication (i.e. TLS for server authentication, and subsequent use of HTTP Digest for client authentication) is an instance of such scenario. HTTP challenges and responses can be fetched from and to different TLS tunnels without noticing where they originally came from. Especially, the attack is easy to perform if the client fails to authenticate the server. If the same HTTP credentials are used with unsecured connection, the attack is also easy to perform.

This is how the "man-in-the-middle" attack works with HTTP Digest and

TLS if the victim (i.e. the client) fails to authenticate the server:

1. The victim contacts the attacker using TLS. If the attacker has a valid server certificate, the client may continue talking to the attacker and use some HTTP authentication compatible protocol, such as Session Initiation Protocol (SIP).

2. The attacker contacts some real proxy/server also using TLS and some HTTP authentication compatible protocol. The proxy/server responds to the attacker with HTTP Authentication challenge.

3. The attacker forwards the HTTP Authentication challenge from the proxy/server to the victim. If the victim is not careful, and check that the identity in the server certificate in TLS matches the realm in the HTTP authentication challenge, it may send a new request which carries a valid response to the HTTP Authentication challenge.

4. The attacker may use the response with the victims HTTP Digest username and password to authenticate itself to the proxy/server.

The man-in-the-middle attack is not possible if the client compares the identities in the TLS server certificate and the HTTP Digest authentication challenge. Note that with HTTP Basic, the client would send the password to the attacker.

Another variant of the "man-in-the-middle" attack is the so-called "interleaving attack". This attack is possible if the HTTP Digest authentication credentials are used in several contexts, and in one of them without protection.

This is how the attack could proceed:

1. The attacker establishes a TLS tunnel to the proxy/server using one-way server authentication. The attacker sends a request to the proxy/server.

2. The proxy/server challenges the attacker with HTTP Digest challenge.

3. The attacker challenges the victim in some other context using the challenge carried in the HTTP Digest challenge. The HTTP Digest challenge need to be modified to the format used in the protocol of this other context.

4. The victim responds with a response.

5. The attacker uses the response from the other context for

authentication in HTTP Digest.

6. The proxy/server accepts the response, and delivers the service to the attacker.

In some circumstances, HTTP Digest AKAv1 may be vulnerable for the interleaving attack. In particular, if ISIM is implemented using USIM the HTTP Digest AKAv1 should not be used with tunneled security protocols unless the AKA related session keys, IK and CK, are somehow used with the solution.

HTTP Digest AKAv2 is not vulnerable for interleaving attack.

5.4 Entropy

AKAv1 passwords should only be used as one-time passwords if the entropy of the used RES value is limited (e.g., only 32 bits). For this reason, the reuse of the same RES value in authenticating subsequent requests and responses is not recommended. Furthermore, 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 with AKAv1.

Passwords generated using AKAv2 can more securely be used for authenticating subsequent requests and responses because the concatenation of AKA credentials (i.e. RES||IK||CK) makes the passwords significantly longer. The user agent does not need to assume that AKAv2 passwords are limited to one-time use only, and it may try to re-use the AKAv2 passwords with the server. However, the length of the RES still matters because the attacker may try to use pre-calculated dictionaries to guess the (RES||IK||CK). The longer the RES is, the more difficult it is for the attacker to guess the (RES||IK||CK).

6. IANA Considerations

This document specifies a new aka-version, "AKAv2", to the aka-version namespace maintained by IANA. The allocation of new aka-versions is up to Expert Review as outlined in [RFC2434].

6.1 Registration Information

To: ietf-digest-aka@iana.org

Subject: Registration of a new AKA version

Version identifier: "AKAv2"

Contacts for further information: vesa.torvinen@ericsson.fi or jari.arkko@ericsson.com

Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A. and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC3261] 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.

[RFC3310] Niemi, A., Arkko, J. and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, September 2002.

Informative References

[AKA-REF] 3rd Generation Partnership Project, "Security Architecture (Release 4)", TS 33.102, December 2001.

[Asokan-Niemi-Nyberg] Asokan, N., Niemi, V. and K. Nyberg, "Man-in-the-Middle in Tunnelled Authentication Protocols", Cryptology ePrint Archive, http://eprint.iacr.org Report 2002/163, October 2002.

[Puthenkulam-binding-draft] Puthenkulam, J., Lortz, V., Palekar, A. and D. Simon, "The Compound Authentication Binding Problem", IETF, Work in progress draft-puthenkulam-eap-binding-02.txt, March 2003.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

Authors' Addresses

Vesa Torvinen
Ericsson
Joukahaisenkatu 1
Turku FIN 20520
Finland

Phone: +358 40 7230822
EMail: vesa.torvinen@ericsson.fi

Jari Arkko
Ericsson
Hirsalantie 1
Jorvas FIN 02420
Finland

Phone: +358 40 5079256
EMail: jari.arkko@ericsson.com

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

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