

Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 31, 2010

Y. Sheffer
Check Point
February 27, 2010

Using EAP-GTC for Simple User Authentication in IKEv2
draft-sheffer-ipsecme-ikev2-gtc-02.txt

Abstract

Despite many years of effort, simple username-password authentication is still prevalent. In many cases a password is the only credential available to the end user. IKEv2 uses EAP as a sub-protocol for user authentication. This provides a well-specified and extensible architecture. To this day EAP does not provide a simple password-based authentication method. The only existing password authentication methods either require the peer to know the password in advance (EAP-MD5), or are needlessly complex when used within IKEv2 (e.g. PEAP). This document codifies the common practice of using EAP-GTC for this type of authentication, with the goal of achieving maximum interoperability. The various security issues are extensively analyzed.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 31, 2010.

Copyright Notice

Internet-Draft

EAP-GTC in IKEv2

February 2010

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](http://trustee.ietf.org/license-info) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

| | | |
|-----------------------------|--|-------------------|
| 1. | Introduction | 3 |
| 2. | Terminology | 4 |
| 3. | Alternatives to EAP-GTC in IKEv2 | 4 |
| 3.1. | Non-password credentials | 4 |
| 3.2. | Using the IKE preshared secret | 4 |
| 3.3. | EAP-MD5 , EAP-MSCHAPv2 and mutual authentication schemes | 4 |
| 3.4. | Mutual "Zero Knowledge" Authentication | 5 |
| 4. | Using EAP-GTC in IKE: Details | 5 |
| 5. | IANA Considerations | 6 |
| 6. | Security Considerations | 6 |
| 6.1. | Key generation and MITM protection | 6 |
| 6.2. | Protection of credentials between the IKE gateway and the AAA server | 6 |
| 6.3. | Server authentication | 7 |
| 7. | Acknowledgments | 7 |
| 8. | References | 7 |
| 8.1. | Normative References | 7 |
| 8.2. | Informative References | 7 |
| Appendix A. | Change Log | 8 |
| A.1. | draft-sheffer-ipsecme-ikev2-gtc-02 | 8 |
| A.2. | draft-sheffer-ipsecme-ikev2-gtc-01 | 8 |
| A.3. | draft-sheffer-ipsecme-ikev2-gtc-00 | 8 |
| A.4. | draft-sheffer-ikev2-gtc-00 | 9 |
| | Author's Address | 9 |

1. Introduction

"Oh dear! It's possible that we have added EAP to IKE to support a case that EAP can't support." -- C. Kaufman.

Despite many years of effort, simple username-password authentication is still prevalent. In many cases a password is the only credential available to the end user.

IKEv2 [[RFC4306](#)] uses the Extensible Authentication Protocol (EAP) as a sub-protocol for user authentication. This provides a well-specified and extensible architecture and enables useful capabilities like SIM authentication. Unfortunately, for a number of reasons EAP still does not provide a simple password-based authentication method. The only existing password authentication methods either require the peer to know the password in advance (EAP-MD5), or are needlessly complex when used within IKEv2 (e.g. PEAP).

Technically, the IKE preshared secret authentication mode can be used for password authentication. In fact even the IKEv2 RFC winks at this practice. But this use jeopardizes the protocol's security and should clearly be avoided (more details below).

EAP is used in IKEv2 at a stage when the remote access gateway has already been authenticated. At this point the user has a high enough level of trust to send his or her password to the gateway. Such an exchange is enabled by the EAP Generic Token Card (GTC) method, which is a simple text transport between the two EAP peers. To quote [[RFC3748](#)]:

The EAP GTC method is intended for use with the Token Cards supporting challenge/response authentication and MUST NOT be used to provide support for cleartext passwords in the absence of a protected tunnel with server authentication.

IKEv2 does indeed provide "a protected tunnel with server

authentication". The current document updates [[RFC3748](#)] by making an exception and allowing the use of GTC to carry secret credentials, in this specific situation. [Section 6](#) further elaborates on the security properties of this solution.

Other protocols provide a similar protected tunnel, for example TLS-EAP, described in [[I-D.nir-tls-eap](#)]. These protocols however are out of scope for this document.

[2.](#) 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 [[RFC2119](#)].

[3.](#) Alternatives to EAP-GTC in IKEv2

This section presents a few of the alternatives to EAP-GTC, and explains why they are either insecure or impractical given today's common identity management infrastructure.

[3.1.](#) Non-password credentials

Certificate-based authentication, especially when combined with hardware protection (e.g. a hardware token), can be deployed in a more secure manner than the form of password authentication which we discuss. However, due to a host of issues to do with cost, inconvenience and reliability this solution has not gained wide market acceptance over the last 10 years.

[3.2.](#) Using the IKE preshared secret

Sec. 2.15 of [RFC 4306](#) points out that the generation of the IKE preshared secret from a weak password is insecure. Such use is vulnerable to off line password guessing by an active attacker. All the attacker needs to do is respond correctly to the first IKE_INIT message, and then record the third IKE message. This is then

followed by a dictionary attack to obtain the password.

[3.3.](#) EAP-MD5 , EAP-MSCHAPv2 and mutual authentication schemes

Challenge-response schemes, like EAP-MD5 and EAP-MSCHAPv2, have a clear security advantage over sending the plaintext password to the gateway. Password-based mutual authentication schemes like SRP have a further advantage in that the gateway's authentication is much stronger than when using certificates alone, since the AAA server proves its knowledge of a per-client credential, and the gateway proves that it has been authorized by the AAA server for that particular client.

Unfortunately all of these methods also suffer from a major drawback: the gateway must have a priori access to the plaintext password. While many RADIUS servers may indeed have such access, other very common deployments do not provide it. One typical example is when the gateway directly accesses an LDAP directory (or a Microsoft Active Directory) to authenticate the user. The usual way to do that

is by issuing an LDAP Bind operation into the directory, using the just-received plaintext password. Often in this case it is the IKE gateway that terminates the EAP protocol, and it needs a way to obtain the raw password.

An additional issue with mutual authentication schemes is their heavy IP encumbrance, which has resulted in a scarcity of standards using them and a low rate of market adoption.

[3.4.](#) Mutual "Zero Knowledge" Authentication

Some newer EAP methods provide for mutual, password-based authentication, without exposing the password to dictionary attacks by either an eavesdropper or the (alleged) peer. An example is [[I-D.sheffer-emu-eap-ike](#)]. Such EAP methods can be cleanly integrated into IKEv2 by using the extension described in [[I-D.ietf-ipsecme-eap-mutual](#)].

In addition, the IPsecME working group is now chartered with producing a similar authentication method directly over IKE, without the need for supporting the EAP protocol.

Neither of these options is widely implemented today, if at all. Either of them is superior to the method described in this document, and implementors are strongly encouraged to migrate to these methods as soon as they are standardized.

[4.](#) Using EAP-GTC in IKE: Details

EAP-GTC is specified in [[RFC3748](#)], Sec. 5.6. This section is non-normative, and is merely an interpretation of this specification in the context of IKEv2.

Simple authentication requires a non secret identity ("user name") and a secret credential ("password"). Both of these are arbitrary Unicode strings, although implementations may impose length constraints.

In the case of EAP-GTC, the user name is conveyed in the IKE IDi payload. According to [[RFC4718](#)], Sec. 3.4, the user name can be encoded in one of two ways: as a simple user name, in which case the ID_KEY_ID identification type is used; or as a combination user name plus realm, in which case the format is a NAI [[RFC4282](#)] and the identification type is ID_RFC822_ADDR. In either case, the user name is a Unicode string encoded as UTF-8. Using the EAP Identity payload is redundant, and if it is used, it should be identical to the IDi payload.

EAP-GTC consists of a simple 2-message exchange. The contents of the Type-Data field in the Request should not be interpreted in any way, and should be displayed to the user. This field contains a Unicode string, encoded as UTF-8.

The password is sent in the EAP Response. The Type-Data field of the Response is also a Unicode string encoded as UTF-8. Note that none of the IDi payload, the EAP Request or the EAP Response is null-terminated.

If either or both the user name and the password are non-ASCII, they should be normalized by the IKE client before the IKE/EAP message is constructed. The normalization method is SASLprep, [[RFC4013](#)].

[5.](#) IANA Considerations

This document does not require any action by IANA.

[6.](#) Security Considerations

[6.1.](#) Key generation and MITM protection

Modern EAP methods generate a key shared between the two protocol peers. GTC does not (and cannot) generate such a key. [RFC 4306](#) mandates that:

EAP methods that do not establish a shared key SHOULD NOT be used, as they are subject to a number of man-in-the-middle attacks [[EAPMITM](#)] if these EAP methods are used in other protocols that do not use a server-authenticated tunnel.

However GTC must never be used in such a situation, since the client would be sending its credentials openly to an unauthenticated server. When using GTC with IKEv2, the implementation (or local administrators) MUST ensure that the same credentials are never used in such a manner.

[6.2.](#) Protection of credentials between the IKE gateway and the AAA server

In the proposed solution, the raw credentials are sent from the IKE gateway to a AAA server, typically a RADIUS server. These credentials and the associated messaging MUST be strongly protected. Some of the existing options include:

- o An IPsec tunnel between the gateway and the AAA server.
 - o RADIUS over TCP with TLS, [[I-D.winter-radsec](#)].
 - o RADIUS over UDP with DTLS, [[I-D.dekok-radext-dtls](#)] (expired).
- The legacy RADIUS security mechanism (Sec. 5.2 of [[RFC2865](#)]) is considered weak and SHOULD NOT be used when better alternatives are available.

[6.3.](#) Server authentication

The client may only send its cleartext credentials after it has positively authenticated the server. This authentication is specified, albeit rather vaguely, in [RFC4306] and is out of scope of the current document. Unauthenticated (BTNS) derivatives of IKE MUST NOT be used with EAP-GTC.

7. Acknowledgments

I would like to thank Yoav Nir and Charlie Kaufman for their helpful comments.

8. References

8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.
- [RFC4013] Zeilenga, K., "SASLprep: Stringprep Profile for User Names and Passwords", [RFC 4013](#), February 2005.
- [RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", [RFC 4306](#), December 2005.

8.2. Informative References

- [EAPMITM] Asokan, N., Niemi, V., and K. Nyberg, "Man-in-the-Middle in Tunneled Authentication Protocols", November 2002, <<http://eprint.iacr.org/2002/163>>.
- [I-D.dekok-radext-dtls] DeKok, A., "DTLS as a Transport Layer for RADIUS", [draft-dekok-radext-dtls-01](#) (work in progress), June 2009.

Eronen, P., Tschofenig, H., and Y. Sheffer, "An Extension for EAP-Only Authentication in IKEv2", [draft-ietf-ipsecme-eap-mutual-00](#) (work in progress), February 2010.

[I-D.nir-tls-eap]

Nir, Y., Sheffer, Y., Tschofenig, H., and P. Gutmann, "TLS using EAP Authentication", [draft-nir-tls-eap-06](#) (work in progress), April 2009.

[I-D.sheffer-emu-eap-eke]

Sheffer, Y., Zorn, G., Tschofenig, H., and S. Fluhrer, "An EAP Authentication Method Based on the EKE Protocol", [draft-sheffer-emu-eap-eke-04](#) (work in progress), January 2010.

[I-D.winter-radsec]

Winter, S., McCauley, M., and S. Venaas, "RadSec Version 2 - A Secure and Reliable Transport for the RADIUS Protocol", [draft-winter-radsec-01](#) (work in progress), February 2008.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", [RFC 4282](#), December 2005.

[RFC4718] Eronen, P. and P. Hoffman, "IKEv2 Clarifications and Implementation Guidelines", [RFC 4718](#), October 2006.

[Appendix A](#). Change Log

[A.1](#). [draft-sheffer-ipsecme-ikev2-gtc-02](#)

Added a short discussion of newer password-based methods.

[A.2](#). [draft-sheffer-ipsecme-ikev2-gtc-01](#)

Republished.

[A.3](#). [draft-sheffer-ipsecme-ikev2-gtc-00](#)

Document renamed.

[A.4. draft-sheffer-ikev2-gtc-00](#)

Initial version.

Author's Address

Yaron Sheffer
Check Point Software Technologies Ltd.
5 Hasolelim St.
Tel Aviv 67897
Israel

Email: yaronf@checkpoint.com

