Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 21, 2011

D. Harkins
Aruba Networks

October 18, 2010

Password-Based Authentication in IKEv2: Selection Criteria and Considerations
draft-harkins-ipsecme-pake-criteria-01.txt

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/1id-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 April 21, 2011.

Abstract

The IPsecME working group has been re-chartered. One of the new charter items is to specify a new password-based authentication

method for IKEv2. This document describes some selection criteria and selection considerations for the WG to use.

Table of Contents

1. Introduction

The new IPsecME WG charter defines a new work item on password-based authentication for IKEv2. It says, in part:

> The WG will develop a standards-track extension to IKEv2 to allow mutual authentication based on "weak" (low-entropy) shared secrets. The goal is to avoid off-line dictionary attacks without requiring the use of certificates or EAP. There are many already-developed algorithms that can be used, and the WG would need to pick one that both is believed to be secure and is believed to have acceptable intellectual property features. The WG would also need to develop the protocol to use the chosen algorithm in IKEv2 in a secure fashion. It is noted up front that this work item poses a higher chance of failing to be completed than other WG work items; this is balanced by the very high expected value of the extension if it is standardized and deployed.

As noted, there are many algorithms that can satisfy this work item and the WG needs to pick one. This memo describes a set of selection critera to consider when making the choice and suggests some techniques to use to prevent the process from degenerating. It is an informational memo for the edification of the WG only. It does not presume to be the only way for the WG to arrive at decision.

This Internet-Draft is not intended to be advanced. It exists solely for easy reference of the criteria on which the WG should base its selection decision. Once that decision has been made this Internet-Draft should quietly expire.

2. Terminology

This document is entirely non-normative.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document hold no special significance, certainly not those described in [RFC2119].

3. Selection Considerations

IKEv2 provides a very high level of security, has no or a very negligible cost for licensing, and has a protocol structure that is well-understood. Therefore a new mode to support authentication with a possibly low-entropy password/passphrase must be added with great care, so as to not unduely affect any of these features.

Candidate protocols must be evaluated against each of these: security of the candidate, intellectual property considerations that would require licensing of any kind, and how well the candidate fits into the existing protocol structure of IKEv2.

3.1. Security

Because the charter work item deals with authentication using a low-entropy shared secret any candidate protocol has to address the security issues of the existing pre-shared key mode in IKE today when using a low-entropy secret, and must not introduce any new avenues of attack.

SEC1: The protocol must be based on a zero-knowledge proof. It must be resistant to passive attack, active attack, and off-line dictionary attack. The only information leaked about the secret from a single run of the protocol is a single bit: whether the single guess was correct or not. Another way to put this is that the advantage an attacker gets is based on interation and not computation.

SEC2: The protocol supports perfect forward secrecy and protection against the Denning-Sacco attack.

SEC3: The protocol does not require the loss of identity protection afforded by IKEv2 today.

SEC4: The protocol does not constrain the "crypto agility" of IKEv2. It must not require fixed and unchangable cryptographic primitives or Diffie-Hellman groups.

SEC5: The protocol should have received review by the cryptographic community, and the more review the better. The protocol should be proven secure under a commonly understood cryptographic model.

SEC6: The protocol should support the ability to parlay the low-entropy secret into a cryptographic-strength credential (such as a strong symmetric key or a certificate and private key) such that the low-entropy secret need only be used once, or very rarely.

SEC7: The protocol should be able to store, and use, a transform of a password to provide resistance to exposure of the password in case of compromise.

SEC8: The protocol is secure regardless of the tranforms negotiated by IKEv2. The security properties of the exchange must not change depending on the negotiated transforms.

3.2. Intellectual Property

Password-authenticated key exchange is an interesting and difficult problem. When a solution is found, there is a natural desire to protect the intellectual property unique to the solution and apply

for a patent. The issue of intellectual property rights (IPR) is a large consideration for a solution to this work item due to the potential added cost to implementation due to licensing issues.

[RFC3669] provides some case studies on how IPR has been handled in other IETF WGs and has a good section on using IPR as a technology evaluation factor. It can be a useful guide to IPR discussions in IPsecME in deciding which protocol to use to satisfy the charter work item.

Patent holders have a financial interest in licensing their technology. This results in claims and counter-claims on whether a particular piece of IPR applies or does not apply to a particular protocol. Many of these claims are subjective. Given that the claimant has an obvious motivation for opining a certain way (either "yes it does apply" or "no it does not apply") the opinion can be suspect. Discussions can easily reach the point of being pointless back-and-forth exchanges because these claimants are not providing legal advice on what is, fundamentally, a legal question.

There are a few things to keep in mind when considering the IPR implications of adopting a particular candidate protocol:

- Every protocol, even protocols that are already patented, may infringe on other patents that are known or unknown.
- Licensing of a patent does not provide protection against incidential infringment of another patent.
- The claims of a patent are what define the IPR. Descriptive text or problem statements that are part of a patent but not part of a claim do not describe IPR, but may be used to interpret the claims.
- Whether a protocol does or does not infringe on a particular patent can only be determined by a court, not by cryptographers, patent holders, lawyers, or other so-called "experts".
- Nothing can prevent you from receiving a threatening letter from a patent holder accusing you of infringing on a some patent.
- Patents are time-limited.
- Information made public before a given date (so called "prior art") may be useful in invalidating claims of a patent.

A WG reaching some consensus on whether a technology infringes on a particular patent, or whether some patent is invalid, is inappropriate. The decision must be arrived at individually by each WG member, although each decision will influence support for selecting a particular protocol and collectively an impression can be made. Unfortunately, that individual decision may involve resolution of competing and fuzzy claims and counter-claims. As [RFC3669] mentions, each WG member should use all legal resources (including

legal counsel) to arrive at a decision whether a particular protocol infringes or does not infringe on a particular patent. The opinion of "experts" may be interesting and potentially insightful but is not the type of opinion required to make a decision.

It is important to avoid pointless "yes it does"/"no it doesn't" exchanges when evaluating IPR and candidate protocols. This can be done by framing the disussion. This framing takes two parts.

First by stating uncontentous facts about the known IPR status of a candidate protocol. These are suggested to be:

IPR1: A public description of the protocol was made on <date>. This allows one to determine when applicable patents may expire or to determine whether some public information could be considered "prior art".
IPR2: A patent or patent application on the protocol has been made. Or, conversely, no patent or patent application on the protocol has been made as of this time. If the protocol is patented this allows one to find out when it will expire.
IPR3: An IPR disclosure on this protocol, or a particular instantiation of this protocol, has been made to the IETF. Or, conversely, no IPR disclosure on this protocol was made because, for instance, it is believed to be free of IPR. This is useful in determining a baseline for licensing costs.

Second, by focusing the discussion of known IPR to address the questions that really matter:

1. does the claim cover the protocol in question?
2. is the claim valid?

Such discussions are focused and useful if they point out which claim from which patent a protocol seems to infringe and, importantly, why. Each such statement can become a separate issue around which an informative discussion can be had.

Some kinds of statements should be discouraged. For example:

- Statements which assume one must prove a negative ("show that this protocol is patent-free") should be discouraged because such a thing is very difficult, if not impossible, to prove.
- Broad accusations that a protocol infringes on IPR without listing the specific claims from a patent on which it supposedly infringes should be discouraged because they can tend to be inflammatory, and more importantly, because they do not specifically address the important questions.

- o Opinions masquerading as facts ("that claim will never stand up in court") should be discouraged or restated ("that claim will be very difficult to uphold").

3.3. Protocol Co-Existance

IKE is a request/response protocol with role enforcement (there is an "initiator" and a "responder"). It negotiates a slew of parameters that govern how it will complete. It provides mutual authentication and derivation of a secret known only to the authenticated peers. It can trade off the strength of the derived key for computation and time costs. It creates and manages security associations that define how to communicate between peers. These are all well understood and well-analyzed features of IKE. Addition of new modes of authentication must be done harmoniously, keeping in mind the existing structure and nature of IKE.

Co-existance considerations must be taken into account when discussing candidate protocols. These include:

MISC1: How many additional round trips does the protocol add to the existing exchange?

MISC2: How much additional computation (e.g. exponentiation) must be performed for each exchange because of the protocol?

MISC3: Does performance differ depending on whether the secret is a large, random octet string or a character string?

MISC4: Can internationalization of character-based passwords be supported?

MISC5: Can the protocol use the same finite cyclic groups (MODP, EC2N, ECP) used in IKEv2 or does it require a new IANA registry or additions of special groups to the existing IANA registry?

MISC6: Does the protocol fit into the request/response nature of IKE or are additional messages required to "sync" the two peers back up?

MISC7: What additional negotiation, if any, is required to use this protocol?

MISC8: Does the the protocol require a trusted third party or clock synchronization to successfully complete?

MISC9: Does the protocol require the use of certain cryptographic primitives-- hash functions, ciphers, finite cyclic groups-- or is it "crypto-agile"?

MISC10: Does the protocol support the use of elliptic curve cryptography or only finite field cryptography?

MISC11: Can the protocol be easily implemented?

4. IANA Considerations

This document does not require any action by IANA.

5. Security Considerations

This document does not define any new protocol, and has no inherent security considerations. It does discuss criteria for the selection of a security protocol, chief among them being security.

6. Acknowledgments

The author would like to thank Yaron Sheffer and Paul Hoffman for the email exchanges the caused this document to be written. It was motivated by Yaron's draft of a similar name.

7. Informative References

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

[RFC3669] Brim, S., "Guidelines for Working Groups on Intellectual Property Issues", RFC 3669, February 2004.

Author's Address

Dan Harkins
Aruba Networks
1322 Crossman Avenue
Sunnyvale, CA 94089-1113
United States of America

Email: dharkins@arubanetworks.com