

IPSecME Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 31, 2014

Y. Nir
Check Point
April 29, 2014

Protecting Internet Key Exchange (IKE) Implementations from Denial of
Service Attacks through Client Puzzles
draft-nir-ipsecme-puzzles-00

Abstract

This document describes an enhancement to the Stateless Cookie mechanism described in [RFC 5996](#). Whereas the original mechanism prevents denial-of-service (DoS) attacks that use multiple spoofed source addresses, the mechanism here is effective against a distributed denial of service attack (DDoS), where the attackers use their own source address. This is accomplished by requiring proof of work by the Initiator before allocating resources at the Responder.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on October 31, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) 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

Internet-Draft

Client Puzzles for IKE

April 2014

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 Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Conventions Used in This Document	3
2.	Protocol Overview	3
3.	Puzzle Notification Format	4
4.	Operational Considerations	5
5.	Security Considerations	6
6.	IANA Considerations	6
7.	Normative References	6
	Author's Address	6

1. Introduction

The Initial Exchange described in [section 1.2 of \[RFC5996\]](#) involves the Initiator sending a single message. The Responder also sends a single message, but also allocates state for a structure called a half-open IKE SA (Security Association). This half-open SA is later authenticated in the Authentication Exchange, but if that exchange doesn't come, the half-open SA is kept for an unspecified amount of time.

This creates an easy attack vector against an Internet Key Exchange (IKE) Responder. Generating the Initial request is cheap, and sending multiple such requests can either cause the Responder to allocate too much resources and fail, or else if resource allocation is limited, legitimate Initiators would also be prevented from setting up IKE SAs.

An obvious defense is limiting the number of half-open SAs opened by a single peer. However, since all that is required is a single packet, an attacker can use multiple spoofed source IP addresses.

[Section 2.6 of RFC 5996](#) offers a mechanism to mitigate this DoS attack: the stateless cookie. When the server is under load, the Responder responds to the Initial request with a calculated "stateless cookie" - a value that can be re-calculated based on values in the Initial request without storing Responder-side state. The Initiator is expected to repeat the Initial request, this time including the stateless cookie.

This mechanism is not effective against attackers that have multiple source IP addresses with return routability, such as bot-nets.

The mechanism described here adds a proof of work for the Initiator, by partially breaking a hash function. This sets an upper bound, determined by the attacker's CPU to the number of negotiations it can force the Responder to participate in.

1.1. Conventions Used in This Document

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. Protocol Overview

As described in [section 2.6 of RFC 5996](#), when a responder detects a large number of half-open IKE SAs, it SHOULD reply to IKE_SA_INIT

Nir

Expires October 31, 2014

[Page 3]

Internet-Draft

Client Puzzles for IKE

April 2014

requests with a response containing the COOKIE notification. When the number of half-open SAs gets even higher, so that there is a danger of degraded ability to reply to legitimate initiations, the responder SHOULD switch to sending puzzles instead of cookies. The puzzle is described in [Section 3](#). The answer to the puzzle is the value to be returned in the Cookie notification.

The Initiator solves the puzzle, figures out what the stateless cookie is, and re-initiates as described in [RFC 5996](#) with the Cookie notification carrying the answer to the puzzle.

3. Puzzle Notification Format

This section details the notification format for the puzzle. This notification is sent from Responder to the Initiator. See [Section 4](#) for Operational Considerations in enabling this feature.

[illegible]

The entire exchange is below:

Initiator	Responder
HDR(A,0), SAI1, KEi, Ni -->	
	<-- HDR(A,0), N(PUZZLE)
HDR(A,0), N(COOKIE), SAI1, KEi, Ni -->	
	<-- HDR(A,B), SAr1, KEr, Nr, [CERTREQ]
HDR(A,B), SK {IDi, [CERT, [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr} -->	
	<-- HDR(A,B), SK {IDr, [CERT, AUTH, SAr2, TSi, TSr}

4. Operational Considerations

[This section needs a lot of expanding]

Not all Initiators support this extension, but all initiators are supposed to support stateless cookies. If this notification is sent to a non-supporting but legitimate initiator, the exchange will fail. Responders are advised to first try to mitigate the DoS using

Nir

Expires October 31, 2014

[Page 5]

Internet-Draft

Client Puzzles for IKE

April 2014

stateless cookies, and only if the number of half-open SAs keeps increasing, switch to using this mechanism.

The difficulty level should be set by balancing the requirement to minimize the latency for legitimate initiators and making things difficult for attackers. A good rule of thumb is for taking about 1 second to solve the puzzle. A typical initiator or bot-net member in 2014 can perform slightly less than a million hashes per second per core, so setting the difficulty level to $n=20$ is a good compromise. It should be noted that mobile initiators, especially phones are considerably weaker than that. Implementations should allow administrators to set the difficulty level, and/or be able to set the difficulty level dynamically in response to load.

Initiators should set a maximum difficulty level beyond which they

won't try to solve the puzzle and log or display a failure message to the administrator or user.

5. Security Considerations

To be added.

6. IANA Considerations

IANA is requested to assign a notify message type from the status types range (16430-40959) of the "IKEv2 Notify Message Types - Status Types" registry with name "PUZZLE".

7. Normative References

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

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", [RFC 5996](#), September 2010.

Nir

Expires October 31, 2014

[Page 6]

Internet-Draft

Client Puzzles for IKE

April 2014

Author's Address

Yoav Nir
Check Point Software Technologies Ltd.
5 Hasolelim st.
Tel Aviv 6789735
Israel

Email: ynir.ietf@gmail.com