Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 5, 2011

Z. Cao
China Mobile
D. Liu
H. Deng
China Mobile
July 4, 2010

EAP Authentication Identity Protection
draft-zcao-emu-id-protection-00

Abstract

The EAP framework does not provide an effective way to protect the peer's identity. This creates the risk of identity forgery. This document revisits the EAP identity protection problem, and proposes a solution to this problem via the use of Cryptographically Binding Identity (CBID).

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 January 5, 2011.

Table of Contents

1. Introduction

In the EAP framework [RFC3748], the EAP peer will respond with its authentication identity in the EAP-Response/Identity message. Based on the configuration with respect to the peer's identity, the EAP Authentication Server will determine which EAP method to start with this peer. But this creates potential security threats towards the EAP identity. For example, suppose user A with identity ID-A is configured to be authenticated with EAP-MD5 which is considered to be a week authentication method, then an attacker M can 'steal' A's identity by responding the EAP-Request/Identity message with IDA, so that the server will authenticate M using EAP-MD5. In this way, attackers obtain an easier way to be authenticated to the system and then can harm the system in multiple ways.

Currently there are no direct solutions to conduct EAP identity protection. One way introduced in RFC3748 is to neglect the EAP identity exchange and let the server start with the same EAP method for every user, and only after a secure tunnel is established can the peer informs its identity to the server. Another common method to avoid identity stolen is to use the anonymous identity, e.g., the users within the same domain use the same ''anon@example.org'' to initiate the EAP authentication. However, this anonymous identity does not prevent the malicious to conduct the identity attack.

This document introduces an EAP identity protection mechanism. Instead of using a na飗e identity such as ''bob'' or ''bob@example.org'', the EAP peer should generate a Cryptography-Binding Identity (CBID) by hashing its public key so that the used EAP identity is bind to the user's public key. The peer will include this crypto-binding ID in the EAP-Response/Identity and sign the message with its private key. In this way, an attacker has no way to forge a valid public key that maps to the CBID and a valid signature representing this public key. By using the CBID, EAP authentication can be kept immune to the EAP identity threat.

2. 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].

3. Proposed Solutions

We introduce our solution in this section.

3.1. Crypto-binding Identity Generation

Suppose the EAP peer has its own RSA public and private key pair (PK, SK), it will generate its crypto-binding identity (CBID) as:

CBID = HASH (PK||OPTIONAL-CONTENT) (1)

Where the HASH algorithm is an one-way function so that it is computational infeasible to do reverse derivation, and the OPTIONAL-CONTENT is reserved to avoid public key collision, e.g. we can use the domain name ''@example.org'' to serve as the OPTIONAL-CONTENT.

We used the SHA-1 algorithm in this document so that the CBID is 160 bit long.

After the CBID is generated, the user will include this identity in the EAP-Response/Identity message, and the server will configure an EAP method with this identity.

3.2. EAP Authentication using Crypto-Binding ID

In this section, we will show how the proposed solution can prevent attackers to forge other peers' identity by using CBID.

When an EAP peer A receives the EAP-Request/Identity, it will respond with its crypto-binding identity CBID-A and a random number Ra together with a signature on the whole message using its private key SK-A and the RSA signature algorithm. The detailed message format will be shown in Section.3.3.

The identity exchange procedure is depicted in Figure 1. The EAP Peer, Authenticator and EAP Server definitions are align with RFC 3748.

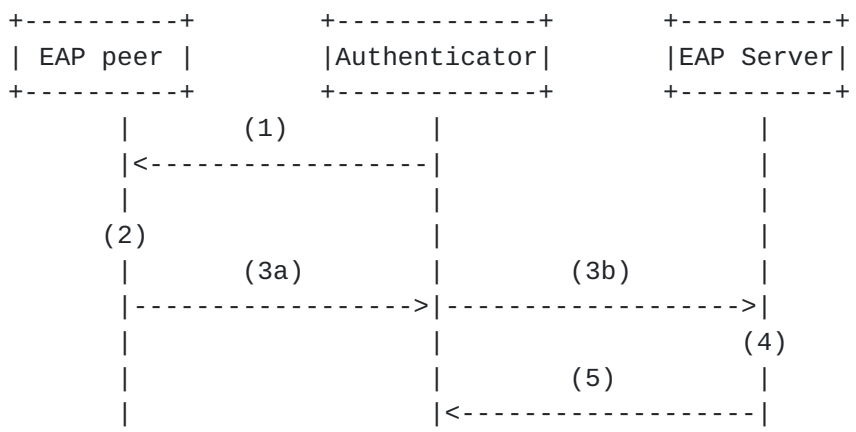

Figure 1: Identity Exchange using CBID

(1) The authenticator sends the EAP-Request/Identity to the peer;

(2) The EAP peer includes its CBID and generates a random number Ra, and then uses the RSA signature algorithm to generate a signature Sig. The peer first prepares a concatenation including the EAP Code, Identifier, Length, Type, CBID and Random number, i.e. Code|| Identifier||Length||Type||CBID||Random. The peer then generates the RSA signature by using the RSASSA-PKCS1-v1_5 [RFC3447] signature algorithm with the SHA-1 hash algorithm. The private key (SK) and the concatenation created above are the inputs to the generation operation.

(3) The EAP peer sends the concatenated EAP-Response/Identity message with to the EAP authenticator, the logic format of this message is as: EAP-Response/ID (CBID||Ra||PK||Sig). The authenticator encapsulates this EAP-Response into the AAA message and forwards it to the EAP authentication server. The authenticator should not check the validity of either the CBID or the RSA Signature.

(4) The EAP authentication server will check the validity of the identity message. First, it checks if the equation CBID=HASH(PK) holds true, if not, the server won't continue. Second, it checks if the signature is valid by taking the public key PK as the verification key. Only if the signature is valid will the server start the EAP authentication method in (5);

(5) The EAP authentication server consults its local configuration and starts authenticating the peer using the corresponding EAP method.

With the above procedure, attackers cannot intrude the EAP framework even if they can eavesdrop the transmitted EAP identity message. First, due to the property of one way hash function, attackers are

not able to find another public key which maps to the same CBID. Secondly, attackers cannot simply replay another user's identity because they do not have access to the corresponding private key to generate the valid signature.

3.3. Extended EAP-Response/Identity Message Format

Figure 2 depicts the extended EAP-Response/Identity message format.

o Code. Code=2, this is an EAP Response message;

o Identifier. The Identifier field is one octet, as specified in RFC3748;

o Length. The Length field is two octets. The length of the whole EAP Response message, in bytes, including the Code (1 byte), Identifier(1 byte), and Length (2 byte), and the Type and Type data(variable length);

o Type. One octet. This message contains peer identity information, so the type value is 1.

o CBID: 160 bits, as generated in Equation(1);

o Random: 24 bits, generated by the peer, the peer should use random generator with good enough randomness;

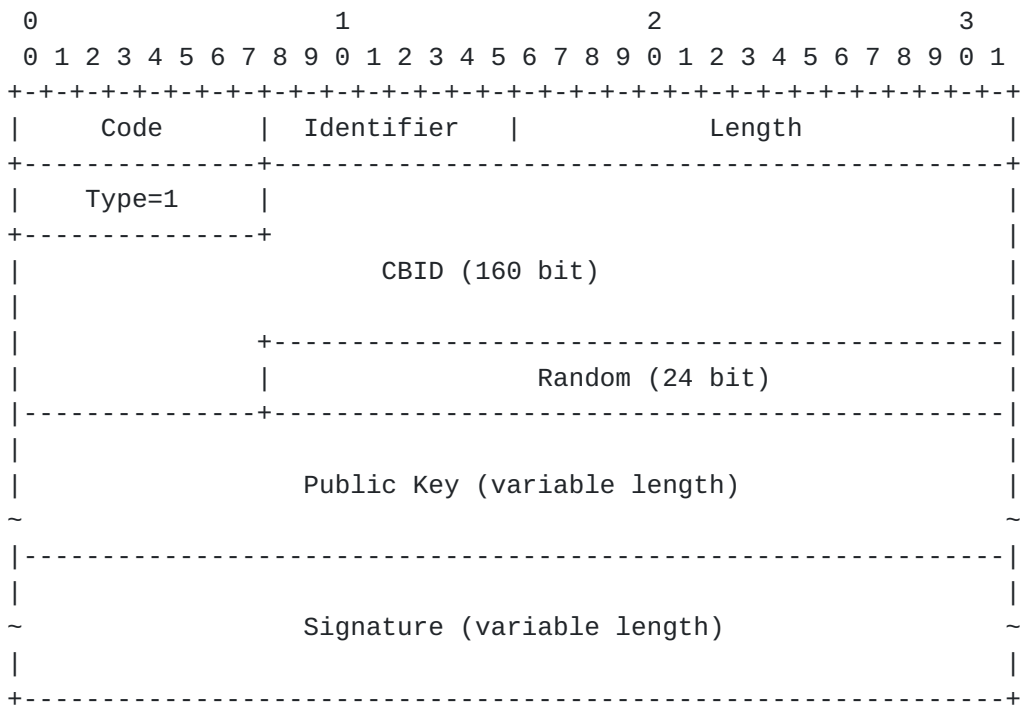

Figure 2: Extended EAP-Response/ID Message Format

Public key: This is a variable-length field containing the public key of the address owner. The public key MUST be formatted as a DER-encoded ASN.1 structure of the type SubjectPublicKeyInfo, defined in the Internet X.509 certificate profile [RFC 3280]. RSA signature algorithm is used, so the algorithm identifier MUST be rsaEncryption, which is 1.2.840.113549.1.1.1, and the RSA public key MUST be formatted by using the RSAPublicKey type as specified in Section 2.3.1 of RFC3279 [RFC 3279]. The RSA key length SHOULD be at least 384 bits. The length of this field is determined by the ASN.1 encoding.

o Signature: the RSA signature by using the RSASSA-PKCS1-v1_5 [RFC 3447] signature algorithm with the SHA-1 hash algorithm.

4. Security Considerations

TBD

5. IANA Considerations

None

6. Acknowledgments

TBD

7. 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.

Authors' Addresses

Zhen Cao
China Mobile
Unit2, 28 Xuanwumenxi Ave,Xuanwu District
Beijing 100053
China

Email: zehn.cao@gmail.com

Dapeng Liu
China Mobile
Unit2, 28 Xuanwumenxi Ave,Xuanwu District
Beijing 100053
China

Email: liudapeng@chinamobile.com

Hui Deng
China Mobile
Unit2, 28 Xuanwumenxi Ave,Xuanwu District
Beijing 100053
China

Email: denghui@chinamobile.com