PPPEXT Working Group B. Aboba
INTERNET-DRAFT Microsoft
Category: Standards Track
<draft-aboba-pppext-eap-iana-02.txt>
12 October 2002
Updates: RFC 2284

EAP IANA Considerations

Abstract

This document describes the IANA considerations for Extensible Authentication Protocol (EAP).

This document updates RFC 2284.

1. Introduction

This document provides guidance to the Internet Assigned Numbers Authority (IANA) regarding registration of values related to the Extensible Authentication Protocol (EAP),defined in [RFC2284], in accordance with BCP 26, [RFC2434].

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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].

1.2. Terminology

The following terms are used here with the meanings defined in BCP 26: "name space", "assigned value", "registration".

The following policies are used here with the meanings defined in BCP 26: "Private Use", "First Come First Served", "Expert Review", "Specification Required", "IETF Consensus", "Standards Action".

2. IANA Considerations

There are two name spaces in EAP that require registration: Packet Codes and Method Types.

EAP is not intended as a general-purpose protocol, and allocations SHOULD NOT be made for purposes unrelated to authentication.

2.1. Recommended Registration Policies

For registration requests where a Designated Expert should be consulted, the responsible IESG area director should appoint the Designated Expert. For Designated Expert with Specification Required, the request is posted to the EAP WG mailing list (or, if it has been disbanded, a successor designated by the Area Director) for comment and review, and MUST include a pointer to a public specification. Before a period of 30 days has passed, the Designated Expert will either approve or deny the registration request and publish a notice of the decision to the EAP WG mailing list or its sucessor. In making the decision, the Designated Expert will take into account the security guidelines described in Section 4. A denial notice must be justified by an explanation and, in the cases where it is possible, concrete suggestions on how the request can be modified so as to become acceptable.

Packet Codes have a range from 1 to 255, of which 1-4 have been allocated. Because a new Packet Code has considerable impact on interoperability, a new Packet Code requires Standards Action, and should be allocated starting at 5.

The original EAP Method Type space has a range from 1 to 255, and is the scarcest resource in EAP, and thus must be allocated with care. Method Types 1-36 have been allocated, with 20 available for re-use. Method Types 37-191 may be allocated following Designated Expert, with Specification Required. Release of blocks of Method Types (more than 1 at a time for a given purpose) should require IETF Consensus. EAP Type Values 192-254 are reserved and allocation requires Standards Action.

Method Type 255 is allocated for Vendor-Specific extensions as described in Section 3, and the use of that should be encouraged instead of allocation from the original global Method Type space, for functions specific only to one vendor's implementation of EAP, where no interoperability is deemed useful.

When used with a Vendor-Id of zero, Method Type 255 can also be used to provide for an expanded Method Type space. Expanded Method Type values 256-4294967295 may be allocated after Type values 1-191 have been allocated, using Designated Expert with Specification Required.

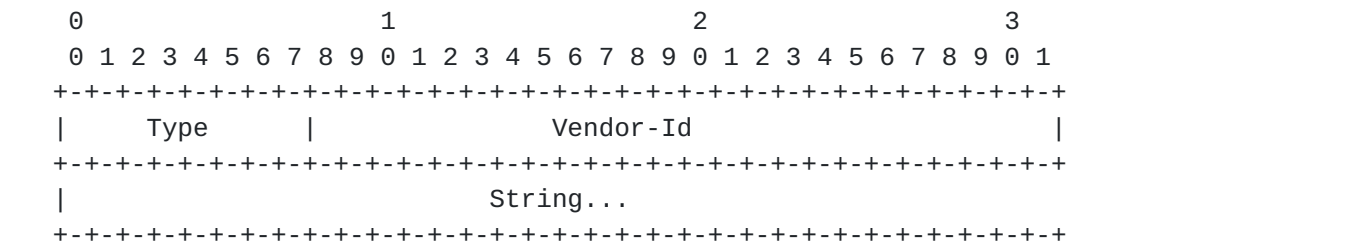
3. Vendor-specific

Description

Due to EAP's popularity, the original Method Type space, which only provides for 255 values, is being allocated at a pace, which if continued, would result in exhaustion within a few years. Since many of the existing uses of EAP are vendor-specific, the Vendor-Specific Method Type is available to allow vendors to support their own extended Types not suitable for general usage. The Vendor-specific Type may also be used to expand the global Method Type space beyond the original 255 values.

Peers not equipped to interpret the Vendor-specific Type, or who support the Vendor-Specific Type, but find the proposed Vendor-Id to be unacceptable, MUST send a Nak, and negotiate a more suitable authentication method.

A summary of the Vendor-specific Type format is shown below. The fields are transmitted from left to right.



Type

255 for Vendor-specific

Vendor-Id

The Vendor-Id is 3 octets and represents the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as allocated by IANA. A Vendor-Id of zero is reserved for use by the IETF in providing an expanded global EAP Type space.

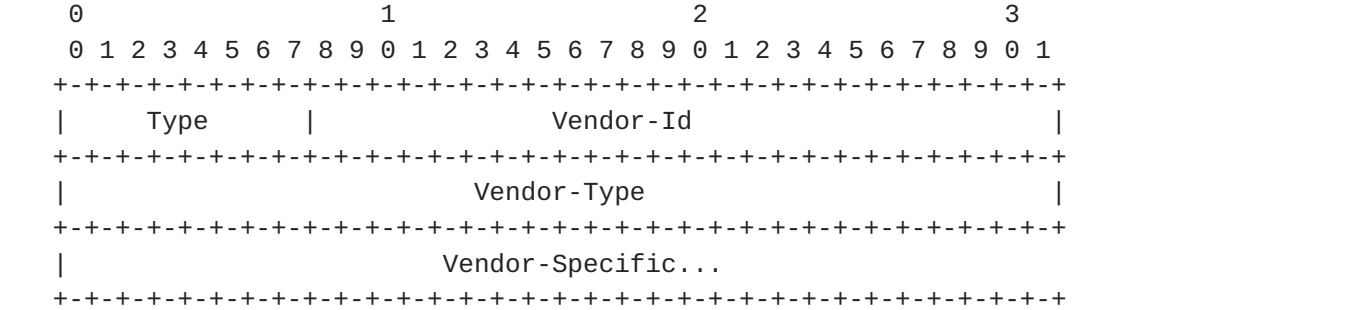
String

The String field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

It SHOULD be encoded as follows. The Vendor-Specific field is dependent on the vendor's definition of that attribute. An example encoding of the Vendor-Specific attribute using this method follows.

Example Implementation



Vendor-Type

The Vendor-Type field is four octets and represents the vendor-specific Method Type. Where a Vendor-Id of zero is present, the Vendor-Type field provides an expanded global EAP Type space, beginning with EAP Type values of 256.

Vendor-Specific

The Vendor-Specific field is dependent on the vendor's definition of that attribute. Where a Vendor-Id of zero is present, the Vendor-Specific field will be used for transporting the contents of EAP Methods of Types 256 or greater.

4. Security Considerations

EAP was designed for use with dialup PPP [RFC1661] and wired [IEEE802] networks such as Ethernet [IEEE8023]. On these networks, an attacker would need to gain physical access to the telephone or switch infrastructure in order to mount an attack. While such attacks have been documented, such as in [DECEPTION], they are assumed to be rare.

However, subsequently EAP has been proposed for use on wireless networks, and over the Internet, where physical security cannot be assumed. On such networks, the security vulnerabilities are greater, as are the requirements for EAP security.

This section documents the threats that exist on physically insecure networks carrying EAP, as well as laying out the security analysis required of an EAP method requesting a Type allocation.

4.1. Threat model

On physically insecure networks, it is possible for an attacker to gain access to the physical medium. This enables a range of attacks, including the following:

[1] An adversary may try to discover user identities by snooping data packets.

[2] An adversary may try to modify or spoof EAP packets.

[3] An adversary may launch denial of service attacks by terminating EAP conversations.

[4] An adversary might attempt to recover the passphrase by mounting an offline dictionary attack.

[5] An adversary may attempt to convince the Peer to connect to an untrusted network.

[6] An adversary may attempt to disrupt the EAP negotiation in order to weaken the authentication, gain access to user passwords or remove confidentiality protection.

[7] An adversary may attempt to mount a denial of service attack by modify

[8] An attacker may attempt to take advantage of weak key derivation techniques used within EAP methods.

[9] An attacker may attempt to take advantage of weak ciphersuites subsequently used after the EAP conversation is complete.

Where EAP is used over wireless networks, an attacker needs to be within the coverage area of the wireless medium in order to carry out these attacks. However, where EAP is used over the Internet, no such restrictions apply.

4.2. Security requirements

In order to address the threats that exist where EAP is used on a physically insecure medium, the following requirements are imposed:

[1] Mutual authentication. Mutual authentication of the communication endpoints MUST be provided in order to protect against rogue Authenticators.

[2] Protected conversation. On a physically insecure network, EAP messages SHOULD be integrity and replay protected, authenticated and confidential so as to protect against downgrade attacks, snooping of identities, and spoofing of packets. This includes protection of packets of types Identity, Nak and Notification, as well as packets sent within the EAP method itself, and success and failure indications. Where EAP is used for ciphersuite or capabilities negotiation, these messages SHOULD be integrity and replay protected, authenticated and confidential.

[3] Key derivation. EAP methods used on physically insecure networks MAY derive keys in order to enable per-packet authentication, integrity and replay protection as well as confidentiality. Where EAP methods derive keys, the distributed keys SHOULD be master session keys, used only for further key derivation, independent of the ciphersuite. This eliminates the need for an EAP method to understand how to derive keys for every ciphersuite. Rather than inventing new key derivation techniques, well analyzed algorithms

SHOULD be used.

[4] Dictionary attack resistance. Where EAP is used on physically insecure networks resistance against dictionary attack SHOULD be provided. Where password authentication is used, users are notoriously prone to selection of poor passwords. Without dictionary attack protection, it is easy for an attacker snooping authentication traffic to gather a large number of authentication exchanges, and successfully obtain a substantial fraction of the passwords used in those exchanges via a dictionary attack. Given the steadily declining prices of computing power, successful dictionary attacks can now be mounted at minimal expense.

[5] Support for fast reconnect. On physically insecure media such as wireless, it is often desirable to improve scalability and minimize connectivity interruptions due to authentication. Where this is desired, EAP methods MAY support "fast reconnect". After an initial authentication conversation, this enables subsequent authentication conversations to take place in shortened form.

[6] Acknowledged success and failure indications. Where EAP is used over an unreliable medium, it is possible for packets to be lost. This can result in the Peer and Authenticator having a different interpretation of the state of the authentication conversation. As a result, where EAP is used over an unreliable medium, EAP methods SHOULD support acknowledged success and failure indications.

Since proposed EAP methods may be used on physically insecure methods, it is necessary to be able to evaluate methods against the above requirements in order to determine their suitability. In order to be suitable for allocation of a Type code, EAP method specifications MUST include the following:

[a] Statement of intended use. This includes a statement of whether the method is intended for use over a physically secure or insecure network, as well as a statement of the applicable media.

[b] Indication of security claims. This includes a statement of the claimed security properties of the method. In particular, the specification MUST include a vulnerability analysis and an indication of whether the method claims to satisfy the requirements for use on physically insecure media.

[c] Description of key hierarchy. EAP methods deriving keys MUST describe how keys for authentication/integrity, encryption and IVs are to be derived from the provided keying material, or a reference to other documents providing such a description.

[d] Indication of vulnerabilities. If the method is intended for use on a physically insecure network, yet does not satisfy the above requirements, the specification MUST indicate which requirements are not satisfied, and discuss the security implications.

5. Normative references

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

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

[RFC2284] Blunk, L., Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

Acknowledgments

Thanks to Glen Zorn of Cisco, and Ashwin Palekar of Microsoft for discussions relating to this document.

Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

EMail: bernarda@microsoft.com
Phone: +1 425 706 6605
Fax: +1 425 936 7329

Intellectual Property Statement

Full Copyright Statement

Expiration Date

This memo is filed as <draft-aboba-pppext-eap-iana-02.txt>, and expires April 19, 2003.