INTERNET-DRAFT
<draft-storey-smtp-client-id-00.txt>
Intended Status: Standards Track
Expires February 17, 2016
August 17, 2015

W. Storey
LinuxMagic

SMTP Service Extension for Client Identity
<draft-storey-smtp-client-id-00.txt>

Abstract

This document defines an extension for the Simple Mail Transfer Protocol (SMTP) called "CID" to provide a method for clients to indicate an identity to the server.

This identity is an additional token that may be used for security and/or informational purposes, and with it a server may optionally apply heuristics using this token.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The [SMTP] protocol and its extensions describe methods whereby an SMTP client may provide identity information to an SMTP server. This document defines an additional such method to provide an identity.

Each existing identity mechanism available is subject to limitations, and none offer a way to identify the SMTP client with absolute confidence.

Typically SMTP clients are identified through the establishment of an authorized identity using the [AUTH] SMTP extension. SMTP servers are often subject to malicious clients attempting to use authorized identities not intended for their use (often referred to as a brute-force attack). If such an attack is successful, then the SMTP server may not be able to identify the impersonation and be unable to restrict such a client. While there are ways to identify the source of the SMTP client such as its IP address or EHLO identity, it would be useful if there was an additional way to uniquely identify the client in a manner presented solely across an encrypted channel.

Using the CID extension, an SMTP client can provide a new identity to the server called its "client identity". The client identity can provide unique characteristics about the client accessing the SMTP service and may be combined with existing identification mechanisms

in order to identify the client. An SMTP server may then apply additional security policies using this identity such as restricting use of the service to clients presenting recognized client identities, or only allowing use of authorized identities that match previously established client identities.

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 [KEYWORDS].

2. The CID Service Extension

The following SMTP service extension is hereby defined:

(1) The name of this [SMTP] service extension is "Client Identity".

(2) The EHLO keyword value associated with this extension is "CID".

(3) The CID keyword has no parameters.

(4) A new [SMTP] verb "CID" is defined.

(5) No parameter is added to any SMTP command.

(6) This extension is appropriate for the submission protocol [SUBMIT].

3. The CID Keyword of the EHLO Command

An SMTP server includes the CID keyword in its EHLO response to tell the SMTP client that the CID service extension is supported.

The CID keyword has no parameters.

The SMTP server MUST include the CID keyword in its initial EHLO response to indicate it supports the CID service extension. The server MUST also include the CID keyword in any subsequent EHLO responses such as a EHLO issued after a successful [STARTTLS] negotiation.

4. The CID Command

CID client-id-type client-id-identity

Arguments:

client-id-type: A string identifying the identity type the client is providing. It MUST be between 1 and 16 alphanumeric characters.

client-id-identity: A string identifying the client. It MUST be between 1 and 128 printable characters.

Restrictions:

The CID command MUST only be issued after a successful EHLO command.

A client MUST NOT issue CID commands containing a client-id-type that was successfully completed in the same session. After a successful CID command completes, a server MUST reject any further CID commands containing the same client-id-type parameter with a 503 reply.

A client MUST NOT issue a CID command unless a TLS session has been negotiated as described in [STARTTLS] or through other means such as over a historical SMTP-SSL connection.

A server MUST reject with a 503 reply any CID command sent prior to establishing a TLS session.

A server MUST reject with a 501 reply any CID command that is not well formatted.

Discussion:

Several SMTP service extensions such as [AUTH] require that an SMTP session be reset to an initial state under conditions such as after applying a security layer. Previously presented client identity information MUST be discarded after such a reset. The SMTP client SHOULD present the client identity to the server again if it wishes to preserve this information for the purposes of logging or security.

An SMTP server MAY choose to require that a client identity be presented, or that a client identity of a particular type be presented. In such a configuration the server MAY choose to reject certain commands or sequences of commands issued by a client with a 503 reply.

A server MAY reject with a 504 reply any CID command that contains a type the server does not support or recognize. However, the server may accept and discard any client identity without issuing a rejection even if it does not recognize the

type. The presented information may be useful for analysis.

A server MAY reject with a 550 reply any CID command that contains a type or identity that the server chooses not to accept for any reason, such as by policy.

A server MAY reject with a 550 reply any CID command that contains a type or identity that the server has chosen to disable or revoke use of either temporarily or permanently.

5. Formal Syntax

The following syntax specification uses the Augmented Backus-Naur Form notation as specified in [ABNF]. Non-terminals referenced but not defined below are as defined by [ABNF].

Except as noted otherwise, all alphabetic characters are case-insensitive.

```
client-id-type-char = ALPHA / DIGIT
                    ;; alphanumeric

client-id-type      = 1*16 client-id-type-char

client-id-identity  = 1*128 VCHAR
                    ;; any printable US-ASCII character
```

6. Discussion

6.1 Utility

The utility of the client identity may be seen by considering the following:

(1) An SMTP client may be present on a device that does not have a useful domain name or network address, such as a mobile device, so its EHLO identity may be ambiguous;

(2) An SMTP client may utilize the same SMTP server with multiple different authorized identities, so an identity that persists across authorized identities is lacking;

(3) An authorized identity may make use of multiple discrete devices over different SMTP sessions, so an identity persisting on one device is lacking;

(4) The SMTP DATA payload does not need to be inspected for this identity;

(5) Connection information, a type of identity, such as network address frequently changes.

6.2 Use Cases

With the client identity the SMTP server has additional information it may use in its interactions with the client. It may:

(1) Restrict use of an authorized identity to a set of client identities, thereby offering an added level of security. For example use of an authorized identity may only be permitted from a single device using the client identity as a form of whitelisting;

(2) Identify that the same client identity is used to access multiple authorized identities, and restrict access to the SMTP service. For example a client that has successfully gained access to many authorized identities may be identified through its use of a shared client identity;

(3) Retain knowledge of client identities previously presented with an authorized identity, and if an identity not previously seen is used, restrict access to the SMTP service;

(4) Require that the SMTP client present a token such as a license key established outside of the SMTP session in order to make use of any authorized identity;

(5) Apply different security policies to clients that provide a client identity versus those which do not. For example, provide clients providing such an identity with additional trust.

6.3. Other SMTP Identities

The [SMTP] protocol and its extensions describe methods whereby an SMTP client may provide identity information to an SMTP server. Some of these identities are listed for contrast:

(1) The client connection source provides an IP address associated with the SMTP session;

(2) The EHLO command allows a client to identify itself with a domain or address for an SMTP session;

(3) The [AUTH] SMTP extension allows the client to establish an authorized identity for an SMTP session;

(4) The MAIL command identifies a specific sender for a mail transaction.

7. Client Identity Types

This document does not specify any identity type that MUST be supported. The MAC and LICENSE types SHOULD be supported, but a server MAY not take any actions using the information.

It is envisioned that in the future it will be useful to propose identity types to support.

(1) MAC

An SMTP client may find it useful to identify the device using which it is establishing the session. This may be done by providing a MAC address. This provides knowledge that persists between different networks and locations yet is stable to a physical client device;

(2) LICENSE

An SMTP client may find it useful to identify the license key of software it is using. Such licenses are typically crafted such that they are unique and useful to identify a software installation.

8. Examples

8.1 MAC Address as Client Identity

```
C: [connection established]
S: 220 server.example.com ESMTP ready
C: EHLO client.example.net
S: 250-server.example.com
S: 250-STARTTLS
S: 250 CID
C: STARTTLS
S: 220 Go ahead
C: <starts TLS negotiation>
C & S: <negotiate a TLS session>
C & S: <check result of negotiation>
C: EHLO client.example.net
S: 250-server.example.com
S: 250 CID
C: CID MAC 08:9e:01:70:f6:46
S: 250 OK
C: MAIL FROM:<sender@example.net>
```

```
   S: 250 OK
   C: RCPT TO:<receiver@example.com>
   S: 250 OK
   C: DATA
   S: 354 Ready for message content
   C: <body>
   C: .
   S: 250 OK
   C: QUIT
   S: 221 server.example.com Service closing transmission channel
```

8.2 Client Identity Without a TLS Session

```
   C: [connection established over a plaintext connection]
   S: 220 server.example.com ESMTP ready
   C: EHLO client.example.net
   S: 250-server.example.com
   S: 250-STARTTLS
   S: 250 CID
   C: CID MAC 08:9e:01:70:f6:46
   S: 503 Bad sequence of commands
   C: MAIL FROM:<sender@example.net>
   S: 250 OK
   C: QUIT
   S: 221 server.example.com Service closing transmission channel
```

The server rejects use of the CID command as no TLS session was yet established.

8.3 Client Identity Leading to Rejection

```
   C: [connection established over a plaintext connection]
   S: 220 server.example.com ESMTP ready
   C: EHLO client.example.net
   S: 250-server.example.com
   S: 250-STARTTLS
   S: 250-AUTH PLAIN
   S: 250 CID
   C: STARTTLS
   S: 220 Go ahead
   C: <starts TLS negotiation>
   C & S: <negotiate a TLS session>
   C & S: <check result of negotiation>
   C: EHLO client.example.net
   S: 250-server.example.com
   S: 250-AUTH PLAIN
   S: 250 CID
   C: AUTH PLAIN dGVzdAB0ZXN0ADEyMzQ=
```

```
   S: 235 2.7.0 Authentication successful
   C: EHLO client.example.net
   S: 250-server.example.com
   S: 250-AUTH PLAIN
   S: 250 CID
   C: CID MAC 08:9e:01:70:f6:46
   S: 550 Server policy does not permit your use of this mail system
   C: QUIT
   S: 221 server.example.com Service closing transmission channel
```

The server rejects use of the mail system after the server decides that the provided client identity and authorized identity do not establish sufficient privileges.

8.4 Malformed CID Command

```
   C: [connection established over a plaintext connection]
   S: 220 server.example.com ESMTP ready
   C: EHLO client.example.net
   S: 250-server.example.com
   S: 250-STARTTLS
   S: 250-AUTH PLAIN
   S: 250 CID
   C: STARTTLS
   S: 220 Go ahead
   C: <starts TLS negotiation>
   C & S: <negotiate a TLS session>
   C & S: <check result of negotiation>
   C: EHLO client.example.net
   S: 250-server.example.com
   S: 250-AUTH PLAIN
   S: 250 CID
   C: AUTH PLAIN dGVzdAB0ZXN0ADEyMzQ=
   S: 235 2.7.0 Authentication successful
   C: EHLO client.example.net
   S: 250-server.example.com
   S: 250-AUTH PLAIN
   S: 250 CID
   C: CID MAC
   S: 501 Syntax error in parameters or arguments
   C: QUIT
   S: 221 server.example.com Service closing transmission channel
```

The server rejects the CID command as it is not well formed as there is only a single parameter provided.

9. Security Considerations

As this extension provides an additional means of communicating information from a client to a server it is clear there is additional information divulged to the server. This may have privacy considerations depending on the client identity type or its contents. For example, it may reveal a MAC address of the device used to communicate with a server that would not previously have been revealed. It is the responsibility of the client to decide whether the benefits outweigh the potential security impacts.

As well, while this service extension requires that the identity information only be transmitted over an encrypted channel to reduce the risk of eavesdropping, it does not specify any policies or practices required in the establishment of such a channel, and so it is the responsibility of the client and the server to determine that the communication medium meets their requirements.

10. IANA Considerations

10.1 SMTP Extension Registration

Section 2.2.2 of [SMTP] sets out the procedure for registering a new SMTP extension.

This extension will need to be registered.

11. References

11.1. Normative References

[ABNF] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[AUTH] Siemborski, R., Ed., and A. Melnikov, Ed., "SMTP Service Extension for Authentication", RFC 4954, DOI 10.17487/RFC4954, July 2007, <http://www.rfc-editor.org/info/rfc4954>.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[SMTP] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

[STARTTLS] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, DOI 10.17487/RFC3207, February 2002, <http://www.rfc-editor.org/info/rfc3207>.

[SUBMIT] Gellens, R. and J. Klensin, "Message Submission for Mail", STD 72, RFC 6409, DOI 10.17487/RFC6409, November 2011, <http://www.rfc-editor.org/info/rfc6409>.

Contributors

Michael Peddemors
LinuxMagic

Authors' Addresses

William Storey
LinuxMagic
#405 - 860 Homer St.
Vancouver, British Columbia
CA V6B 2W5

EMail: william@linuxmagic.com