Internet-Draft
Intended status: Standards Track
Expires: September 18, 2018

D. Bider
Bitvise Limited

March 18, 2018

Extended authentication information in Secure Shell (SSH)
draft-ssh-ext-auth-info-01.txt

Abstract

This memo defines a way for SSH server applications to send additional information to clients as part of authentication failure. A mechanism to relay such information can reduce the need for end user support in situations where a client would successfully authenticate, but cannot log in for a policy reason, such as password age or public key size.

Status

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), 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/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright

1. Overview and Rationale

Secure Shell (SSH) is a common protocol for secure communication on the Internet. In [RFC4252], SSH defines a standard failure message, SSH_MSG_USERAUTH_FAILURE, for use with "password", "publickey", and other authentication methods.

The SSH_MSG_USERAUTH_FAILURE message was designed under the assumption that the server never needs to inform the client about exact reasons behind an authentication failure. In practice, there are situations where revealing such information is beneficial, and is not a risk. In these situations, not revealing the cause of failure deprives client software and end users of information needed to appropriately respond.

This memo describes a mechanism which leverages [SSH-EXT-INFO] for client software to signal that it is willing to receive extra information as part of the SSH_MSG_USERAUTH_FAILURE message. A format for the additional information is described, as well as definitions for a number of common status codes.

1.1. Requirements Terminology

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. Indicating Support

Extended information cannot be sent to clients that do not indicate support: widely used clients disconnect on unexpected data. Therefore, SSH clients and servers that support this extension SHALL implement [SSH-EXT-INFO]. When sending SSH_MSG_EXT_INFO to a server that signals support for that message, a client MAY include this extension:

```
string extension-name  = "ext-auth-info"
string extension-value = (empty)
```

The client MUST send an empty extension value. A server that does not expect an extension value MUST ignore it, regardless of the value. Future specifications MAY define new meanings for this value.

3. Extended Format of SSH_MSG_USERAUTH_FAILURE

When sending SSH_MSG_USERAUTH_FAILURE to a client that signals support for this mechanism as per Section 2, the server MAY send the message in original format, as specified in [RFC4252]:

```
byte          SSH_MSG_USERAUTH_FAILURE
name-list     authentications that can continue
boolean       partial success
```

If the server decides additional information is safe to send, the server MAY extend the format of SSH_MSG_USERAUTH_FAILURE as follows:

```
byte          SSH_MSG_USERAUTH_FAILURE
name-list     authentications that can continue
boolean       partial success
uint32        N = number of ext-auth-info pairs
the following two fields repeated N times:
    string    ext-auth-info pair name
    string    ext-auth-info pair value (binary)
```

An ext-auth-info pair name follows the format of an algorithm or method name as specified in [RFC4251], Section 6.

The remainder of this section describes initially defined ext-auth-info pairs.

3.1. "keyboard-interactive" Submethods

The name and value for this ext-auth-info pair are encoded as follows:

```
string    name  = "kbdi-submethods"
name-list value = available submethods for "keyboard-interactive"
```

Note that a name-list is a special case of a string. The value of this ext-auth-info pair is therefore a name-list, not a string containing an encoded name-list.

A server MAY send this ext-auth-info pair regardless of whether the authentication method "keyboard-interactive" is included in the field "authentications that can continue" in SSH_MSG_USERAUTH_FAILURE.

A client MAY use information in this ext-auth-info pair to indicate a submethod preference during "keyboard-interactive" authentication, or to make a choice between "keyboard-interactive" and other available authentication methods.

3.2. Authentication Status

The name and value for this ext-auth-info pair are encoded as follows:

```
string name  = "auth-status"
string value = binary encoding of the following 3 or more fields:
    string    authentication status name
    string    message (in UTF-8 encoding without BOM)
    string    language tag (as per [RFC5646])
    <optional status-specific data>
```

If the server sends this ext-auth-info pair, it MUST send all three fields that are part of value (and perhaps optional status-specific data). It is not permissible to send e.g. only the authentication status name, but no message or language tag.

After the language tag, clients MUST tolerate optional data. If a client does not understand the optional data, it MUST ignore it.

An authentication status name follows the format of an algorithm or method name as specified in [RFC4251], Section 6.

3.2.1. Authentication Status Names

The following authentication status names are defined:

"internal-error"
: MAY be sent in response to any authentication request. The request could not be processed due to an internal server error. It is appropriate to contact the server administrator.

"transient-conflict"
: MAY be sent in response to any authentication request. The request could not be processed due to a transient server-side conflict. The issue may be resolved if the request is tried again, or the connection is re-attempted.

"account-disabled"
: MAY be sent in response to any authentication request. Credentials were valid, but the account is disabled.

"account-restriction"
: MAY be sent in response to any authentication request. Credentials were valid, but the account is restricted in a non-absolute manner (e.g. logon hours) that prevents login.

"pk-size-restriction"
: MAY be sent in response to public key authentication. The public key sent by the client is known to the server, but does not meet the

server's key size criteria.

"pk-alg-restriction"
MAY be sent in response to public key authentication. The public key sent by the client is known to the server, but the key or signature uses an algorithm not supported or accepted by the server.

"password-expired"
MAY be sent in response to password authentication. The password was correct, but is expired and must change, AND cannot be changed in the current session. If the password can be changed, the server SHOULD instead send SSH_MSG_USERAUTH_PASSWORD_CHANGEREQ.

"password-must-change"
MAY be sent in response to password authentication. The password was correct, is not expired, but must change, AND cannot be changed in the current session. If the password can be changed, the server SHOULD instead send SSH_MSG_USERAUTH_PASSWORD_CHANGEREQ.

"password-cannot-change"
MAY be sent in response to a password change request. Password change cannot be performed regardless of the new password requested.

"gss-no-mechanism"
MAY be sent in response to a GSSAPI authentication request that enumerates no supported mechanisms.

"gss-identity"
MAY be sent in response to a GSSAPI authentication request when the server cannot verify that the GSSAPI identity is the same as that named in the SSH authentication request.

3.2.2. Authentication conditions WITHOUT status names

Authentication status names are intentionally NOT defined for the following conditions:

- Password change request: Password ill-formed
- Password change request: Password does not meet policy requirements

In these cases, the server SHOULD instead send (potentially another) SSH_MSG_USERAUTH_PASSWORD_CHANGEREQ with an appropriate message.

4. IANA Considerations

4.1. Additions to existing tables

IANA is requested to insert the following entries into the table Extension Names (added in [SSH-EXT-INFO]) under Secure Shell (SSH) Protocol Parameters [RFC4250]:

Extension Name	Reference	Note
ext-auth-info	[this document]	Section 2

4.2. New table: Extended Authentication Information Pair Names

Under Secure Shell (SSH) Protocol Parameters, IANA is requested to create a new table, Extended Authentication Information Pair Names, with initial content:

Pair Name	Reference	Note
kbdi-submethods	[this document]	Section 3.1
auth-status	[this document]	Section 3.2

4.3. New table: Authentication Status Names

Under Secure Shell (SSH) Protocol Parameters, IANA is requested to create a new table, Authentication Status Names, with initial content:

Extension Name	Reference	Note
internal-error	[this document]	Section 3.2.1
transient-error	[this document]	Section 3.2.1
account-disabled	[this document]	Section 3.2.1
account-restriction	[this document]	Section 3.2.1
pk-size-restriction	[this document]	Section 3.2.1
pk-alg-restriction	[this document]	Section 3.2.1
password-expired	[this document]	Section 3.2.1
password-must-change	[this document]	Section 3.2.1
password-cannot-change	[this document]	Section 3.2.1
gss-no-mechanism	[this document]	Section 3.2.1
gss-identity	[this document]	Section 3.2.1

5. Security Considerations

Servers MUST NOT send extended authentication information if this would reveal sensitive information to an untrusted client.

For example, the status "account-disabled" is meant to be sent to a user who would successfully authenticate, and the only reason they cannot log in is because their account is disabled. Extended information with this status SHOULD NOT be sent to a user who is trying to log into a disabled account with an incorrect password.

6. References

6.1. Normative References

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

[RFC4251] Ylonen, T. and Lonvick, C., Ed., "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

[RFC4252] Ylonen, T. and Lonvick, C., Ed., "The Secure Shell (SSH) Authentication Protocol", RFC 4252, January 2006.

[RFC5646] Phillips, A., Ed. and Davis, M., Ed., "Tags for Identifying Languages", RFC 5646, September 2009.

[SSH-EXT-INFO] Bider, D., "Extension Negotiation in Secure Shell (SSH)", draft-ietf-curdle-ssh-ext-info-15.txt, September 2017, <https://tools.ietf.org/html/draft-ietf-curdle-ssh-ext-info-15>.

6.2. Informative References

[RFC4250] Lehtinen, S. and Lonvick, C., Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, January 2006.

Author's Address

Denis Bider
Bitvise Limited
4105 Lombardy Ct
Colleyville, TX 76034
United States of America

Phone: +1 817 313 8515
EMail: ietf-ssh3@denisbider.com
URI: https://www.bitvise.com/