Network Working Group
Internet-Draft
Expires February 8, 2004

S. Suehring
Sentry Insurance
J. Salowey
Cisco Systems

August 8, 2003

SCP/SFTP/SSH URI Format
draft-ietf-secsh-scp-sftp-ssh-uri-00.txt

Status of this Memo

This Internet Draft will expire on February 8, 2004.

Copyright Notice

Abstract

This document describes the Uniform Resource Identifiers used to locate resources for the SCP, SFTP, and SSH protocols. The document describes the generic syntax involved in URI definitions as well as specific definitions for each protocol. These specific definitions may include user credentials such as username and password and also may include other parameters such as fingerprint. In addition, security considerations and examples are also provided within this document.

General Syntax

The URI for each protocol shall consist of the scheme and the scheme specific portion separated by a colon ":", as discussed in RFC 2396 [1]. This specification shall adopt the definitions "port", "host", "scheme", "userinfo", and "authority" from RFC 2396.

SSH URI

The SSH scheme shall consist of the protocol acronym followed by a colon ":" and a double slash "//" in accordance with RFC 2718 [2].

The first component of the scheme specific portion MAY include credentials (userinfo) consisting of a username and optionally also including a password. Including the password in the URL is NOT RECOMMENDED. The username and password components are separated by a single colon ":".

Following the userinfo, if present, the at-sign "@" shall precede the authority section of the URI. Optionally, the authority section MAY also include the port preceded by a colon ":". If the port is not included, port 22 is assumed. Following the port additional parameters may be specified. These parameters are defined in the connection parameters section.

```
ssh_URI = "ssh://" [ userinfo "@" ] host [ ":" port ]
   [;conn-parameter=value]
```

SCP and SFTP URI

For SCP and SFTP, the scheme portion (scp: or sftp:) is followed by a double slash "//".

Both SCP and SFTP URLs are terminated by a single slash "/" followed by the path information to the requested resource.

The first component of the scheme specific portion MAY include credentials (userinfo) consisting of a username and optionally also including a password. Including the password in the URL is NOT RECOMMENDED. The username and password components are separated by a single colon ":".

Following the userinfo, if present, the at-sign "@" shall precede the authority section of the URL. Optionally, the authority section MAY also include the port preceded by a colon ":". If the port is not included, port 22 is assumed. Following the port additional parameters may be specified. These parameters are defined in the connection parameters section.

```
scp_URI = "scp://" [ userinfo "@" ] host [ ":" port ]
   [ ; parameter = value ] [ abs_path ]
```

Following the port additional parameters may be specified. These parameters are defined in the connection parameters section. Following the path additional sftp specific parameters may be specified.

```
   sftp_URI = "sftp://" [ userinfo "@" ] host [ ":" port ]
      [;conn-parameter=value] [ abs_path ] [;sftp-parameter=value]
```

Parameters

SSH connection parameters

The following parameters are associated with an SSH connection and are applicable to SSH, SFTP and SCP. All parameters are optional and MUST NOT overwrite configured defaults. Individual parameters are separated by a comma (",").

fingerprint

The fingerprint parameter contains the fingerprint of the host key for the host specified in the URL. The fingerprint is encoded as in [3]. This parameter MUST NOT overwrite a key that is already configured for the host. They fingerprint MAY be used to validate the authenticity of the host key if the URL was obtained from an authenticated source with its integrity protected. If this parameter is not included then the validity of the host key is validated using another method. See Security Considerations section for additional considerations. There MUST be only one fingerprint parameter for a given URL.

cipher

The cipher parameter indicates an acceptable encryption mechanism to use in making the connection. The value is the string specifying the SSH cipher type. This parameter MUST NOT add a mechanism to a configured list of default configured acceptable encryption types. If this parameter is not specified then the default configured cipher list is used. There may be more than one cipher parameter.

integrity

The integrity parameter indicates an acceptable data integrity mechanism to use in making the connection. The value is the string specifying the SSH data integrity type. This parameter MUST NOT add a mechanism to a configured list of default configured acceptable data integrity types. If this parameter is not specified then the default configured data integrity list is used. There may be more than one integrity parameter.

key-xchg

The key-xchg parameter indicates an acceptable key exchange mechanism to use when making the connection. The value is the string specifying the SSH key exchange type. This parameter MUST NOT add a mechanism to a configured list of default configured acceptable key exchange types. If this parameter is not specified then the default configured key exchange list is used. There may be more than one key-xchg parameter.

host-key-alg

The host-key-alg parameter indicates an host key to use when making the connection. The value is the string specifying the SSH host key type. This parameter MUST NOT add a mechanism to a configured list of default configured acceptable host key types. If this parameter is not specified then the default configured host key type list is used. There may be more than one host-key-alg parameter.

user-auth

The user-auth parameter indicates a user authentication mechanism to use when making the connection. The value is the string specifying the SSH user authentication mechanism type. This parameter MUST NOT add a mechanism to a configured list of default configured acceptable user authentication mechanism types. If this parameter is not specified then the default configured user authentication mechanism type list is used. There may be more than one user-auth parameter.

SFTP Parameters

The SFTP parameters determine how to handle the file transfer character translation.

newline

The newline parameter determines how the server translates new line indicators. The possible choices are usually "\r" or "\n" or "\r\n". The default is "\r\n".

typecode

The typecode identifies the type of file which determines how it will be treated. Possible values are "i" for binary files, "a" for text files, and "d" for directory listings.

Examples

The following section shows basic examples of URLs for each protocol. This section should not be considered to include all possible combinations of URLs for each protocol.

```
ssh://user@host

ssh://user@host:2222

ssh://joeuser@example.com;fingerprint=c1:b1:30:29:d7:b8:de:6c
    :97:77:10:d7:46:41:63:87,cipher=aes-cbc
```

```
      scp://user:password@host/file.txt

      sftp://user@host/dir/path/file.txt
      sftp://joeuser@example.com:2222;fingerprint=c1:b1:30:29:d7:b8
          :de:6c:97:77:10:d7:46:41:63:87,cipher=
          aes-cbc/pub/docs/test.txt;typecode=a
```

Security Considerations

In general, URIs themselves have no security considerations. However, since the password for each scheme can optionally be included within the URL it should be noted that doing so poses a security risk. Since URLs are usually sent in the clear with no encryption or other security, any password or other credentials (userinfo) included could be seen by a potential attacker.

The fingerprint should only be used to validate the host key only if the URL can be determined to be authentic from a trusted entity. For example, the URL may be received through secure email or HTTPS from a trusted and verifiable source. It is possible that the SSH implementation may not be able to determine if the URL is authentic in which case it SHOULD prompt the user to either allow or disallow the connection based on the information provided. The SSH implementation MUST NOT overwrite a currently configured public key based on the URL alone.

The other connection parameters MUST NOT add any mechanism to the list of configured acceptable mechanisms defined in the SSH client.

Normative References

[1] Berners-Lee, T., Fielding, R., Masinter, L., "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[2] Masinter, L., et. al., "Guidelines for new URL Schemes", RFC 2718, November 1999.

[3] Markus Friedl, "SSH Fingerprint Format",
http://www.ietf.org/internet-drafts/
  draft-ietf-secsh-fingerprint-01.txt,
work in progress

Non-Normative References

Mealling, M., Denenberg, R., "Report from the Joint W3C/IETF URI Planning Interest Group: Uniform Resource Identifiers (URIs), URLs, and Uniform Resource Names (URNs): Clarifications and Recommendations", RFC 3305, August 2002.

Author Information

Steve Suehring
Sentry Insurance
1800 North Point Dr, G2/61-17
Stevens Point, WI 54481
suehring@braingia.com

Joseph Salowey
Cisco Systems
2901 Third Avenue
Seattle, WA 98121
E-mail: jsalowey@cisco.com

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.