Network Working Group
Internet-Draft
Expires: December 16, 2005

S. Suehring

J. Salowey
Cisco Systems
June 14, 2005

SCP/SFTP/SSH URI Format
draft-ietf-secsh-scp-sftp-ssh-uri-02.txt

Status of this Memo

This Internet-Draft will expire on December 16, 2005.

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.

Table of Contents

1. Introduction

This document describes the Uniform Resource Identifiers (URIs) to be used with the SSH, SCP, and SFTP protocols.

2. General Syntax

The URI for each protocol shall consist of the scheme and the scheme specific portion separated by a colon ":", as discussed in [RFC3986] This specification shall adopt the definitions "port", "host", "scheme", "userinfo", and "authority" from [RFC3986].

2.1 SSH URI

The SSH scheme shall consist of the protocol acronym followed by a colon ":" and a double slash "//" in accordance with [RFC2718].

The first component of the scheme specific portion MAY include credentials (userinfo) consisting of a username and optionally also including a password, separated by a colon ":". Including the password in the URI is NOT RECOMMENDED and is deprecated in accordance with [RFC3986]

One or more optional connection parameters (conn-parameters) may be specified within the userinfo section of the URI. These conn-parameters are separated from the credentials by a semi-colon ";" and from each other by a comma ",".

Following the userinfo, if present, and the conn-parameters, 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, the default port is assumed.

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

2.2 SCP and SFTP URI

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

Both SCP and SFTP URIs 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, separated by a colon ":". Including the

password in the URI is NOT RECOMMENDED and is deprecated in accordance with [RFC3986]

One or more optional connection parameters (conn-parameters) may be specified within the userinfo section of the URI. These conn-parameters are separated from the credentials by a semi-colon ";" and from each other by a comma ",".

Following the userinfo, if present, and the conn-parameters, 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, the default port is assumed.

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

The URIs for SFTP and SCP are hierarchical URIs where each component of the abs_path consists of path elements separated by a '/'. This formatting is meant to represent the path information as in Section 5 of [I-D.ietf-secsh-filexfer].

3. Parameters

3.1 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 (","). Additional parameters MAY be used.

fingerprint

The fingerprint parameter contains the fingerprint of the host key for the host specified in the URL. The fingerprint is encoded as host-key-alg-fingerprint. Host-key-alg is host public key algorithm defined in [I-D.ietf-secsh-transport] and the fingerprint format is [I-D.ietf-secsh-publickeyfile]. For use in a URI, the fingerprint shall use a single dash "-" as a separator

instead of the colon ":" as described in [I-D.ietf-secsh-publickeyfile]. This parameter MUST NOT overwrite a key that is already configured for the host. The 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 per host-key-alg for a given URL.

3.2 SFTP Parameters

The SFTP parameters determine how to handle the file transfer character translation. Additional parameters MAY be used.

newline

The newline parameter determines how the server translates new line indicators. The default is CRLF and implemented in accordance with Section 4.3 of [I-D.ietf-secsh-filexfer].

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.

4. 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://user;fingerprint=ssh-dss-c1-b1-30-29-d7-b8-de-6c-97-77-10-d7-46-41-63-87@example.com

scp://user@host.example.com/file.txt

sftp://user@host/dir/path/file.txt

sftp://user;newline=CR,fingerprint=ssh-dss-c1-b1-30-29-d7-b8-de-6c-97-77-10-d7-46-41-63-87@example.com:2222/

5. Security Considerations

In general, URIs themselves have no security considerations. However, since the password for each scheme can optionally be included within the URI it should be noted that doing so poses a security risk. Since URIs 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.

Care must also be taken in handling fingerprints associated with URIs because URIs transmitted or stored without protection may be modified by an attacker. In general an implementation cannot determine the source of a URI so a fingerprint received in a URI should have no more trust associated with it than a raw public key received in the SSH protocol itself. If a locally configured key exists for the server already it MUST NOT be automatically overwritten with information from the URI. If the host is unknown then the implementation should treat the fingerprint received with the same caution that it does with any unknown public key. The client MAY offer the fingerprint and URI for external validation before allowing a connection based on this information. If the client chooses to make a connection based on the URI information and it finds that the public key in the URI and the public key offered by the server do not match then it SHOULD provide a warning and provide a means to abort the connection. Sections 4.1 and 9.2.4 of [I-D.ietf-secsh-architecture] provide a good discussion of handling public keys received in the SSH protocol.

6. References

6.1 Normative References

[I-D.ietf-secsh-architecture]
Ylonen, T. and C. Lonvick, "SSH Protocol Architecture", draft-ietf-secsh-architecture-22 (work in progress), March 2005.

[I-D.ietf-secsh-filexfer]
Galbraith, J., "SSH File Transfer Protocol", draft-ietf-secsh-filexfer-09 (work in progress), June 2005.

[I-D.ietf-secsh-publickeyfile]
Galbraith, J. and R. Thayer, "SSH Public Key File Format", draft-ietf-secsh-publickeyfile-08 (work in progress), April 2005.

[I-D.ietf-secsh-transport]
Lonvick, C., "SSH Transport Layer Protocol", draft-ietf-secsh-transport-24 (work in progress), March 2005.

[RFC2718] Masinter, L., Alvestrand, H., Zigmond, D., and R. Petke, "Guidelines for new URL Schemes", RFC 2718, November 1999.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

6.2 Informative References

[RFC3305] Mealling, M. and R. Denenberg, "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.

Authors' Addresses

Steve Suehring
PO BOX 1033
Stevens Point, WI 54481
US

Email: suehring@braingia.com

Joseph Salowey
Cisco Systems
2901 3rd Ave
Seattle, WA 98121
US

Email: jsalowey@cisco.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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