

Network Working Group
Internet-Draft
Expires: June 10, 2002

D. Moffat
Sun Microsystems
December 10, 2001

SSH Agent Forwarding
draft-ietf-secsh-agent-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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/ietf/lid-abstracts.txt>.

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

This Internet-Draft will expire on June 10, 2002.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

SSH is a protocol for secure remote login and other secure network services over an insecure network. One of the common authentication mechanisms used with SSH is public key. This document describes the authentication agent forwarding protocol, which runs as a channel over [[SSH-TRANS](#)] it is designed to ensure that the sensitive private keys never leave the users control even when using SSH to login over multiple hops.

Internet-Draft

SSH Agent Forwarding

December 2001

Table of Contents

1.	Introduction	3
1.1	Agent Operations	3
2.	Security Considerations	3
3.	Additional Information	4
	References	4
	Author's Address	4
	Full Copyright Statement	5

1. Introduction

This protocol is designed to facilitate an ad hoc secure single sign on mechanism using the SSH protocol. A typical scenario is that a user has their private keys stored on their laptop (host A) and uses the SSH protocol to remotely connect to their corporate VPN (host B) access point. Then uses further SSH connections to reach a specific host (host C) within the enterprise network.

Without agent forwarding the user is required to have a copy of their private key on host A and host B so that the connection to host C can be made using public key authentication. The key pairs used for the host A to B and the host B to C connection maybe the same but this is not always the case.

This presents a security risk since the users private key(s) must be stored on host B which is likely to be a host the end user is not in control of even though they do trust it. It is likely that the private keys on host A and host B are stored in an encrypted format, this means the user has at least two passwords to enter to make the connection from A to C.

Ideally the private keys should remain on a device in the direct control of the end user (host A in this example) and all encryption and signing operations involving the private key should be performed on this device, regardless of the location of the entity requesting the operation.

1.1 Agent Operations

The following interactions with the agent are required: ADD, DELETE, LIST, SIGN.

An agent implementation MUST support requests to forward operations using all public key types, defined in [[SSH-USERAUTH](#)] even those that

the implementation doesn't support natively.

2. Security Considerations

This protocol is designed only to run as a channel of the SSH protocol.

The goal of this extension is to ensure that the users private keys never leave the machine they are physically at. Ideally the private keys should be stored on a password protected removable media such as a smartcard.

Moffat

Expires June 10, 2002

[Page 3]

Internet-Draft

SSH Agent Forwarding

December 2001

3. Additional Information

The current document editor is: Darren.Moffat@Sun.COM. Comments on this internet draft should be sent to the IETF SECSH working group, details at: <http://ietf.org/html.charters/secsh-charter.html>

References

- [FIPS-186] Federal Information Processing Standards Publication, ., "FIPS PUB 186, Digital Signature Standard", May 1994.
- [SSH-ARCH] Ylonen, T., "SSH Protocol Architecture", I-D [draft-ietf-architecture-11.txt](#), July 2001.
- [SSH-TRANS] Ylonen, T., "SSH Transport Layer Protocol", I-D [draft-ietf-transport-11.txt](#), July 2001.
- [SSH-USERAUTH] Ylonen, T., "SSH Authentication Protocol", I-D [draft-ietf-userauth-13.txt](#), July 2001.
- [SSH-CONNECT] Ylonen, T., "SSH Connection Protocol", I-D [draft-ietf-connect-14.txt](#), July 2001.

Author's Address

Darren J Moffat

Sun Microsystems
901 San Antonio Road
Palo Alto 94303
USA

EMail: Darren.Moffat@Sun.COM

Moffat

Expires June 10, 2002

[Page 4]

Internet-Draft

SSH Agent Forwarding

December 2001

Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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