Groupe de travail Réseau
Request for Comments : 4335
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Galbraith, VanDyke Software
P. Remaker, Cisco Systems, Inc

janvier 2006

Extension Break de canal de session Secure Shell (SSH)

Résumé
L'extension Break de canal de session donne le moyen d'envoyer un signal BREAK sur une session de terminal Secure Shell (SSH).

Table des matières

1. Introduction

Le canal de session Secure Shell (SSH) [RFC4254] fournit un mécanisme pour que le client/utilisateur entre de façon interactive les commandes et reçoive le résultat à partir d'un hôte distant tout en tirant parti de la confidentialité et des caractéristiques d'intégrité du transport SSH. SSH est de plus en plus utilisé pour remplacer Telnet pour les applications d'accès terminales.

Une application courante du protocole Telnet est le "serveur de console" [Harris] par lequel un terminal virtuel de réseau (NVT, *Network Virtual Terminal*) peut être connecté à un accès asynchrone physique RS-232/V.24, faisant apparaître le NVT Telnet comme un terminal rattaché en local à cet accès, et faisant apparaître cet accès physique comme un appareil adressable par le réseau. Un certain nombre de fabricants d'équipements informatiques majeurs fournissent des fonctions administratives de haut niveau par un accès série asynchrone et s'attendent généralement à ce que le terminal rattaché soit capable d'envoyer un signal BREAK.

Un signal BREAK est défini comme le signal TxD tenu dans un état SPACE ("0") pendant un temps supérieur au temps d'un caractère complet. En pratique, un signal BREAK dure normalement de 250 à 500 ms.

Le protocole Telnet fournit un moyen pour envoyer un signal "BREAK", que la [RFC0854] définit comme "un signal en dehors de l'ensemble US-ASCII auquel est donné généralement une signification locale dans de nombreux systèmes". Les fabricants de serveurs de console interprètent le signal BREAK TELNET comme un signal BREAK physique, qui peut alors donner l'accès à la gamme complète des fonctions administratives disponibles sur un accès de console de série asynchrone.

L'absence d'une facilité similaire dans le canal de session SSH a forcé les utilisateurs à continuer d'utiliser Telnet pour la fonction de "serveur console".

2. Conventions utilisées dans le document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Les types de données "octet", "booléen", "uint32", et "chaîne" sont définis dans la [RFC4251].

3. Demande Break

La demande spécifique du canal suivante peut être envoyée sur un canal de session (comme décrit dans la [RFC4254]) pour demander que l'hôte distant effectue une opération BREAK.

octet	SSH_MSG_CHANNEL_REQUEST
uint32	canal receveur
chaîne	"break"
booléen	want_reply *(veut une réponse)*
uint32	longueur de "break" en millisecondes

Si la longueur de BREAK ne peut pas être contrôlée par l'application qui reçoit cette demande, le paramètre Longueur de BREAK DEVRAIT être ignoré et la longueur de signal BREAK par défaut de la carte à puce ou du pilote de carte à puce sous-jacent DEVRAIT être envoyée.

Si l'application qui reçoit cette demande peut contrôler la longueur de BREAK, on fait les suggestions suivantes concernant la durée de BREAK. Si une demande de durée de BREAK supérieure à 3000 ms est reçue, elle DEVRAIT être interprétée comme demande d'un BREAK de 3000 ms. Ce garde-fou empêchera une demande de BREAK d'une longueur déraisonnable de causer l'indisponibilité d'un accès pendant jusqu'à 49,7 jours en exécutant le BREAK. Les applications qui exigent un BREAK plus long peuvent choisir d'ignorer cette suggestion. Si une demande de durée de BREAK de moins de 500 ms est reçue, elle DEVRAIT être interprétée comme un BREAK de 500 ms car la plupart des appareils vont reconnaître un BREAK de cette longueur. Les applications qui exigent un BREAK plus court peuvent choisir d'ignorer cette suggestion. Si le paramètre Longueur de BREAK est 0, le BREAK DEVRAIT être interprété comme la longueur de signal BREAK par défaut de la carte à puce ou pilote de carte à puce sous-jacent. Si il n'existe pas de valeur par défaut, 500 ms peut être utilisé comme longueur de BREAK.

Si la connexion SSH ne se termine pas sur un accès série physique, l'indication BREAK DEVRAIT être traitée d'une manière cohérente avec l'utilisation générale de BREAK comme un signal d'attention/interruption ; par exemple, un processeur de service qui exige une facilité hors bande pour attirer l'attention d'un système qu'il gère.

Dans un cas où la connexion SSH se renvoie en cascade sur une autre connexion, le BREAKDEVRAIT être passé à la connexion suivante. Par exemple, une session Telnet provenant d'une coquille SSH devrait entraîner un BREAK initié par SSH, et un client SSH initié à partie d'une connexion Telnet DEVRAIT passer une indication BREAK provenant de la connexion Telnet.

Si le booléen "want_reply" est établi, le serveur DOIT répondre en utilisant un message SSH_MSG_CHANNEL_SUCCESS ou SSH_MSG_CHANNEL_FAILURE [RFC4254]. Si un BREAK de quelque sorte a été effectué, SSH_MSG_CHANNEL_SUCCESS DOIT être envoyé. Si un BREAK n'a pas été effectué, SSH_MSG_CHANNEL_FAILURE DOIT être envoyé.

Cette opération DEVRAIT être prise en charge pat tout client SSH général.

4. Considérations sur la sécurité

De nombreux systèmes informatiques traitent les consoles de série comme locales et sûres, et interprètent un signal BREAK comme une instruction d'arrêter l'exécution du système d'exploitation ou d'entrer dans des modes de configuration privilégiés. À cause de cela, une attention particulière devrait être apportée à s'assurer que l'accès de SSH à des accès à capacité de BREAK est limité aux utilisateurs qui ont les privilèges appropriés pour exécuter de telles fonctions. Autrement, la prise en charge de la facilité BREAK PEUT être mise en œuvre comme configurable accès par accès ou serveur par serveur.

Les mises en œuvre qui interprètent littéralement le paramètre Longueur de BREAK sans imposer la limite de temps de BREAK suggérée peuvent causer un déni de service ou des résultats inattendus de la part des appareils rattachés qui reçoivent le très long signal BREAK.

5. Considérations relatives à l'IANA

L'IANA a alloué le nom de demande de canal de protocole de connexion "break" conformément à la [RFC4250].

6. Références

6.1 Références normatives

[RFC0854] J. Postel et J. Reynolds," Spécification du protocole TELNET", STD 8, mai 1983.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC4250] S. Lehtinen et C. Lonvick, éd., "Numéros alloués du protocole Secure Shell (SSH)", janvier 2006. *(P.S. ; MàJ par* RFC8268)

[RFC4251] T. Ylonen et C. Lonvick, "Architecture du protocole Secure Shell (SSH)", janvier 2006. *(P.S. ; MàJ par* RFC8308)

[RFC4252] T. Ylonen et C. Lonvick, éd., "Protocole d'authentification Secure Shell (SSH)", janvier 2006. *(P.S .; MàJ par* RFC8308, 8332)

[RFC4253] C. Lonvick, "Protocole de couche Transport Secure Shell (SSH)", janvier 2006. *(P.S., MàJ par* RFC6668, 8268, 8308, 8332,)