Groupe de travail Réseau
**Request for Comments : 5018**
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

G. Camarillo, Ericsson

septembre 2007

# Établissement de connexion dans le protocole de contrôle à codage binaire de la prise de parole (BFCP)



**Résumé**
Le présent document spécifie comment un client du protocole de contrôle à codage binaire de la prise de parole (BFCP, *Binary Floor Control Protocol*) établit une connexion avec un serveur de contrôle de la prise de parole BFCP en dehors du contexte d'un échange offre/réponse. L'authentification du client et du serveur se fonde sur la sécurité de la couche Transport (TLS, *Transport Layer Security*).

## Table des Matières



## 1. Introduction

Comme exposé dans la spécification du protocole de contrôle à codage binaire de la prise de parole (BFCP, *Binary Floor Control Protocol*) [RFC4582], un client BFCP a besoin d'un ensemble de données afin d'établir une connexion BFCP avec un serveur de contrôle de la prise de parole. Ces données incluent l'adresse de transport du serveur, l'identifiant de conférence, et l'identifiant de l'utilisateur.

Une fois qu'un client a obtenu ces informations, il doit établir une connexion BFCP avec le serveur de contrôle de la prise de parole. La façon dont cette connexion est établie dépend du contexte du client et du serveur de contrôle de la prise de parole. Comment établir une telle connexion dans le contexte d'un échange d'offre/réponse [RFC3264] du protocole de description de session (SDP, *Session Description Protocol*) [RFC4566] entre un client et un serveur de contrôle de la prise de parole est spécifié dans la [RFC4583]. Le présent document spécifie comment un client établit une connexion avec un serveur de contrôle de la prise de parole en dehors du contexte d'un échange d'offre/réponse SDP.

Les entités BFCP qui établissent une connexion en dehors d'un échange d'offre/réponse SDP ont besoin de mécanismes d'authentification différents des entités qui utilisent les échanges d'offre/réponse. C'est parce que les échanges

d'offre/réponse fournissent aux parties un canal initial protégé en intégrité que les clients et les serveurs de contrôle de la prise de parole peuvent utiliser pour échanger les empreintes de leurs certificats auto-signés. En dehors du modèle d'offre/réponse, un tel canal n'est normalement pas disponible. Le présent document spécifie comment authentifier les clients en utilisant une clé pré-partagée (PSK, *Pre-Shared Key*) de la sécurité de la couche transport (TLS, *Transport Layer Security*) [RFC4279] et comment authentifier les serveurs en utilisant des certificats de serveur

## 2. Spécification des exigences

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].

## 3. Établissement de la connexion TCP

Comme on l'a déclaré à la Section 1, un client BFCP a besoin d'un ensemble de données pour établir une connexion BFCP avec un serveur de contrôle de la prise de parole. Ces données incluent l'adresse de transport du serveur, l'identifiant de conférence, et l'identifiant d'utilisateur. Il sort du domaine d'application du présent document de spécifier comment un client obtient cette information. Le présent document suppose que le client obtient cette information en utilisant une méthode hors bande.

Une fois que le client a l'adresse de transport (c'est-à-dire l'adresse et l'accès IP) du serveur de contrôle de la prise de parole, il initie une connexion TCP avec lui. C'est-à-dire, le client effectue une ouverture TCP active.

Si le client a le nom d'hôte du serveur de contrôle de la prise de parole au lieu de son adresse IP, le client DOIT effectuer une recherche dans le DNS afin de résoudre le nom d'hôte en une adresse IP. Les clients effectuent finalement une recherche A ou AAAA (ou les deux) dans le DNS sur le nom d'hôte.

Afin de traduire la cible de l'ensemble correspondant d'adresses IP, les clients IPv6 seul ou à double pile DOIVENT utiliser les fonctions de résolution de nom qui mettent en œuvre les algorithmes de choix d'adresse de source et de destination spécifiés dans la [RFC3484]. (Sur de nombreux hôtes qui prennent en charge IPv6, des API comme getaddrinfo() fournissent cette fonctionnalité et se substituent aux API existantes comme gethostbyname().)

L'avantage de la complexité supplémentaire est que cette technique va résulter en une liste ordonnée d'adresses de destination IPv6/IPv4 fondée sur les mérites relatifs des paires de source/destination correspondantes. Il va en résulter le choix d'une adresse de destination préférée. Cependant, les algorithmes de choix de source et destination de la [RFC3484] dépendent d'une large prise en charge du système d'exploitation et de la mise en œuvre uniforme des interfaces de programmation d'application qui se comportent de cette façon.

Les développeurs devraient examiner avec attention les problèmes décrits par Roy et al. dans la [RFC4943] à l'égard des délais de résolution d'adresse et des règles de choix d'adresse. Par exemple, les mises en œuvre de getaddrinfo() peuvent retourner des listes d'adresses contenant des adresses IPv6 mondiales au sommet de la liste et des adresses IPv4 dans le bas, même quand l'hôte est seulement configuré avec une portée IPv6 locale (par exemple, une liaison locale) et une adresse IPv4. Cela va, bien sûr, introduire un délai pour réaliser la connexion.

La spécification de BFCP [RFC4582] décrit un certain nombre de situations où la connexion TCP entre un client et le serveur de contrôle de la prise de parole doit être rétablie. Cependant, cette spécification ne décrit pas le processus de rétablissement parce que ce processus dépend de la façon dont la connexion a d'abord été établie.

Quand la connexion TCP existante est close suivant les règles de la [RFC4582], le client DEVRAIT rétablir la connexion avec le serveur de contrôle de la prise de parole. Si une connexion TCP ne peut pas livrer un message BFCP provenant du client au serveur de contrôle de la prise de parole et arrive en fin de temporisation, le client DEVRAIT rétablir la connexion TCP.

## 4. Usage de TLS

La [RFC4582] exige que toutes les entités BFCP mettent en œuvre TLS [RFC4346] et recommande qu'elles l'utilisent dans toutes leurs connexions. TLS assure la protection de l'intégrité et contre la répétition, et facultativement de la confidentialité. Le serveur de contrôle de la prise de parole DOIT toujours agir comme serveur TLS.

Un serveur de contrôle de la prise de parole qui reçoit un message BFCP sur TCP (et non TLS) DEVRAIT demander l'utilisation de TLS en générant un message d'erreur avec un code d'erreur de 9 (Utiliser TLS).

## 5. Authentification

BFCP prend en charge l'authentification du client sur la base de secrets pré-partagés et l'authentification du serveur sur la base de certificats du serveur.

### 5.1 Authentification du serveur fondée sur le certificat

À l'établissement d'une connexion TLS, le serveur de contrôle de la prise de parole DOIT présenter son certificat au client. Le certificat fourni au niveau de TLS DOIT être directement signé par une des ancres de confiance de l'autre partie ou être validé en utilisant un chemin de certification qui se termine sur une des ancres de confiance de l'autre partie [RFC3280].

Un client qui établit une connexion avec un serveur connait le nom d'hôte ou l'adresse IP du serveur. Si le client connaît le nom d'hôte du serveur, le client DOIT le vérifier par rapport à l'identité du serveur telle que présentée dans le message Certificat du serveur, afin d'empêcher les attaques par interposition.

Si une extension subjectAltName de type dNSName est présente, elle DOIT être utilisée comme identité. Autrement, le champ Nom commun (le plus spécifique) dans le champ Sujet du certificat DOIT être utilisé. Bien que l'utilisation du nom commun existe dans la pratique, elle est déconseillée et les autorités de certification sont encouragées à utiliser à la place le subjectAltName.

La confrontation est effectuée en utilisant les règles de confrontation spécifiées dans la [RFC3280]. Si plus d'une identité d'un type donné est présente dans le certificat (par exemple, plus d'un nom dNSName) une correspondance dans un membre de l'ensemble est considérée comme acceptable. Les noms dans les champs Nom commun peuvent contenir le caractère générique *, qui est considéré correspondre à tout composant d'un seul nom de domaine ou fragment de composant (par exemple, *.a.com correspond à foo.a.com mais pas à bar.foo.a.com ; f*.com correspond à foo.com mais pas bar.com).

Si le client ne connaît pas le nom d'hôte du serveur et contacte directement le serveur en utilisant l'adresse IP du serveur, le subjectAltName iPAddress doit être présent dans le certificat et doit correspondre exactement à l'adresse IP connue du client.

Si le nom d'hôte ou l'adresse IP connue du client ne correspond pas à l'identité dans le certificat, les clients en mode utilisateur DOIVENT le notifier à l'utilisateur (les clients PEUVENT donner à l'utilisateur l'opportunité de continuer la connexion dans tous les cas) ou terminer la connexion avec une erreur "Mauvais certificat". Les clients automatisés DOIVENT enregistrer l'erreur dans un journal d'événements approprié (s'il est disponible) et DEVRAIENT terminer la connexion (avec une erreur "Mauvais certificat"). Les clients automatisés PEUVENT fournir un réglage de configuration qui désactive cette vérification, mais DOIVENT fournir un réglage qui la permette.

### 5.2 Authentification du client fondée sur un secret pré-partagé

L'authentification du client se fonde sur un secret pré-partagé entre client et serveur. L'authentification est effectuée en utilisant PSK-TLS [RFC4279].

La spécification de BFCP rend obligatoire la prise en charge de la suite de chiffrement TLS_RSA_WITH_AES_128_CBC_SHA. De plus, les clients et serveurs qui prennent en charge la présente spécification DOIVENT prendre en charge aussi la suite de chiffrement TLS_RSA_PSK_WITH_AES_128_CBC_SHA.

## 6. Considérations sur la sécurité

L'authentification du client et du serveur comme elle est spécifiée dans le présent document se fonde sur l'utilisation de TLS. Donc, il est fortement RECOMMANDÉ que TLS avec un chiffrement non nul soit toujours utilisé. Les clients et les serveurs de contrôle de la prise de parole PEUVENT utiliser d'autres mécanismes de sécurité pour autant qu'ils fournissent des propriétés de sécurité similaires (c'est-à-dire, la protection contre la répétition et de l'intégrité, la confidentialité, et l'authentification du client et du serveur).

TLS PSK s'appuie simplement sur une clé pré-partagée sans spécifier la nature de la clé. En pratique, de telles clés ont deux sources : des mots de passe de texte et des clés binaires générées de façon aléatoire. Quand les clés sont déduites de mots de passe, le mode TLS PSK est sujet à des attaques de dictionnaire hors ligne. Dans les modes d'échange Diffie-Hellman (DHE, *Diffie-Hellman Exchange*) et RSA, un attaquant qui peut monter une seule attaque par interposition sur la paire client/serveur peut alors monter une attaque de dictionnaire sur le mot de passe. Dans les modes sans DHE ou RSA, un attaquant qui peut enregistrer les communications entre une paire de client/serveur peut monter une attaque de dictionnaire sur le mot de passe. En conséquence, il est RECOMMANDÉ que, lorsque possible, les clients utilisent les suites de chiffrement d'authentification de serveur fondées sur le certificat avec des PSK déduites d'un mot de passe afin de se défendre contre les attaques de dictionnaire.

De plus, les mots de passe DEVRAIENT être choisis avec assez d'entropie pour fournir une protection contre les attaques de dictionnaire. Parce que l'entropie d'un texte varie considéablement et est généralement bien moindre que celle d'une chaîne binaire aléatoire équivalente, aucune règle pure et dure de longueur de mot de passe n'est possible. Cependant, en général les mots de passe DEVRAIENT être choisis avec au moins 8 caractères et pris dans un réservoir contenant des caractères majuscules et minuscules, des nombres, et des caractères spéciaux du clavier (noter qu'un mot de passe de 8 caractères ASCII a une entropie maximum de 56 bits et en général beaucoup moins). [PUB112] donne des lignes directrics sur les problèmes que cela pose. Si possible, les phrases de passe sont préférables aux mots de passe. Il est RECOMMANDÉ que les mises en œuvre prennent en charge , au minimum, des mots ou phrases de passe de 16 caractères. De plus, une paire coopérante de client et serveur PEUT choisir de déduire la clé partagée TLS PSK de la phrase de passe via une fonction de déduction de clé fondée sur un mot de passe comme PBKDF2 [RFC2898]. Parce que une telle fonction de déduction de clé peut incorporer des fonctions d'itération pour renforcer la clé, elle fournit une protection supplémentaire contre les attaques de dictionnaire en augmentant la quantité de travail que doit effectuer l'attaquant.

Quand les clés sont générées au hasard et sont de longueur suffisante, les attaques de dictionnaire ne sont pas efficaces parce que ces clés ont une très faible probabilité d'être dans le dictionnaire de l'attaquant. Lorsque possible, les clés DEVRAIENT être générées en utilisant un générateur de nombres aléatoire fort comme spécifié dans la [RFC4086]. Une longueur minimum de clé de 80 bits DEVRAIT être utilisée.

Le reste de cette section analyse certaines des menaces contre BFCP et comment les traiter.

Un attaquant peut tenter de se faire passer pour un client (un participant à la conférence ou son président) afin de générer une fausse demande de prise de parole ou pour accorder ou refuser des demandes existantes de parole. L'usurpation d'identitié de client est évitée en utilisant TLS. Le serveur de contrôle de la prise de parole suppose que des attaquants ne peuvent pas captures des connexions TLS de clients authentifiés.

Un attaquant peut tenter de se faire passer pour un serveur de contrôle de la prise de parole. Un attaquant qui réussit serait capable de faire penser aux clients qu'ils ont la parole et vont essayer d'accéder à une ressource (par exemple, envoyer des supports) sans avoir de droits légitimes à y accéder. L'usurpation de serveur de contrôle de la prise de parole est évitée en faisant que les serveurs de contrôle de la prise de parole présentent leurs certificats de serveur au moment de l'établissement de la connexion TLS.

Des attaquants peuvent tenter de modifier les messages échangés entre un client et un serveur de contrôle de la prise de parole. La protection de l'intégrité fournie par les connexions TLS empêche cette attaque.

Des attaquants peuvent tenter de capturer des messages dans le réseau pour obtenir l'accès à des informations confidentielles entre le serveur de contrôle de la prise de parole et un client (par exemple, pourquoi une demande de prise de parole est refusée). La confidentialité de TLS empêche cette attaque. Donc, il est RECOMMANDÉ que TLS soit utilisé avec un algorithme de chiffrement non nul.

## 7. Remerciements

Sam Hartman, David Black, Karim El Malki, et Vijay Gurbani ont fourni des commentaires utiles sur le présent document. Eric Rescorla a effectué une analyse détaillée de la sécurité de ce document.

## 8. Références

### 8.1 Références normatives

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

[RFC3264] J. Rosenberg et H. Schulzrinne, "Modèle d'offre/réponse avec le protocole de description de session (SDP)", juin 2002. *(P.S. ; MàJ par* RFC8843, 9143)

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3484] R. Draves, "Choix d'adresse par défaut pour le protocole Internet version 6 (IPv6)", février 2003. (*Remplacée par la* RFC6724) *(P.S.)*

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

[RFC4279] P. Eronen et H. Tschofenig, éd., "Suites de chiffrement de clés pré-partagées pour la sécurité de la couche Transport (TLS)", décembre 2005. *(P.S.)*

[RFC4386] S. Boeyen, P. Hallam-Baker, "Service de localisation de répertoire d'infrastructure de clé publique X.509 pour l'Internet", février 2006. *(Expérimentale)*

[RFC4566] M. Handley, V. Jacobson et C. Perkins, "SDP : Protocole de description de session", juillet 2006. *(P.S. ; remplacée par RFC8866)*

[RFC4582] G. Camarillo et autres, "Protocole de contrôle à codage binaire de la prise de parole (BFCP)", novembre 2006. *(P.S. ; remplacée par RFC*8855*)*

[RFC4583] G. Camarillo, "Format de protocole de description de session (SDP) pour les flux du protocole de contrôle à codage binaire de la prise de parole (BFCP)", novembre 2006. *(P.S. ; remplacée par RFC*8856*)*

[PUB112] National Institute of Standards and Technology (NIST), "Password Usage", FIPS PUB 112, mai 1985.

### 8.2 Références pour information

[RFC2898] B. Kaliski, "PKCS n° 5 : Spécification de la cryptographie fondée sur un mot de passe, version 2.0", septembre 2000. *(Info. ; remplacée par* RFC8018)

[RFC4943] S. Roy et autres, "L'hypothèse "en liaison" dans la découverte de voisin IPv6 est considérée comme dommageable", septembre 2007. *(Information)*

## Adresse de l'auteur

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

mél : Gonzalo.Camarillo@ericsson.com

## Déclaration complète de droits de reproduction



**Propriété intellectuelle**

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

**Remerciement**

Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif de l'IETF (IASA).