Groupe de travail Réseau
Request for Comments : 4383
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Baugher, Cisco
E. Carrara, Royal Institute of Technology
01/02/06

Utilisation de l'authentification tolérante aux pertes de flux à synchronisation efficace (TESLA) dans le protocole de transport en temps réel sécurisé (SRTP)

Résumé
Le présent mémoire décrit l'utilisation de la transformation d'authentification tolérante aux pertes de flux à synchronisation efficace (RFC 4082) dans le protocole de transport sûr en temps réel (SRTP, *Secure Real-time Transport Protocol*) pour assurer l'authentification de l'origine des données pour les flux de données en diffusion et diffusion groupée.

Table des matières

1. Introduction....1
1.1 Conventions de notation....2
2. SRTP....2
3. TESLA....2
4. Usage de TESLA avec SRTP....3
4.1. Extension TESLA....3
4.2 Format de paquet SRTP....3
4.3 Extension du contexte cryptographique SRTP....4
4.4 Traitement SRTP....5
4.5 Format de paquet SRTCP....6
4.6 MAC TESLA....7
4.7 PRF....8
5. Amorçage et terminaison de TESLA....8
6. Paramètres par défaut de SRTP TESLA....8
7. Considérations sur la sécurité....9
8. Remerciements....9
9. Références....9
9.1 Références normatives....9
9.2 Références pour information....10
Adresse des auteurs....10
Déclaration complète de droits de reproduction....10

1. Introduction

Les communications en diffusion et en diffusion groupée introduisent de nouveaux défis pour la sécurité par rapport à la communication en envoi individuel. De nombreuses applications de diffusion et diffusion groupée ont besoin d'une "authentification de l'origine des données" (DOA, *Data Origin Authentication*), ou "authentification de source", afin de garantir que le message reçu a pour origine une certaine source, et n'a pas été manipulé durant la transmission. Dans la communication en envoi individuel, une association de sécurité d'homologues entre un envoyeur et un receveur peut fournir l'authentification de l'origine des données en utilisant un chiffrement à clés symétriques (comme un code d'authentification de message, (MAC, *Message Authentication Code*). Quand la communication est strictement entre deux homologues, l'envoyeur et le receveur s'accordent sur une clé qui n'est connue que d'eux.

Dans les groupes, cependant, une clé est partagée entre plus de deux membres, et cette approche de clé symétrique ne garantit pas l'authentification de l'origine des données. Quand il y a une association de sécurité de groupe [RFC4046] au lieu d'une association de sécurité entre deux homologues, un des membres peut altérer le paquet et se faire passer pour tout autre membre. Le MAC dans ce cas garantit seulement que le paquet n'a pas été manipulé par un attaquant hors du groupe (et donc qui n'est pas en possession de la clé de groupe) et que le paquet a été envoyé par une source au sein du groupe.

Certaines applications ne peuvent pas tolérer d'ambiguïté sur la source et ont besoin d'identifier le véritable envoyeur parmi tous les autres membres du groupe. Une façon courante de résoudre le problème est d'utiliser un chiffrement asymétrique, comme une signature numérique. Cette méthode, souffre malheureusement d'une forte redondance en termes de temps (pour signer et vérifier) et de bande passante (pour convoyer la signature dans le paquet).

Plusieurs schémas ont été proposés pour fournir une authentification efficace de l'origine des données dans les scénarios de diffusion et de diffusion groupée. L'authentification tolérante aux pertes de flux à synchronisation efficace (TESLA, *Timed Efficient Stream Loss-tolerant Authentication*) est un de ces schémas.

Le présent mémoire spécifie l'authentification TESLA pour SRTP. TESLA SRTP peut assurer l'authentification de l'origine des données aux applications RTP qui utilisent des associations de sécurité de groupe (comme les applications RTP en diffusion groupée) pour autant que les receveurs restent fidèles aux invariants de sécurité de TESLA [RFC4082].

1.1 Conventions de notation

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].

La présente spécification suppose que le lecteur est familiarisé avec SRTP et TESLA. Quelques uns de leurs détails sont expliqués dans ce document, et le lecteur peut les trouver dans leurs spécifications respectives, [RFC3711] et [RFC4082]. Cette spécification utilise les mêmes définitions que TESLA pour les termes courants et suppose que le lecteur est familiarisé avec les algorithmes et protocoles de TESLA [RFC4082].

2. SRTP

Le protocole de transport sûr en temps réel (SRTP, *Secure Real-time Transport Protocol*) [RFC3711] est un profil de RTP, qui peut fournir la confidentialité, l'authentification du message, et la protection contre la répétition pour le trafic RTP et pour le protocole de contrôle RTP, le protocole de contrôle du transport en temps réel (RTCP, *Real-time Transport Control Protocol*). Noter que le terme "SRTP" peut souvent être utilisé pour indiquer aussi SRTCP.

SRTP est un cadre qui permet d'ajouter de nouvelles fonctions de sécurité et de nouvelles transformation. SRTP ne définit actuellement pas de mécanisme pour fournir l'authentification de l'origine des données pour les associations de sécurité de groupe. Heureusement, l'ajout de TESLA au cadre cryptographique SRTP est direct.

L'extension de TESLA à SRTP est définie dans la présente spécification, qui suppose que le lecteur est familiarisé avec la spécification SRTP [RFC3711], sa structure de paquet, et ses règles de traitement. TESLA est un algorithme d'authentification de message de remplacement qui authentifie les messages à partir de la source quand une clé est partagée entre deux receveurs ou plus.

3. TESLA

TESLA fournit une authentification retardée des données par paquet et est spécifié dans la [RFC4082].

En plus de sa définition de paquet de données SRTP donnée ici, TESLA a besoin d'un protocole de synchronisation initial et d'une procédure initiale d'amorçage. Le protocole de synchronisation permet à l'envoyeur et au receveur de comparer leurs horloges et de déterminer une limite supérieure de leur différence. Le protocole de synchronisation sort du domaine d'application du présent document.

TESLA exige aussi une procédure initiale d'amorçage pour échanger les paramètres initiaux et l'affectation initiale de la chaîne de clés [RFC4082]. Pour SRTP, on suppose que l'amorçage est effectué hors bande, éventuellement en utilisant le

protocole de gestion de clés qui échange les paramètres de sécurité pour SRTP, par exemple, [RFC3547], [RFC3830]. L'amorçage initial de TESLA sort du domaine d'application du présent document.

4. Usage de TESLA avec SRTP

La présente spécification est une extension à la spécification de SRTP [RFC3711] et décrit l'utilisation de TESLA avec seulement une chaîne de clés et l'authentification retardée [RFC4082].

4.1. Extension TESLA

TESLA est une transformation d'authentification FACULTATIVE pour SRTP. Quand elle est utilisée, TESLA ajoute les champs montrés à la Figure 1 à chaque paquet. Les champs ajoutés par TESLA sont appelés "extensions d'authentification TESLA" tandis que "étiquette d'authentification" ou "étiquette de protection d'intégrité" indique l'étiquette normale de protection de l'intégrité SRTP, quand la clé maîtresse SRTP est partagée par plus de deux points d'extrémité [RFC3711].

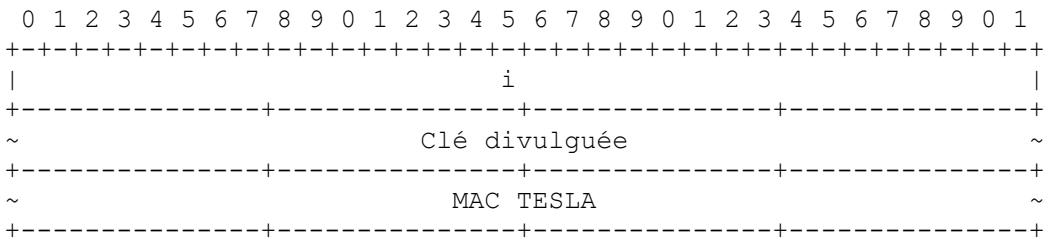


Figure 1 : extension d'authentification TESLA

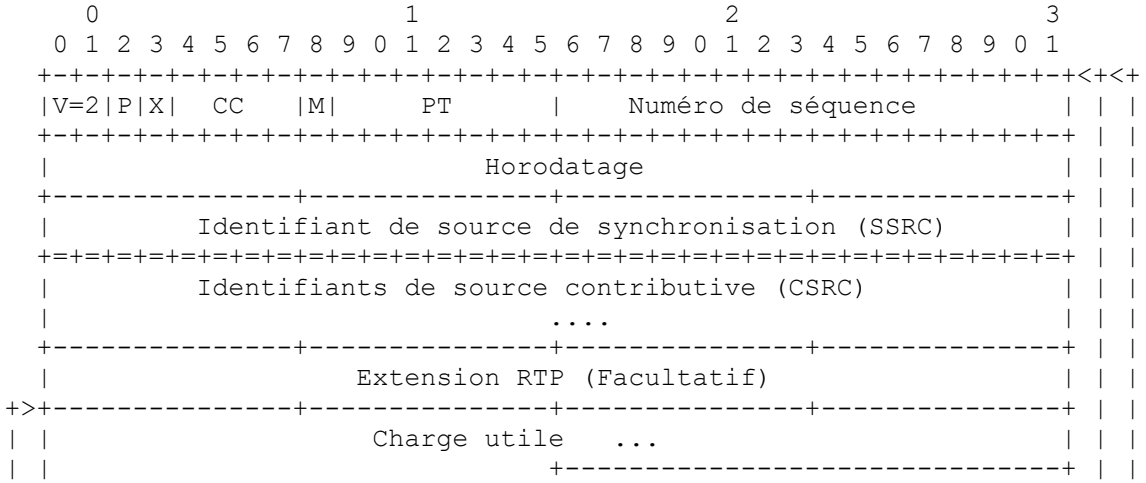
i : 32 bit, OBLIGATOIRE. Identifiant de l'intervalle de temps i, correspondant à la clé K_i, qui est utilisée pour calculer le MAC TESLA du paquet en cours (et des autres paquets envoyés dans l'intervalle de temps i en cours).

Clé divulguée : longueur variable, OBLIGATOIRE. La clé divulguée (K_(i-d)), qui peut être utilisée pour authentifier les paquets antérieurs provenant d'intervalles de temps précédents [RFC4082]. Un paramètre du paragraphe 4.3 établit la taille de ce champ.

MAC (code d'authentification de message) TESLA : longueur variable, OBLIGATOIRE. C'est le MAC calculé en utilisant la clé K'_i (déduite de K_i) [RFC4082], qui est divulguée dans un paquet suivant (dans le champ Clé divulguée). La couverture du MAC est définie au paragraphe 4.6. Un paramètre du paragraphe 4.3 établit la taille de ce champ.

4.2 Format de paquet SRTP

La Figure 2 illustre le format du paquet SRTP quand TESLA est appliqué. Quand elle est appliquée à RTP, l'extension d'authentification TESLA DEVRA être insérée avant le MKI SRTP (facultatif) et l'étiquette d'authentification (recommandée) (MAC SRTP).



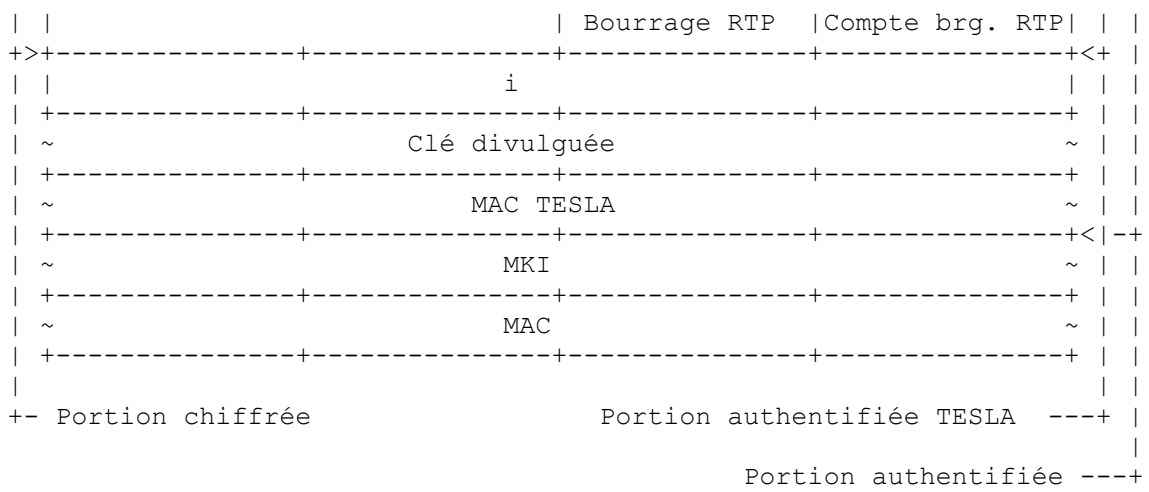


Figure 2 : Format du paquet SRTP quand TESLA est appliqué

Comme dans SRTP, la "Portion chiffrée" d'un paquet SRTP consiste en le chiffrement de la charge utile RTP (incluant le bourrage RTP quand il est présent) du paquet RTP équivalent.

La "Portion authentifiée" d'un paquet SRTP consiste en l'en-tête RTP, la portion chiffrée du paquet SRTP, et l'extension d'authentification TESLA. Noter que la définition est étendue par rapport à la [RFC3711] par l'inclusion de l'extension d'authentification TESLA.

La "Portion authentifiée TESLA" d'un paquet SRTP consiste en l'en-tête RTP et la portion chiffrée du paquet SRTP. Comme le montre la Figure 2, le MAC SRTP couvre jusqu'au champ MKI mais n'inclut pas le MKI. Il est nécessaire pour l'intégrité du paquet que l'étiquette MAC SRTP-TESLA soit couverte par la vérification d'intégrité de SRTP. SRTP ne couvre pas le champ MKI (parce qu'il n'a pas besoin d'être couvert pour l'intégrité de paquet SRTP). Afin de rendre contiguës les deux étiquettes (MAC SRTP-TESLA et SRTP-MAC) on aura besoin de redéfinir la spécification SRTP pour inclure le MKI dans la couverture SRTP-MAC. Ce changement est impossible, de sorte que le champ MKI sépare le MAC TESLA du MAC SRTP dans la disposition de paquet de la Figure 2. Ce changement du format de paquet ne présente pas de problème à une mise en œuvre qui prend en charge la nouvelle transformation d'authentification SRTP-TESLA.

Les longueurs des champs Clé divulguée et MAC TESLA sont des paramètres du paragraphe 4.3. Comme dans SRTP, les champs qui suivent la charge utile du paquet ne sont pas nécessairement alignés sur des limites de 32 bits.

4.3 Extension du contexte cryptographique SRTP

Quand TESLA est utilisé, la définition du contexte cryptographique du paragraphe 3.2 de SRTP DEVRA inclure les extensions suivantes.

Paramètres dépendants de la transformation

1. un identifiant pour la PRF (PRF TESLA) mettant en œuvre la fonction unidirectionnelle F(x) dans TESLA (pour déduire les clés dans la chaîne) et la fonction unidirectionnelle F'(x) dans TESLA (pour déduire les clés pour le MAC TESLA, à partir des clés dans la chaîne) par exemple, pour indiquer HMAC-SHA1. Voir à la Section 6 la valeur par défaut.

2. un entier non négatif, n_p, qui détermine la longueur du résultat F ; c'est-à-dire, la longueur des clés dans la chaîne (qui est aussi la clé divulguée dans un paquet SRTP). Voir à la Section 6 la valeur par défaut.

3. un entier non négatif, n_f, qui détermine la longueur du résultat de F', c'est-à-dire, de la clé pour le MAC TESLA. Voir à la Section 6 la valeur par défaut..

4. un identifiant pour le MAC TESLA qui accepte le résultat de F'(x) comme sa clé, par exemple, pour indiquer HMAC-SHA1. Voir à la Section 6 la valeur par défaut.

5. un entier non négatif, n_m, déterminant la longueur du résultat du MAC TESLA. Voir à la Section 6 la valeur par défaut.

6. le début de la session T_0.

7. la durée de l'intervalle T_int (en ms).

8. le délai de divulgation de clé d (en nombre d'intervalles).

9. la limite supérieure D_t (en s) du retard de l'horloge du receveur par rapport à l'horloge de l'envoyeur (cette quantité doit être calculée hors bande par les homologues).

10. un entier non négatif, n_c, déterminant la longueur de la chaîne de clés, K_0...K_n-1 de la [RFC4082] (voir aussi la Section 6 du présent document) qui est déterminée sur la base de la durée attendue du flux.

11. la clé initiale de la chaîne à laquelle l'envoyeur s'est engagé.

F(x) est utilisé pour calculer la chaîne de clés dans SRTP TESLA, comme défini à la Section 6. Aussi conformément à TESLA, F'(x) calcule une clé de MAC TESLA avec des entrées comme définies à la Section 6.

La Section 6 du présent document définit les valeurs par défaut pour les paramètres spécifiques de la transformation TESLA.

4.4 Traitement SRTP

Le traitement de paquet SRTP est décrit au paragraphe 3.3 de la spécification SRTP [RFC3711]. L'utilisation de TESLA change légèrement le traitement, car le MAC SRTP est vérifié à l'arrivée du paquet pour prévenir les attaques de DoS, mais le paquet courant n'est pas authentifié par TESLA. Chaque paquet est mis en mémoire tampon jusqu'à ce qu'un paquet suivant divulgue sa clé TESLA. La vérification TESLA elle-même consiste en certaines étapes, comme la vérification des invariants de sécurité TESLA, qui sont décrits aux paragraphes 3.5 à 3.7 de la [RFC4082]. Les termes "calcul TESLA" et "vérification TESLA" impliquent ici toutes ces étapes, qui ne sont pas toutes détaillées dans la suite de ce document. En particulier, on notera que la vérification TESLA implique de vérifier la condition de sûreté (paragraphe 3.5 de la [RFC4082]).

Comme mentionné dans la [RFC4082], si le paquet est réputé "non sûr", le receveur considère alors que le paquet n'est pas authentifié. Il devrait éliminer les paquets non sûrs, mais, à ses propres risques, il peut choisir de les utiliser non vérifiés. Donc, si la condition de sûreté ne tient pas, il est RECOMMANDÉ d'éliminer le paquet et d'enregistrer l'événement.

4.4.1 Traitement chez l'envoyeur

Le traitement chez l'envoyeur est décrit au paragraphe 3.3 de la [RFC3711], jusqu'à l'étape 5, incluse. Après cela, le processus est le suivant :

6. Quand TESLA est appliqué, identifier la clé dans la chaîne TESLA qui va être utilisée dans l'intervalle de temps en cours, et la clé de MAC TESLA qui en est déduite. Exécuter le calcul TESLA pour obtenir l'extension Authentification TESLA pour le paquet en cours, en ajoutant l'identifiant d'intervalle actuel (comme champ i) la clé divulguée de la chaîne pour l'intervalle de divulgation précédent (c'est-à-dire, la clé pour l'intervalle i est divulguée dans l'intervalle i+d) et le MAC TESLA sous la clé en cours de la chaîne. Cette étape utilise les paramètres relatifs à TESLA provenant du contexte de chiffrement comme pour l'étape 4.

7. Si l'indicateur MKI dans le contexte de chiffrement SRTP est réglé à un, ajouter le MKI au paquet.

8. Quand TESLA est appliqué, et si l'authentification SRTP (étiquette externe) est requise (à cause du DoS) calculer l'étiquette d'authentification comme décrit à l'étape 7 du paragraphe 3.3 de la spécification SRTP, mais avec la couverture définie dans la présente spécification (voir au paragraphe 4.6).

9. Si nécessaire, mettre à jour le compteur de débordement (étape 8 du paragraphe 3.3 de la [RFC3711]).

4.4.2 Traitement à réception

Le traitement chez le receveur est décrit au paragraphe 3.3 de la [RFC3711], jusqu'à l'étape 4, incluse.

Pour authentifier et protéger contre la répétition le paquet actuel, le traitement est le suivant :

D'abord, vérifier si le paquet a été répété (conformément au paragraphe 3.3 de la [RFC3711]). Noter, cependant, que la liste de répétitions SRTP contient les indices SRTP des paquets reçus récemment qui ont été authentifiés par TESLA (c'est-à-dire que les mises à jour de liste de répétition NE DOIVENT PAS se fonder sur le MAC SRTP). Si le paquet est jugé être répété, il DOIT être éliminé, et l'événement DEVRAIT être enregistré.

Ensuite, effectuer la vérification de l'étiquette de protection d'intégrité SRTP (pas du MAC TESLA) si elle est présente, en utilisant le compteur de débordement provenant du paquet courant, l'algorithme d'authentification indiqué dans le contexte cryptographique, et la clé d'authentification de session. Si la vérification échoue, le paquet DOIT être éliminé sans autre traitement, et l'événement DEVRAIT être enregistré.

Si la vérification réussit, retirer et mémoriser le MKI (si il est présent) et les champs d'étiquette d'authentification du paquet. Le paquet est mis en mémoire tampon, en attendant la divulgation de la clé TESLA dans un paquet suivant.

L'authentification TESLA est effectuée sur un paquet quand la clé est divulguée dans un paquet suivant. On rappelle qu'une clé pour l'intervalle i est divulguée durant l'intervalle i+d, c'est-à-dire, la même clé est divulguée dans les paquets envoyés sur d intervalles de longueur t_int. Si l'identifiant d'intervalle i provenant du paquet (paragraphe 4.1) a avancé de plus de d intervalles depuis la plus forte valeur de i reçue jusqu'alors, des paquets ont été perdus, et une ou plusieurs clés DOIVENT être calculées comme décrit au paragraphe 3.2, second alinéa de la spécification TESLA [RFC4082]. Le calcul est effectué par récurrence pour toutes les clés divulguées perdues, depuis le nouvel intervalle reçu jusqu'au dernier intervalle reçu.

Quand une nouvelle clé divulguée est reçue ou calculée, on effectue la vérification TESLA du paquet en utilisant le compteur de débordement provenant du paquet, les paramètres de sécurité TESLA provenant du contexte cryptographique, et la clé divulguée. Si la vérification échoue, le paquet DOIT être éliminé sans autre traitement, et l'événement DEVRAIT être enregistré. Si la vérification TESLA réussit, retirer l'extension d'authentification TESLA du paquet.

Pour déchiffrer le paquet en cours, le traitement est le suivant :

Déchiffrer la portion chiffrée du paquet, en utilisant l'algorithme de déchiffrement indiqué dans le contexte cryptographique, la clé de chiffrement de session, et le sel (si il en est un utilisé) trouvé à l'étape 4 avec l'indice de l'étape 2.

(Noter que l'ordre de déchiffrement et la vérification TESLA ne sont pas obligatoires. Il est RECOMMANDÉ que la vérification TESLA soit effectuée avant le déchiffrement. Les concepteurs d'application TESLA peuvent choisir de mettre en œuvre des techniques de traitement optimiste telles que la notification de résultat de vérification TESLA après le déchiffrement ou même après le traitement du texte source. La vérification optimiste sort du domaine d'application du présent document.)

Mettre à jour le compteur de débordement et le plus fort numéro de séquence, s_l, dans le contexte cryptographique en utilisant l'indice de paquet estimé de l'étape 2. Si la protection contre la répétition est fournie, mettre aussi à jour la liste de répétitions (c'est-à-dire que la liste de répétitions est mise à jour après que la vérification de l'authentification TESLA a réussi).

4.5 Format de paquet SRTCP

La Figure 3 illustre le format du paquet SRTCP quand TESLA est appliqué. L'extension d'authentification TESLA DEVRA être insérée avant le MKI et l'étiquette d'authentification. On rappelle de la [RFC3711] que dans SRTCP le MKI est FACULTATIF, tandis que le bit E, l'indice SRTCP, et l'étiquette d'authentification sont OBLIGATOIRES. Cela signifie que le MAC SRTP (externe) est OBLIGATOIRE aussi quand TESLA est utilisé.

Comme dans SRTP, la "Portion chiffrée" d'un paquet SRTCP consiste en le chiffrement de la charge utile RTCP du paquet RTCP composé équivalent, à partir du premier paquet RTCP, c'est-à-dire, depuis le neuvième (9) octet à la fin du paquet composé.

La "Portion authentifiée" d'un paquet SRTCP consiste en le paquet RTCP équivalent entier (éventuellement composé), le fanion E, l'indice SRTCP (après l'application de tout chiffrement à la charge utile) et l'extension TESLA. Noter que la définition est étendue de la [RFC3711] par l'inclusion de l'extension d'authentification TESLA.

On définit la "Portion TESLA authentifiée" d'un paquet SRTCP comme consistant en l'en-tête RTCP (8 premiers octets) et la portion chiffrée du paquet SRTCP.

Le traitement d'un paquet SRTCP est similaire à celui de SRTP (paragraphe 4.3) mais il y a des changements spécifiques de SRTCP décrits au paragraphe 3.4 de la spécification SRTP [RFC3711] et au paragraphe 4.6 du présent mémoire.

Figure 3 : format du paquet SRTCP quand TESLA est appliqué

Noter que quand des champs supplémentaires sont ajoutés à un paquet, cela va augmenter la taille du paquet et donc la taille moyenne de paquet RTCP.

4.6 MAC TESLA

Notons M' les données du paquet authentifié par TESLA. Dans le cas de SRTP, M' DEVRA consister en la portion authentifiée de SRTP TESLA (en-tête RTP et portion chiffrée SRTP ; voir la Figure 2) du paquet enchaînée avec le compteur de débordement (ROC) du même paquet : M' = ROC || portion authentifiée TESLA.

Dans le cas de SRTCP, M' DEVRA consister seulement en la portion authentifiée SRTCP TESLA (en-tête RTCP et portion chiffrée SRTCP).

L'étiquette normale d'authentification (FACULTATIVE pour SRTP, OBLIGATOIRE pour SRTCP) DEVRA être appliquée avec la même couverture que spécifiée dans la [RFC3711]. C'est-à-dire :

- pour SRTP : Portion authentifiée || ROC (avec la définition étendue de portion d'authentification SRTP comme au paragraphe 4.2).
- pour SRTCP : Portion authentifiée (avec la définition étendue de portion d'authentification SRTP comme au paragraphe

4.2).

La transformation prédéfinie d'authentification dans SRTP, HMAC-SHA1 [RFC2104], est aussi utilisée pour générer le MAC TESLA. Pour SRTP (et respectivement SRTCP) le HMAC DEVRA être appliqué à la clé dans la chaîne TESLA correspondant à un intervalle de temps particulier, et à M' comme spécifié ci-dessus. Le résultat HMAC DEVRA alors être tronqué aux n_m bits de gauche. Les valeurs par défaut sont à la Section 6.

Comme avec SRTP, l'algorithme prédéfini d'authentification HMAC-SHA1 PEUT être remplacé par un autre algorithme qui sera spécifié dans une future RFC Internet.

4.7 PRF

TESLA exige une fonction pseudo aléatoire (PRF) pour mettre en œuvre
* une fonction unidirectionnelle F(x) pour déduire la chaîne de clés, et
* une fonction unidirectionnelle F'(x) pour déduire (à partir de chaque clé de la chaîne) la clé qui est réellement utilisée pour calculer le MAC TESLA.

Quand TESLA est utilisé avec SRTP, le choix par défaut de la PRF DEVRA être HMAC-SHA1. Les valeurs par défaut sont à la Section 6.

D'autres PRF peuvent être choisies, et leur utilisation DEVRA suivre les lignes directrices de la [RFC3711] quand elles ajoutent de nouveaux paramètres de sécurité.

5. Amorçage et terminaison de TESLA

Les extensions au contexte cryptographique SRTP incluent un ensemble de paramètres TESLA dont la liste figure au paragraphe 4.3 du présent document. De plus, TESLA DOIT être amorcé à l'établissement de la session (pou l'échange de paramètres et l'engagement de clé initial) par un système régulier d'authentification des données (un algorithme de signature numérique est RECOMMANDÉ). Les procédures de gestion de clé peuvent prendre soin de cet amorçage avant le commencement d'une session SRTP lorsque l'authentification TESLA est utilisée. Le mécanisme d'amorçage sort du domaine d'application du présent document (il pourrait, par exemple, faire partie du protocole de gestion de clés).

Un facteur critique pour la sécurité de TESLA est que l'envoyeur et le receveur doivent être plus ou moins synchronisés. TESLA exige qu'une limite à la dérive d'horloge soit connue (D_t). L'utilisation de TESLA dans SRTP suppose que la synchronisation soit garantie par des schémas hors bande (par exemple, la gestion de clés). C'est-à-dire que cela n'est pas du domaine de SRTP.

On devrait aussi noter que TESLA a des exigences de fiabilité en ce qu'une clé est divulguée pour un paquet dans un paquet suivant, qui peut être perdu. Comme une clé dans un paquet perdu peut être déduite d'un futur paquet, TESLA est robuste à la perte de paquet. Ce flux de clés s'arrête cependant quand le flux de paquets porteur de clés de l'envoyeur des données s'arrête à la conclusion de la session RTP. Pour éviter cette fâcheuse condition limite, on envoie des paquets nuls avec les clés TESLA pour une période entière de divulgation de clé à la suite de l'intervalle dans lequel le flux cesse : des paquets "NUL" DEVRAIENT être envoyés pour d intervalles de durée t_int (points 8 et 9 du paragraphe 4.3). Le taux de paquets "NUL" DEVRAIT être le taux moyen du flux de supports de la session.

6. Paramètres par défaut de SRTP TESLA

Les procédures de gestion de clé établissent les paramètres de fonctionnement de SRTP TESLA, dont la liste figure au paragraphe 4.3 du présent document. Les paramètres de fonctionnement apparaissent dans le contexte cryptographique SRTP et ont les valeurs par défaut qui sont décrites dans cette section. À l'avenir, une RFC Internet POURRA définir d'autres réglages pour SRTP TESLA différents de ceux spécifiés ici. En particulier, on notera que les réglages définis dans le présent mémoire peuvent avoir un gros impact sur la bande passante, car ils ajoutent 38 octets à chaque paquet (quand les valeurs du champ Longueur sont celles par défaut). Pour certaines applications, cette surcharge peut représenter une augmentation de plus de 50 % à la taille du paquet. D'autres réglages pourraient chercher à réduire le nombre et la longueur des divers champs et résultats de TESLA. Aucune de ces optimisations n'est envisagée dans le présent mémoire.

Il es RECOMMANDÉ que le MAC SRTP soit tronqué à 32 bits, car le MAC SRTP assure seulement l'authentification de

groupe et sert seulement de protection contre les attaques de DoS externes.

Les valeurs par défaut pour les paramètres de sécurité sont mentionnées dans le tableau suivant.

Paramètre	**Prise en charge obligatoire**	**Par défaut**
PRF TESLA	HMAC-SHA1	HMAC-SHA1
Longueur de résultat binaire n_p	160	160
Longueur de résultat binaire n_f	160	160
MAC TESLA	HMAC-SHA1	HMAC-SHA1
Longueur de résultat binaire (tronqué) n_m	80	80

Comme montré ci-dessus, les mises en œuvre de TESLA DOIVENT prendre en charge HMAC-SHA1 [RFC2104] pour le MAC TESLA et la PRF TESLA. Le générateur de chaîne de clés TESLA est défini de façon récurrente comme suit [RFC4082].

K_i=HMAC_SHA1(K_{i+1},0), i=0..N-1

où N-1=n_c d'après le contexte cryptographique.

Le générateur de clé de MAC TESLA est défini comme suit [RFC4082].

K'_i=HMAC_SHA1(K_i,1)

Le MAC TESLA utilise un résultat tronqué de dix octets [RFC2104] et est défini comme suit.

HMAC_SHA1(K'_i, M')

où M' est comme spécifié au paragraphe 4.6.

7. Considérations sur la sécurité

Les attaques de déni de service (DoS, *Denial of Service*) sur l'authentification retardée sont discutées dans [PCST]. TESLA exige que le receveur mette en mémoire tampon avant l'authentification ; donc, le receveur peut subir une attaque de déni de service due à un flot de paquets bogués. Pour traiter ce problème, le MAC SRTP externe, fondé sur la clé de groupe, PEUT être utilisé en plus du MAC TESLA. La petite taille du MAC SRTP (32 bits par défaut) est motivée par le fait que ce MAC est purement pour la prévention de DoS provenant d'attaquants externes au groupe. L'étiquette de résultat plus courte signifie qu'un attaquant a de meilleures chances de faire accepter un paquet falsifié, qui sont d'environ 2^31 tentatives en moyenne. Comme première ligne de défense contre une attaque de déni de service, une étiquette courte est probablement adéquate ; une victime va probablement avoir l'évidence qu'il est soumis à une attaque avant d'accepter un paquet falsifié, qui va ensuite échouer à la vérification TESLA. La [RFC4082] décrit d'autres mécanismes qui peuvent être utilisés pour empêcher le DoS, à la place du MAC externe de clé de groupe. Si ils sont utilisés, ils doivent être ajoutés comme étapes de traitement (suivant les lignes directrices de la [RFC4082]).

L'utilisation de TESLA dans SRTP définie dans la présente spécification est soumise aux considérations de sécurité discutées dans la spécification SRTP [RFC3711] et dans la spécification TESLA [RFC4082]. En particulier, la sécurité de TESLA dépend du calcul de la "condition de sûreté" comme définie au paragraphe 3.5 de la [RFC4082].

SRTP TESLA dépend de la sécurité effective des systèmes qui effectuent l'amorçage (synchronisation) et la gestion de clés. Ces systèmes sont extérieurs à SRTP et ne sont pas examinés dans la présente spécification.

La longueur du MAC TESLA est par défaut de 80 bits. La RFC 2104 exige que la longueur du MAC soit d'au moins 80 bits et au moins de la moitié de la taille du résultat de la fonction de hachage sous-jacente. La taille du résultat de SHA-1 est de 160 bits, de sorte que ces deux exigences sont satisfaites avec le MAC de 80 bits spécifié dans le présent document. Noter que les mises en œuvre de IPsec tendent à utiliser 96 bits pour leurs valeurs de MAC pour aligner l'en-tête sur une limite de 64 bits. Ces deux tailles de MAC sont très au delà de la portée des techniques courantes de cryptanalyse.

8. Remerciements

Les auteurs tiennent à remercier Ran Canetti, Karl Norrman, Mats Naslund, Fredrik Lindholm, David McGrew, et Bob Briscoe de leur aide précieuse.

9. Références

9.1 Références normatives

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

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

[RFC3711] M. Baugher et autres, "Protocole de transport sécurisé en temps réel (SRTP)", mars 2004. *(P.S.)*

[RFC4082] A. Perrig et autres, "Authentification de flux tolérante aux pertes en temps efficace (TESLA) : Introduction à la transformation d'authentification de source de diffusion groupée", juin 2005. *(Information)*

9.2 Références pour information

[PCST] Perrig, A., Canetti, R., Song, D., Tygar, D., "Efficient and Secure Source Authentication for Multicast", dans Proc. of Network et Distributed System Security Symposium NDSS 2001, pp. 35-46, 2001.

[RFC3547] M. Baugher, B. Weis, T. Hardjono et H. Harney, "Le domaine d'interprétation de groupe", juillet 2003. *(Obsolète, voir la* RFC6407)

[RFC3830] J. Arkko et autres, "MIKEY : Gestion de clé multimédia pour l'Internet", août 2004. (*MàJ par* RFC4738) *(P.S.)*

[RFC4046] M. Baugher et autres, "Architecture de gestion de clé de groupe de diffusion groupée sécurisée (MSEC)", avril 2005. *(Info.)*

Adresse des auteurs

Les questions et commentaires devraient être adressés aux auteurs et à msec@ietf.org .

Mark Baugher
Cisco Systems, Inc.
5510 SW Orchid Street
Portland, OR 97219 USA
téléphone : +1 408-853-4418
mél : mbaugher@cisco.com

Elisabetta Carrara
Royal Institute of Technology
Stockholm
Sweden
mél : carrara@kth.se

Déclaration complète de droits de reproduction

Propriété intellectuelle

Remerciement

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