Sécurité DIAMETER

EFORT
http://www.efort.com

1. Introduction

Le réseau Diameter est composé de l'ensemble des réseaux Diameter des opérateurs mobiles, reliés via des carriers internationaux ou des liaisons directes (interconnexion nationale). Tous les réseaux Diameter ne sont malheureusement pas sécurisés au même niveau et il arrive que certains noeuds de ce réseau Diameter soient reliés à l'Internet. Un attaquant ayant des connaissances techniques peut très bien via un réseau Diameter faiblement sécurisé et interconnecté via les carriers internationaux aux autres réseaux Diameter des autres opérateurs mener de telles attaques. Les opérateurs doivent donc mettre en oeuvre une politique de sécurité Diameter pour empêcher au maximum les attaques, de façon similaire à ce qui est mis en œuvre dans les réseaux de signalisation SS7/SIGTRAN afin de prévenir un grand nombre d'attaques (e.g., obtention de l'IMSI d'un usager, localisation de l'UE d'un usager, modification du profil d'un usager, SMS facking et spoofing dans le contexte SMS in MME, etc.). Le but pour un opérateur mobile est d'identifier les attaques DIAMETER, d'identifier comment les détecter et enfin de définir les mesures à mettre en œuvre pour les bloquer via notamment un firewall Diameter configuré avec des politiques de filtrage prenant en compte le plus grand nombre possible de scénarii d'attaques.
Le but de ce tutoriel est de présenter l'écosystème interconnecté Diameter notamment pour des raisons de roaming, présenter certains problèmes de sécurité liés au protocole Diameter et identifier des solutions aux problèmes.

2. Applications Diameter

Différentes architectures de réseau et de service mobiles utilisent Diameter et ses applications notamment :

- Evolved Packet Core qui représente le réseau Coeur 4G (Applications S6a, S13)
- non-3GPP access to ePC pour accéder au réseau ePC via l'accès WiFi et notamment utiliser le service VoWiFi (Applications SWm, SWa, SWx, STa et S6b)
- Policy and Charging Control (Applications Gx, Gy, Gz, Sd, St, Sy, Ro, Rf, Rc, Re, Rx, S9, Gxa, Gxb, Gxc)
- SMS in MME afin que le SMS soit directement géré par le MME et non pas par le MSC quand le client est sous couverture 4G (Applications S6c, SGd, Gdd)
- Location based services pour permettre la localisation d'un UE depuis des plates-formes de service (Applications SLh, SLg)
- LTE-M/NB-IoT pour le support des devices IoT dans le contexte 4G (Tsp, S6m, S6n, S6t, Nt, T6a, T6ai, T7, Ns)
- IP Multimedia Subsystem pour offrir des services tels que VoLTE et VoWiFi (Applications Cx, Sh)
- GAA/GBA pour l'authentification de service sur la base de la carte SIM (Applications Zh, Zn)
- etc.

Plus de 130 interfaces (applications) basées sur Diameter ont été spécifiée par 3GPP.

Les applications Diameter candidates à l'interconnexion entre opérateurs sont :

- S6a entre MME visité et HSS nominal dans le contexte 4G
- S9 entre PCRF visité et PCRF nominal dans le contexte 4G
- SGd entre MME visité et SMSC nominal dans le contexte 4G
- S6c entre SMSC quelconque et HSS dans le contexte 4G
- SLh entre GMLC visité et HSS nominal dans le contexte 4G
- SLg entre GMLC nominal et MME visité dans le contexte 4G
- T7 entre IWK-SCEF et SCEF dans le contexte LTE-M/NB-IoT

3. Agent Diameter

Le protocole de base Diameter (IETF RFC 3588 puis la nouvelle version RFC 6733) définit la fonction des agents Diameter.
Diameter Exented NAPTR (IETF RFC 6408) définit des améliorations pour les mécanismes de routage de Diameter. Afin de prendre en charge l'évolutivité, la résilience et la maintenabilité et de réduire l'exportation des topologies de réseau, il est fortement recommandé d'utiliser un Diameter Edge Agent.
L'agent Diameter est appelé Diameter Edge Agent (DEA) et est considéré comme le seul point de contact entrant et sortant du réseau d'un opérateur mobile au niveau de l'application Diameter.
Le protocole de base Diameter définit quatre types d'agent Diameter, à savoir l'agent relai Diameter, l'agent proxy Diameter, l'agent de redirection Diameter et l'agent de traduction Diameter.
Pour la signalisation dans les situations de roaming LTE, seuls les agents relai, proxy et de traduction sont pertinents.

Un agent relai Diameter est une fonction spécialisée dans l'acheminement des messages Diameter
Un agent relai n'inspecte pas le contenu du message. Cela a pour conséquence que l'agent relai ne peut pas réaliser de filtrage de message sur la base du contenu, e.g., sur la base des AVPs (Attribute Value Pairs).
Lorsqu'un agent relai reçoit une requête Diameter, il la route aux autres nœuds Diameter sur la base d'informations présentes dans le message, e.g., Application ID et Destination realm. Une table de routage est balayée pour trouver le nœud Diameter qui correspond au prochain saut.
Un agent relai ne connaît pas les applications qu'il route; il maintient l'état de la transaction afin que la réponse suive le même chemin que la rquête, mais ne maintient pas l 'état de la session.

Un agent proxy Diameter inclut les fonctions de l'agent relai Diameter en plus des fonctions suivantes :
Un proxy Diameter peut traiter les AVPs non liés au routage. En d'autres termes, un proxy Diameter peut traiter des messages pour certaines applications Diameter.
Un proxy Diameter peut inspecter le contenu réel du message pour réaliser des politiques (e.g., masquage de la topologie)
Un proxy Diameter connaît les applications qu'il route. il conserve l'état de la transaction et peut garder l'état de la session.

Un agent de traduction Diameter réalise la traduction entre deux protocoles (e.g. RADIUS et Diameter, MAP et Diameter, CAP et Diameter). Il peut être utilisé pour réaliser des scénarii d'interfonctionnement.
Selon sa table de routage, un DEA peut jouer le rôle de proxy pour certaines applications Diameter (i.e., ajouter/supprimer/modifier des AVP, inspecter des AVPs, etc.) et jouer le rôle de relai pour toutes les autres applications (i.e., route les messages sur la base des informations Application ID et Destination realm). Toutefois, chaque élément de réseau Diameter peut uniquement se déclarer comme un seul type d'agent à chacun de ses peers Diameter.
Il est recommandé que le DEA affiche l 'Application ID relai aux agents des carriers internationaux (agents externes). En utilisant le mode relai, le routage entre réseaux est indépendant des applications internes. Le DEA est libre d'afficher le rôle proxy aux peers Diameter internes, et le DEA peut réaliser le filtrage pour les applications internes et externes.
Il est donc recommandé que tout DEA soit capable de jouer le rôle de relai ou proxy pour toutes les applications prises en charge par l'opérateur mobile en interne vers les nœuds de destination internes ou les agents internes.
Si le DEA agit uniquement en tant qu'agent relai, des mesures de protection doivent être prises au niveau des nœuds de destination finale.

Toutefois, si les recommandations ci-dessus ne peuvent pas être implémentées par un opérateur mobile, ce dernier peut externaliser le déploiement d'un agent relai Diameter vers un carrier IPX via un agent Diameter IPX.
Il est fortement recommandé dans la spécification GSMA PRD IR.88 de déployer des proxys Diameter pour chaque application Diameter supportée par l'opérateur mobile.
Ils peuvent être implémentés à l'intérieur du domaine de l'opérateur mobile, à l'intérieur du DEA ou sous-traités au carrier IPX. Ceci afin de fournir des fonctionnalités telles que le contrôle d'admission / d'accès, le contrôle de politique et la prise en charge d'éléments d'information spéciaux (e.g., AVP).
L'agent DEA ou l'agent Diameter IPX peut également mettre en œuvre un masquage de la topologie afin d'empêcher que les noms d'hôte et les adresses des éléments de réseau soient exposés à des réseaux externes. La mise en œuvre du masquage de la topologie ne doit pas altérer d'autres fonctionnalités liées à la validation du chemin.

La figure 1 décrit l'architecture de signalisation Diameter en situation de roaming international.
Diameter Edge Agent (DEA) est une fonction de l 'agent Diameter qui joue le rôle d 'élément de frontière (border element) d 'un réseau EPS (Evoled Packet System) pour la signalisation Diameter. Il est fortement recommandé aux opérateurs de ne pas exposer les éléments ePC aux réseaux externes pour des raisons de sécurité.
Parmi les fonctions des DEAs, figurent la capacité de cacher la topologie ePC, notamment MME, HSS, PCRF et 3GPP AAA Server, la capacité d'analyser le contenu des commandes Diameter (AVPs), et la capacité de réaliser un partage de charge de la signalisation Diameter sur un ensemble de ressource d 'un pool (si possible).
La fonction DEA est généralement implantée dans les réseaux EPS des opérateurs mobiles, à moins que l'opérateur mobile ne dispose pas d'agent dans son réseau EPS, auquel cas, il peut s'appuyer sur la fonction DEA proposée par son HUB international.
La fonction DEA requiert un rôle de Proxy Agent dans le réseau mobile afin d'être capable de cacher la topologie du réseau ePC et un rôle de relai vis-à-vis des carriers intrnationaux.
Diameter Routing Agent (DRA) a pour rôle de réaliser le routage des commandes Diameter à l'intérieur d 'un réseau, avec des capacités de partage de charge pour différentes applications Diameter et pour différents domaines (Realms) internes.
Il est reconnu qu'au niveau international, les mêmes critères de routage et de fonctionnalités sont requis de la part des HUB internationaux afin de fournir la connectivité entre réseaux d'opérateurs mobiles qui disposent d'accords de roaming.
En particulier, les HUB internationaux qui sont des fournisseurs IPX doivent adresser et connecter différents réseaux d'opérateurs mobiles, ce qui signifie un ou plusieurs domaines (Realms) Diameter qui leurs sont associés.

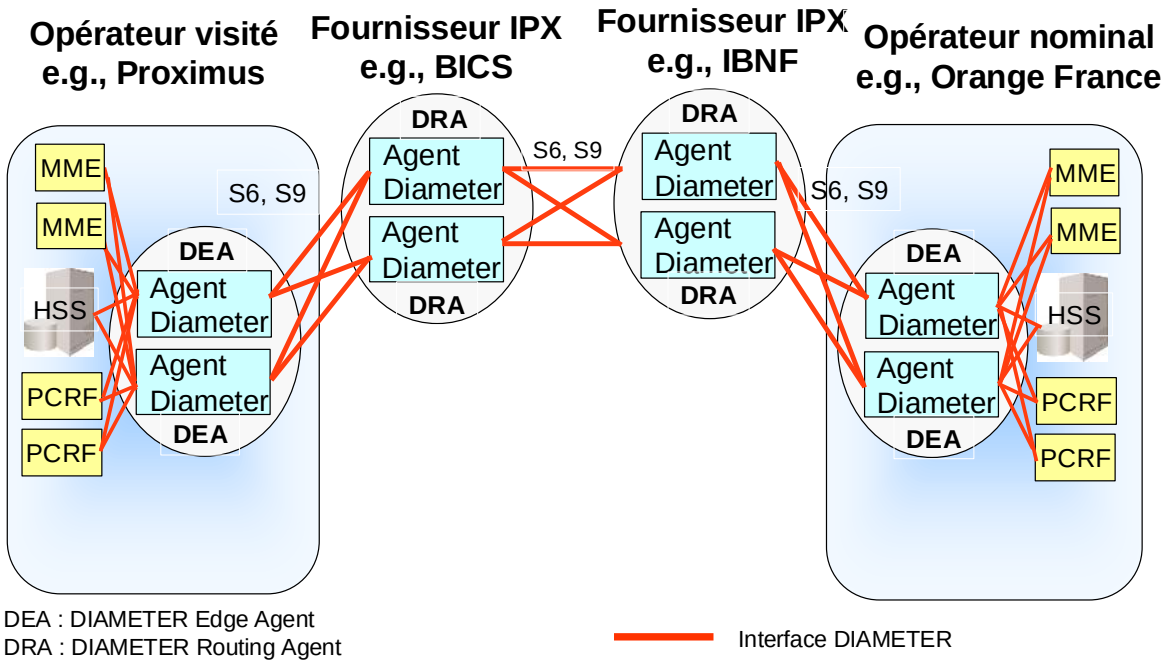


Figure 1 : Roaming international avec des agents Diameter

L'idée de remplacer un grand nombre d'accords de roaming bilatéraux par un nombre M d'accords avec des fournisseurs de roaming virtuel qui sont des aggrégateurs interesse de nombreux opérateurs mobiles.
Le 'Virtual Roaming Hub' est un système qui fournit les services de roaming entre deux opérateurs A et B qui ne disposent pas directement d'accords de roaming entre eux.
A la figure 2, le petit opérateur mobile XYZ via le service Roaming HUB LTE de l'opérateur IPX BICS peut prendre en charge des clients Orange France en roaming alors que cet opérateur XYZ n 'a pas signé d'accord de roaming bilatéral avec Orange France.
La commande Diameter Update Location Request (ULR) est émise par le réseau XYZ au Roaming Hub qui a le réseau d'Orange France parmi ses réseaux enregistrés.
Le Roaming Hub a sa propre adresse dans le réseau de signalisation Diameter et doit disposer d'un accord de roaming avec l'opérateur XYZ et d 'un accord de roaming avec l 'opérateur Orange France.
Le principe réside dans le fait que toutes les commandes Diameter qui normalement devraient être échangés entre les opérateurs XYZ et Orange France soient délivrées au 'Roaming Hub'.
La commande Diameter UPDATE LOCATION REQUEST(1) est relayée de l'opérateur XYZ via le Roaming Hub à Orange France.
L'opérateur Orange France considère que son client est pris en charge par le Roaming Hub avec lequel il a un accord de roaming et non pas par l'opérateur XYZ.

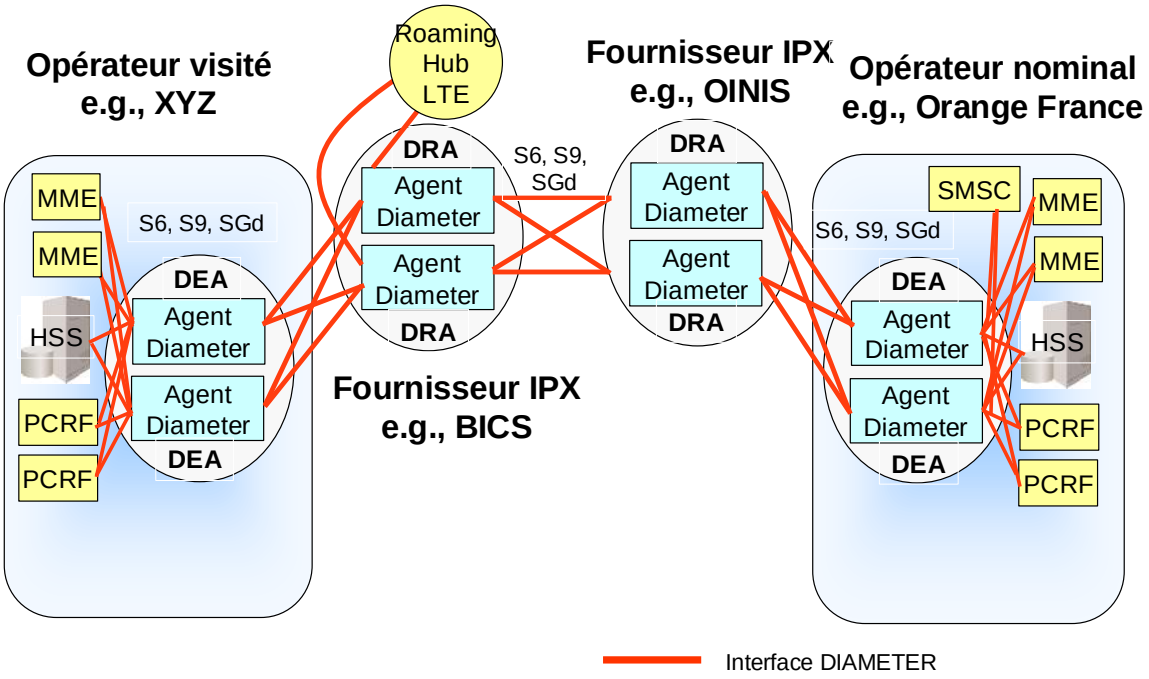


Figure 2 : Service HUB IPX : Signalisation Diameter dans le contexte Roaming LTE

Etablissement de la connexion Diameter
Avant toute tentative d'attaque, une connexion doit d'abord être établie entre l'attaquant et le DEA en utilisant les commandes CER (Capability Exchange Request) et CEA (Capability Exchange Answer).
L'établissement de la connexion peut être configuré pour accepter uniquement les peers connus et disposer d'une table de peer pour le routage, ou pour accepter des peers inconnus (découverte des peers).
Si le DEA est configuré pour accepter des peers inconnus, l'attaquant a juste besoin d'établir une connectivité IP avec le DEA.
Les raisons d'accepter des peers inconnus pourraient être :

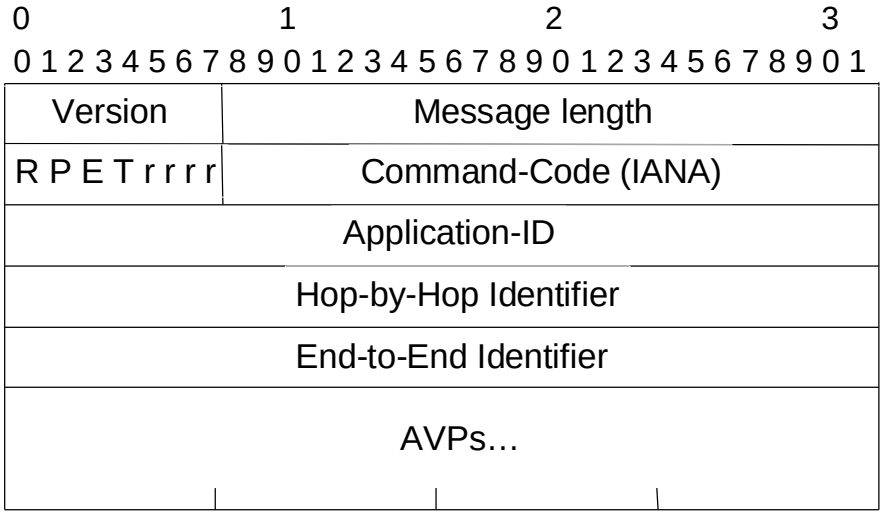
- Une mauvaise configuration du DEA
- Une plus grande simplicité pour traiter les demandes de connexions DIAMETER de nouveaux peers; et / ou
- Revente de la connectivité IPX.

La table de peers ne contient que les peers directement connectés (par exemple d'autres DEAs). Tous les routages doivent utiliser des adresses IP statiques et des peers connus.
Certains nœuds Diameter (par exemple MME) peuvent avoir des tables qui définissent quels messages peuvent être reçus et lesquels sont autorisés à être envoyés.
Par exemple, un MME peut être configuré uniquement pour envoyer des commandes CER et pour rejeter toute commande CER entrante quel que soit le nœud émetteur.
Une telle table rend plus difficile pour un attaquant la possibilité d'établir directement une connexion à un nœud (e.g., à partir d'un nœud interne compromis, en contournant le DEA) et fournit un moyen de filtrage plus efficace.
En outre, ce type de configuration est recommandé dans le cas où le DEA ne fournit pas de filtrage, ce qui signifie que la sécurité doit être appliquée directement au niveau MME.

4. Format de commande Diameter

Le protocole Diameter comprend un protocole de base qui définit le format du PDU, quelques primitives, et des services de sécurité de base. Le PDU est structuré en AVP

(Attribute Value Pair), les 256 premiers AVPs étant réservés pour faciliter la migration de RADIUS à Diameter.
Une commande Diameter (requête ou réponse Diameter) consiste en un en-tête de taille fixe (20 octets) suivi par un nombre variable d'AVPs. Le format du message est montré à la figure 3.
- Le champ « Version » indique le numéro de version de DIAMETER. La valeur de ce champ est positionnée à 1.
- Le champ « Message Length » indique la longueur totale du message en octets.
- Le fanion de commande spécifie 4 bits R, P, E et T:
R : Le bit R signifie « Request ». Il indique si le message est une requête ou une réponse. 1 Request; 0=Réponse.
P : Le bit P signifie Proxiable. Il indique si le message peut être routé par un agent proxy ou un agent relai ou un agent de redirection (P=1) ou s'il doit être traité localement (P=0).
E : Le bit E signifie Error. Il indique si le messafe contient des erreurs protocolaires ou sémantiques. Lorsque la requête génère une erreur protocolaire, le message de réponse est retourné avec sont bit E positionné à la valeur 1 indiquant une erreur protocolaire.
T : Le bit T signifie reTransmitted. Il indique si le message a été retransmis suite à un failover ou est utilisé pour supprimer à la réception des messages dupliqués.
r(eserved) - Les bits r sont réservés pour usager futur. Ils sont positionnés à 0 et ignorés par le récepteur.
- command-code (4 octets) est utilisé pour communiquer la commande associée au message. Chaque message Diameter doit contenir un code de commande afin que le récepteur sache identifier l'action à réaliser pour chaque message.
- Application-ID (4 octets) identifie l'application spécifique à laquelle appartient le message, tel que Mobile IP, Accounting, etc.
- Hop-by-hop identifier : transporte un identificateur utilisé afin d'associer la requête et la réponse sur ce saut (hop). L'émetteur de la réponse doit s'assurer que la valeur de cet identificateur est la même que celle présente dans la requête correspondante.
- End-to-end identifier : Est utilisé afin de détecter des messages dupliqués. L'identificateur dans la réponse doit être identique à celui de la requête correspondante. L'identification doit être unique pour au moins 4 minutes. Cet identificateur ainsi que l'AVP Origin-Host (décrit plus tard) sont utilisés ensemble afin de détecter des duplications de message. Une requête dupliquée ne doit pas conduire à l'envoi de deux réponses.



R=Request bit, P=Proxiable bit, E=Error bit, T=reTransmission bit
AVP = Attribute Value Pair
The Diameter application identifier assigned to the S6a/S6d interface application is 16777251

Figure 3 : Format d'une commande Diameter

Le **Hop-by-hop Identifier** est un identificateur de saut d'une longueur de 4 octets.
Ce champ permet de numéroter les messages à chaque relai ou proxy.
Un numéro est choisi au hasard par l'entité qui fait transiter une requête. Le numéro laissé par l'entité précédente dans le message est sauvegardé par l'agent et remplacé par son propre ID. Ce processus se répète tout le long du chemin. Le serveur qui répond à la requête, reprend le même numéro pour la réponse. Ainsi, les relais voient transiter les réponses avec les numéros attendus. Pour poursuivre la chaîne, ils remettent l'ID de leur prédécesseur qu'ils avaient mémorisé.
Considérons l'exemple présenté à la figure 4 :

- Un message arrive avec un ID Hop-By-Hop égal à 1.
- Le premier agent Relai/Proxy sauvegarde l 'ID présent dans la requête et le remplace par le sien (ici le 3). Le même processus se répète à chaque agent relai/proxy.
- Le second agent Relai/Proxy sauvegarde l ' ID présente dans la requête (ID = 3) et le remplace par le sien (ici le 4).
- Le serveur reprend le dernier ID Hop-By-Hop placé dans la requête et l'insère dans la réponse (ID = 4)
- Le second agent retrouve dans sa table des requêtes l'ID qui correspond à la réponse qui vient d'arriver. Il remet l'ID d'origine et fait transiter le message (remplacement de l 'ID = 4 par l 'ID = 3).
- Le premier agent retrouve dans sa table des requêtes l'ID qui correspond à la réponse qui vient d'arriver. Il remet l'ID d'origine et fait transiter le message (remplacement de l 'ID = 3 par l 'ID = 1).

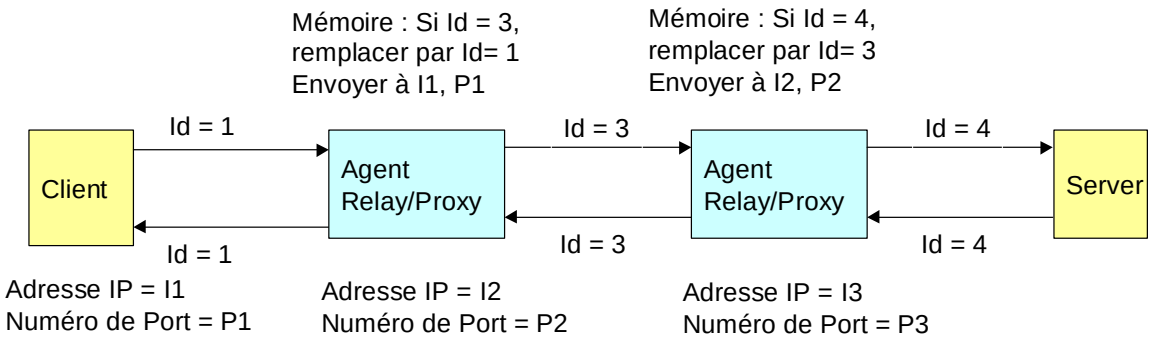


Figure 4 : Fonctionnement du Hop-by-hop identifier

5. Problème de sécurité du routage saut par saut Diameter

La figure 5 présente le problème de sécurité du routage saut par saut Diameter.
Le premier diagramme qui correspond au scénario nominal présente un identifiant de l'émetteur avec Origin-Realm et Origin-Host qui n'est pas falsifié.
Comme indiqué sur le premier diagramme, le HSS (ou tout autre nœud Diameter de la chaîne de la requête) pourrait facilement rejeter la demande en fonction de l'analyse de l 'AVP Origin-Realm, c'est-à-dire que l 'Origin-Realm ne figure pas sur une liste autorisée de partenaires autorisés pour cette requête.
Le second diagramme qui correspond au scénario frauduleux présente un identifiant de l 'émetteur falsifié (faked) et un Origin-Realm et Origin-Host valides sont utilisés. L'attaquant pourrait utiliser un Origin-Realm et un Origin-Host d'un partenaire valide du MNO attaqué (par exemple, un partenaire de roaming connu sur un site web). Le HSS répondra à la requête Diameter lorsque l'origine de la demande est autorisée (c'est-à-dire sur la liste des partenaires autorisés), ce qui serait le cas si l'identité d 'un partenaire était utilisée. La procédure de routage réelle enverrait alors la réponse à l'attaquant et non pas au partenaire et ce via l'utilisation du Hop-by-hop identifier.

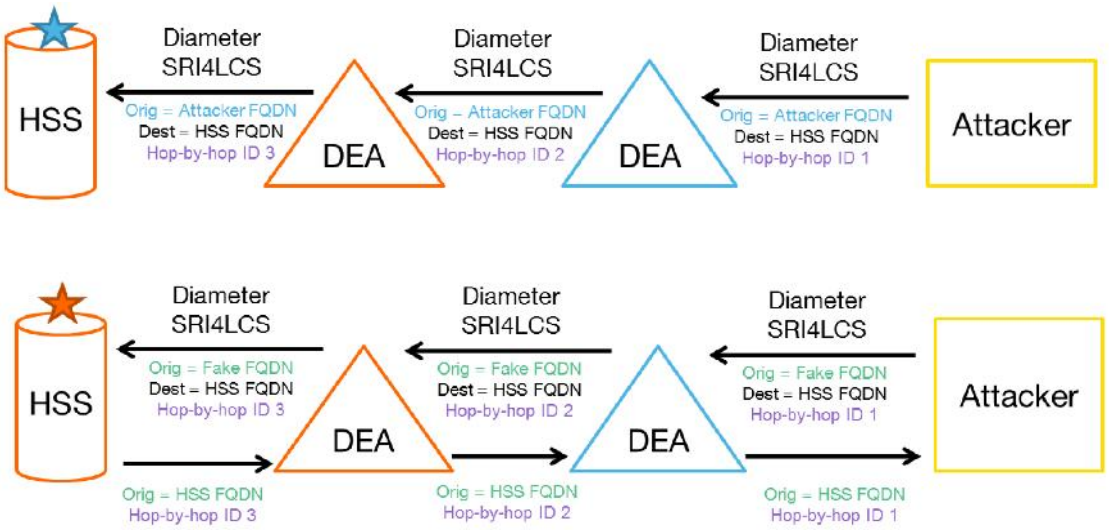


Figure 5 : Problème de sécurité du routage saut par saut Diameter

6. Contre-mesures pour les problèmes de sécurité saut par saut Diameter

Le filtrage de l 'AVP Origin-Realm par le fournisseur de service Diameter fournit une solution au problème de sécurité saut par saut.
Le premier nœud Diameter sur le chemin de requête (i.e., agent DEA) doit implémenter des mécanismes anti-usurpation (anti-spoofing) pour toutes les applications Diameter.
Pour ce faire, le DEA doit au minimum implémenter une liste de peers autorisés pour chaque peer avec lequel il est connecté. Si un message sur une application est reçu avec un Origin-Realm qui ne fait pas partie de cette liste, la requête doit être rejetée avec une erreur configurable. L'utilisation d'une erreur Diameter commune est recommandée, par exemple, 5012. 5012: DIAMETER_UNABLE_TO_COMPLY. Cette erreur est renvoyée lorsqu'une demande est rejetée pour des raisons non spécifiées.
Le filtrage de l'AVP Origin-Realm doit être appliqué comme un contrôle fondamental pour filtrer les attaques les plus évidentes.

7. Filtrage DIAMETER

Le filtrage Diameter consiste à autoriser certains messages et connexions Diameter à l'intérieur d'une zone de sécurité (e.g., à l'intérieur du réseau nominal ou à l'intérieur d'un domaine bien défini et bien sécurisé) tel que:

- Adresse IP source ou adresse IP destination pour le message Diameter;
- Code de commande Diameter (également appelé souvent le type de message Diameter);
- ID d'application Diameter (correspondant à une interface spécifique définie comme 3GPP S6a, S9, S13, etc.);
- AVP tels que:
    - AVPs standard (Origin-Host et Origin-Realm);
    - AVPs spécifiques de messages (Requested-EUTRAN-Authentication-Info, AVP 1408); ou
    - AVP propriétaires.

Le filtrage spécifique Diameter peut faire partie de la fonctionnalité d'un nœud existant ou d'un ajout sur une interface.

La formation EFORT « Sécurité dans les Réseaux de Signalisation SS7, SIGTRAN et Diameter » décrit les problèmes de sécurité relatifs aux réseaux de signalisation SS7, SIGTRAN et Diameter et décrit la mise en œuvre de firewall pour le filtrage du trafic de signalisation, notamment MAP, CAP, ISUP et Diameter. La formation décrit toutes les règles de filtrage requises et leur intégration dans les firewalls de signalisation.

Références

RFC 6733, Diameter Base Protocol, October 2012.
FS.19, Diameter Interconnect Security, Version 1.0, 14 December 2016