

## Clavister une solution globale de la sécurisation de la VoIP

Clavister Security Gateway, avec son module SIP ALG qui pallie aux failles du protocole SIP, ajouté à l'aspect sécurisé de sa QoS, et à la redondance de ses équipements, apporte aux *services de Voix sur IP (IPBX) une fiabilité équivalente aux PABX classiques*.

Poissy, Novembre 2008

La plupart des sociétés utilisent la téléphonie IP sur leurs propres réseaux privés ce qui leur permet de mieux gérer les contraintes qualité de service et sécurité. Mais de nombreux risques sont associés à la Voip,

Les protocoles SIP et RTP ne cryptent pas les communications incluant les paquets de signalisation, les flux voix, les numéros de téléphones (URI : Uniform Resource Identifiers), ou tout autre paramètre transporté par les messages SIP. Toutes ces données peuvent être collectées avec un simple sniffer. Les hackers ont de nombreuses possibilités d'exploiter les systèmes de téléphonie sur IP (VoIP) tant que ces paramètres de sécurité ne seront pas implémentés dans le service VoIP.

Les clients et les fournisseurs d'accès VoIP sont donc vulnérables à plusieurs tentatives d'attaques basées sur l'usurpation d'identité contre les services de téléphonie standard et cellulaire. Les objectifs des hackers sont les mêmes ; le vol d'information et d'identité mais aussi l'utilisation frauduleuse des services de VoIP. Plusieurs attaques se concentrent sur les points finaux. Les systèmes d'opérations (OS), les protocoles Internet, les applications et les interfaces d'administration des téléphones VoIP et des softphones s'exécutant sur les ordinateurs sont TOUS vulnérables à des accès frauduleux, à des virus et des vers, et à plusieurs attaques Déni-De-Service (DoS) qui exploitent les protocoles Internet standards et VoIP.

[Le module Clavister SIP ALG de la « Security Gateway » de Clavister répond aux nombreuses failles de sécurité qui doivent être prises en considération avant d'implémenter une solution VoIP.](#)

Il y a 3 types de problèmes de sécurité qui s'adressent au SIP ALG : attaques par messages SIP/SDP malformés, attaques par Buffer Overflow, et les attaques par piratage d'enregistrement. En complément de ces types d'attaques, le SIP ALG supporte également plusieurs mesures de sécurité qui permettent de mettre en place une installation VoIP très sécurisée, telle qu'une typologie réseau cachée, une segmentation réseau, et une inspection protocolaire.

### **Attaques par messages SIP/SDP malformés**

Le SIP ALG fournit une protection contre les messages SIP/SDP malformés, telle qu'une duplication des entêtes « From » et « To » ou un URI (Uniform Resource Identifiers) malformé. De plus, le SIP ALG valide les paquets SIP décomposés. Par exemple, le SIP ALG valide les paramètres d'authentification, les noms de domaine (FQDN), les adresses IP, les ports, etc. Il y a également des contrôles contrôlant le nombre maximum d'entête MAX-FORWARD pour que cette valeur ne soit pas compromise, et pour que l'entête EXPIRES ne soit pas invalide, etc. Lors de la détection d'un message SIP invalide, le Clavister Security Gateway informera l'utilisateur en lui envoyant un message d'erreur SIP.

### **Attaques par Buffer Overflow**

Un buffer overflow (ou dépassement de mémoire) est un exploit sur un programme à l'écoute d'une requête utilisateur. Par exemple : Un programme est en attente de l'entrée des informations d'un utilisateur telles que son nom. Plutôt que de renseigner son nom, le hacker lance une commande exécutable qui atteint la mémoire allouée dans la pile où les informations utilisateurs sont stockées. La commande est dans la plupart des cas « très courte ». Dans un environnement Linux, par exemple, la commande est typiquement EXEC("sh"), qui dit au système d'ouvrir une fenêtre de commandes, appelée « root shell ». Cette commande permet au hacker d'avoir le contrôle complet du système d'opération.

Il est vital d'un point de vue sécurité de se protéger contre les attaques de ce type. Pour contrer ce type d'attaques, le SIP ALG alloue uniquement la taille mémoire requise et restreint la taille de chaque paramètre à 1024 octets. La taille globale d'un message SIP est limitée à 6048 octets et du SDP à 4000 octets. Pour ce type de violation, le Clavister Security Gateway informera l'utilisateur envoyant un message

## Registration Hijacking

Le type d'attaque, connu sous le nom «Registration Hijacking », consiste à récupérer, après plusieurs tentatives, le mot de passe d'un utilisateur connu. Le SIP ALG compte le nombre de tentatives échues lors des requêtes d'authentification des utilisateurs. Une fois que le seuil est atteint, les requêtes d'enregistrement suivantes seront refusées et blacklistées pendant un certain temps. Cela permettra de bloquer toutes tentatives de vol de mot de passe d'utilisateur connu.

## Protection DoS

Un déni de service (attaque DoS) en général, les attaques DoS s'exécutent en :

- Forçant l'ordinateur cible à redémarrer, ou à utiliser ses ressources de telle sorte à ce qu'il ne puisse plus fonctionner comme souhaité.
- Fermant la communication entre les utilisateurs et la machine victime, ce qui implique qu'ils ne peuvent plus communiquer de façon adéquate.

Le Clavister Security Gateway supporte plusieurs stratégies pour éviter les attaques DoS ainsi que les attaques distribuées, appelées DDoS.

## Dissimulation de la Topologie

Un autre aspect important de la sécurité est la dissimulation de la topologie réseau. Le SIP ALG permet de le faire grâce au NAT (Network Address Translation). Le protocole SIP contient énormément d'informations concernant la couche applicative, telles que les adresses IP et les ports utilisés. Ces informations sont très sensibles et doivent donc être « gardées en sécurité » !

## Segmentation Réseau

Etant donné que le réseau VoIP est une pièce cruciale de l'infrastructure d'une société, il est conseillé de construire un réseau séparé pour le réseau VoIP. En utilisant des VLANs (Réseaux LANs virtuels), on peut conserver la même segmentation sans avoir à utiliser (ou rajouter) de nouvelles interfaces physiques. Clavister supporte complètement les VLANs et offre les mêmes fonctionnalités que les interfaces physiques, ce qui rend l'administration très facile et très granulaire.

## Analyse protocolaire

Le module firewall (ou parefeu) dans le Clavister Security Gateway surveille les aspects sécurité de la couche réseau, c'est-à-dire l'identité des 2 points communicants, la source et/ou la destination des paquets, et les ports utilisés. Il s'agit d'un mécanisme de défense très efficace, mais le SIP ALG peut faire beaucoup mieux en analysant complètement les flux audio et/ou vidéo, à la recherche d'anomalies et en agissant selon les résultats.

**Le SIP ALG améliore fortement la sécurité imposée du protocole SIP, avec des risques minimisés de failles de sécurité et d'attaques.**

[En terme de Qualité de Service Clavister apporte une dimension très sécuritaire.](#)

De multiples solutions QoS se basent sur les applications, mais d'un point de vue sécurité, il est inconcevable que les applications, c'est-à-dire les utilisateurs, décident de la priorité de leur activité dans le réseau.

Clavister qui supporte le protocole Differentiated Services va plus loin et propose un service de QoS en appliquant des limites et des garanties au trafic réseau, plutôt que ce soit les applications et les utilisateurs qui les fixent eux-mêmes. La QoS Clavister est donc adaptée pour gérer la bande passante dans un réseau LAN, ainsi que dans une ou plusieurs zones d'étranglements (zone où le trafic est dense) dans un réseau MAN ou WAN par exemple.

La gestion du trafic fonctionne en :

- Appliquant des limites de bande passante, mise en attente des paquets qui dépasseraient les limites configurées, puis de les envoyer lorsque l'utilisation de la bande passante est plus faible.
- Rejetant les paquets si le buffer stockant les paquets est plein. Les paquets droppés seront « choisis » par les responsables de la gestion dans le réseau.
- Priorisant le trafic selon le choix de l'administrateur; si le trafic avec une priorité élevée augmente lorsqu'il y a beaucoup de trafic, les paquets avec une priorité faible seront temporairement stockés pour permettre un cheminement rapide des paquets avec priorité élevée.
- Fournissant des garanties de bande passante. C'est possible en allouant une certaine portion de la bande passante (montant garanti) aux paquets avec priorité élevée,.
- 

Clavister Security Gateway dispose d'un gestionnaire de bande passante dans son noyau, qui supporte les fonctionnalités clés suivantes : Gestionnaire Bande Passante basée sur des « pipes », Intégration avec des règles dans Clavister Security Gateway Prioritisation du Trafic et Limitation de Bande Passante, Groupage, Gestion Dynamique de la Bande Passante, Chaîne de « pipes » Intégration pour IPSec

**Avec la solution UTM de Clavister aucun matériel supplémentaire n'est nécessaire étant donné que tous les modules sont inclus dans le noyau Clavister Security Gateway. La mise en place de la VoIP n'entraîne donc**

**pas de coûts supplémentaires tout en préservant un haut niveau de Sécurité, de Qualité et de Fiabilité maximum**

## **A propos de Clavister**

Clavister AB est une entreprise suédoise privée qui développe des produits pour la sécurité des systèmes d'information. Son offre principale, Clavister Security Service Platform, est une plate-forme de sécurité intégrée qui surveille le trafic entrant et sortant sur un réseau et protège contre les intrusions, virus, vers, chevaux de Troie et attaques DoS. En plus de protéger les ressources critiques de l'entreprise, Clavister SSP bloque également l'utilisation indésirable du web. Elle ne nécessite qu'un service minimal, peut être gérée de manière centralisée, offre des possibilités de configuration exceptionnellement souples et, grâce à son évolutivité, s'adapte à toutes les situations, depuis les plus petits déploiements jusqu'aux réseaux d'opérateurs télécoms.

Clavister a été fondée en 1997. Son entité de recherche et développement est située à Örnköldsvik. Ses solutions sont vendues en Europe et en Asie au travers d'agences locales de Clavister qui supportent un réseau de distributeurs et revendeurs. Clavister offre également sa technologie en OEM à des industriels.

Pour plus d'informations, consultez le site <http://www.clavister.fr>.

<b>Information Clavister France</b>	<b>Information Presse</b>
<b>Roberto Correnti</b> Tél : 01 75 43 78 90 roberto.correnti@clavister.fr	<b>ITGS PR</b> <b>Bernard MOAL</b> Tél : 01 58 88 39 59 bmoal@itgspr.fr