| BTS SN opEC | TELECOMMUNICATIONS PROTOCOLE SSH SERVEUR ASTERISK | DR E5 |
|---|---|---|



# I. PRESENTATION RAPIDE DU SERVEUR SIP ASTERISK

## I.1. INTRODUCTION

Actuellement, tout le monde utilise la VoIP (Voice over IP) ou de la ToIP (Telephony over IP). Depuis plusieurs années, ce secteur est en pleine croissance grâce à deux composantes essentielles : les utilisateurs (grand public comme entreprises) qui sont en majorité séduits et les constructeurs/éditeurs qui investissent énormément pour proposer des offres les plus complètes possibles.

En 2002, le projet Asterisk sort au grand jour et fait son entrée dans un marché encore naissant. C'est un PBX (Private Branch eXchange) logiciel qui propose des fonctionnalités avancées pour une somme dérisoire car la (bonne) surprise est que sa licence GPL (donc projet libre et open-source). D'abord utilisé plus ou moins expérimentalement, il commence à convaincre peu à peu les entreprises de toute taille.

Asterisk est un serveur téléphonique IP (PBX-IP) open source capable de concurrencer des systèmes commerciaux tels que les Call Manager de Cisco System.

## I.2. PRESENTATION RAPIDE

Asterisk supporte pratiquement tous les protocoles de VoIP, fonctionne sous plusieurs plateformes (Linux, BSD, Windows et MacOSX) et est compatible avec la majorité des équipements de téléphonie numériques ou analogiques. Il a été conçu dans ce sens, pour pouvoir interfacer n'importe quel hardware ou software de téléphonie.
Créé à l'origine par Mark Spencer de la société américaine Digium Inc. (devenu le *sponsor* d'Asterisk), ce projet a fortement évolué grâce à la contribution de nombreuses personnes à travers le monde (esprit open source) : amélioration du code, création de documentation (tout utilisateur expérimenté est invité à créer des tutoriaux de prise en main rapide), support technique sur les forums, support financier.

Mais pourquoi le nom Asterisk ? Ce nom vient tout simplement du symbole éponyme * qui sous les environnements Unix joue le rôle de joker lors de la recherche ou de sélection de répertoires ou de fichiers.

Le principe de la VoIP permet de réduire les coûts téléphonique de l'entreprise (réseau convergé, capacité liaisons WAN utilisées, équipe technique unique) ou de l'utilisateur (utilisation d'Internet au lieu du réseau RTC ce qui réduit les coûts).

## I.3. FONCTIONNEMENT / DEFINITIONS

Asterisk fournit tous les services de base d'un PABX comme la connexion des postes entre eux (qu'ils soient locaux ou distants), messagerie unifiée, services Web intégrés (ex: annuaire, gestion salle de conférence, etc.), service de répondeur interactif (IVR), musique d'attente, interconnexion avec le réseau téléphonique public, etc.
Asterisk est basé comme le Cisco Call Manager sur le principe de canaux (Channels), de plan de numérotation (Dial Plan) et de contextes (search spaces pour le Cisco Call Manager).

Quand un appel arrive sur canal, par exemple le canal SIP, le but du PABX - grâce au plan de numérotation - est de trouver le canal de sortie qui peut être le même canal SIP dans le cas d'un appel en VoIP à l'intérieur du bâtiment, ce canal de sortie peut également être un des autres types de canaux géré par Asterisk. Les contextes servent à réduire (ou augmenter) les possibilités de sortie d'un appel. Cela peut par exemple servir pour autoriser les appels à l'international pour certains utilisateurs seulement, pour créer des services d'IVR (lors d'un appel sur un numéro, on fait appel à un contexte qui déroule le script du répondeur automatique, etc.).

Asterisk utilise de multiples canaux d'entrée/sortie qui peuvent être de type IP comme MGCP, IAX, SIP, H.323, skinny, etc. ou de type téléphonie classique avec entre autre Zap (FXS et FXO), ISDN (BRI et PRI).

## I.4. LE PROTOCOLE SIP

Protocole de signalisation de vidéo et voix sur IP qui est basé sur des messages en clair et fonctionnant sur le port 5600 en TCP et UDP.

## I.5. LE PROTOCOLE RTP

Le but de RTP et de fournir un moyen uniforme de transmettre sur IP des données soumises à des contraintes de temps réel (audio, vidéo, ...). Le rôle principal de RTP consiste à mettre en œuvre des numéros de séquence de paquets IP pour reconstituer les informations de voix ou vidéo même si le réseau sous-jacent change l'ordre des paquets.
Plus généralement, RTP permet :
- d'identifier le type de l'information transportée ;
- d'ajouter des marqueurs temporels et des numéros de séquence l'information transporte ;
- de contrôler l'arrivée à destination des paquets.

## I.6. LE PROTOCOLE IAX

C’est le protocole de signalisation de voix/ vidéo sur IP utilisé par Asterisk (Inter Asterisk eXchange). Ce protocole fonctionne sur le port 4569 en UDP et transporte à la fois les données (voix) et la signalisation. L’intérêt principal de ce protocole est d’être fait pour traverser le NAT (Network Address Translation) et qu’il est possible de créer des trunks IAX (trames sont marquées ou taggées pour que les commutateurs sachent à quel Vlan elles appartiennent) entre les serveurs dans lesquels les communications RTP sont multiplexées ainsi on économise les surcharges d'entêtes IP.

# II. LE PROTOCOLE SSH

## II.1. INTRODUCTION

Le protocole SSH (Secure SHell) a été mis au point en 1995 par le Finlandais Tatu Ylönen. Il s'agit d'un protocole permettant à un client (un utilisateur ou bien une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée : les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.
Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).
La version 1 du protocole (SSH1) proposée dès 1995 avait pour but de servir d'alternative aux sessions interactives (shells) telles que Telnet, rsh, rlogin et rexec. Ce protocole possédait toutefois une faille permettant à un pirate d'insérer des données dans le flux chiffré. C'est la raison pour laquelle en 1997 la version 2 du protocole (SSH2) a été proposée.
Secure SVell Version 2 propose également une solution de transfert de fichiers sécurisé (SFTP, Secure File Transfer Protocol). SSH est un protocole, c'est-à-dire une méthode standard permettant à des machines d'établir une communication sécurisée. A ce titre, il existe de nombreuses implémentations de clients et de serveurs SSH. Certains sont payants, d'autres sont gratuits ou open.

## II.2. FONCTIONNEMENT DE SSH

L'établissement d'une connexion SSH se fait en plusieurs étapes :
Dans un premier temps le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé (couche de transport sécurisée).
Dans un second temps le client s'authentifie auprès du serveur pour obtenir une session.

## II.3. MISE EN PLACE DU CANAL SECURISE

La mise en place d'une couche de transport sécurisée débute par une phase de négociation entre le client et le serveur afin de s'entendre sur les méthodes de chiffrement à utiliser. En effet le protocole SSH est prévu pour fonctionner avec un grand nombre d'algorithmes de chiffrement, c'est pourquoi le client et le serveur doivent dans un premier temps échanger les algorithmes qu'ils supportent.
Ensuite, afin d'établir une connexion sécurisée, le serveur envoie sa clé publique d'hôte (host key) au client. Le client génère une clé de session de 256 bits qu'il chiffre grâce à la clé publique du serveur, et envoie au serveur la clé de session chiffrée ainsi que l'algorithme utilisé. Le serveur déchiffre la clé de session grâce à sa clé privée et envoie un message de confirmation chiffré à l'aide de la clé de session. A partir de là le reste des communications est chiffré grâce à un algorithme de chiffrement symétrique en utilisant la clé de session partagée par le client et le serveur. Toute la sécurité de la transaction repose sur l'assurance qu'ont le client et le serveur de la validité des clés d'hôte de l'autre partie. Ainsi, lors de la première connexion à un serveur, le client affiche généralement un message demandant d'accepter la connexion (et présente éventuellement un condensé de la clé d'hôte du serveur) : Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)? Afin d'obtenir une session véritablement sécurisée, il est conseillé de demander oralement à l'administrateur du serveur de valider la clé publique présentée. Si l'utilisateur valide la connexion, le client enregistre la clé hôte du serveur afin d'éviter la répétition de cette phase. A l'inverse, selon sa configuration, le serveur peut parfois vérifier que le client est bien celui qu'il prétend être.
Ainsi, si le serveur possède une liste d'hôtes autorisés à se connecter, il va chiffrer un message à l'aide de la clé publique du client (qu'il possède dans sa base de données de clés d'hôtes) afin de vérifier si le client est en mesure de le déchiffrer à l'aide de sa clé privée (on parle de challenge).

## II.4. L’AUTENTIFICATION

Une fois que la connexion sécurisée est mise en place entre le client et le serveur, le client doit s'identifier sur le serveur afin d'obtenir un droit d'accès. Il existe plusieurs méthodes :
La méthode la plus connue est le traditionnel mot de passe. Le client envoie un nom d'utilisateur et un mot de passe au serveur au travers de la communication sécurisé et le serveur vérifie si l'utilisateur concerné a accès à la machine et si le mot de passe fourni est valide.
Une méthode moins connue mais plus souple est l'utilisation de clés publiques. Si l'authentification par clé est choisie par le client, le serveur va créer un challenge et donner un accès au client si ce dernier parvient à déchiffrer le challenge avec sa clé privée.

# III. LE PABX DAMALISK

Le PABX Damalisk utilisé dans la section est basé sur un serveur téléphonique Asterisk auquel est ajouté des fonctionnalités logicielles et matérielles.
Il est possible de s’y connecter au moyen d’un client SSH (carte SD dédiée).