# Best Practices for VoIP-SIP Security

| | |
|---|---|
| **Etat** | Document public HESSO |
| **Auteurs** | Alistair Doswald (HEIG), Prof. Juergen Ehrensberger (HEIG), Xavier Hahn (HEIG), Prof. Stefano Ventura (HEIG) |
| **Auteurs responsables** | Sébastien Contreras (EIG), Prof. Gérald Litzistorf (EIG) |
| **Date de création** | 27 avril 2006 |
| **Version** | 1.3 |
| **Dernière mise à jour** | 20 décembre 2006 |
| **Chemin intranet** | http://extratic.rcso.ch/Vadese/Security/WP6 |

# 1 Introduction

Ce document a pour objectif principal d'aider les responsables IT et administrateurs réseau dans la mise en œuvre d'une infrastructure VoIP *(Voice over IP)* et respecte la structure suivante :

**§2 Architecture**

Cette partie précise la terminologie utilisée (PBX, IPBX, IP-enabled PBX, …), tente une classification et propose 3 scénarios d'utilisation.

**§3 Principaux risques**

Ce paragraphe énumère les risques majeurs (*Denial of Service*, écoute clandestine, détournement du trafic, vols de services, …) qui doivent être évalués **avant** toute mise en œuvre.

Seule une analyse rigoureuse des risques peut garantir le succès de cette infrastructure VoIP appropriée aux besoins et au budget de l'utilisateur.

Les attaques relatives sont détaillées au §6

**§4 Eléments de sécurité**

L'arsenal des moyens techniques (segmentation, authentification, chiffrement, …) est présenté **bien que certaines mesures organisationnelles puissent donner des résultats satisfaisants à un coût différent.**

Voir §7 pour la liste de recommandations *Best Practices*.

**§5 Matrices Attaques - Solutions**

Cette matrice apporte une réponse technique du §4 à chaque risque identifié au §3

**§6 Attaques potentielles**

Suite du §3 qui contient la liste des techniques utilisées

**§7 Nos propositions de *Best Practices***

Suite du §4 qui explique le fonctionnement des divers systèmes de défense

**§8 Références**

Ce document est axé sur les protocoles SIP *(Session Initiation Protocol)* et RTP *(Real-Time Transport Protocol)*; alors que la méthodologie utilisée doit lui permettre de convenir à d'autres architectures basées sur des protocoles VoIP tels que H.323, MGCP, Skinny, …

Il se veut indépendant des plate-formes utilisées et ne traite, de ce fait, pas les méthodes spécifiques à un type d'équipement *(hardphone*, …*)*

Les méthodes de sécurisation non spécifiques à la VoIP ne seront pas développées dans ce document. Cependant, des liens vers d'autres documents de référence (*Best Practices*) sont inclus de manière à couvrir la sécurité de l'infrastructure VoIP dans son ensemble.

# 2 Architecture

## 2.1 Références VoIP-SIP

La bonne compréhension de ce *Best Practice* (BP dans la suite du document) nécessite la connaissance des bases de la VoIP, et plus particulièrement du protocole SIP. Le document [TutoSIP] mentionné en référence est un tutorial SIP permettant de comprendre les bases de ce protocole. Pour des informations plus détaillées, voir [IPTelCook].

## 2.2 Problématique

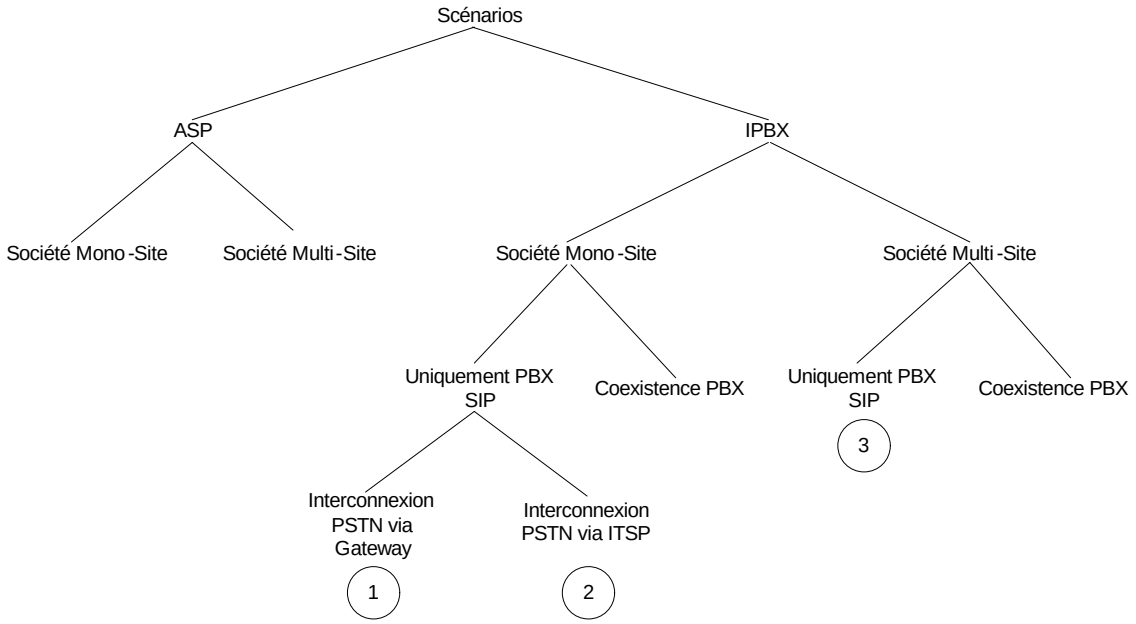
Nous proposons, face aux innombrables configurations possibles de réseaux VoIP, une **classification** basée sur des tendances observées dans l'utilisation des systèmes tels que :

- PBX : *Private Branch eXchange* (Autocommutateur téléphonique privé), installation privée de commutation pouvant transmettre la voix; elle est située dans les locaux de l'organisme utilisateur final et offre sur place la connexion entre les terminaux qui y sont branchés, y compris le service de composition, et peut assurer les connexions entre ces terminaux et d'autres réseaux de communication, y compris le PTSN[1].
- IP-PBX ou IPBX : *Internet Protocol PBX*, cette installation a toute les fonctions d'un PBX, mais fonctionne avec la communication IP par paquets. Pour SIP il s'agit du *proxy*, du *registrar* et du service de localisation.
- IP-enabled PBX : Un PBX hybride pouvant également s'interfacer avec un système VoIP
- IP Centrex : IP Centrex est un système ASP. L'IPBX est fourni par un tiers, avec éventuellement un *gateway* dans l'entreprise pour fournir le service aux appareils non-VoIP[2].
- *IP Phones* : Ce terme est utilisé lorsque l'on parle indifféremment de *hardphones* ou de *softphones*
- ASP *(Application Service Provider)* : Fournisseur de services

Un **premier niveau** de classification sépare les sociétés qui délèguent la problématique à un ASP tel que Cablecom en Suisse (désignés aussi comme des ITSP : *Internet Telephony Service Provider*) avec celles qui utilisent leur propre IPBX. Dans le premier cas, la situation est relativement simple étant donné qu'on ne trouve que des « SIPphones » dans l'entreprise, et donc la sécurisation ne se fera qu'au niveau de ces téléphones et de la connexion avec l'ASP. Les entreprises qui possèdent leur propre IPBX et du matériel SIP présentent une situation plus complexe.

[1] Définition pris sur http://www.crtc.gc.ca/dcs/frn/glossary.htm

[2] Cf. http://www.ip-centrex.org/whatis/index.html




Un **deuxième niveau** distingue les entreprises mono-site et multi-site. Bien que les emplacements individuels d'une entreprise multi-site puissent souvent être traités comme un cas mono-site, on ajoute les problèmes supplémentaires de la communication entre les sites et du plan de numérotation local. Il est aussi possible que certains sites utilisent des services VoIP qui ne sont pas implémentés en local, mais qui sont utilisés depuis d'autres sites (typiquement le site principal). Ce cas dans le scénario ASP multi-site n'est pas significatif, car les services relatifs aux services de téléphonie sont fournis par le *provider* lui même.

**Finalement**, parmi les entreprises qui possèdent leur IPBX, nous distinguons ceux qui avaient un système de téléphonie avec PBX, et qui l'ont gardé pour ne faire qu'une migration partielle vers la VoIP, et ceux qui n'utilisent plus que la VoIP. Pour ces derniers, il subsiste la question de la communication vers l'extérieur, qui peut se faire soit via un *gateway* vers le PSTN, soit par IP via un ITSP (*Internet Telephony Service Provider*).

De la figure ci-dessus, nous conservons 3 scénarios marqués par un cercle.

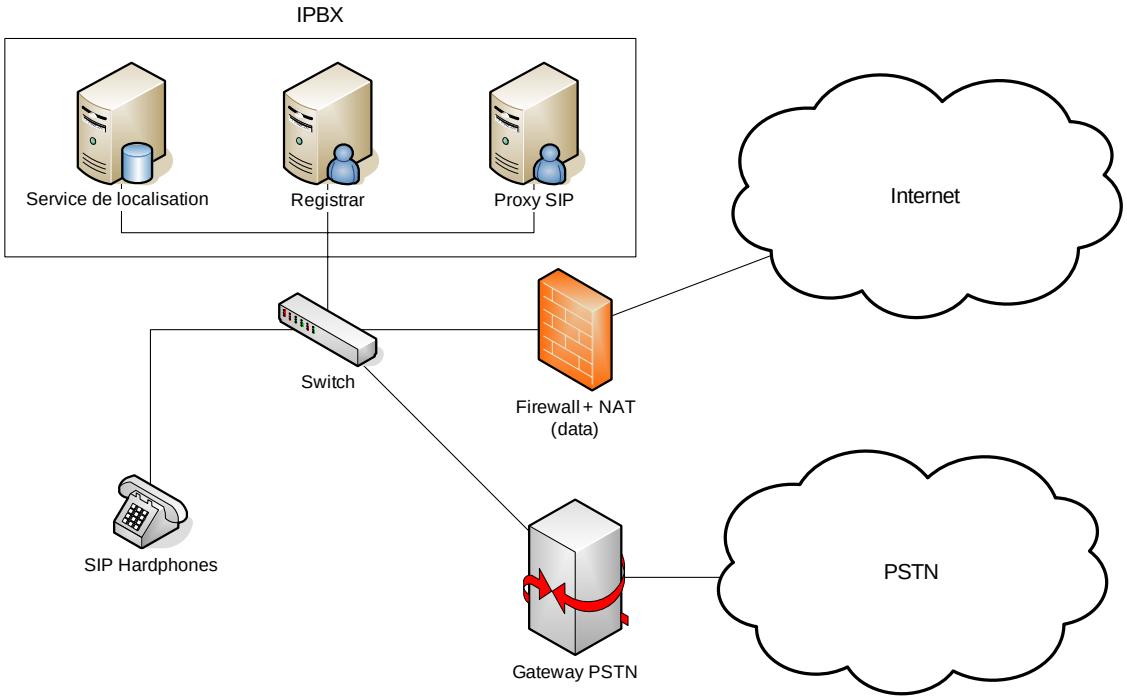
## 2.3 Scénarios

Les 3 scénarios suivants nous semblent représentatifs des architectures utilisées aujourd'hui.

### 2.3.1 Entreprise mono-site avec son propre IPBX, utilisant un *gateway* vers le PSTN pour ses communications vers l'extérieur

Dans cette situation, l'entreprise communique en interne via VoIP, mais ne désire pas que ses communications passent par *internet*. Le *firewall*+NAT et l'*internet* montrés ici ne concernent donc que les données traditionnelles, et non les donnés VoIP. Toute communication entrante ou sortante passe donc via le *gateway* sur le PTSN.

Scénario 1 : Entreprise mono-site avec son propre IPBX , utilise un Gateway PSTN pour ses communications externes




Cette situation est un bon exemple pour une entreprise qui désire profiter de la VoIP avec une communication gratuite au sein de l'entreprise, mais sans faire passer ses communications VoIP sur *internet*. L'avantage réside dans le fait que les conversations ne peuvent pas se faire intercepter en dehors du réseau de l'entreprise, et que l'entreprise à un contrôle total sur la sécurité de ses communications. Par contre l'utilisation d'un *gateway* présente quelques risques (comme le vol de service ou le *toll fraud*).

**Mesures de base à prendre pour sécuriser ce scénario (voir §7) :**

*IP Phones* : S.01, S.02, S.07, S.06, S.10 ou S.11, (S.12 et/ou S.13) ou S.14

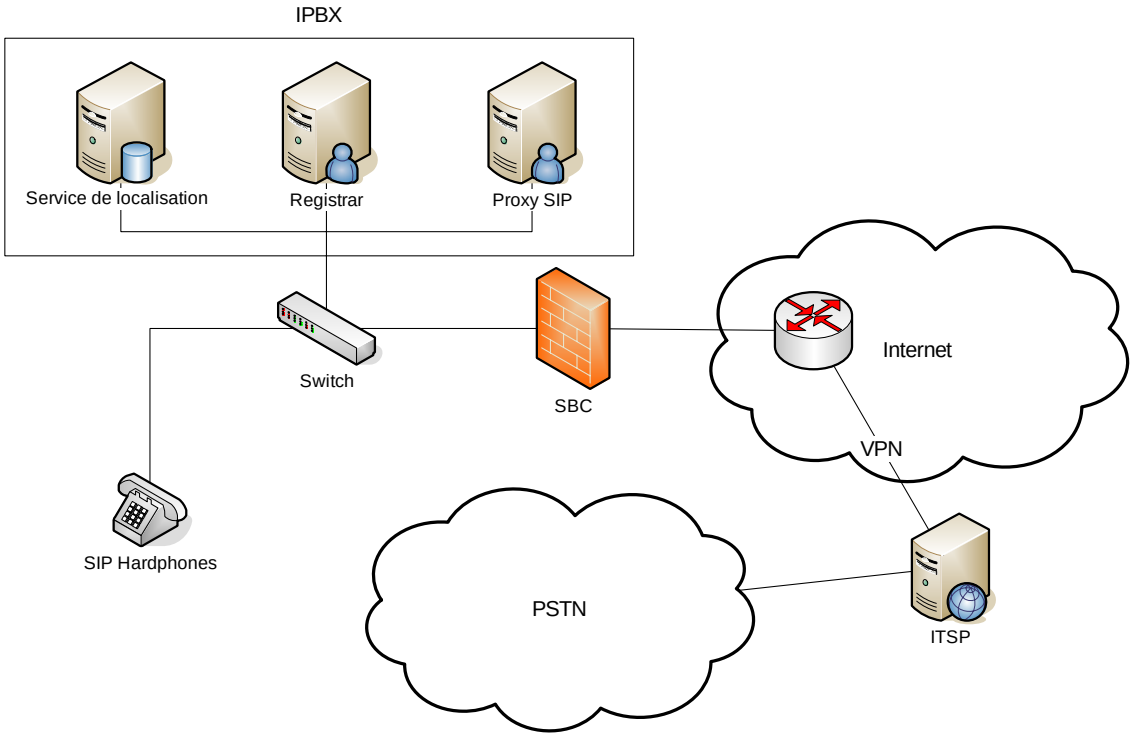
Réseau : S.03, S.04, S.05, S.08

IPBX : S.01, S.10 ou S.11, (S.12 et/ou S.13) ou S.14

### 2.3.2 Entreprise mono-site avec son propre IPBX, utilisant un ITSP pour ses communications vers l'extérieur

L'entreprise maintient tous les services VoIP locaux dans l'entreprise, mais fait partir toutes les communications sortantes vers un ITSP (c'est le proxy SIP qui s'en occupe). Cet ITSP devra prendre des décisions de routage, c'est-à-dire décider si le trafic doit continuer à passer sur *internet* ou bien passer sur le PTSN. Pour des raisons de haute disponibilité, l'entreprise peut disposer de serveurs (*proxy*, *registrar* et service de localisation) redondants.

Scénario 2 : Entreprise mono-site avec son propre IPBX , mais utilise un ITSP pour ses communications externes




Le facteur prix est un argument essentiel pour les entreprises qui désirent *router* leur communication VoIP via *internet*. Utiliser un ITSP peut réduire le coût des communications vers l'extérieur. Un inconvénient majeur de ce choix a pour conséquence que l'entreprise n'a aucun contrôle sur la sécurité et la QoS de ses communications entrantes et sortantes.

**Mesures de base à prendre pour sécuriser ce scénario (voir §7) :**

*IP Phones* : S.01, S.02, S.07, S.06, S.10 ou S.11, (S.12 et/ou S.13) ou S.14

Réseau : S.03, S.04, S.05, S.08

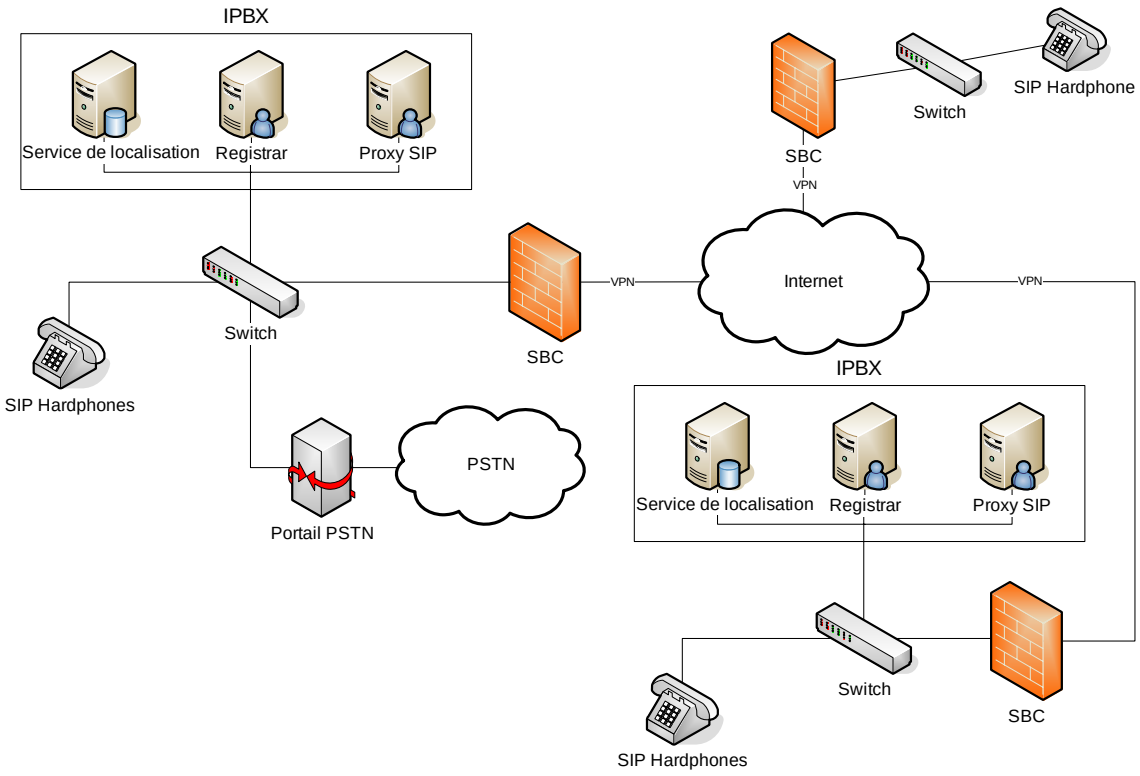
IPBX : S.01, S.10 ou S.11, (S.12 et/ou S.13) ou S.14

SBC : S.15

### 2.3.3 Entreprise multi-site avec un ou plusieurs IPBX, n'utilisant que SIP

Une entreprise multi-site doit avoir une solution pour faire passer ses communications d'un site à l'autre. La solution retenue utilise un réseau privé virtuel VPN (*Virtual Private Network*). Etant donné qu'un SVPN (Secure VPN) dégrade la communication, d'autres solutions de VPN sont recommandés. On voit bien dans cet exemple que certains sites doivent communiquer avec d'autre pour pouvoir utiliser certains services.

Scénario 3 : Entreprise multi -sites, certains sites doivent communiquer avec d'autres sites pour avoir accès à certains services (comme l'accès à l'extérieur )




Ce scenario est très similaire au premier étudié. Toutes les communications au sein de l'entreprise (quel que soit le site) sont gratuites, et il n'est pas nécessaire que tous les sites déploient du matériel coûteux pour profiter des différents services. De plus, si la communication inter-site est sécurisée, il n'y a pas plus de risque que dans un cas mono-site.

**Mesures de base à prendre pour sécuriser ce scénario (voir §7) :**

*IP Phones* : S.01, S.02, S.07, S.06, S.10 ou S.11, (S.12 et/ou S.13) ou S.14

Réseau : S.03, S.04, S.05, S.08

IPBX : S.01, S.10 ou S.11, (S.12 et/ou S.13) ou S.14

SBC : S.15

Connexion inter-site : utiliser un VPN

### 2.3.4 Services supplémentaires

Le ***softphone***, un téléphone SIP logiciel, est un élément problématique qu'on peut trouver dans certains réseaux. Il a le désavantage d'obligatoirement lier le réseau VoIP avec le réseau de donnés, et donc de rajouter toutes les vulnérabilités que l'on peut trouver dans un PC.

La **mobilité** va permettre à un employé (télétravailleur) d'utiliser le réseau téléphonique de l'entreprise via *internet* depuis chez lui ou encore depuis un hôtel alors qu'il est en déplacement. Cette communication doit être sécurisée, idéalement via VPN.

Des serveurs **ENUM**, de **redirection**, de **présence** ou de **conférence** peuvent être rajoutés dans des réseaux afin d'augmenter les fonctionnalités de la VoIP, ou permettre la messagerie instantanée. Le ***voice-mail*** ou un système de **réponse interactive** peut aussi être rajouté, mais ils ne sont pas nécessairement rajoutés au système VoIP. Il est possible pour un système qui utilise toujours un PBX que ces services y soient connectés.

Les services tels que **DNS**, **DHCP** et **NTP** ne peuvent être partagés avec le réseau DATA. Ils doivent posséder leurs propres serveurs sur le réseau VoIP (cf. p. 9 de [NsaGuid]).

Des serveurs **STUN** ou **TURN** (ou les deux, cf. § 4.5.2) peuvent être utilisés pour traverser le *firewall* et le NAT. Ces serveurs se situent hors du réseau protégé et risquent d'introduire de nouvelles vulnérabilités dans le réseau.

De manière générale il est recommandé d'avoir une certaine **redondance**. Ainsi il est possible qu'une entreprise dispose de plusieurs alternatives de transmission vers l'extérieur, ou même plusieurs *providers* en cas de problème. C'est aussi possible qu'une entreprise ait un *gateway* de secours en cas de panne pour pouvoir joindre les services d'urgence.

# 3 Principaux risques

L'énumération suivante propose un premier niveau de **classification** des principaux risques connus liés à l'utilisation de la VoIP en entreprise :

- **DoS**

  Attaques entraînant l'indisponibilité d'un service/système pour les utilisateurs légitimes.

- **Ecoute clandestine**

  Attaques permettant d'écouter l'ensemble du trafic de signalisation et/ou de données. Le trafic écouté n'est pas modifié.

- **Détournement du trafic**

  Attaques permettant de détourner le trafic au profit de l'attaquant. Le détournement peut consister à rediriger un appel vers une personne illégitime ou à inclure une personne illégitime dans la conversation.

- **Identité**

  Attaques basées sur la manipulation d'identité (usurpation, …).

- **Vols de services**

  Attaques permettant d'utiliser un service sans avoir à rémunérer son fournisseur.

- **Communications indésirées**

  Attaques permettant à une personne illégitime d'entrer en communication avec un utilisateur légitime.

Le tableau ci-dessous détaille ces risques avec la terminologie approprié.

Il précise dans la colonne de droite l'identifiant utilisé au § 6.1

| Catégorie | Sous-catégories | Méthode | Attaque |
|---|---|---|---|
| DoS | | | |
| | Interruption de la communication en cours | | |
| | | Spoofed messages | |
| | | | A.01 |
| | | | A.02 |
| | Empécher l'établissement de la communication | | |
| | | Spoofed messages | |
| | | | A.03 |
| | | Dégradation QoS | |
| | | | A.04 |
| | | | A.05 |
| | | | A.06 |
| | Rendre la communication inaudible | | |
| | | flux RTP parasite | |
| | | | A.07 |

| | | | |
|---|---|---|---|
| | Epuisement de resources | | |
| | | flooding | |
| | | | A.08 |
| | | | A.09 |
| Ecoute clandestine | | | |
| | Conversation | | |
| | | Reconstruction à partir des paquets RTP | |
| | | | A.10 |
| | | Déchiffrement des paquets RTP | |
| | | | A.11 |
| | | Ajout d'un participant (INVITE) | |
| | | | A.12 |
| | Obtention d'info. sur les propriétés de la communication | | |
| | | Sniffing de paquets SIP | |
| | | | A.13 |
| | Obtention d'info. sur le contenu de la communication | | |
| | | Récupération du DTMF | |
| | | | A.14 |
| Détournement du trafic | | | |
| | d'appel | | |
| | | Rerouting | |
| | | | A.15 |
| | | | A.16 |
| | | | A.17 |
| | | | A.18 |
| | de signalisation | | |
| | | Man in the Middle | |
| | | | A.19 |
| | | | A.20 |
| Identité | | | |
| | Usurpation d'identité | | |
| | | Spoofed messages | |
| | | | A.21 |
| | Dissimulation d'identité | | |
| | | | A.22 |
| Vols de services | | | |
| | Tromper la taxation | | |
| | | Tunneling RTP | |
| | | | A.23 |
| | | Usurpation d'identité | |
| | | | A.24 |
| Communications indésirées | | | |
| | Appel spam | | |
| | | | A.25 |
| | IM spam | | |
| | | | A.26 |
| | inscriptions dans la liste blanche | | |
| | | | A.27 |

# 4 Eléments de sécurité

Les méthodes de sécurisation proposées s'appuient sur les éléments suivants :

- La **sécurité de base** contient des BP (en partie sous forme de liens vers des documents de référence) pas forcément spécifiques à la VoIP qui permettent de partir sur une infrastructure « saine »
- La **séparation des équipements DATA et VoIP** permet à elle seule de parer une grande partie des attaques, notamment les attaques concernant l'écoute clandestine
- L'**authentification** permet de s'assurer de l'identité des interlocuteurs
- Le **chiffrement** doit garantir la confidentialité et l'intégrité des données échangées
- La **sécurité périmétrique** permet de protéger le réseau VoIP de l'entreprise face aux risques externes

## 4.1 Sécurité de base

### 4.1.1 *Best Practices "sécurité réseau"*

La majorité des entreprises mettant en place une infrastructure VoIP choisissent un réseau IP convergé (un même réseau physique pour les données et la VoIP) pour des raisons économiques et pratiques. Il est donc évident que la sécurité de l'infrastructure VoIP est fortement liée à la sécurité du réseau IP.

Le document « *Network Infrastructure – Security Technical Implementation Guide* » [DodNet] peut être utilisé comme référence pour sécuriser un réseau IP, notamment le paragraphe §3.5 (*Firewalls*).

### 4.1.2 Sécurité physique

La sécurité physique est un des éléments clefs permettant d'obtenir une bonne sécurité VoIP.

Sa mise en œuvre permet, entre autres, de diminuer fortement les risques d'écoutes clandestines et les risques de DoS dus, par exemple, au débranchement de l'alimentation d'un *switch* ou d'un serveur.

L'accès aux équipements réseaux (*routers*, *switch*,...) et aux serveurs VoIP devrait donc être restreint aux seules personnes autorisées.

Les solutions choisies pour garantir la sécurité physique dépendent du niveau de sécurité requis (pièces fermées à clefs, lecteurs de cartes, biométrie, gardes,…).

De plus, des mesures organisationnelles devraient être prises de manière à interdire aux employés de déconnecter un câble réseau (d'un PC ou d'un *hardphone*). En effet, un employé mal intentionné pourrait déconnecter son *hardphone* de manière à connecter un ordinateur. Cet ordinateur se retrouverait donc connecté au VLAN VoIP; ce qui est inadmissible (même si l'accès aux *switches* est sécurisé comme décrit dans S.08).

**Sources :** P. 5 de [NIST] & p. 34 §3.2 de [DoD]

## 4.2 Séparation des équipements DATA et VoIP

La manière la plus efficace d'améliorer la sécurité d'un réseau VoIP est de **séparer les équipements DATA des équipements VoIP en deux zones (DATA + VoIP) de sécurité**.

Si le niveau de sécurité requis est élevé et que les moyens le permettent, il est recommandé de subdiviser la zone VoIP en fonction des types d'équipements VoIP (ex : zone serveurs VoIP, zone *hardphones*, zone *softphones*,…).

Cette séparation peut se faire de manière physique (deux réseaux physiquement indépendants avec *switches* séparés) ou de manière logique. La séparation logique est souvent préférée pour des raisons budgétaires.

En cas de présence de *softphones* dans l'architecture, un VLAN *softphones* doit être créé. Pour plus d'informations, concernant les zones de sécurité pouvant être mise en œuvre, consulter les pages 2 et 3 de [NsaArch]

Au §7, les solutions S.03 et S.04 permettent d'effectuer une séparation logique des réseaux DATA et VoIP. Il est fortement conseillé d'appliquer ces deux solutions afin d'obtenir une défense en profondeur.

Les solutions S.05, S.06, S.07, S.08 et S.09 permettent de préserver la séparation établie grâce à S.03 et S.04.

### *4.2.1 Best Practices "Sécurité du poste client" et notes sur les softphones*

Ce paragraphe concerne les machines ayant un *softphone* car **les *softphones* posent deux problèmes majeurs !**

Premièrement, les *softphones* sont installés sur un *Operating System* (OS). Ces OS comportent des failles et de nouvelles vulnérabilités sont découvertes quotidiennement. La surface d'attaque des *softphones* est donc beaucoup plus importante que celle des *hardphones* étant donné quelle est la somme de la surface d'attaque du *softphone* et de celle de l'OS.

Le document « Guide *to securing Windows XP* » [NistXP] peut être utilisé comme référence pour sécuriser un poste client Windows XP.

Les principaux *BP* à appliquer sont :

- Mise à jour des *patches* de sécurité de l'OS (§4.3 de [NistXP])
- Politique de gestion des mots de passe (§6.1 de [NistXP])
- Installation d'un anti-virus et mise à jour régulière de sa base de signature (§8.5 de [NistXP])

De plus, ces *softphones* étant installés sur des machines (PC) reliées au réseau DATA, **la séparation préconisée des réseaux DATA et VoIP devient difficile.**

D'après les recommandations du [NIST], « *softphone systems should not be used where security or privacy is a concern* ».

Si toutefois vous décidez d'intégrer des *softphones* dans votre architecture réseau, les *best practices* suivants sont recommandés :

- S.09, S.10 ou S.11, (S.12 et/ou S.13) et S.14 → voir §7

## 4.3 Authentification

Suite à la séparation des équipements DATA et VoIP, l'authentification constitue le second point crucial pour la sécurité.

Plusieurs méthodes d'authentification sont possibles selon le niveau de sécurité requis.

La **sécurité minimale** est obtenue en mettant en œuvre une authentification ***HTTP Digest* entre les IP phones et les serveurs VoIP**. Cette méthode d'authentification est la plus répandue et n'est pas propriétaire. Malheureusement, elle ne permet pas l'authentification mutuelle et est peu robuste face aux attaques *offline* de type *brute force*.

Un meilleur niveau de sécurité peut être obtenu grâce à la mise en œuvre d'un protocole fournissant une **authentification mutuelle** (authentification de l'*IP Phone* par le serveur et authentification du serveur par l'*IP Phone*) tels que :

- SIPS
- IPSec
- protocoles propriétaires

## 4.4 Chiffrement

Un chiffrement (partiel ou total) sera requis si la confidentialité des conversations l'exige.

Plusieurs variantes peuvent être mis en œuvre :

- Chiffrement des flux de signalisation (SIPS ou solution propriétaire)
- Chiffrement des flux médias (SRTP ou propriétaire)
- IPSec

Note :

Remarquons que l'écoute est possible sur un réseau téléphonique classique (PBX - PSTN) et que les risques d'écoutes sont tout aussi importants que dans une entreprise mettant en œuvre de la VoIP non chiffrée.

Le chiffrement des communications VoIP permet d'obtenir un niveau de sécurité (notamment en terme de confidentialité) bien supérieure à un réseau téléphonique classique.

Pour plus d'informations concernant les écoutes clandestines sur le réseau téléphonique classique et sur la VoIP, consulter les pages 231-232 de [VoixSurIP].

## 4.5 Sécurité périmétrique

La sécurité périmétrique concerne les équipements placés en bordure du réseau VoIP et permet de se protéger contre les attaques externes.

### 4.5.1 SBC

**Présentation**

Un SBC (*Session Border Controller*) est un dispositif placé en bordure de réseau sachant gérer les flux VoIP.

Beaucoup de personnes comparent les SBC à des *firewalls* VoIP-*aware*.

Cependant les fonctionnalités qu'ils offrent, bien que très différentes suivant les marques, vont bien au-delà du *firewalling*; par exemple :

- *Call Admission Control*
- Conversion de *codec media*
- Réécriture du trafic de signalisation
- Ouvrir sur le *firewall* les ports nécessaires aux communications VoIP
- NAT *Traversal* / STUN
- ALG
- ...

**Architecture interne d'un SBC**

Un SBC est composé de deux modules :

- Un module *SBC Signalisation* chargé de contrôler l'accès des messages de signalisation VoIP au réseau
- Un module *SBC Media* chargé de contrôler l'accès des paquets RTP au réseau. Ce module fait office de *proxy* RTP

Ces deux modules peuvent être regroupés dans un seul boîtier (*single-box SBC*) ou alors être dans deux boîtiers séparés (*dual-box SBC*).

La solution *single-box* est plus simple à mettre en œuvre et devrait être préférée pour les infrastructures VoIP de petite à moyenne taille.

La solution *dual-box* permet quand à elle une plus grande souplesse dans son déploiement et permet de satisfaire aux besoins. Elle nécessite cependant la mise en œuvre d'un protocole tel que MEGACO/MGCP afin de permettre la communication entre le module *SBC Signalisation* (appelé *Call Agent* dans la RFC de MGCP) et le(s) module(s) *SBC Media* (appelé *media gateway* dans la RFC de MGCP).

**Avec ou sans *firewall***

Etant donnée qu'un SBC peut intégrer ou pas un *firewall*, il est conseillé d'en ajouter un au besoin.

Dans ce cas, il sera nécessaire de mettre en œuvre un protocole tel que MEGACO/COPS pour la communication SBC - *firewall* ainsi que pour la configuration automatique du *firewall*.

### 4.5.2 STUN / TURN

STUN *(Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators*, RFC3489) est un protocole permettant aux applications de découvrir la présence de *firewalls*+NAT entre elles et *internet*.

Il permet aussi de déterminer quelle adresse IP publique a été allouée par le NAT.

C'est un protocole de type client-serveur où une application, comme par exemple un *softphone* peut inclure un client STUN qui va envoyer des requêtes à un serveur STUN. Les réponses du serveur permettront au client NAT de déduire le type de NAT utilisé ainsi que l'adresse et le n° de port qui lui auront été alloués.

TURN *(Traversal Using Relay NAT)* est un protocole permettant à un élément situé derrière un NAT ou un *firewall* de recevoir des données entrantes. Dans les derniers *drafts*, TURN a été intégré à STUN, devenant ainsi une nouvelle fonctionnalité de STUN.

Son fonctionnement est lui aussi client-serveur; le client (inclus dans une application) fait une requête au serveur STUN, qui va lui répondre l'adresse par lequel il va pouvoir être atteint (fonctionnement comme un relai de données).

# 5 Matrice attaques - solutions

Nous concluons par cette matrice qui synthétise la problématique et met en relation les solutions de sécurisation (§ 7) avec les attaques potentielles (§ 6).

Pour l'utiliser :

- **Colonnes de gauche** = la liste des attaques, avec identifiant et nom.
- **Partie supérieure =** la liste des solutions, classées par type avec identifiant et nom.
- Une **croix** dans la matrice indique que l'attaque est contrée par la solution.

Pour une analyse plus détaillée :

- Cette matrice peut se lire de **deux manières.**
- **Verticalement**, elle permet de voir quelle(s) attaque(s) est(sont) contrée(s).
- **Horizontalement**, elle permet de voir la(les) solution(s) appropriée(s).
- **Légende**

| | |
|---|---|
| x | La solution neutralise l'attaque. |
| x | La solution couvre un des vecteurs de l'attaque. Cependant, d'autres vecteurs peuvent encore permettre de réaliser l'attaque. |
| x | La solution couvre l'attaque, mais il se peut qu'une personne se soit appropriée des données d'authentification d'un utilisateur légitime. |
| — | Solution liée à la solution comprenant une croix à sa gauche. |

*(Matrice à la page suivante)*

| | | | | | | | Séparation réseaux DATA/VoIP | | | | | | | Auth. | | Chiffrement | | | Sécurité périmétr. | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | BP sécurité réseau | BP Sécurité du poste client | Sécurité Physique | S.01 Mise à jour du logiciel (IPBX/softphone/hardphone) | S.02 Verrouillage config. | S.03 Séparation niveau 3 | S.04 Séparation VLAN | S.05 Filtrage Inter-Vlan | S.06 Carte réseau 802.1q | S.07 Ports supp. : Désact. ou 802.1q | S.08 Sécuriser l'accès aux ports des switchs | S.09 DMZ pour les services convergés | S.10 HTTP Digest Authentication | S.11 Authentification mutuelle | S.12 Chiff. des flux de signalisation (SIPS,...) | S.13 Chiff. des flux médias (SRTP,...) | S.14 Chiff. des flux (IPSec,...) | S.15 SBC : Call admission control / seuils | S.16 Utilisation de serveurs dédiés pour STUN | S.17 Vérification de l'identité du serveur STUN | S.18 Continuation de l'écoute des réponses après la première | S.19 Limitation de la bande passante allouée par personne |
| **DoS** | A.01 DoS SIP CANCEL | | | | | | X | — | — | — | — | X | | X | X | X | | X | | | | | |
| | A.02 DoS SIP BYE | | | | | | X | — | — | — | — | X | | X | X | X | | X | | | | | |
| | A.03 DoS SIP FAILURE | | | | | | X | — | — | — | — | X | | X | X | X | | X | | | | | |
| | A.04 QoS dégradé du à réutilisation SSRC | | | | | | X | — | — | — | — | X | | X | X | | X | X | | | | | |
| | A.05 Injection de paquets RTP | | | | | | X | — | — | — | — | X | | | | | | X | | | | | |
| | A.06 Modification du codec audio | | | | | | X | — | — | — | — | X | | | | | | X | | | | | |
| | A.07 Rendre le flux audio inaudible | | | | | | X | — | — | — | — | X | | | | | | X | | | | | |
| | A.08 Registration table overflow | | | | | | | | | | | | | X | X | X | | X | X | | | | |
| | A.09 Proxy server flooding | | | | | | X | — | — | — | — | X | | X | X | X | | X | X | | | | |
| **Ecoute clandestine** | A.10 Physical eavesdropping | | | | | | X | — | — | — | — | X | | | | X | X | X | | | | | |
| | A.11 Cassage de Cipher | | | | | | X | — | — | — | — | X | | | | | | | | | | | |
| | A.12 Re-INVITE / Session replay | | | | | | X | — | — | — | — | X | | X | X | X | | X | | | | | |
| | A.13 Suivi des appels (1) | | | | | | X | — | — | — | — | X | | | | X | | X | | | | | |
| | A.14 Suivi des appels (2) | | | | | | X | — | — | — | — | X | | | | | X | X | | | | | |
| **Détournement du trafic** | A.15 Hijacking thanks to registrar (1) | | | | | | X | — | — | — | — | X | | X | X | X | | X | | | | | |
| | A.16 Hijacking thanks to registrar (2) | | | | | | X | — | — | — | — | X | | X | X | X | | X | | | | | |
| | A.17 Hijack. registration by SIP REGISTER | | | | | | X | — | — | — | — | X | | X | X | X | | X | | | | | |
| | A.18 Hijacking registration | | | | | | X | — | — | — | — | X | | X | X | X | | X | | | | | |
| | A.19 Call redirection using 301/302 mess. | | | | | | X | — | — | — | — | X | | | | X | | X | | | | | |
| | A.20 Call redirection using 305 mess. | | | | | | X | — | — | — | — | X | | | | X | | X | | | | | |
| **ID** | A.21 Request spoofing | | | | | | X | — | — | — | — | X | | | | X | | X | | | | | |
| | A.22 Masquage d'appels | | | | | | | | | | | | | X | X | | | | | | | | |
| **Vol serv** | A.23 Tromper la taxation | | | | | | | | | | | | | | | | | | | | | | |
| | A.24 Vol de service avec usurpation d'ident. | | | | | | X | — | — | — | — | X | | X | X | X | | X | | | | | |
| **Comm Indés** | A.25 Appel spam | | | | | | | | | | | | | X | X | X | | X | | | | | |
| | A.26 IM spam | | | | | | | | | | | | | X | X | X | | X | | | | | |
| | A.27 Presence spam | | | | | | | | | | | | | X | X | X | | X | | | | | |

# 6 Attaques potentielles

## 6.1 Liste des attaques

### 6.1.1 DoS en utilisant les messages de requête SIP CANCEL

**Nom anglais** : DoS using SIP CANCEL messages

**Identifiant** : A.01

**Source d'attaque** : LAN/VPN, externe avec SIP

**Cible** : SIP

**But** : impact sur la disponibilité

**Description** :

Cette attaque permet d'annuler un appel entrant sur un terminal particulier ou d'annuler un appel sortant initié par un terminal.

Le message CANCEL est normalement utilisé pour annuler une requête précédemment envoyée par un terminal. L'attaquant doit tout d'abord écouter le réseau afin de récupérer un message de requête entre l'appelant et l'appelé (la cible), en général un message INVITE si l'on souhaite effectuer une attaque DoS.

Après avoir analysé le message afin de récupérer suffisamment d'informations sur l'appel, l'attaquant peut façonner un faux message CANCEL et l'envoyer à l'appelé afin d'annuler le message INVITE.

Aucun des deux partis ne peut placer d'appel et le dessein de l'attaquant a été accompli.

Il est toutefois bon de remarquer que le message CANCEL n'a aucun effet sur une requête que l'UAS (l'appelé) a déjà acceptée. Malgré tout, un message INVITE met un certain temps pour générer une réponse, ce sont donc des cibles faciles pour l'attaque décrite ci-dessus, puisque l'attaquant a du temps pour analyser le message INVITE et façonner le message CANCEL.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau afin de repérer un message d'initialisation d'une connexion SIP.

Il doit aussi être capable d'insérer un message CANCEL juste après la réception du message INVITE par la cible.

**Sources** :

- **Secure IP Telephony using Multi-layered Protection**
  Brennen Reynolds and Dipak Ghosal
  Department of Computer Science - University of California
  http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/3.pdf
  *(Dernière visite le 11 mai 2006)*
- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.2 DoS en utilisant les messages de requête SIP BYE

**Nom anglais** : DoS using SIP BYE messages

**Identifiant** : A.02

**Source d'attaque** : LAN/VPN, externe avec SIP

**Cible** : SIP

**But** : impact sur la disponibilité

**Description** :

Cette attaque permet de couper une communication existante entre deux terminaux.

Le message de requête BYE est normalement utilisé pour terminer une session établie par SIP. L'attaquant doit tout d'abord écouter le réseau afin de récupérer un message de requête entre l'appelant et l'appelé.

Après avoir analysé le message afin de récupérer suffisamment d'informations sur la communication en cours, l'attaquant peut façonner un faux message BYE et l'envoyer soit à l'UAC (l'appelant), l'UAS (l'appelé) ou les deux afin de terminer la communication.

Le dessein de l'attaquant a été accompli et les deux partis doivent effectuer un nouvel appel.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau afin de repérer un message d'initialisation d'un appel.

Il doit aussi être capable d'insérer un message CANCEL juste après la réception du message INVITE par la cible.

**Sources** :

- **Secure IP Telephony using Multi-layered Protection**
  Brennen Reynolds and Dipak Ghosal
  Department of Computer Science - University of California
  http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/3.pdf
  *(Dernière visite le 11 mai 2006)*
- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.3 DoS en utilisant les messages de réponse SIP FAILURE (4xx)

**Nom anglais** : DoS using SIP FAILURE (4xx) messages

**Identifiant** : A.03

**Source d'attaque** : LAN/VPN, externe avec SIP

**Cible** : SIP

**But** : impact sur la disponibilité

**Description** :

Cette attaque permet d'empêcher un appel d'aboutir.

Les messages de réponse SIP Request Failure (4xx) sont normalement utilisés pour répondre à un message de requête SIP lorsque quelque chose ne s'est pas passé correctement. Il faut noter que les réponses 4xx sont des réponses définitives d'un serveur et le client ne devrait pas réessayer la même requête sans une modification.

L'attaquant doit tout d'abord écouter le réseau afin de récupérer un message de requête entre l'appelant et l'appelé (un message de requête de type INVITE serait le meilleur candidat pour ce genre d'attaque). Après avoir analysé le message afin de récupérer suffisamment d'informations sur la communication qui va prendre place, il peut façonner un faux message de réponse 404 (Not Found) ou 410 (Gone) ou n'importe quel autre code possible (mais les messages 404 et 410 sont de bons exemples) et l'envoyer à l'UAC (l'appelant) avant que l'UAS (l'appelé) ait une chance de répondre au message de requête SIP initial.

Le dessein de l'attaquant a été accompli et la communication ne peut prendre place puisque l'UAC pense que l'UAS n'existe pas (ou plus).

Note : Des attaques similaires en utilisant des messages du type 5xx (Server failures) ou 6xx (Global failures) sont possibles.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau afin de repérer un message d'initialisation d'une connexion SIP.

Il doit aussi être capable d'insérer un message FAILURE juste après la réception du message INVITE par la cible.

**Sources** :

- **Secure IP Telephony using Multi-layered Protection**
  Brennen Reynolds and Dipak Ghosal
  Department of Computer Science - University of California
  http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/3.pdf
  *(Dernière visite le 11 mai 2006)*
- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.4 Perte de performance QoS en réutilisant la SSRC de RTP

**Nom anglais** : Drop of QoS Performance by reusing RTP's SSRC

**Identifiant** : A.04

**Source d'attaque** : LAN/VPN

**Cible** : RTP

**But** : impact sur la disponibilité

**Description** :

Cette attaque a pour but d'utiliser une SSRC (synchronization source, source de synchronisation) déjà existante afin de provoquer une perte dans la performance QoS (qualité de service).

L'attaquant devra tout d'abord connaître la SSRC utilisée par l'appelant d'une communication RTP mise en place par deux utilisateurs légitimes en écoutant le trafic RTP.

Ensuite, l'attaquant devra forger un paquet RTP en utilisant la même SSRC afin de créer des collisions et ainsi une perte dans les performances QoS, car l'appelé devra détecter la collision.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau afin de repérer une communication et ainsi savoir quel est la SSRC utilisée.

**Sources** :

- **RFC 1889 - RTP: A Transport Protocol for Real-Time Applications**
- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.5 Injection de paquets RTP

**Nom anglais** : RTP packet injection

**Identifiant** : A.05

**Source d'attaque** : LAN/VPN

**Cible** : Serveur registrar

**But** : impact sur la disponibilité

**Description** :

Cette attaque a pour but de perturber une communication en cours.

L'attaquant devra tout d'abord écouter un flux RTP de l'appelant vers l'appelé, analyser son contenu et façonner un paquet RTP contenant un en-tête similaire mais avec un plus grand numéro de séquence et timestamp afin que ce paquet soit reproduit avant les autres paquets (s'ils sont vraiment reproduits).

Ainsi la communication sera perturbée et l'appel ne pourra pas se dérouler correctement.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau afin de repérer une communication et ainsi repérer les timestamp des paquets RTP.

Il doit aussi être capable d'insérer des messages RTP forgés ayant un timestamp modifié.

**Sources** :

- **RFC 1889 - RTP: A Transport Protocol for Real-Time Applications**
- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.6 Modification du codec audio

**Nom anglais** : Audio codec modification

**Identifiant** : A.06

**Source d'attaque** : LAN/VPN

**Cible** : RTP / Terminaux : soft/hard phones

**But** : impact sur la disponibilité et l'intégrité des données

**Description** :

Cette attaque a pour but d'utiliser l'absence de contrôle du flux média afin de changer certains de ses paramètres et créer plus de trafic que désiré.

L'attaquant va profiter de la cécité de SIP par rapport au flux média, puisqu'il peut être modifié sans que SIP soit au courant de ces changements. Ceci a pour résultat qu'une interruption de la conversation ne sera pas (mais devrait être) détecté par les proxies.

Un changement de codec pourrais avoir comme résultats l'utilisation de plus gros paquets et donc d'utiliser plus de bande passante et affamer les autres communications.

**Réalisation** :

L'attaquant doit être capable de repérer un flux média et de le modifier.

**Sources :**

- **RFC 1889 - RTP: A Transport Protocol for Real-Time Applications**

### 6.1.7 Rendre le flux audio inaudible

**Nom anglais** :

**Identifiant** : A.07

**Source d'attaque** : LAN/VPN

**Cible** : RTP / Terminaux : soft/hard phones

**But** : impact sur la disponibilité et l'intégrité des données

**Description** :

Une communication légitime est établie entre les deux interlocuteurs. L'attaquant va envoyer un flux RTP parasite chargé de se superposer au flux RTP légitime.

Pour ce faire, l'attaquant doit avoir sniffé le réseau afin de connaître le port UDP utilisé par le flux RTP ainsi que le codec audio utilisé. Une fois ses valeurs connues, il suffit d'utiliser un logiciel tels que *JM Studio* [JMF] afin d'envoyer le flux RTP parasite.

**Réalisation** :

L'attaquant doit être capable de récupérer le port UDP et le codec utilisé par le flux RTP à rendre inaudible.

**Sources :**

- **RFC 1889 - RTP: A Transport Protocol for Real-Time Applications**

### 6.1.8 Débordement de la table des enregistrements

**Nom anglais** : Registration table overflow

**Identifiant** : A.08

**Source d'attaque** : LAN/VPN, externe avec SIP

**Cible** : SIP

**But** : impact sur la disponibilité

**Description** :

Cette attaque a pour but de provoquer un débordement de la table des enregistrements afin d'empêcher les utilisateurs légitimes de s'enregistrer sur le serveur *registrar*.

L'attaquant envoie un grand nombre de messages de requête REGISTER (avec des URIs différentes) au serveur des enregistrements afin de remplir la table des enregistrements et ainsi empêcher les utilisateurs légitimes de s'enregistrer et d'utiliser le service.

**Réalisation** :

L'attaquant doit être capable d'envoyer des messages d'enregistrement au serveur registrar.

**Sources** :

- **RFC 1889 - RTP: A Transport Protocol for Real-Time Applications**

### 6.1.9 Inondation du serveur proxy

**Nom anglais** : Proxy server flooding

**Identifiant** : A.09

**Source d'attaque** : LAN/VPN

**Cible** : SIP

**But** : impact sur la disponibilité

**Description** :

Cette attaque a pour but d'inonder les serveurs proxy avec des messages INVITE afin d'empêcher les utilisateurs légitimes de placer des appels.

L'attaquant envoie un gros volume de messages INVITE à un proxy, qui doit normalement les transférer vers le destinataire. Le problème est que le nombre de sessions concurrentes supportées par un serveur proxy est limité, les ressources sont donc rapidement épuisées, ce qui a pour conséquence que les appels placés par des utilisateurs légitimes en utilisant le proxy victime ne peuvent prendre place.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau afin de repérer un message d'initialisation d'une connexion SIP.

Il doit aussi être capable d'insérer un message FAILURE juste après la réception du message INVITE par la cible.

**Sources** :

- **Security Considerations**
  Jeremy George
  SIP.edu Cookbook
  http://mit.edu/sip/sip.edu/security.shtml
  *(Dernière visite le 12 mai 2006)*

### 6.1.10 Ecoute clandestine physique

**Nom anglais** : Physical eavesdropping

**Identifiant** : A.10

**Source d'attaque** : LAN/VPN, externe avec SIP

**Cible** : RTP / Terminaux : soft/hard phones

**But** : impact sur la confidentialité des données

**Description** :

Cette attaque a pour but d'écouter ou d'enregistrer une conversation en cours.

L'attaquant gagne l'accès au réseau physique et utilises des outils pour espionner directement sur les câbles. Il peut le faire entre un UA et le switch ou entre deux switches. Il peut ensuite rejouer le contenu des paquets.

**Réalisation** :

- L'attaquant doit avoir un accès physique aux câbles réseau et être capable d'écouter le trafic.

**Sources :**

- **RFC 1889 - RTP: A Transport Protocol for Real-Time Applications**

### 6.1.11 Cassage de cipher

**Nom anglais** : Cipher breakage

**Identifiant** : A.11

**Source d'attaque** : LAN/VPN, externe avec SIP

**Cible** : RTP / Terminaux : soft/hard phones

**But** : impact sur la confidentialité des données

**Description** :

Cette attaque a pour but de connaître le contenu d'un paquet en le déchiffrant.

Ecouter les messages de signalisation SIP afin de récupérer la clé DES (champ k) afin de pouvoir par la suite déchiffrer le contenu des paquets audio cryptés avec le cipher et ainsi connaître le contenu de la conversation.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau et récupérer des conversations chiffrées ainsi que les messages SIP contenant la clé DES.

Il doit aussi avoir une méthode pour tenter de décrypter les messages.

**Méthodes de sécurisation** :

- *Utiliser un cipher plus fort.*

**Sources :**

- **RFC 1889 - RTP: A Transport Protocol for Real-Time Applications**

### 6.1.12 Re-INVITE / Répétition de session – « Mid Session tricks »

**Nom anglais** : Re-INVITE / Session Replay – Mid Session tricks

**Identifiant** : A.12

**Source d'attaque** : LAN/VPN

**Cible** : SIP

**But** : impact sur la confidentialité, la disponibilité et l'intégrité des données

**Description** :

Cette attaque a pour but d'enregistrer un appel ou modifier les paramètres de configuration d'un appel.

L'attaquant doit tout d'abord écouter le réseau et récupérer un message INVITE entre un appelant et un appelé. Il peut ensuite introduire un message INVITE façonné dans la conversation en cours de telle manière à ce que les paramètres soient pris en compte (par exemple les paramètres de routage) et qu'un troisième parti soit introduit dans la conversation, par exemple pour faciliter l'enregistrement de la conversation.

**Réalisation** :

L'attaquant doit pouvoir écouter les messages SIP et en insérer des forgés.

**Sources** :

- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.13 Suivre des appels (1)

**Nom anglais** : Call Tracking (1)

**Identifiant** : A.13

**Source d'attaque** : LAN/VPN

**Cible** : Terminaux : soft/hard phones

**But** : impact sur la confidentialité des données

**Description** :

Cette attaque a pour but de connaître qui est en train de communiquer, quel est le timing et la longueur de la communication.

L'attaquant doit récupérer les messages INVITE et BYE en écoutant le réseau et peut ainsi savoir qui communique, à quelle heure et pendant combien de temps.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau et récupérer les messages INVITE et BYE.

**Sources :**

- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.14 Suivre des appels (2)

**Nom anglais** : Call Tracking (2)

**Identifiant** : A.14

**Source d'attaque** : LAN/VPN, externe avec SIP

**Cible** : RTP / Terminaux : soft/hard phones

**But** : impact sur la confidentialité des données

**Description** :

Cette attaque a pour but de capturer des informations sensibles sur les interlocuteurs.

Le but de l'attaque est de récupérer le DTMF (Dual Tone Multi Frequency) parmi l'ensemble du trafic vocal. Cela permettra à l'attaquant de récupérer des informations qui peuvent aller des informations concernant la boîte vocale (numéro de téléphone, numéro de la boîte vocale, mot de passe) aux informations sur les cartes d'appels voir même des numéros de carte de crédit.

Toutes informations passées via DTMF peuvent être récupérées par ce moyen.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau et récupérer paquets RTP de la communication.

La cible doit aussi être en train d'utiliser les tonalités DTMF sur quelque chose d'intéressant (mots de passes, etc.).

**Sources :**

- **VoIP - The Next Generation of Phreaking - Revision 1.1**
  Ofir Arkin - @stake
  http://blackhat.com/presentations/win-usa-02/arkin-winsec02.ppt
  *(dernière visite le 15 mai 2006)*

### 6.1.15 Détournement d'appel à l'aide du serveur registrar (1)

**Nom anglais** : Call hijacking helped by the registrar server (1)

**Identifiant** : A.15

**Source d'attaque** : LAN/VPN

**Cible** : Serveur registrar

**But** : impact sur la confidentialité

**Description** :

Cette attaque a pour but de détourner un appel en altérant les liaisons du serveur *registrar*.

L'attaquant profite du rôle du serveur registrar dans le système tout d'abord en récupérant les liaisons d'une URI particulière afin de récupérer la liste des adresses lui correspondant. Ensuite, il va associer son URI avec tous les enregistrements corrects dans un message de requête REGISTER et en stipulant à ces enregistrements une priorité plus élevée en utilisant le paramètre « q ».

Ce paramètre indique une préférence relative pour ce champ Contact particulier par rapport aux autres liaisons pour cette adresse d'enregistrement.

Ceci a pour conséquence que le dessein de l'attaquant a abouti car son URI sera utilisée à la place de celle de l'utilisateur légitime.

**Réalisation** :

L'attaquant doit être capable d'envoyer et recevoir des données du serveur registrar.

Il doit aussi être capable de forger des requêtes REGISTER truquées.

**Sources** :

- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.16 Détournement d'appel à l'aide du serveur registrar (2)

**Nom anglais** : Call hijacking helped by the registrar server (2)

**Identifiant** : A.16

**Source d'attaque** : LAN/VPN

**Cible** : Serveur registrar

**But** : impact sur la confidentialité et la disponibilité

**Description** :

L'attaquant profite du rôle du serveur registrar dans le système tout d'abord en récupérant les liaisons d'une URI particulière afin de récupérer la liste des adresses lui correspondant. Ensuite, il va associer son URI avec tous les enregistrements corrects dans un message de requête REGISTER et en stipulant à ses enregistrements une priorité plus faible en utilisant le paramètre « q ».

Ce paramètre indique une préférence relative pour ce champ Contact particulier par rapport aux autres liaisons pour cette adresse d'enregistrement.

Ensuite, l'attaquant va effectuer une attaque DoS sur tous les enregistrements ayant une priorité plus élevée afin que le proxy ne puisse pas leur envoyer de message et passe automatiquement à l'entrée suivante, par exemple celles qui ont une priorité plus faibles (celles de l'attaquant).

**Réalisation** :

L'attaquant doit être capable d'envoyer et recevoir des données du serveur registrar.

Il doit aussi être capable de forger des requêtes REGISTER truquées.

**Sources** :

- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.17 Détournement de l'enregistrement en façonnant des messages SIP REGISTER

**Nom anglais** : Registration hijacking by forging SIP REGISTER requests

**Identifiant** : A.17

**Source d'attaque** : LAN/VPN

**Cible** : SIP / Serveurs registrar

**But** : impact sur la confidentialité, la disponibilité et l'intégrité des données

**Description** :

Cette attaque a pour but de rediriger les appels vers l'attaquant en sabotant le serveur registrar.

L'attaquant doit tout d'abord écouter le réseau afin de récupérer un message du type REGISTER. Ensuite, après avoir analysé ce message, il peut façonner un message REGISTER et se réenregistrer auprès du serveur registrar avec une nouvelle URI pour la victime.

Ceci ayant comme résultat de rediriger tous les appels entrants qui seront envoyés vers la nouvelle URI (p.ex. celle de l'attaquant) permettant ainsi à l'attaquant de plagier la cible de l'attaque et ainsi mener à bien son dessein.

**Réalisation** :

L'attaquant doit pouvoir écouter les messages SIP REGISTER, l'analyser et renvoyer un message REGISTER truqué au serveur regitrar.

**Sources** :

- **Secure IP Telephony using Multi-layered Protection**
  Brennen Reynolds and Dipak Ghosal
  Department of Computer Science - University of California
  http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/3.pdf
  *(Dernière visite le 11 mai 2006)*
- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.18 Détournement d'enregistrement

**Nom anglais** : Registration hijacking

**Identifiant** : A.18

**Source d'attaque** : LAN/VPN

**Cible** : SIP / Serveurs registrar

**But** : impact sur la confidentialité, la disponibilité et l'intégrité des données

**Description** :

Cette attaque a pour but de rediriger les appels vers l'attaquant en sabotant le serveur registrar.

En récupérant sur le réseau un message de requête REGISTER, l'attaquant est capable de le modifier et d'en envoyer un nouveau dans l'intervalle de temps originellement définie par le « *timestamps*» spécifié dans le message REGISTER d'origine mais avec le champ « expires » contenant la valeur « 0 » afin de supprimer les liaisons de l'utilisateur légitime.

Ainsi, la victime ne pourra plus enregistrer son téléphone comme étant une adresse de contact convenable et tous les appels pour la victime seront redirigés vers l'attaquant.

**Réalisation** :

L'attaquant doit pouvoir écouter les messages SIP REGISTER, l'analyser et renvoyer un message REGISTER truqué au serveur registrar.

**Sources** :

- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.19 Redirection d'appel en utilisant des messages de réponse du type 301/302

**Nom anglais** : Call redirection using 301/302 response messages

**Identifiant** : A.19

**Source d'attaque** : LAN/VPN

**Cible** : Terminaux : soft/hard phones

**But** : impact sur la confidentialité

**Description** :

Cette attaque a pour but de rediriger le trafic de signalisation vers un parti qui n'est pas l'appelé.

L'attaquant doit tout d'abord écouter le réseau afin de récupérer un message de requête du type INVITE entre l'appelant et l'appelé. Ensuite, après avoir analysé le message et récupéré suffisamment d'informations sur la communication qui va prendre place, il peut façonner un faux message de réponse du type 301 (Moved Permanently) ou 302 (Moved Temporarly) et l'envoyer à l'UAC (l'appelant) avant que l'UAS (l'appelé) ait eu le temps de répondre au message de requête SIP original.

Une fois que l'UAC aura reçu le message de réponse susmentionné, il effectuera une nouvelle tentative d'appel à l'adresse mentionnée par l'attaquant. Le dessein de l'attaquant aura donc abouti.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau et de récupérer un message du type INVITE.

Il doit aussi être capable de forger des messages de réponse du type 301 ou 302 et de l'envoyer avant la réponse légitime.

**Sources** :

- **Secure IP Telephony using Multi-layered Protection**
  Brennen Reynolds and Dipak Ghosal
  Department of Computer Science - University of California
  http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/3.pdf
  *(Dernière visite le 11 mai 2006)*
- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.20 Redirection d'appel en utilisant les messages de réponse du type 305

**Nom anglais** : Call redirection attack using 305 response messages

**Identifiant** : A.20

**Source d'attaque** : LAN/VPN

**Cible** : SIP

**But** : impact sur la confidentialité, la disponibilité et l'intégrité des données

**Description** :

Cette attaque a pour but de rediriger le trafic de signalisation, afin de le modifier, vers un serveur proxy corrompu.

Les messages de réponses de redirection (3xx) sont envoyés par les UAS et donnent normalement des informations sur la nouvelle localisation de l'utilisateur ou sur un des services alternatifs susceptibles de satisfaire l'appel (ce qui est le cas du code 305, indiquant que la ressource demandée doit être accédée à travers le proxy donné dans le champ Contact).

L'attaquant doit tout d'abord écouter le réseau afin de récupérer un message de requête SIP entre l'appelant et l'appelé. Après avoir analysé le message afin de récupérer suffisamment d'informations, il peut façonner un message de réponse du type 305 et l'envoyer à l'expéditeur du message récupéré. Ce dernier devra ensuite faire transiter le trafic de signalisation à travers le proxy spécifié et les messages de réponse prendront automatiquement le même chemin.

Le dessein de l'attaquant aura abouti puisque le trafic de signalisation aura été redirigé à travers un proxy (probablement compromis) lui laissant ensuite la possibilité de modifier les paquets le traversant.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau et de repérer un message de signalisation d'une communication en cours.

Il doit aussi être capable de façonner un message de redirection et de l'envoyer avant la réponse légitime.

Enfin, il doit être capable de se comporter comme un proxy SIP, afin de faire croire au client qu'il discute bien avec le serveur légitime.

**Sources** :

- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.21 Contrefaçon de requête

**Nom anglais** :Request spoofing

**Identifiant** : A.21

**Source d'attaque** : LAN/VPN

**Cible** : SIP / Terminaux : soft/hard phones

**But** : impact sur la confidentialité, la disponibilité et l'intégrité des données

**Description** :

Cette attaque a pour but de modifier l'identité de l'expéditeur d'un message afin de faire croire au destinataire d'un appel qu'il parle à un utilisateur légitime alors qu'en fait il parle à l'attaquant

L'attaquant va tout d'abord écouter le réseau afin de récupérer un message de requête soit du type REGISTER, soit du type INVITE et modifie certains champs contenus dans l'en-tête avant d'envoyer ce faux message de requête.

Ceci a pour conséquence que l'appelé pense qu'il parle à un utilisateur spécifique alors qu'en fait il parle à l'attaquant.

Ainsi, la victime ne pourra plus enregistrer son téléphone comme étant une adresse de contact convenable et tous les appels pour la victime seront redirigés vers l'attaquant.

**Réalisation** :

L'attaquant doit pouvoir écouter les messages SIP REGISTER ou INVITE, l'analyser, le modifier et le réexpédier une fois truqué.

**Sources** :

- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.22 Masquage d'appel

**Nom anglais** : Call masquerading

**Identifiant** : A.22

**Source d'attaque** : LAN/VPN, externe avec SIP

**Cible** : SIP / Terminaux : soft/hard phones

**But** : impact sur la disponibilité des données

**Description** :

Cette attaque a pour but de dissimuler l'identité de l'appelant afin que l'appelé prenne l'appel.

L'appelant cache son identité afin que l'appelé ne puisse pas savoir qui appelle et réponde au téléphone. Ceci a pour conséquence que l'utilisateur peut être exposé à des téléprospecteurs, des publicités enregistrées, etc.

**Réalisation** :

L'attaquant doit pouvoir appeler la cible en masquant son numéro de téléphone.

**Sources :**

- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.23 Tromper la taxation

**Nom anglais** :Billing fooling

**Identifiant** : A.23

**Source d'attaque** : LAN/VPN

**Cible** : SIP / Terminaux : soft/hard phones

**But** : impact sur l'intégrité des données

**Description** :

Cette attaque a pour but de passer des appels gratuits.

L'attaquant et son complice vont mettre en place un schéma où les messages SIP seront dissimulés à l'intérieur de messages RTP/RTCP.

Le proxy SIP sera incapable de détecter le trafic de signalisation (SIP), alors que le flux de média (RTP/RTCP) continuera de transiter. Le CDR (*Call Detail Recording*) ne sera pas exécuté et ainsi, les deux partis peuvent effectuer des appels téléphoniques gratuits.

**Réalisation** :

Les attaquants doivent être capable de modifier les paquets RTP/RTCP qu'ils s'envoient afin d'ajouter des informations de signalisation (SIP).

**Sources** :

- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.24 Vol de service en utilisant les accréditations de l'utilisateur légitime

**Nom anglais** : Theft of service using a legitimate client's credentials

**Identifiant** : A.24

**Source d'attaque** : LAN/VPN

**Cible** : SIP

**But** : impact sur l'intégrité

**Description** :

Cette attaque a pour but d'effectuer des appels gratuits en utilisant les informations d'un utilisateur légitime.

L'attaquant doit tout d'abord écouter le réseau afin de récupérer un message de requête REGISTER partant d'un UAC et allant vers le serveur registrar. Après avoir analysé le message récupéré, l'attaquant envoie un message de réponse du type 301 (Moved Permanently) pour faire croire à l'utilisateur que le serveur registrar SIP a été déplacé en lui donnant comme nouvelle adresse un de ses serveurs. Ainsi, l'utilisateur va s'enregistrer sur le proxy illégitime de l'attaquant qui pourra ainsi récupérer les informations de l'utilisateur légitime et les utiliser.

Ensuite, l'attaquant pourra usurper l'identité de l'utilisateur légitime et effectuer des appels gratuits ou rediriger le trafic vers un serveur d'enregistrement.

**Réalisation** :

L'attaquant doit être capable d'écouter le réseau et de récupérer un message du type REGISTER entre la cible et le serveur registrar.

Il doit aussi être capable d'envoyer un message de redirection à la cible avant la réponse légitime et singer le fonctionnement du serveur registrar afin de récupérer les informations de l'utilisateur légitime.

Enfin, il doit être capable d'utiliser les informations récupérées illégitimement pour s'enregistrer sur le vrai serveur registrar et effectuer des appels gratuits.

**Sources** :

- **RFC 3261 - SIP: Session Initiation Protocol**

### 6.1.25 Appel spam

**Nom anglais** :*Spam call*

**Identifiant** : A.25

**Source d'attaque** : LAN/VPN, externe avec SIP, externe Internet

**Cible** : Terminaux : soft/hard phones

**But** : impact sur l'intégrité des données

**Description** :

Cette attaque a pour but de jouer un message préenregistré à la personne décrochant le combiné.

Ce type de spam est défini comme étant une série d'essais d'initiation de session (par ex. des requêtes INVITE), essayant d'établir une session de communication vocale.

Quand l'appelant décroche le combiné, l'attaquant (spammeur) relaie son message à travers le media temps réel.

**Réalisation** :

L'attaquant doit être capable d'appeler la victime.

**Sources** :

- **The Session Initiation Protocol (SIP) and Spam**
  **draft-rosenberg-sipping-spam-02**
  J. Rosenberg, C. Jennings, Cisco, J. Peterson, Neustar
  6 Mars 2006; Expire le 7 septembre 2006
  http://www.ietf.org/internet-drafts/draft-ietf-sipping-spam-02.txt
  *(Dernière visite le 15 mai 2006)*

### 6.1.26 IM (messagerie instantanée) spam

**Nom anglais** :*Instant messaging spam (SPIM)*

**Identifiant** : A.26

**Source d'attaque** : LAN/VPN, externe avec SIP

**Cible** : Terminaux : soft/hard phones

**But** : impact sur l'intégrité des données

**Description** :

Cette attaque a pour but de générer un grand nombre de messages instantanés (souvent publicitaires) sur les terminaux des utilisateurs.

L'attaquant envoie un grand nombre de messages instantanés non sollicités, contenant le message que le spammeur désire passer. Le spam est envoyé en utilisant le message de requête SIP MESSAGE.

Toutefois, n'importe quel autre message de requête qui affiche automatiquement du contenu sur l'écran d'un terminal utilisateur pourrait fonctionner. Par exemple les requêtes INVITE avec de larges en-têtes Subject (car le champ Subject est parfois affiché à l'utilisateur) ou des INVITE contenant des corps du type texte ou HTML.

**Réalisation** :

L'attaquant doit être capable d'envoyer des SIP MESSAGES à la cible, voir des INVITE.

**Sources :**

- **The Session Initiation Protocol (SIP) and Spam**
  **draft-rosenberg-sipping-spam-02**
  J. Rosenberg, C. Jennings, Cisco, J. Peterson, Neustar
  6 Mars 2006; Expire le 7 septembre 2006
  http://www.ietf.org/internet-drafts/draft-ietf-sipping-spam-02.txt
  *(Dernière visite le 15 mai 2006)*

### 6.1.27 Présence spam

**Nom anglais** : Presence spam

**Identifiant** : A.27

**Source d'attaque** : LAN/VPN, externe avec SIP

**Cible** : Terminaux : soft/hard phones

**But** : impact sur l'intégrité des données

**Description** :

Cette attaque a pour but de se mettre sur la liste blanche (liste d'amis) d'un utilisateur afin de lui envoyer des messages instantanés ou d'initier d'autres formes de communication.

L'attaquant envoie une grande quantité de messages de requête de présence (par exemple des requêtes SUBSCRIBE), dans l'espoir d'entrer dans la liste blanche ou la « liste d'amis » d'un utilisateur afin de lui envoyer des messages instantanés ou d'initier d'autres formes de communication.

Contrairement aux spam messages instantanés, le spam de présence ne transporte pas réellement de contenu dans le message, il joue uniquement sur la patience de l'utilisateurs qui finira par accepter la requête et mettra l'utilisateur sur la liste blanche afin de ne plus recevoir la demande.

L'attaque peut aussi se faire en envoyant la demande à un grand nombre d'utilisateurs, afin de maximiser les chances d'avoir une personne acceptant la demande.

**Réalisation** :

L'attaquant doit être capable d'envoyer des requêtes (par exemple du type SUBSCRIBE) à la cible.

**Sources :**

- **The Session Initiation Protocol (SIP) and Spam**
  **draft-rosenberg-sipping-spam-02**
  J. Rosenberg, C. Jennings, Cisco, J. Peterson, Neustar
  6 Mars 2006; Expire le 7 septembre 2006
  http://www.ietf.org/internet-drafts/draft-ietf-sipping-spam-02.txt
  *(Dernière visite le 15 mai 2006)*

### 6.1.28 Dénis de service distribué contre une cible

**Nom anglais** : Distributed Deny of Service (DDoS)

**Identifiant** : A.28

**Source d'attaque** : LAN/VPN, Externe Internet

**Cible** : N'importe quel ordinateur sur le réseau (via clients STUN)

**But** : impact sur la disponibilité

**Description** :

Cette attaque a pour but de lancer une attaque dénis de service distribué à l'aide de STUN

L'attaquant distribue à un grand nombre de clients une MAPPED-ADDRESS truquée qui pointe sur la cible. Cela va faire croire aux clients STUN que leurs adresses sont égales à celles de la cible.

Les clients vont ensuite donner cette adresse afin d'y recevoir du trafic (par exemple, des messages SIP ou H.323). Tout ce trafic va donc se focaliser sur la cible. L'attaque peut ainsi créer une grosse surcharge de trafic sur la cible, surtout lorsqu'elle est utilisée avec des clients qui utilisent STUN pour initialiser des applications multimédia.

**Réalisation** :

L'attaquant doit être capable de renvoyer une réponse STUN truquée aux clients, à la place du serveur STUN légitime.

**Sources** :

- **RFC 3489 : STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) – section 12.1.1**

### 6.1.29 Museler un client

**Nom anglais** : Silencing a Client

**Identifiant** : A.29

**Source d'attaque** : LAN/VPN, Externe Internet

**Cible** : Client STUN

**But** : impact sur la disponibilité

**Description** :

Cette attaque a pour but d'empêcher le client de communiquer avec le serveur qu'il souhaitait atteindre.

Dans cette attaque, l'attaquant cherche à empêcher un utilisateur d'accéder à un service activé par STUN (par exemple, un client utilisant STUN pour activer du trafic multimédia basé sur SIP). Pour ce faire, l'attaquant renvoie au client une MAPPED-ADDRESS truquée ne pointant vers rien du tout. Ceci a comme résultat que le client ne recevra jamais les paquets attendus lorsqu'il émettra vers la MAPPED-ADDRESS.

Il est important de remarquer que cette attaque n'est pas très intéressante pour l'attaquant. Elle n'impacte qu'un seul client, qui n'est bien souvent pas la cible désirée. De plus, si l'attaquant peut effectuer cette attaque, il pourrait aussi faire un

déni de service sur la cible par d'autres moyens, comme l'empêcher de recevoir des réponses du serveur STUN, voir du serveur DHCP.

**Réalisation** :

L'attaquant doit être capable de renvoyer une réponse STUN truquée aux clients, à la place du serveur STUN légitime.

**Sources** :

- **RFC 3489 : STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) – section 12.1.2**

### 6.1.30 Se faire passer pour un client

**Nom anglais** : Assuming the Identity of a Client

**Identifiant** : A.30

**Source d'attaque** : LAN/VPN, Externe Internet

**Cible** : Client STUN

**But** : impact sur la confidentialité

**Description** :

Cette attaque a pour but de faire transiter les paquets des clients STUN par soi afin d'effectuer des écoutes clandestines.

L'attaquant utilise la même technique que pour l'attaque ST.2, c'est-à-dire retourner une réponse STUN forgée avec une MAPPED-ADDRESS choisie par l'attaquant. Ici la différence est qu'au lieu de spécifier une adresse n'existant pas, il va spécifier sa propre adresse. Il va ainsi recevoir tous les paquets de la cible. Il lui suffit ensuite de réexpédier les paquets qu'il reçoit vers le client légitime.

Cette attaque lui permet alors d'observer tous les paquets envoyés au client. Toutefois, afin de lancer cette attaque, l'attaquant doit déjà avoir réussi à observer des paquets du client vers le serveur STUN. Dans la plupart des cas (par exemple lorsque l'attaque est lancée d'un réseau d'accès), cela veut dire que l'attaquant pourrait déjà observer les paquets envoyés au client. Cette attaque peut donc être utile pour observer le trafic par des attaquants sur le chemin du client vers le serveur STUN, mais généralement pas sur le chemin des paquets routés vers le client.

**Réalisation** :

L'attaquant doit être capable de renvoyer une réponse STUN truquée aux clients, à la place du serveur STUN légitime.

**Sources** :

- **RFC 3489 : STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) – section 12.1.4**

## 6.2 Remarques concernant les attaques liées à STUN (tiré de RFC3489 s. 12.2)

Il est important de noter que les attaques de cette nature (injection de paquets avec une MAPPED-ADDRESS faussée) demandent que l'attaquant soit capable d'intercepter les requêtes envoyées du client au serveur (ou d'effectuer une attaque Man in the middle) car les requêtes STUN contiennent un identifiant de transaction,

choisi par le client, qui est un nombre aléatoire avec 128 bits d'entropie. Le serveur remet cette valeur dans ses réponses et le client ignorera toutes les réponses n'ayant pas une ID de transaction correspondant.

C'est pourquoi, pour qu'un attaquant donne une réponse truquée acceptée par le client, il doit connaître l'ID de transaction de la requête. La grande variété de nombres aléatoires ainsi que la nécessité de connaître quand le client va envoyer une requête empêche toute attaque tentant de deviner l'ID de transaction.

Nous allons maintenant regarder quelques méthodes permettant de récupérer cet ID de transaction.

**Méthode # : 1 Compromettre un serveur STUN légitime**

Dans cette attaque, l'attaquant va compromettre un serveur STUN légitime à l'aide d'un virus ou d'un cheval de Troie. Ceci permettra alors au l'attaquant de contrôler le serveur STUN et de contrôler le type de réponses qu'il va générer.

Compromettre un serveur STUN de la sorte peut aussi permettre de découvrir les ports ouverts. Cette connaissance peut amener la possibilité de créer des attaques de déni de service sur ces ports (voir de dénis de service distribués si le NAT est du type full cone). Ceci ne représente toutefois pas une menace majeure car la découverte de ports ouverts est relativement triviale en sondant les ports.

**Méthode # : 2 Attaques DNS**

Les serveurs STUN sont découverts en utilisant les enregistrements DNS SRV. Si un attaquant peut compromettre le DNS, il peut injecter de faux enregistrements qui mappent un nom de domaine vers l'adresse IP d'un serveur STUN contrôlé par l'attaquant. Ceci permettra ensuite d'injecter de fausses réponses.

**Méthode # : 3 Routeur ou NAT espion**

Plutôt que de compromettre le serveur STUN, un attaquant pourrait faire générer à un serveur STUN des réponses avec une mauvaise MAPPED-ADDRESS en compromettant un routeur ou un NAT sur le chemin du client au serveur STUN. Lorsque la requête STUN passe à travers le routeur ou NAT espion, il réécrit l'adresse source du paquet afin qu'elle devienne celle de la MAPPED-ADDRESS désirée. Cette adresse ne peut pas être arbitraire.

Si l'attaquant est sur Internet (publique), et l'attaquant ne modifie pas la requête STUN, l'adresse doit avoir la propriété que les paquets envoyés du serveur STUN vers cette adresse seront routés à travers le routeur compromis. Ceci car le serveur STUN enverra directement les réponses à l'adresse source de la requête STUN. Avec une adresse source modifiée, le seul moyen pour qu'il puisse atteindre le client est que le routeur compromis les dirige au bon endroit.

Toujours si l'attaquant est sur Internet mais peut cette fois-ci modifier les requêtes STUN, il peut insérer un attribut RESPONSE-ADDRESS dans la requête, contenant l'adresse source de la requête STUN. Ceci aura comme action de faire que le serveur renvoie les réponses au client, indépendamment de l'adresse source que le serveur STUN voit. Ceci donne la possibilité à l'attaquant de forger une adresse arbitraire lorsqu'il transfère la requête STUN.

Si l'attaquant est sur un réseau privé (c'est-à-dire qu'il y a des NATs entre lui et le serveur STUN), l'attaquant ne pourra pas forcer le serveur à générer des MAPPED-ADDRESS arbitraires dans les réponses. Il pourra uniquement forcer le serveur STUN

à générer des MAPPED-ADDRESS qui routeront vers le réseau privé. Ceci car le NAT entre l'attaquant et le serveur STUN réécrira l'adresse source de la requête STUN, la liant à l'adresse publique routant vers le réseau privé. Malheureusement, il est possible qu'un NAT de mauvaise qualité veuille mapper une adresse publique allouée à une autre adresse publique (par opposition à une adresse privée interne), dans ce cas l'attaquant pourrait forger l'adresse source dans une requête STUN qui pourrait être une adresse publique arbitraire. Toutefois, ce genre de comportements est plutôt rare pour un NAT.

**Méthode # : 4 Man In The Middle**

Comme alternative à la méthode 3, si l'attaquant arrive à placer un élément sur le chemin du client au serveur, l'élément peut agir comme un « man in the middle ». Dans ce cas, il peut intercepter une requête STUN et générer une réponse STUN directement avec n'importe quelle valeur désirée pour le champ MAPPED-ADDRESS. Comme alternative, il peut transférer la requête STUN au serveur (après quelques modifications), recevoir la réponse et la transférer au client. S'il transfère cette adresse, elle a les mêmes limitations que pour la méthode 3.

**Méthode # : 5 Injection de réponse plus DoS**

Dans cette approche, l'attaquant n'a pas besoin d'être un « man in the middle » (comme pour les méthodes 3 et 4). Il a uniquement besoin de pouvoir écouter le segment réseau qui transporte les requêtes STUN. Ceci peut être fait aisément dans des réseaux à accès multiple comme Ethernet ou un réseau 802.11 non protégé. Pour injecter une réponse faussée, l'attaquant écoute le réseau pour récupérer une requête STUN. Lorsqu'il en voit une, il lance simultanément une attaque DoS sur le serveur STUN, et génère sa propre réponse STUN avec la valeur MAPPED-ADDRESS désirée. La réponse STUN générée par l'attaquant va atteindre le client et l'attaque DoS contre le serveur va empêcher la réponse légitime du serveur de joindre le client. Il peut être discuté que l'attaquant puisse le faire sans être obligé de faire un DoS sur le serveur, tant que la réponse faussée arrive avant la réponse légitime chez le client, et que le client n'utilise que la première réponse.

**Méthode # : 6 Duplication**

Cette méthode est similaire à la 5, l'attaquant écoute le réseau et récupère une requête STUN. Lorsqu'il l'a vue, il génère sa propre requête STUN vers le serveur. Cette requête est identique à celle qu'il a vue, mais avec une adresse source truquée. Cette adresse truquée est égale à celle que l'attaquant désire avoir placée dans la MAPPED-ADDRESS de la réponse STUN.

En fait, l'attaquant génère un « flood » de ce genre de paquets. Le serveur STUN va recevoir la requête originale, suivie d'une inondation de paquets dupliqués faussés. Si cette inondation est suffisamment puissante pour congestionner les routeurs ou d'autres équipements, il y a une bonne probabilité de chance pour que la vraie réponse se perde, et le résultat sera que seules les réponses truquées seront reçues par le client STUN. Ces réponses sont toutes identiques et contiennent toutes la MAPPED-ADDRESS que l'attaquant souhaitait que le client utilise.

Comme pour la méthode 5, il est possible de ne pas avoir besoin de créer une inondation de paquets, pour autant que la réponse faussée arrive plus rapidement que la réponse réelle vers le client, et que le client ignore la seconde réponse (bien qu'elle soit différente).

Il est bon de noter que dans cette approche, lancer une attaque DoS contre le serveur STUN ou le réseau IP, afin d'empêcher la réponse valide d'être reçue ou envoyée, est problématique. L'attaquant a besoin d'avoir le serveur STUN accessible pour gérer ses propres requêtes. A cause de la retransmission périodique de la requête du client, ceci laisse une toute petite fenêtre d'opportunité pour l'attaque. L'attaquant doit démarrer l'attaque DoS immédiatement après la requête du client, afin d'éliminer la réponse correcte, puis arrêter l'attaque DoS afin d'envoyer ses propres requêtes, le tout avant la prochaine retransmission du client. A cause de l'espacement très petit des retransmissions (entre 100ms et quelques secondes), ceci est très difficile à faire.

- Outre les attaques DoS, il peut y avoir d'autres façons d'empêcher la requête du client d'atteindre le serveur. Une manipulation à la couche 2, par exemple, pourrait être efficace.

# 7 Nos propositions de *Best Practices*

## 7.1 Sécurité de base

### *7.1.1* Mise à jour du software (IPBX, *hardphone et softphone*)

**Identifiant** : S.01

**Description de la solution** :

L'IPBX, les *hardphones* et les *softphones* contiennent tous un logiciel. Le code de ces logiciels peut contenir des failles (*buffer overflow*,…) et donc être vulnérable à diverses attaques.

Il est donc très important de maintenir à jour la version de ces logiciels, notamment lorsqu'une faille de sécurité les concernant a été découverte.

Pour ce faire, il faut :

- Consulter régulièrement les sites des fabricants *hardware*/logiciel des équipements introduit dans l'infrastructure VoIP, ou mieux, être inscrit à leurs *newsletters* de manière à être automatiquement informés si une nouvelle version/*patch* est disponible
- Tester le *patch* sur des équipements de test
- Mettre à jour les équipements de production si le test précédent est concluant

**Sources** :

- P. 6 de [NsaGuid]

### 7.1.2 Verrouillage de la configuration (*hardphone/softphone*)

**Identifiant** : S.02

**Description de la solution** :

Une fois le *hardphone/softphone* configuré, il est important de verrouiller par mot de passe sa configuration afin d'empêcher qu'un utilisateur ne puisse modifier les paramètres (désactiver l'authentification,…).

De plus, des mesures organisationnelles devraient être prises de manière à interdire aux employés toute modification de la configuration des équipements de l'infrastructure VoIP.

**Disponibilité de la solution** :

Sur tout *hardphone/softphone* possédant une fonction de verrouillage

**Sources** :

- p. 34 de [DoD]

## 7.2 Séparation des équipements DATA et VoIP

### 7.2.1 Séparation au niveau IP (*layer* 3)

**Identifiant** : S.03

**Description de la solution** :

Cette solution consiste à attribuer une plage d'adresses IP (ex : 192.168.1.x) au réseau DATA. Ce réseau comprendra tous les équipements qui étaient présents avant l'introduction de la VoIP : postes clients, serveurs (*fileserver*, *Domain Controller*,…), etc.

Une plage d'adresses IP différente (ex : 192.168.2.x) sera attribuée aux équipements VoIP.

Une fois cette séparation effectuée, il est possible de définir des ACL sur les équipements de *Layer 3* (*switches L3/routers/firewalls*) afin de n'autoriser les communications qu'entre les adresses IP autorisées.

De plus, si des services tels que DNS, DHCP ou NTP sont nécessaires, le réseau VoIP doit posséder ses propres serveurs (cf. p. 9 de [NsaGuid]).

**Disponibilité de la solution** :

Disponible sur tout type de réseau

**Sources** :

- p. 37 [DoD]

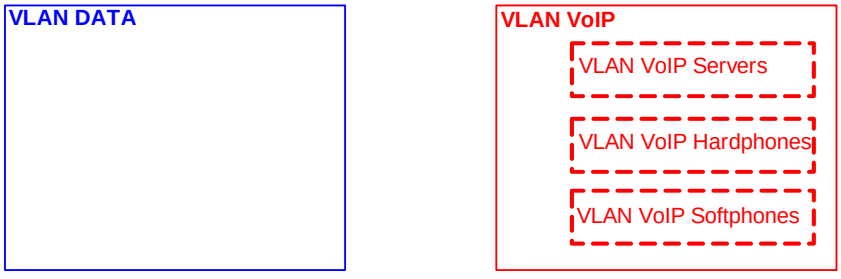
### 7.2.2 Séparation grâce aux VLAN (*layer* 2)

**Identifiant** : S.04

**Description de la solution** :

La deuxième étape de notre défense en profondeur consiste à définir un VLAN DATA dédié aux équipements réseaux présents dans le réseau DATA et un VLAN VoIP dédié aux équipements VoIP. Afin d'obtenir une meilleure séparation, il est conseillé de créer à la place du VLAN VoIP, un VLAN pour chaque catégorie d'équipement VoIP comme :

- Les *hardphones* → VLAN VoIP Hardphones
- Les *softphones* → VLAN VoIP Softphones
- Les serveurs → VLAN VoIP Servers
- …



Cela permet d'établir des règles de filtrage plus fines et d'améliorer la QoS. De plus, si une attaque survient sur le VLAN VoIP Softphone, cela n'affectera pas le bon fonctionnement des autres systèmes VLAN VoIP.

Sil n'est pas possible (pour des raisons de fonctionnalité notamment) d'interdire toute communication entre les VLAN DATA et VoIP, un filtrage Inter-VLAN (au niveau des *switchs* et/ou des *routers*) et/ou des *firewalls* doivent être mis en place afin de filtrer rigoureusement le trafic entre les VLAN.

**Disponibilité de la solution** :

*Switches* possédant la fonctionnalité de VLAN.

**Sources** :

- p. 38 de [DoD]

### 7.2.3 Filtrage Inter-VLAN

**Identifiant** : S.05

**Description de la solution** :

Les communications entre les VLAN mis en place en S.04 doivent être rigoureusement filtrées de manière à n'autoriser que les flux nécessaires. Le filtrage doit être de type liste blanche (seuls les flux définis sont autorisés).

Ce filtrage peut être effectué :

- en définissant des ACL sur les *switches* et/ou les *routers* interconnectant les VLAN
- en plaçant un *firewall* entre les VLAN

Les règles de filtrage devraient être basées sur les adresses IP, les numéros de ports/protocoles et les *flags* TCP/IP de manière à être le plus strict possible et à n'autoriser que les communications nécessaires.

Par exemple, les *IP Phones* n'ont pas besoin d'envoyer un flux média (ex : RTP) aux serveurs VoIP. Donc, au lieu d'autoriser toutes communications entre les VLAN VOIP Hardphones/Softphones et le VLAN VoIP Servers, seul le trafic concernant le protocole de signalisation (ex : SIP) devraient être autorisé.

**Disponibilité de la solution** :

*Switches*/*routers*/*firewalls* permettant de créer des règles de routage Inter-VLAN

**Sources** : fig. 3 et p. 10 de [NsaGuid]

### 7.2.4 Utilisation d'une carte réseau supportant 802.1Q

**Identifiant** : S.06

**Description de la solution** :

Le principal danger lorsque l'on installe un *softphone* sur un ordinateur provient du fait que cet ordinateur, déjà connecté au réseau DATA, devient un terminal VoIP, ce qui est contraire au *best practice* S.04.

Il existe cependant une solution pour maintenir la séparation des VLANS.

Cette solution consiste à équiper les ordinateurs d'une carte Ethernet supportant le protocole 802.1q et de les configurer pour utiliser ce protocole. De telles cartes

Ethernet permettent de séparer le trafic DATA du trafic VoIP (issue du *softphone*) en mettant chaque type de trafic dans leur VLAN respectif.

L'OS, la carte Ethernet et le *softphone* doivent supporter 802.1q.

**Disponibilité de la solution** :

Ordinateur et *softphone* disposant d'une carte 802.1q

**Sources** :

- p. 43 de [DoD]

### 7.2.5 Désactivation ou protection (802.1q) des ports réseaux supplémentaires

**Identifiant** : S.07

**Description de la solution** :

Certains *hardphones* possèdent un (ou plusieurs) port afin de permettre la connexion d'un ordinateur ou d'un autre équipement réseau. Ce port additionnel a pour but de n'utiliser qu'une seule prise réseau pour connecter plusieurs équipements : le *hardphone* fonctionne donc comme un *hub*. Le *hardphone* et l'ordinateur se retrouve donc tout deux sur le même réseau/vlan ce qui est contraire au *best practice* S.04.

La solution consiste à désactiver le(s) port(s) supplémentaire(s) ou à activer le protocole 802.1q sur le *hardphone*. La séparation entre les réseaux/vlan DATA et VoIP est ainsi maintenue.

**Disponibilité de la solution** :

*Hardphone* supportant 802.1q.

**Sources** :

- p. 39 de [DoD]

### 7.2.6 Sécuriser l'accès aux ports des *switches* (ACL,...)

**Identifiant** : S.08

**Description de la solution** :

La séparation établit grâce aux solutions S.03 et S.04 peut être compromise si un individu à la possibilité de connecter une machine à un port d'un *switch*.

Afin d'éviter cela, les sécurités suivantes peuvent être mise en place (classées par ordre croissant d'efficacité) :

- les ports non utilisés devraient être désactivés
- les ports non utilisés devraient être placés dans un VLAN inutilisé
- une ACL (placée au niveau du port ou du *switch* entier) devraient être créée afin de n'autoriser l'accès qu'aux adresses MAC définies
- une authentification 802.1x devrait être mise en place (si les *switches* et les *IP phones* le permettent)

La solution basée sur les ACL est celle préconisée.

Note : Les quatre sécurités énumérées sont cumulables

**Disponibilité de la solution** :

*Switches* possédant une fonction de filtrage par adresse MAC.

*Switches* et *IP phones* permettant la mise en œuvre de 802.1x.

**Sources** :

- P. 9 de [NsaGuid]
- P. 40 § 3.5.2.2 de [DoD]

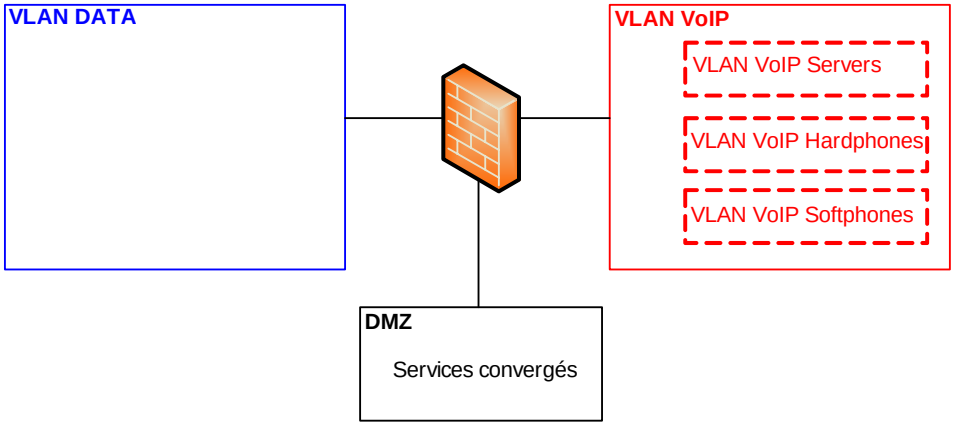
### 7.2.7 Placer les services convergés dans une DMZ

**Identifiant** : S.09

**Description de la solution** :

Afin de ne pas compromettre la séparation des VLAN DATA et VoIP, les services convergés (services nécessitant un accès au VLAN DATA et au VLAN VoIP) doivent être placés dans une DMZ.

Les règles du *firewall* doivent être le plus strict possible afin de n'autoriser que les flux nécessaires.




**Disponibilité de la solution** :

*Firewall* mis en place entre les VLAN

**Sources** : p. 10 de [NsaGuid]

## 7.3 Authentification

### 7.3.1 Authentification HTTP Digest des messages SIP

**Identifiant** : S.10

**Description de la solution** :

*HTTP Digest Authentication* permet au serveur d'authentifier les messages SIP REGISTER et/ou INVITE envoyés par un *IP Phone*. Les attaques basées sur l'usurpation d'identité du client ne sont alors plus possibles (pourvu que la politique de gestion des mots de passes soit efficace).

La mise en place de cette authentification nécessite de configurer HTTP Digest :

- sur le registrar
- sur les *IP Phones*

Cette configuration consiste généralement à :

- définir le domaine d'authentification
- saisir le mot de passe (secret partagé entre le registrar et l'*IP Phone*)

Cette méthode d'authentification étant sensible aux attaques *offline* de type *brute force*, il est recommandé de définir une politique de mots de passes imposant la complexité et une longueur minimale au mot de passe.

**Disponibilité de la solution** :

*IP phones* et registrar supportant l'authentification HTTP Digest des messages SIP

**Sources** :

- p. 42-43 de [NsaGuid]
- [Master]

### 7.3.2 Authentification mutuelle

**Identifiant** : S.11

**Description de la solution** :

L'authentification mutuelle permet au serveur d'authentifier le client et au client d'authentifier le serveur. Les attaques basées sur l'usurpation d'identité ne sont alors plus possibles.

Les méthodes d'authentification mutuelles suivantes peuvent être mise en œuvre :

- SIPS
- H.235 pour H.323
- Protocoles propriétaires

La mise en place d'une méthode d'authentification mutuelle nécessite de configurer la méthode choisie :

- sur l'IPBX
- sur les *IP Phones*

**Disponibilité de la solution** :

IPBX et *IP Phones* supportant au moins une méthode d'authentification mutuelle en commun.

**Sources** :

- p. 42-43 de [NsaGuid]

## 7.4 Chiffrement

### 7.4.1 Chiffrement du flux de signalisation : SIPS,…

**Identifiant** : S.12

**Description de la solution** :

Le chiffrement du flux de signalisation permet de garantir la confidentialité et l'intégrité des données échangées. Les écoutes clandestines sur ce type de flux sont donc prévenues.

Les protocoles pouvant être mis en œuvre sont :

- SIPS (en remplacement de SIP)
- Protocoles propriétaires

Il est toutefois important de remarquer que le chiffrement du flux va introduire un *overhead*. Cet *overhead* peut devenir important pour les serveurs VoIP si le nombre d'appels simultanés devient important. Il est donc important de tester la charge générée par la mise en place du chiffrement de manière à connaître les limites de l'infrastructure VoIP et à permettre de dimensionner les équipements VoIP.

**Concernant SIPS :**

SIPS est basé sur TLS.

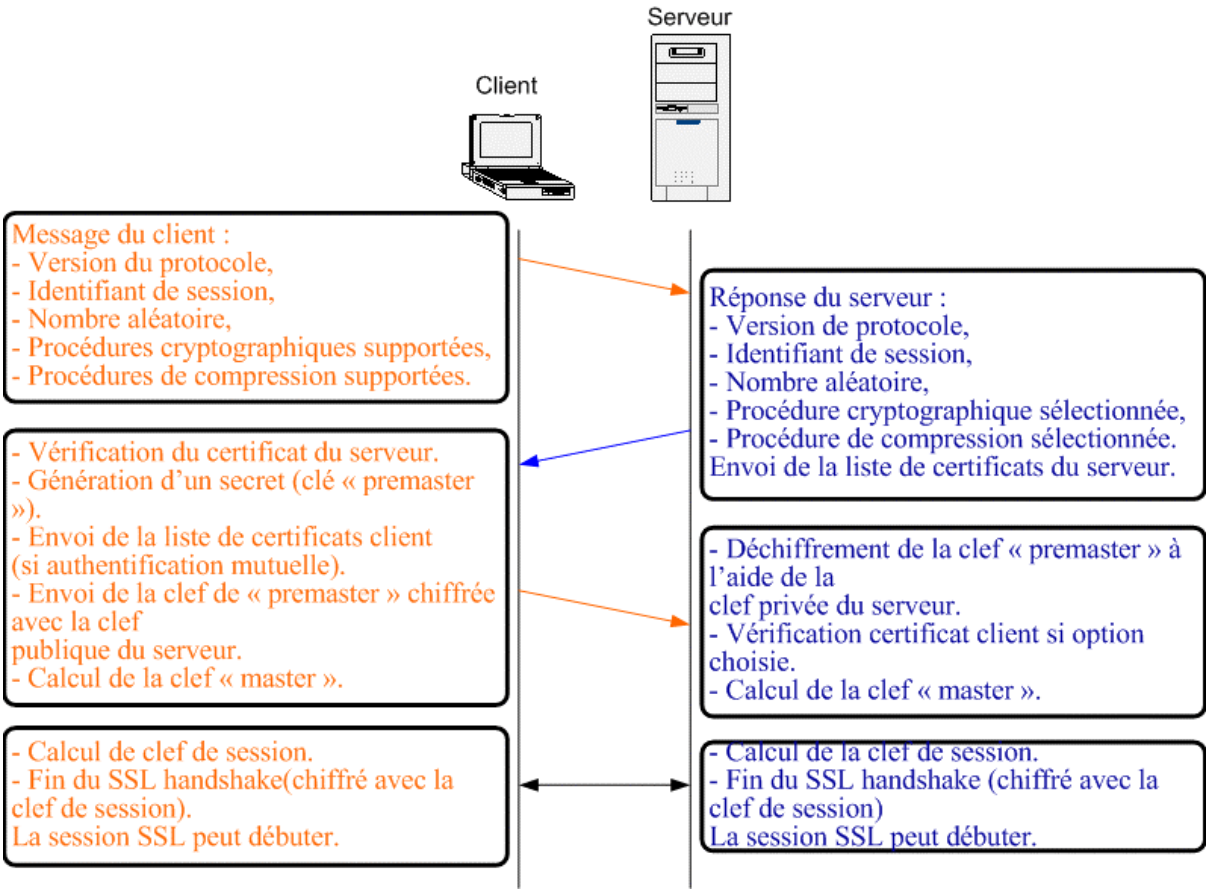
L'intégrité des données est garantie grâce aux MACs (*Message Authentification Code*) basé sur les fonctions de hachage MD5 (16 octets) ou SHA-1 (20 octets).

Il fournit, en plus du chiffrement, selon la configuration :

- l'authentification simple (serveur authentifié auprès de l'*IP Phone*)
- l'authentification mutuelle entre les serveurs et les *IP Phones*.

L'authentification des entités est basée sur le protocole X.509, et elle a lieu durant la phase d'*handshake* de TLS. C'est aussi durant cette phase que sont négociés les algorithmes utilisés (*cypher* et MAC) ainsi que la génération de la clé symétrique de session pour le chiffrement des données.

Le diagramme en flèche suivant détaille les principaux échanges lors d'un *handshake* TLS.




**Disponibilité de la solution** :

Serveur et *IP Phones* supportant au moins une méthode de chiffrement du flux de signalisation en commun.

**Sources** :

- P. 42-43 de [NsaGuid]

### 7.4.2 Chiffrement du flux média : SRTP,...

**Identifiant** : S.13

**Description de la solution** :

Le chiffrement du flux média permet de garantir la confidentialité et l'intégrité des données échangées. Les écoutes clandestines sur ce type de flux sont donc prévenues.

De plus, ce chiffrement fournit l'authentification mutuelle entre les *IP Phones*.

Les protocoles pouvant être mis en œuvre sont :

- SRTP (en remplacement de RTP)
- H.235 pour H.323
- Protocoles propriétaires

Il est important de noter que le chiffrement du flux va introduire un *overhead*, ce qui peut nuire à la qualité de la conversation. En effet, les flux temps réels comme

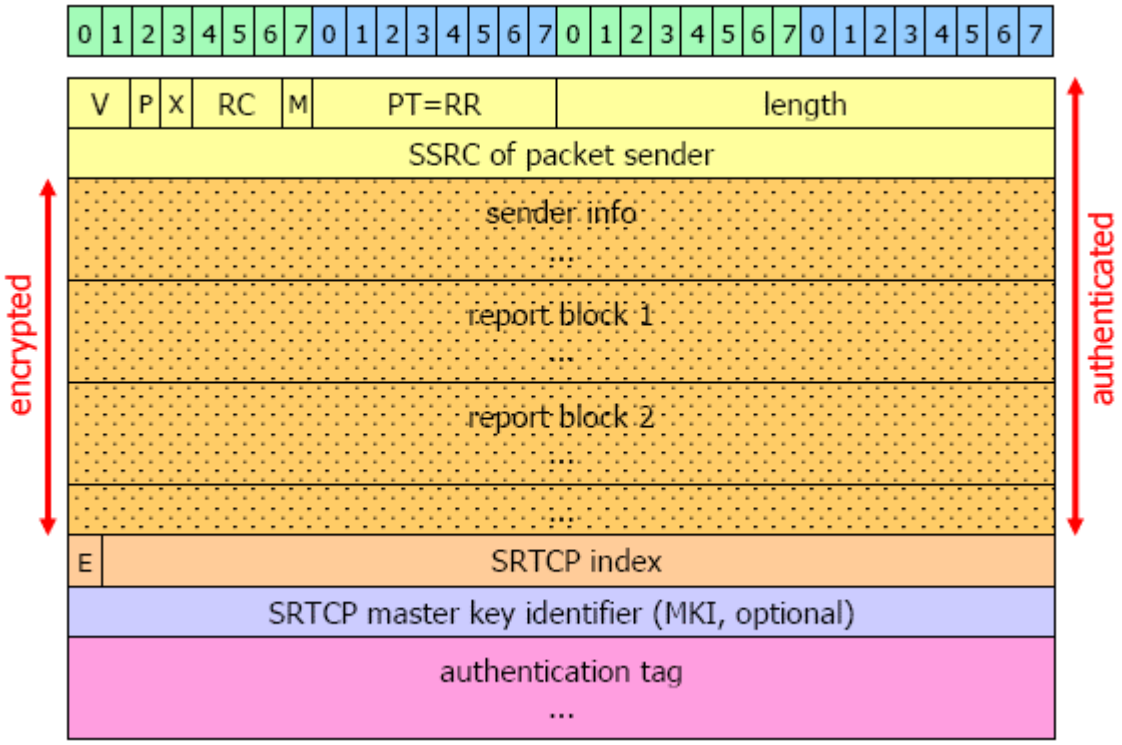
l'audio sont très sensibles aux délais de temps (*time delay*) ainsi qu'aux variations de délais (gigue ou *jitter*). Il faut donc tester que l'*overhead* engendré par l'algorithme de chiffrement soit tolérable (par tolérable, on sous-entend que l'*overhead* ne dégrade pas trop la qualité de la conversation).

**Concernant SIP (et plus précisément, RTP) :**

Le protocole SRTP (*Secured Real-Time Transport* Protocol) est une extension du protocole RTP qui fournit la confidentialité, l'authentification et une protection contre la répétition aux trafics RTP et RTCP. L'utilisation d'AES (*Advanced Encryption Standard*) en mode *stream cipher* garanti une bonne sécurité tout en n'augmentant pas la taille de la cargaison chiffrée. Le *tag* d'authentification utilisé pour vérifier l'intégrité des données ajoute 10 octets à chaque paquet RTP/RTCP mais peut être réduit à 4 octets si la transmission doit être effectué sur un canal de communication lent.

RTP et RTCP peuvent donc être sécurisés de manière cryptographique respectivement par SRTP et SRTCP (*Secured Real-Time Transport Control Protocol*) tout en ne provoquant pas de problèmes significatifs sur la qualité de la transmission.

Voici le format d'un paquet SRTP :




On peut voir facilement que seul le corps de cargaison RTP est chiffré. Le champ MKI est optionnel et permet d'identifier la clé primaire depuis laquelle les autres clés de sessions sont dérivées. Le MKI peut être utilisé par le récepteur pour retrouver la clé primaire correcte lorsque le besoin d'un renouvellement de clé survient.

Le numéro de séquence sur 16 bits est utilisé de manière simultanée avec le compteur de *rollover* (*Rollover Counter*) de 32 bits qui se trouve être une partie du contexte cryptographique, pour la session SRTP, afin de se prémunir contre les *replay attacks*.

Le *tag* d'authentification est un *checksum* cryptographique (HMAC SHA-1) calculé sur l'entête et le corps du paquet RTP. Son utilisation permet de prémunir les messages contre une modification non autorisée. La longueur par défaut du *tag* est de 10 octets mais peut être réduit si le canal de transmission ne permet pas une grande augmentation de la taille des paquets RTP.

La sécurisation des paquets RTCP se fait de manière similaire à celle de RTP. L'unique différence est l'obligation d'utiliser le *tag* d'authentification afin d'éviter à un attaquant de terminer un flux média RTP en envoyant un message SIP BYE.

**Disponibilité de la solution** :

IPBX et *IP Phones* supportant au moins une méthode de chiffrement du flux media en commun.

**Sources** :

- P. 42-43 de [NsaGuid]
- **Advanced Encryption Standard**
  Wikipedia, the free encyclopedia
  Version du 18 mai 2006
  http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
  *(Dernière visite le 19 mai 2006)*

### 7.4.3 Chiffrement avec IPSec (ou autre technologie VPN)

**Identifiant** : S.14

**Description de la solution** :

Le chiffrement des flux avec IPSec (ou une autre technologie VPN) permet de garantir la confidentialité et l'intégrité des flux échangés. L'authentification mutuelle des protagonistes est également assurée.

Les protocoles pouvant être mis en œuvre sont :

- IPSec
- Autre technologie VPN

Il est important de noter que le chiffrement du flux va introduire un *overhead*. Il faut donc tester que cette overhead est tolérable avant de mettre en œuvre un VPN.

**Concernant SIP (et plus précisément SIP protégé par IPSec) :**

IPSec est un mécanisme général pouvant être utilisé pour protéger les messages SIP au niveau IP. Avec SIP, chaque *proxy* sur le chemin doit avoir accès en lecture/écriture sur l'entête des messages SIP afin de pouvoir ajouter/retirer des entêtes VIA. Afin de permettre l'utilisation d'IPSec ESP (*Encapsulating Security Payload*) ou AH (Authentification Header), son fonctionnement doit être basé sur un mode *Hop-By-Hop*.

IPSec est basé sur un assortiment de mécanismes protégeant les données échangées sur le réseau. Il fonctionne à la couche IP et traite tous les paquets IP. Ainsi, il protège toutes les applications et peut être implémenté dans tous les appareils utilisant le réseau de manière point à point voir lien à lien.

Son but est donc d'éviter l'espionnage du flux de données et l'accès illicite aux ressources. Il permet de garantir la confidentialité et l'authenticité des données

échangées. Il fournit également une protection contre les *replays-attacks*. Il est bon de remarquer qu'il permet un haut niveau de protection s'il est utilisé avec des algorithmes forts et dans un environnement sécurisé.

Ces fonctionnalités sont fournies par des mécanismes cryptographiques :

- *Message Authentication Code* (MAC) = Authenticité des données
- Chiffrement des données = Confidentialité des données
- Numéro de séquence = protection contre les *replays-attacks*

Ces mécanismes sont implémentés à l'aide de deux extensions du protocole IP :

- AH (*Authentification Header*) qui permet d'assurer l'authenticité des datagrammes IP
- ESP (*Encapsulating Security Payload*) qui assure la confidentialité des données et/ou leur authenticité

AH et ESP peuvent fonctionner avec plusieurs algorithmes cryptographiques, toutefois l'IETF préconise l'utilisation de **triple DES** (128 bits) pour le chiffrement et **HMAC-MD5** ou **HMAC-SHA1** pour l'authenticité.

**Disponibilité de la solution** :

IPBX et *IP Phones* supportant IPSec (ou autre technologie VPN)

**Sources** :

- P.42 de [NsaGuid]
- Travail de diplôme Ludovic Maret
- **IPsec : des bases au protocole IKE**
  Ghislaine Labouret – HSC
  Intervention réalisée au séminaire WebSec 2000, le 21 mars 2000
  http://www.hsc.fr/ressources/presentations/websec2000/index
  *(Dernière visite le 19 mai 2006)*

## 7.5 Sécurité périmétrique

### 7.5.1 SBC : Définitions de seuils / *Call Admission Control*

**Identifiant** : S.15

**Description de la solution** :

Les attaques DoS entraînent par définition un nombre anormalement élevé de transactions réseau.

Grâce au SBC, l'administrateur réseau a la possibilité de définir des seuils, basés sur divers critères, permettant de limiter le trafic entrant et/ou sortant d'un réseau. De cette manière, le SBC évite de surcharger les *switchs* et de mettre hors-service certains équipements et/ou le réseau.

Il est recommandé de placer les seuils sur les éléments suivants :

- Limitation du trafic de signalisation VoIP par session
- Limitation du trafic de signalisation VoIP par utilisateur enregistré (*subscriber*)
- Limitation du trafic de signalisation VoIP par réseau
- Limitation globale volume de signalisation VoIP

Il est également recommandé de placer les mêmes types de seuils non plus par rapport à la signalisation VoIP en général, mais par rapport au type de message de signalisation VoIP.

**Disponibilité de la solution** :

SBC supportant les seuils pour faire du *Call Admission Control*

**Sources** :

- P.40-41 de [SBCdc]

### 7.5.2 Utilisation de serveurs dédiés pour STUN

**Identifiant** : S.16

**Attaques prévenues** : (référence à leur identifiant) 12354, 23423

**Description de la solution** :

Il est aussi recommandé que les serveurs STUN tournent sur des serveurs dédiés à STUN, avec tous les ports TCP et UDP désactivés excepté les ports STUN. Ceci permettra d'éviter des virus ou chevaux de Troie d'infecter les serveurs STUN, et ainsi empêcher qu'ils soient compromis. (permettant d'éviter la méthode 1 décrite dans les attaques, voir chap. 3).

**Disponibilité de la solution** :

Possibilité d'avoir un serveur STUN dédié

**Sources** :

- **RFC 3489 : STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)**

### 7.5.3 Vérification de l'identité du serveur STUN

**Identitifant :** S.17

**Attaques prévenues :**

**Description de la solution :**

STUN contient un mécanisme de vérification d'intégrité des messages, demandant au client STUN de tout d'abord faire une demande de secret partagé envers le serveur STUN. Le serveur STUN va ensuite lui répondre en lui indiquant un nom d'utilisateur et un mot de passe. Lorsque le client va ensuite faire sa requête, il va y insérer un champ « Message Integrity » ainsi qu'un username, qui permettra au serveur de vérifier l'intégrité du message. Les réponses vont ensuite contenir elles aussi un champs permettant de vérifier l'intégrité des messages.

Cette fonctionnalité n'est pas obligatoire, elle est notée « SHOULD » dans la RFC de STUN. Il faut donc vérifier qu'elle soit bien activée et que les demandes et les réponses possèdent bien ce champ « Message Integrity » et qu'elles soient bien vérifiées à chaque transaction.

**Disponibilité de la solution** :

Le serveur STUN utilisé doit avoir la fonctionnalité de vérification de l'intégrité des messages.

**Sources** :

- **RFC 3489 : STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)**

### 7.5.4 Client STUN : Continuation de l'écoute des réponses après réception de la première réponse

**Identifiant :** S.18

**Attaques prévenues :**

**Description de la solution :**

La réception d'une réponse de la part du serveur STUN (que ce soit une erreur ou une Binding Response) doit normalement terminer les transmissions de cette requête. Toutefois, les clients doivent continuer à écouter les réponses durant 10 secondes après la première réponse. Si durant ces dix secondes une réponse contenant des informations autres est reçue, il est probable qu'une attaque est en cours.

Il est donc important de vérifier que les clients STUN utilisés fassent cette vérification et avertissent l'utilisateur le cas échéant. Cette solution ne résout pas directement le problème, mais avertit l'utilisateur en cas d'attaque, qui pourra prendre ses dispositions pour la bloquer et/ou couper toute communication en cours.

**Disponibilité de la solution** :

Les clients STUN utilisés doivent faire cette vérification.

**Sources** :

- **RFC 3489 : STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)**

### 7.5.5 Relais STUN : Limitation de la bande passante allouée par personne

**Identifiant** : S.19

**Attaques prévenues** :

**Description de la solution** :

Puisque les serveurs STUN implémentant les fonctions de relais allouent des ressources, ils sont susceptibles d'être victimes d'attaques du type déni de service, toutes les requêtes d'allocation sont authentifiés ce qui permet d'éviter à un attaquant inconnu de lancer une attaque. Toutefois, un attaquant authentifié pourrait générer de multiples requêtes d'allocation.

Pour empêcher un simple utilisateur malicieux d'allouer toutes les ressources du serveur, il est recommandé qu'un serveur implémente une limite modeste de bande passante qui peut être allouée par personne.

Toutefois, un tel mécanisme n'empêche pas un large nombre d'utilisateurs mal intentionnés de demander un faible nombre de ressources. Ce genre d'attaques sont possibles en utilisant des botnets, et sont difficiles à détecter et empêcher.

**Disponibilité de la solution** :

Le serveur STUN utilisé doit avoir cette fonctionnalité

**Sources** :

- **Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)**
  anciennement TURN, version du 27 février 2006, expire le 31 août 2006
  http://www.ietf.org/internet-drafts/draft-ietf-behave-rfc3489bis-04.txt
  *(dernière visite le 12 octobre 2006)*

# 8 Références

[TutoSIP] L. Schweizer, **Tutorial SIP**,
http://www.iict.ch/Tcom/Projets/VoIP/VoIP_and_Mobility/Tutoriaux/Tutorial_SIP.pdf

[IPTelCook] **IP Telephony Cookbook**,
http://www.terena.nl/activities/iptel/contents1.html

[DodNet] **Network Infrastructure – Security Technical Implementation Guide**
http://iase.disa.mil/stigs/stig/network-stig-v6r4.pdf

[NistXP] **Guide to securing Windows XP**
http://csrc.nist.gov/itsec/SP800-68.zip

[NsaArch] **Recommended IP Telephony Architecture**
http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/voip/I332-009R-2006.pdf

[NsaGuid] **Security Guidance for Deploying IP telephony Systems**
http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/voip/I332-016R-2005.PDF

[NIST] **NIST - Security Considerations for Voice Over IP Systems**,
http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

[DoD] **IP Telephony & VoIP : Security technical implementation guide**
http://csrc.nist.gov/pcig/STIGs/VoIP-STIG-V2R2.pdf

[Junip] Juniper Networks, **Enterprise VoIP Security : Best Practices**,
http://www.juniper.net/solutions/literature/white_papers/200179.pdf

[Digest] **Study of Digest Authentication for Session Initiation Protocol**
http://www.site.uottawa.ca/~bob/gradstudents/DigestAuthenticationReport.pdf

[VoixSurIP] **La voix sur IP**
ISBN 2-10-007-480-6

[SBCdc] Data Connection, **Session Border Controllers**

http://www.dataconnection.com/network/download/whitepapers/sessionbordercontroller.pdf

[RFCSip] **RFC 3261: Session Initiation Protocol**
http://www.ietf.org/rfc/rfc3261.txt

[IPTelScenar] **IP-telephony scenarios**,
http://www.uninett.no/sip/scenarier.en.html