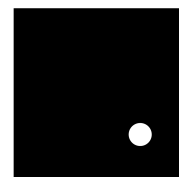


L'INFORMATIQUE  
COMMUNICANTE

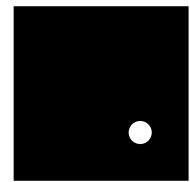
# La sécurité de la Téléphonie sur IP

Eric Nizard  
Avril 2007



## Table des matières

<b>1</b>	<b>LA TOIP POSE-T-ELLE DES PROBLEMES DE SECURITE SPECIFIQUES ?</b>	<b>3</b>
1.1	Qu'est-ce que la téléphonie sur IP ?	3
1.1.1	Principes de base de la téléphonie sur IP	3
1.1.2	Enjeux de la Téléphonie sur IP	3
1.1.3	Modèles d'architecture de Téléphonie sur IP	4
1.2	Quelles sont les vulnérabilités de la téléphonie sur IP ?	5
<b>2</b>	<b>TYPES DE MENACES</b>	<b>6</b>
2.1	Fraude	6
2.2	Rupture de confidentialité	6
2.3	Rupture d'intégrité	6
<b>3</b>	<b>EVALUER LES RISQUES</b>	<b>7</b>
3.1	Champ d'évaluation	7
3.2	Evaluation qualitative	7
3.3	Evaluation quantitative	7
3.4	Traçabilité des attaques – réévaluation des risques	7
<b>4</b>	<b>DISPOSITIFS DE SECURISATION</b>	<b>8</b>
4.1	Maîtrise de son système	8
4.2	Sécurité des flux de téléphonie sur IP	8
4.2.1	Etanchéisation des flux IP de téléphonie par VLAN	8
4.2.2	Pare-feu spécifiques	9
4.2.3	Protocole sécurisé : SRTP (Secure RTP)	9
4.3	Sûreté de fonctionnement de l'architecture	9
4.3.1	Sûreté de fonctionnement du serveur d'appel	9
4.3.2	Sûreté de fonctionnement des passerelles TDM	10
4.3.3	Disponibilité des postes téléphoniques critiques	10
4.4	Sécurité d'un sous-système radio	10
4.5	Sécurisation des applications de communications	11
4.6	Sécurité du déploiement	11
4.7	Sécurité de l'exploitation : sauvegarde des programmes et des paramètres	12
4.8	Un effet d'aubaine ? La sécurité des personnes	12
<b>5</b>	<b>SYNTHESE DES RISQUES ET DES PARADES</b>	<b>13</b>
<b>6</b>	<b>IMPACT D'UN SINISTRE : FONCTIONNEMENT EN MODE DEGRADE</b>	<b>14</b>
<b>7</b>	<b>INSTITUTIONS DE REFERENCE SUR LA SECURITE DE LA TOIP</b>	<b>15</b>
<b>8</b>	<b>ANNEXE : SKYPE ET LA SECURITE</b>	<b>17</b>



# 1 La ToIP pose-t-elle des problèmes de sécurité spécifiques ?

## 1.1 Qu'est-ce que la téléphonie sur IP ?

### 1.1.1 Principes de base de la téléphonie sur IP

#### **IP = Protocole Internet (1975)**

Norme mondiale d'échange d'informations entre ordinateurs (réseaux IP)

#### **Voix sur IP (1995)**

Ensemble de technologies pour adapter aux réseaux IP :

- la signalisation
- la voix (numérisation, compression / décompression, mise en paquets)

#### **Téléphonie sur IP (2003)**

Mise au point des technologies de VoIP pour :

- Bâtir un réseau IP entre systèmes pour remplacer les liens directs
- Utiliser des téléphones natifs VoIP
- Téléphoner à partir des ordinateurs (« softphones » sur PC)
- Mixer les ressources : postes classiques et postes VoIP
- Intégrer la téléphonie dans l'informatique (cf. centres de contacts) ...

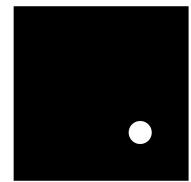
#### **Déploiement de la ToIP (2006 ...)**

- Quel moteur ?
- Quelle stratégie ? Interne ? Externe ? Mixte ?
- Quelle méthode ? Câblage, LAN, validation de QoS ...
- Quel rythme ? Comment migrer ?

### 1.1.2 Enjeux de la Téléphonie sur IP

#### **Enjeux stratégiques**

- Meilleure qualité du contact téléphonique avec le public (aide à la décision, historique)
- Nouvelles fonctions évoluées de téléphonie (ex. outil de management, indicateur de la Qualité de l'Accueil téléphonique, vitrine de l'institution ou de la société)
- Notions de centre de contacts distribué, standards mutualisés
- Mobilité favorisée – Travail à distance transparent
- Améliorer ipso facto l'infrastructure réseau (effet d'aubaine)



### Enjeux économiques

- Economie de maintenance et évolution des infrastructures (câblage, LAN, WAN)
- Economie sur le budget télécom (abonnements et communications)
- Economies d'investissement en autocommutateurs (PABX)
- Des postes IP standards et faciles à installer

### Enjeux d'organisation

- N'utiliser et ne gérer qu'un seul réseau V/D (Téléphonie = application du système d'information) – convergence des équipes d'exploitation et de support
- Certains sites sont des extensions de sites plus importants = évolutions faites en temps réel sur les sites importants (moins de déplacements)
- Réduction du recours du nombre de sous-traitants locaux
- Mise en place de partenariats plus actifs entre les sites

#### 1.1.3 Modèles d'architecture de Téléphonie sur IP

En 2007, une entreprise qui souhaite renouveler toute ou partie de son système téléphonique, se tournera nécessairement vers la téléphonie sur IP

En fonction de son activité, sa taille, ses évolutions prévues, sa politique budgétaire ... ainsi que du degré de criticité de sa téléphonie, elle adoptera l'un des modèles d'architectures suivants, voire une combinaison de plusieurs d'entre eux :

#### Fournisseur de Téléphonie Internet (FTI)

- Service au poste (à l'unité)
- Service multi poste via une ... box

#### IP PBX

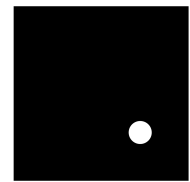
- PBX privé traitant la VoIP, pouvant être :
  - Mixte (ou hybride) « circuit » et VoIP
  - Pur VoIP
- Avec une gestion interne ou externe
- Local ou distant (IP abolit les distances)

#### IP Centrex

- Service de type IP PBX, mutualisé, distant, opéré par un opérateur
- Accessible en haut débit (ADSL, ...)

#### Et aussi ... Intégration dans les applications

- « Click to Call »
- Microsoft Office Communicator (MOC), Live Communication Server (LCS)
- Skype



## 1.2 Quelles sont les vulnérabilités de la téléphonie sur IP ?

Les systèmes téléphoniques deviennent de vrais systèmes informatiques, avec la vulnérabilité intrinsèque de ces derniers.

En particulier, le protocole IP (Internet Protocol !!) est la voie de communication cible idéale pour les hackers.

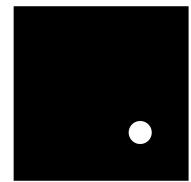
Donc tout système accessible via IP est une cible potentielle de l'ensemble des menaces pesant sur les réseaux IP.

Un deuxième niveau de vulnérabilité concerne les ressources de ToIP elles-mêmes : serveurs et passerelles.

Il est donc nécessaire de se prémunir des malveillances et des intrusions sur les systèmes mis en œuvre via une juste évaluation des risques.

Les autres vulnérabilités traditionnelles sont :

- Certaines fonctions du système lui-même
  - la fonction DISA (accès au PABX de l'entreprise pour du télétravail)
  - le renvoi vers un n° extérieur
  - la conférence à 3 (avec enregistrement)
  - Least Cost Routing trafiqué
- Les accès de télémaintenance (soit via IP soit via modem)
- Les modems en général
- Tickets de taxation :
  - Lecture : permet d'ausculter les communications téléphoniques
  - Ecriture sauvage ou destinée à nuire à un individu
- Télécopieurs : manque de confidentialité
- Les câbles téléphoniques (écoutes)
- Détournement des appels entrants à caractère commercial par un concurrent



## **2 Types de menaces**

### **2.1 Fraude**

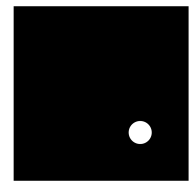
- Usurpation d'identité,
- Téléphoner en imputant la taxe sur un autre,
- Aboutements d'appels vers des appels surtaxés
- Falsification de la taxation,
- Utilisation abusive des ressources (ex : vol de minutes pour revente)

### **2.2 Rupture de confidentialité**

- Entrée en Tiers (sans bip),
- Interception et Enregistrement des conversations
- Ecoute téléphonique
- Ecoute des boîtes vocales.

### **2.3 Rupture d'intégrité**

- Intrusion sur le système téléphonique,
- Attaques virales du système (virus, vers, chevaux de Troie...)
- Destruction ou altération des données,
- Altération de fichiers (annuaire, boîtes vocales)
- V-Bombing : spam sur les messageries vocales
- Recomposition des messages vocaux,
- Modification des données de programmation,
- Déni de service.
- Dégradations physiques des équipements (serveurs, infrastructure) et des postes



### **3 Evaluer les risques**

Elaborer la matrice à 3 dimensions d'évaluation des risques :

- champ d'évaluation
- évaluation qualitative
- évaluation quantitative

#### **3.1 Champ d'évaluation**

Sur le système téléphonique et ses éléments auxiliaires :

- Terminaux
- Passerelles
- Serveurs de conférence
- Serveurs d'appel
- Serveurs de management
- Systèmes de taxation
- Réseau IP

#### **3.2 Evaluation qualitative**

- Risques de Fraude,
- Risques de Dysfonctionnements, atteinte à la disponibilité
- Risques d'atteinte à la Confidentialité
- Risque d'atteinte à la Qualité
- Risques de destruction

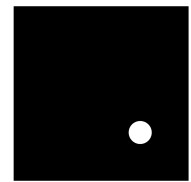
#### **3.3 Evaluation quantitative**

L'évaluation quantitative des risques doit être considérée comme une activité à part entière dans un projet de sécurité d'un système de téléphonie sur IP, en accord avec la politique de sécurité de l'entreprise.

#### **3.4 Traçabilité des attaques – réévaluation des risques**

Un système de ToIP doit avoir la capacité de fournir des statistiques relatives aux attaques dont il est objet. Il en va de même pour le réseau IP d'infrastructure.

Ces informations doivent être compilées régulièrement afin de réévaluer les risques et donc de faire évoluer les dispositifs de sécurisation.



## **4 Dispositifs de Sécurisation**

Ce sont des dispositifs de prévention et de neutralisation des diverses attaques et piratage pouvant s'exercer sur le système de téléphonie.

L'application de ces dispositifs doit se faire en conformité avec la politique générale de sécurité.

Les principaux types de dispositifs sont les suivants :

- Maîtrise de son système
- Résilience – sûreté de fonctionnement de l'architecture
- Sécurisation des flux de téléphonie sur IP

### **4.1 Maîtrise de son système**

Le système téléphonique doit être sous le contrôle de l'entreprise qui l'utilise.

Voici dans l'ordre de contrôle décroissant les modèles d'architecture de ToIP :

1. Système de ToIP interne
2. Système de ToIP externalisé
3. IP Centrex
4. Applications de Voix sur IP sur PC (Skype ...)

### **4.2 Sécurité des flux de téléphonie sur IP**

La sécurisation des flux de téléphonie sur IP s'effectue à travers un schéma conceptuel de sécurité qui comprend les dispositifs suivants :

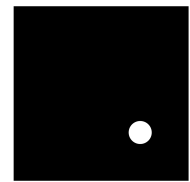
- Etanchéisation par VLAN
- Protection par Firewall
- Authentification et cryptage par VPN sécurisé
- Filtrage par « Access Lists »

#### **4.2.1 Etanchéisation des flux IP de téléphonie par VLAN**

L'ensemble des composants du système qui sont connectés au réseau IP constituant l'infrastructure du système ont la capacité de constitution de VLAN garantissant l'étanchéité des flux.

Le système interdit tout appel en provenance d'un équipement ne faisant pas partie de l'un des VLAN configurés à l'installation.

Le gestionnaire de réseau du site dispose de la faculté de reconfigurer l'un ou l'autre de ces VLAN pendant la durée de vie du système.



#### 4.2.2 Pare-feu spécifiques

Ces pare feu, outre leur fonction au niveaux protocolaires IP, TCP et UDP, analysent le contenu des communications SIP ou H.323 pour traquer les virus cachés dans ces protocoles.

#### 4.2.3 Cryptage

Cisco propose le cryptage de la voix depuis la v 4.1 du Call Manager (postes 7940G et 7960G).

Les autres ont suivi.

Mais attention aux performances !!

#### 4.2.4 Protocole sécurisé : SRTP (Secure RTP)

RFC 3711 : <http://www.ietf.org/rfc/rfc3711.txt>

Etat : « proposed standard »

#### Apports

- Confidentialité
- Authentification
- Protection contre le rejeu

#### Exemples d'implémentation

- Minisip : <http://www.minisip.org/index.html>
- Softphone sous Linux

Encore peu d'offres de constructeurs et d'opérateurs

Inter opérabilité à vérifier au cas par cas

### 4.3 Sûreté de fonctionnement de l'architecture

#### 4.3.1 Sûreté de fonctionnement du serveur d'appel

Redondance des fonctions de serveur d'appel et de signalisation.

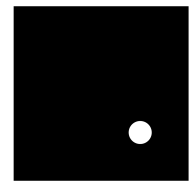
Les deux unités fonctionnent simultanément, se répartissant en permanence la charge complète de l'installation via un dispositif d'équilibrage de charge.

En cas de défaillance de l'une des deux unités, l'autre a la capacité de reprendre à sa charge une certaine quantité de postes.

Tenir compte des fourchettes de pourcentage moyen et instantané de charge de chaque serveur.

De plus chacune des deux unités est renforcée par les dispositifs de sécurisation suivants :

- Une unité centrale à tolérance de pannes
- Un double attachement au réseau Ethernet d'infrastructure en respectant les interfaces des commutateurs LAN
- Une alimentation électrique redondée et sécurisée



### 4.3.2 Sûreté de fonctionnement des passerelles TDM

Pour minimiser les dévoiements de câblage et optimiser la sûreté de fonctionnement des passerelles TDM, il est prudent de fournir et d'installer une passerelle TDM dans chaque local technique où aboutit une arrivée Trunk (T2, SIP Trunking ...) d'Opérateur.

Chaque passerelle possède :

- Une alimentation électrique redondée et sécurisée
- Un double attachement au réseau Ethernet d'infrastructure

### 4.3.3 Disponibilité des postes téléphoniques critiques

Lors de la collecte des données, l'utilisateur définit un certain nombre de postes téléphoniques dont la disponibilité est particulièrement critique, même en cas de défaillance d'une partie du système ou de l'infrastructure.

Ces postes bénéficient dans l'architecture de plusieurs niveaux de double desserte :

- commutateur LAN ondulé avec PoE
- routeur (si site distant)
- serveur d'appel de référence

En cas de défaillance, d'un élément situé à un niveau de desserte donné, l'autre prend le relais.

## 4.4 Sécurité d'un sous-système radio

Les technologies radio les plus en vue sont : DECT, Wi-Fi.

### DECT

La norme DECT ne s'appuie pas sur IP.

Cependant aujourd'hui les industriels proposent des bornes DECT

Un sous-système DECT (ainsi que la totalité des postes qu'il dessert) a potentiellement la capacité de fonctionner de manière autonome même en cas d'indisponibilité des serveurs d'appel.

Ce fonctionnement autonome permet à un poste DECT de continuer à émettre et recevoir des appels aussi bien avec un autre poste DECT qu'avec les réseaux extérieurs.

Il suffit pour cela :

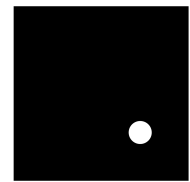
- de raccorder un nombre approprié de liens Opérateur entrants et sortants directement sur le système DECT, sans passer par le système téléphonique filaire.
- de redonder l'architecture du sous-système central DECT

### Wi-Fi

C'est plus compliqué.

En effet, les menaces pèsent sur :

- le réseau Wi-Fi
- IP
- Le système téléphonique



La difficulté est accrue par le fait que les performances du Wi-Fi sur IP sont de facto moindres que celles du DECT.

## 4.5 Sécurisation des applications de communications

La sécurisation des applications de communications ACD, AVI, messagerie vocale ou unifiée ... leur permet un certain degré de tolérance de pannes.

Le(s) serveur(s) bénéficie(nt) :

- d'un double attachement au réseau IP d'infrastructure
- d'une double alimentation électrique

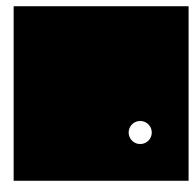
## 4.6 Sécurité du déploiement

### Prérequis

- Analyser la qualité du service offert au téléphone
  - o Accueil des appelants extérieurs
  - o Remontée des fiches clients
- Analyser les coûts existants
  - o Coûts des abonnements
  - o Coûts inter sites
  - o Coûts des communications vers l'extérieur
- Analyser la qualité de service des infrastructures
  - o Réseau WAN
  - o Réseau LAN
  - o Câblage
- Analyser la gouvernance
  - o Ressources humaines utilisées
  - o Optimisations possibles
- Analyser le degré de vétusté des installations téléphoniques

### Organisation et Gestion de projet

- Définir et attribuer les responsabilités
- Former les équipes
- Planifier et organiser l'exploitation
- Accompagner les utilisateurs au changement



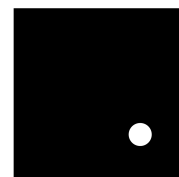
#### **4.7 Sécurité de l'exploitation : sauvegarde des programmes et des paramètres**

Le système doit être équipé d'un dispositif permettant la sauvegarde automatique (programmable) des données (paramétrage des postes, annuaire LDAP) et des programmes nécessaires à son bon fonctionnement dans un système tiers et potentiellement, dans le sous-système de sauvegarde du système d'information.

Il est nécessaire d'impliquer les exploitants préalablement à la mise en service.

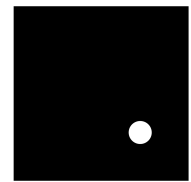
#### **4.8 Un effet d'aubaine ? La sécurité des personnes**

Le couplage entre le système téléphonique et un système de géolocalisation des personnes (par triangulation par exemple) permet d'accroître la sécurité de ces personnes (itinérantes dans un grand site industriel ou un hôpital par exemple).



## 5 Synthèse des risques et des parades

Périmètre	Risques	Parades	Commentaires
Postes	Usurpation identité	Authentification forte	Pas encore implémenté
	Interception flux	SRTP : authentification, cryptage	Standard en cours de finalisation. Pas encore implémenté.
	Interception flux	Cryptage	Augmente la bande passante nécessaire et donc implique un bon dimensionnement
	Déni de service, vers PC et softphone	Mise à jour régulière des patchs de sécurité	
	Forçage tension sur 802.3af	Gérer le 802.3af sur un équipement passif non attaquant	
Réseau LAN-WAN	Mélange trafic entre postes et serveurs	VLAN dédié pour la voix	
	Déni de service vers serveurs	Protection par Access List (ACL)	ACL implique commutateurs LAN performants
	Déni de service vers serveurs	Firewall et NAT symétrique si nécessaire	
	Protection flux d'administration	SNMP V3	
Serveurs	Déni de service	Mise à jour régulière des patchs de sécurité	
	Attaques virales	OS durcis et limités au minimum de fonctions nécessaires	
	Déni TCP SYN	Filtrage en amont des sessions TCP : firewall de niveau 7, terminaison dans média gateway, ...	
	Accès à l'interface d'administration	SSH	
	Accès physique non autorisé	Mise en salle blanche	



## **6 Impact d'un sinistre : fonctionnement en mode dégradé**

Comment assurer la continuité du système téléphonique après un sinistre ?

### **Cas des Systèmes téléphoniques à forte intégration informatique**

Exemples : centre d'appel & téléphonie de salles de marché.

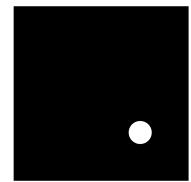
La solution est assujettie au PCA informatique.

### **Cas du système téléphonique général de l'entreprise**

Les dispositions suivantes auront été prises et inscrites dans le PCA de l'activité téléphonique :

- Mise en œuvre d'un numéro 0800 – en cas de sinistre le reroutage de ce type de numéro vers un autre site est très simple (peut être effectué par le client de l'Opérateur par Internet)
- Reroutage des numéros géographiques par plages SDA combiné avec la mise en service d'un mini centre d'appels
- Utilisation massive du GSM pour les appels sortants

Les procédures du PCA doivent avoir été planifiées et transmises aux exploitants préalablement à la mise en service du système téléphonique.



## 7 Institutions de référence sur la sécurité de la ToIP



La VOIPSA (<http://www.voipsa.org/>) est une collaboration entre

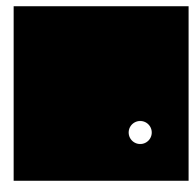
- Vendeurs
  - *de solutions de sécurité : SecureLogix, Spirent, Symantec*
  - *d'équipements 3com, Alcatel, Avaya, Netcentrex, Siemens*
  - *de services : Ernst & Young*
- Universités
  - *Columbia, Southern Methodist*



## Voice over Packet Security Forum

Your single (open) source for NGN/VoIP Security issues and solutions

- Initiative
  - Universitaires
  - Opérateurs : BT, SBC, Telcordia
- Buts : informer et échanger, conférences, tests, ...
- Philosophie « Open Source »
- <http://www.vopsecurity.org/>
- Mailing list
- Outil de test : VoIP security scanner (SiVus)



L'INFORMATIQUE  
COMMUNICANTE

### **A propos de L'INFORMATIQUE COMMUNICANTE**

L'INFORMATIQUE COMMUNICANTE (LIC), créée en 1990, est une Société spécialisée dans le Conseil, l'Expertise et le transfert de compétences en réseaux et systèmes de communication.

Elle s'investit notamment particulièrement sur les projets de mise en œuvre de systèmes de Téléphonie sur IP en entreprise depuis plusieurs années.

### **Contact**

Eric NIZARD (Directeur)

[eric.nizard@lic.fr](mailto:eric.nizard@lic.fr)

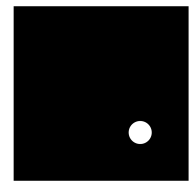
L'INFORMATIQUE COMMUNICANTE

215, Rue Jean-Jacques Rousseau

92136 Issy-les-Moulineaux Cedex

Tél : 01 46 62 91 00

[www.lic.fr](http://www.lic.fr)



## **8 Annexe : Skype et la sécurité**

Skype est l'un des premiers systèmes de VoIP "Peer to Peer". Les données audio sont acheminées sans passer par un serveur. Elles sont restituées par un système de Codecs (RFC 3951 et 3952).

La principale inquiétude n'est pas virale. Comme tout logiciel, Skype a ses propres failles de sécurité mais elles sont comblées automatiquement en ligne, ce qui ne pose guère de problème pour une application 100 % Internet.

La possibilité de mettre sur écoute des utilisateurs de Skype, elle, inquiète plus, surtout dans un cadre critique comme celui de bon nombre d'entreprises.

Dans Skype, tous les protocoles sont propriétaires. Ils disposent de leur propre réseau et on ne sait pas trop par où transitent les informations. Vous vous retrouvez à envoyer des communications sur un réseau que vous ne contrôlez pas.

Les principales raisons de bannir Skype de l'entreprise :

- non respect des protocoles de VoIP
- vulnérabilités multiples : "Man in the middle", virus pouvant être dissimulés via le codage des données audio Skype, failles de sécurité permettant de prendre le contrôle du PC à distance
- les communications ne peuvent pas être enregistrées (problème légal)

La difficulté est de contrôler que Skype n'est pas installé, ou, au moins que les flux Skype ne franchissent pas les firewalls de l'entreprise.

Les données transitant par Skype sont en effet encapsulées dans :

- HTTP (port 80), le protocole du Web, ou
- SSL (port 443),

Ils sont donc extrêmement difficiles à distinguer d'autres flux particulièrement sécurisés.