



## TÉLÉCOMS

# La sécurité, maillon faible de la téléphonie sur IP

La technologie de la voix sur IP ouvre des brèches dans les systèmes d'information des entreprises.

**P**eut-on faire confiance à la téléphonie sur Internet ? C'est la question que se sont posée des spécialistes, réunis en fin d'année dernière à l'initiative de la Délégation générale pour l'armement (DGA), lors de ses 13<sup>es</sup> Journées sur la sécurité des systèmes d'information. Car, si la DGA s'intéresse à la voix sur IP (« Internet Protocol »), c'est pour une raison toute simple. Dans un avenir plus ou moins éloigné, les militaires devront, comme les civils, passer à cette technologie qui va devenir aussi courante que l'est aujourd'hui le bon vieux téléphone commuté. La réponse qu'ils ont obtenue des spécialistes invités à venir s'exprimer sur la question n'a pas dû les rassurer. Comme le résume Eric Wiatrowski, « chief security officer » de l'opérateur Orange, paraphrasant Churchill : « *Je vous promets du sang et des larmes, mais au bout la victoire.* »

La raison de fond est simple. La téléphonie classique est un monde de spécialistes utilisant des protocoles très spécifiques. Avec la téléphonie sur IP, une conversation téléphonique devient un flux informatique parmi d'autres, et le téléphone un simple ordinateur possédant une adresse IP. Première conséquence : le nombre des pirates potentiels explose. Hervé Schauer, fondateur de la société de conseil HSC Consultants, peint un tableau noir : « *On entre dans le paradis du pirate informatique. La dimension du problème change. Les gens ne réalisent pas qu'une véritable catastrophe est en train de s'annoncer.* »

### Des milliers de failles

De fait, une rapide démonstration est éloquent. Citali, une entreprise de conseil en sécurité informatique, a mis au point un petit boîtier espion doté d'un microprocesseur et d'un disque dur. Objectif : montrer les failles de la téléphonie IP. Il suffit de le brancher sur n'importe quelle prise du réseau informatique de l'entreprise pour écouter certaines conversations utilisant le protocole IP. « *Notre boîtier se fait passer sur le réseau pour un flux Web sécurisé, comme si quelqu'un était en train d'acheter sur un site de commerce électronique. Une fois la connexion établie, le boîtier est pilotable à distance* », explique Philippe Bourcier, consultant chez Citali.

Une vulnérabilité dont les raisons sont pourtant parfaitement connues : les failles contenues dans les protocoles de communication, notamment SIP et H323, qui permettent d'encoder la voix dans des paquets IP. Si le premier

est défendu par la communauté Internet, tandis que le second a été mis au point par l'Union internationale des télécommunications, aucun des deux n'a pris en compte la sécurité, confirment tous les spécialistes. Cela se traduit par des milliers de failles constituant autant de faiblesses exploitables par les pirates. Comme si cela ne suffisait pas, ces protocoles sont implantés de façon différente selon les constructeurs. « *En conséquence, pour fonctionner, les systèmes se rabattent sur le plus petit dénominateur commun. Ce qui crée des failles supplémentaires* », confirme Eric Wiatrowski.

### Du spam au « spit »

Les risques sont connus. Outre celui de voir ses communications écoutées, la téléphonie IP est aussi sensible aux spams. Un acronyme a déjà été trouvé : « spit » (« spam over Internet telephony »), qui signifie également cracher en anglais). C'était même le sujet d'inquiétude numéro un évoqué lors d'un colloque orga-



nisé l'an dernier par la VoIP Security Alliance à Berlin. Le risque, c'est ce que les spécialistes appellent le DNS (déni de service). L'objectif du pirate est alors de mettre en panne un système informatique. Cela peut être en le bombardant d'appels, ou en utilisant des virus informatiques.

Récemment, une compagnie d'assurances a vu son système de messagerie unifiée (le système gérant à la fois les e-mails et les messages vocaux) rendu inopérant pendant des semaines. « *La panne a sans doute été causée par un ver informatique caché dans le paquet IP d'une conversation téléphonique* », explique Gérard Kaas, fondateur de Checkphone, une société spécialisée dans la sécurité informatique et dont Telecom Media Fund vient de prendre 51 % du capital pour 10 millions de dollars.

#### Attention à la facturation

Autre risque, la fraude à la facturation. Le talon d'Achille, ce sont les centaines de fonctionnalités

## Voix sur IP et téléphonie sur IP

Les deux notions sont souvent confondues à tort.

**La voix sur IP**, ou « voice over IP » (VoIP), est une technologie d'intégration de la voix aux paquets de données IP (« Internet Protocol ») circulant sur un réseau, qu'il s'agisse d'Internet ou d'un réseau de télécommunications privé.

**La téléphonie sur IP** désigne les services de téléphonie mis en place grâce à cette technologie sur un réseau de télécommunications ouvert au public ou privé (au sein d'une entreprise ou d'un organisme), et utilisant principalement le protocole IP. On peut ainsi raccorder des téléphones IP et des logiciels sur PC raccordés sur le même réseau IP (« softphone »).

Source : [www.frameip.com/toip](http://www.frameip.com/toip)

d'un système de téléphonie sur IP : renvoi de poste, conférence, « squat » (le fait de retrouver son profil d'utilisateur depuis n'importe quel poste)... « *Le cas classique, c'est le serveur de messagerie piraté qui renvoie certains appels vers un numéro téléphonique surtaxé situé dans un pays exotique. Et, bien entendu, c'est l'entreprise qui paie la facture au profit des individus à qui appartient ce service* », précise Gérard Kaas.

## Séparer et crypter

Il existe bien sûr des mesures techniques, comme celles utilisées par Renault (lire ci-dessous) comme la séparation des réseaux. On peut également chiffrer les communications pour éviter les écoutes.

En attendant des avancées, comme la norme 802.1 X, mise au point pour sécuriser le Wi-Fi, certains restent encore méfiants. C'est le cas de la Délégation générale pour l'armement, qui recommande au monde de la défense de ne pas utiliser la téléphonie sur IP pour l'instant.

« *Aujourd'hui, nos réseaux informatiques ne sont pas connectés à Internet. Nous avons pour cet usage des stations dédiées, explique Bernard Minier, spécialiste des réseaux au Centre d'électronique de l'armement (Celar), le centre d'expertise de la DGA. Avec la téléphonie IP, nous ouvrons nos réseaux à Internet. C'est un danger. Pour passer du monde militaire au monde civil, il nous faudra donc des passerelles hyper-sécurisées. Aujourd'hui, on ne sait pas comment faire.* »

FRANK NIEDERCORN

