



Éditorial

(In)Sécurité de la VoIP

Guillaume Lehembre 

La voix sur IP (VoIP) se démocratise de plus en plus dans l'entreprise suite, entre autre, au cycle de renouvellement des PABX mais aussi au niveau du grand public avec l'adoption massive des offres *Triple Play*. La mise en place de ces nouvelles technologies pose inévitablement la question de la sécurité, en particulier dans le monde professionnel. La disponibilité est aussi un point critique car, en pratique, il ne faut pas espérer avoir un taux d'indisponibilité avec la ToIP équivalent à celle de la technologie commutée (de l'ordre de quelques minutes par an). Comment tendre vers une sécurité proche de celle d'un réseau commuté sur lequel la plupart des attaques nécessitent une intervention physique ? Comment se protéger des attaques du monde IP, maîtrisées par le plus grand nombre, et impactant de plein fouet la VoIP ?

Répondre à ces questions n'est pas chose facile et la configuration par défaut des équipements ne va généralement pas dans le sens de la sécurité. La sécurité de la VoIP ne se résume donc pas au simple chiffrement des données.

Les risques liés à la VoIP se situent à différents niveaux :

- *Réseau* : interception des communications, dénis de service, etc.,
- *Système* : fuite d'information, exploitation de vulnérabilités, etc.,
- *Protocolaire* : usurpation d'identité, sur-facturation, rejeu, dénis de service, etc.

Limiter les possibilités de connexion et d'action d'un équipement autre qu'un téléphone dans le VLAN voix, reste le premier pas vers la sécurisation de la VoIP en entreprise : protections DHCP, limitation d'adresses MAC par port (dans l'optique d'une solution 802.1X toujours pas supportée par les téléphones VoIP du marché), protection ARP, filtrage strict inter-client, etc. La minimisation et le durcissement des équipements de VoIP est la seconde étape : suivi des correctifs de sécurité, minimisation de la configuration et restriction des accès aux interfaces d'administration, journalisation, etc.

Enfin, la plupart des attaques protocolaires peuvent être contenues en s'assurant de l'authentification des

parties à tous les niveaux (relais applicatifs, serveurs d'authentification, etc.), et ce, au sein même du protocole de signalisation choisi.

L'authentification du protocole de signalisation et le chiffrement du protocole de transport de la voix peuvent ensuite être implémentés en supplément, tout en s'assurant que la qualité de service est toujours au rendez-vous ; le chiffrement peut par exemple être fortement pénalisant en terme de performance suivant les équipements.

La sécurité des offres *Triple Play* repose en partie sur le cloisonnement imposé par les modems et la plateforme d'accès. L'utilisation de modem tiers combiné à des lacunes de filtrage dans l'architecture peuvent avoir des conséquences désastreuses à grande échelle : dénis de service, interception de trafic, etc.

Les attaques applicatives sur la VoIP n'en sont qu'à leurs balbutiements car il existe relativement peu d'outils et de piles pour certains protocoles. On peut raisonnablement penser que les possibilités d'attaques vont s'étendre et que la sécurité de la VoIP restera un sujet d'actualité, et de polémique, pendant longtemps. Néanmoins, une partie de la sécurisation de la VoIP repose sur des principes connus depuis longtemps ... mais en pratique rarement mis en place dans les réseaux de données actuels.

L'aspect limitant de la sécurité de la VoIP restera toujours le maintien d'un niveau de qualité de service satisfaisant, ce qui est loin d'être évident vu l'impact actuel sur les performances de certaines mesures de sécurité (chiffrement, etc.). ●

À propos de l'auteur

Guillaume Lehembre est un consultant sécurité français travaillant pour le cabinet HSC (Hervé Schauer Consultants – <http://www.hsc.fr>) depuis 2004. Il a travaillé sur différents audits, études et tests d'intrusion et a acquis une expérience certaine dans la sécurité des réseaux sans fils. Il a réalisé des interventions publiques sur ce sujet et a publié plusieurs articles, dont un article dans le numéro 14 de hakin9 intitulé *Sécurité Wi-Fi – WEP, WPA et WPA2*. Il rédige un éditorial mensuel dans hakin9 depuis janvier 2007. Guillaume dispense plusieurs formations dont une sur la sécurité VoIP. Guillaume peut être contacté à l'adresse suivante : Guillaume.Lehembre@hsc.fr.