La voix dissimule des codes secrets

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 2 juin 2008

La communication sur IP peut abriter deux niveaux de compréhension. Des messages peuvent ainsi se cacher via la stéganographie, une alternative à la cryptographie. Un système exploité par les terroristes.

Dissimuler des messages secrets sur VoIP, c'est possible via la stéganographie. C'est ce qu'ont démontré deux chercheurs de la Warsaw University of Technology en Pologne. Pour mémoire, la stéganographie consiste à cacher une information en la noyant dans une masse de données plus grande, et non en la chiffrant. Avec la voix sur IP, les réseaux d'information transportent des données sous forme de paquets. Or les réseaux peuvent en perdre un certain nombre - quand les liens sont saturés ou la liaison mauvaise. Des mécanismes existent pour détecter la perte et les restituer si besoin, mais ils n'arrivent pas en même temps que les autres. Or les chercheurs ont montré qu'en utilisant ces paquets perdus il était possible de faire passer des messages secrets sans se faire détecter : ces derniers ne sont en effet pas analysés par les autorités de contrôle.

Un sous canal

"Il s'agit donc d'intégrer un sous canal à un canal", explique Quentin Berdugo, consultant en sécurité chez Hapsis. "Une technique qui peut servir aux terroristes, à l'espionnage industriel, au crime organisé etc.". En pratique, deux individus pourraient par ce moyen communiquer à travers une conversation banale, en noyant des données texte de préférence, sans qu'on puisse détecter la présence de cette seconde couche de communication. "En établissant un chat au milieu d'une conversation téléphonique par exemple". Techniquement cela est possible car la voix nécessite une bande passante importante."Une lettre écrite nécessite 8 bit, alors qu'une conversation en requiert des dizaines de milliers par seconde", explique Quentin Berdugo. "Avec un rapport de 1 à 10 000, le texte est noyé au milieu du volume voix et déjoue tout système d'écoute".

En temps réel et bidirectionnel

La stéganographie était déjà utilisée dans les images : on y modifie des pixels, et les logiciels sont capables d'en extraire l'information. Selon Quentin Berdugo, ce qui représente la grande nouveauté avec la stéganographie sur VoIP est l'immédiateté du système. "Il est en effet plus facile d'établir un canal en temps réel et bidirectionnel via la voix", affirme-t-il. Un système qui profite bien sûr de l'expansion exponentielle de la VoIP à l'échelle internationale. Reste que l'intérêt des chercheurs est surtout d'alerter. En effet, cet usage de la VoIP est réservé aux organisations criminelles ou illégales. Les entreprises ont certes des informations à dissimuler, mais doivent rarement cacher le fait même qu'elles communiquent. Elles préfèrent donc adopter le chiffrement plutôt que la stéganographie.

Post-scriptum :

http://www.atelier.fr/securite/10/0...