Ecole d'ingénieurs
du Canton de Vaud

Tél. : + 41 24 423 21 11
Fax : + 41 24 425 00 50

mailto:info@eivd.ch
http://www.eivd.ch

Travail de diplôme 2003
Département E+I Télécommunications

Ecole d'ingénieurs du Canton de Vaud
Route de Cheseaux 1, case postale
CH - 1401 Yverdon - les - Bains

VoIP Intrusion Detection

Description

La téléphonie par voix sur IP (VoIP), est désormais une technologie arrivée à maturité et dont le déploiement dans les entreprises ainsi que dans les réseaux publics est désormais de plus en plus fréquent. Si la VoIP a, par le passé, négligé les aspects de sécurité au profit de l'efficacité et de la rentabilité, elle doit maintenant au risque d'être discréditée proposer des solutions de déploiement fiables et sécurisées.

Mandat

L'objectif de ce travail de diplôme est double :

- Effectuer une étude exhaustive de la sécurité appliquée à la VoIP sous toutes ses formes. Cette étude doit présenter les vulnérabilités ainsi que les aspects de protection pour des solutions IP PBX ou IP-Centrex ou Hosted PBX.
- Mettre sur pied un banc de test ou laboratoire permettant de mettre en évidence les vulnérabilités de la VoIP ainsi que l'efficacité des nouveaux outils de protection et en particulier ses protections pour au moins deux systèmes de la VoIP (SIP et/ou MGCP).

Solution réalisée

Dans un premier temps, la solution réalisée permet d'établir une communication entre deux réseaux différents. Cela signifie qu'un "Outbound Proxy" a été mis en place, permettant ainsi de contourner les différents problèmes causés par les NATs.

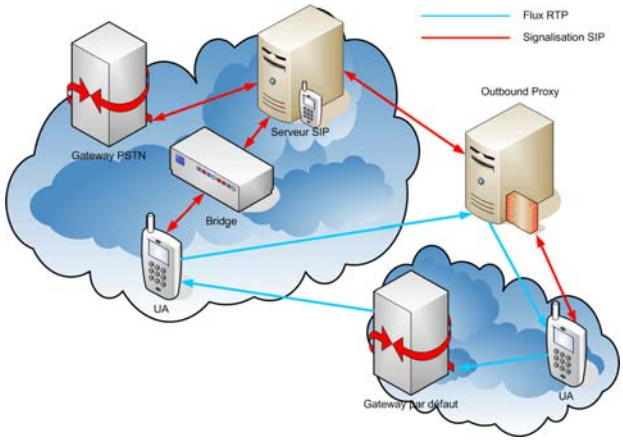
Puis, dans un deuxième temps, cet "Outbound Proxy" a été doté d'un firewall permettant d'établir les phases de signalisation du protocole SIP, ainsi que la transmission des flux RTP transportant la voix. Pour ce dernier point, il est à noter que l'ouverture et la fermeture des ports est effectuée de manière dynamique.

Ensuite, un mécanisme d'authentification des requêtes SIP a été réalisé. Ce mécanisme utilise "MD5". C'est-à-dire que lorsque le serveur reçoit une requête de la part de l'un des agents, il soumet un challenge à ce dernier. La requête ne sera exécutée que si l'agent répond correctement au challenge.

Et finalement, l'accès au gateway PSTN a été restreint à l'aide d'un bridge.

Résultat

La solution réalisée a été mise en place sur la DMZ de l'école, dotant ainsi cette dernière d'un service de téléphonie sur IP sécurisé.



Architecture de la solution mise en place

Auteur: **FIAUX Alexandre**
Répondants internes: **VENTURA Stefano**
SCHWEIZER Laurent
Prof. responsable: **VENTURA Stefano**
Sujet proposé par: **VENTURA Stefano**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale