heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud
http://www.heig-vd.ch

Travail de diplôme 2006

HEIG-VD
Route de Cheseaux 1
CH - 1401 Yverdon-les-Bains

Sécurité avec le protocole SIP

Description

Ce projet s'inscrit dans une suite de développements et d'études sur la mobilité et la sécurité avec le protocole SIP. Tout l'aspect de la mobilité a été étudié dans une étude précédente et le projet de diplôme s'est focalisé sur la sécurité.

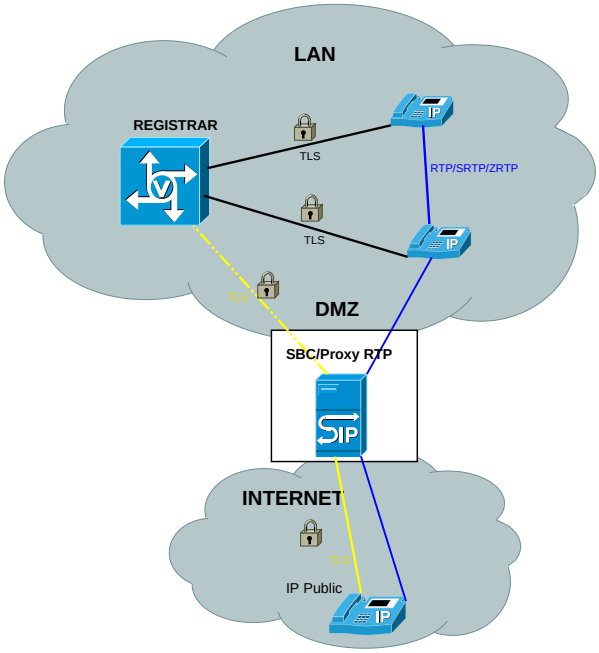
Le but du projet était de mettre en place une plateforme SIP sécurisée, et de tester, dans la mesure une plateforme de mobilité fournie par l'université de Tor Vergata à Rome.

Cahier des charges

- Etude de la mobilité avec le protocole SIP
  - Mobilité vertical (Wifi2UMTS)
  - Mobilité horizontal (Wifi2Wifi)
- Etude de solutions de sécurité dans la VoIP
  - Sécurité avec le protocole SIP pour la signalisation
  - Sécurité du flux média avec SRTP

Réalisation

Le choix de la plateforme s'est porté sur OpenSER, un proxy SIP multi-fonctions supportant le TLS pour la signalisation et sous licence GPL. L'UA utilisé est Minisip qui est lui aussi sous GPL, c'est un des seuls softphones qui supporte TLS. Comme hardphone, j'ai utilisé un SNOM360 qui possède le support TLS. Comme le chiffrement de la voix ne dépend pas du serveur SIP mais des UAs, certains tests ont été effectués entre différents UAs mais sans succès.



L'utilisation de TLS fonctionne bien, bien que sujette à certains problèmes(réutilisation du même socket pour différentes transactions). Une étude théorique a aussi été portée sur le protocole DTLS qui est semblable à TLS mais orienté datagramme.

Conclusion

La plateforme OpenSER est un excellent proxy SIP avec en plus des fonctions telles que Registrar,nathelper ou encore media proxy. OpenSER peut aussi se coupler avec une passerelle Asterisk vers le réseau PSTN. Le support de TLS et sa licence fait de lui un produit des plus intéressant.
L'utilisation de TLS pour chiffrer le flux de signalisation contraint l'utilisation du protocole TCP au lieu d'UDP. Des développemts avec le protocole DTLS pourrait améliorer les performances.

Auteur :	Galland Grégoire
Répondant externe :	Saverio Niccolini
Prof.responsable :	Ventura Stefano
Sujet proposé par :	NEC

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale