Manuscrit
sur les travaux de recherches de :
Thomas Guillet

présenté pour obtenir le grade de

DOCTEUR de TÉLÉCOM PARISTECH
Spécialité **: Informatique et Réseaux**

Sécurité de la téléphonie sur IP

Soutenance le XX octobre 2010 devant le jury composé de :
Rapporteurs :
Professeur Bernard COUSIN Université de Rennes 1
Professeur Pascal LORENZ Institut Universitaire de Technologie de Colmar
Examinateurs :
Professeur Omar ABOU KHALED University of Applied Sciences of Western Switzerland
Capitaine de vaisseau Henri d'AGRAIN Etat-major de la marine – Bureau SIC
Professeur Elena MUGELLINI University of Applied Sciences of Western Switzerland
Docteur ingénieur Michel PELLET DGA
Professeur Pascal URIEN Télécom ParisTech
Directeur de Thèse :
Maître de conférence Ahmed SERHROUCHNI Télécom ParisTech

Résumé

Ces travaux portent sur la sécurité de la téléphonie déployée dans les réseaux Internet. Ce service est sans aucun doute, après le Web et la messagerie, l'application qui imposera l'infrastructure IP (Internet Protocol) comme le standard de transport de tout type d'information ou de média. Cette migration de la téléphonie classique vers le tout IP semble être incontournable mais elle pose des problèmes en matière de sécurité. Si des attaques existaient déjà avec la téléphonie classique, l'usage d'un réseau IP les rend plus facilement réalisables. Notre analyse souligne les limites des solutions usuelles, principalement au travers des problèmes d'interopérabilité. De plus eu égard à l'hétérogénéité des infrastructures de ToIP, la protection de bout-en-bout des appels n'est pour le moment pas considérée, sauf par les services étatiques.

Dans un premier temps, nous avons cherché les possibilités de renforcer la sécurité de SIP (Session Initiation Protocol) de l'IETF, protocole actuellement massivement adopté dans les infrastructures de téléphonie. Nous avons proposé des solutions innovantes et validées pour consolider les mécanismes existants de manière complètement transparente pour les infrastructures. Nous avons choisi de nous focaliser sur l'authentification, car c'est le premier mécanisme rencontré par les usagers ou les systèmes. Les solutions présentées ci-après proposent de nouvelles propriétés de sécurité en définissant une sémantique pour des champs dit « opaques ». Ces contributions consolident la sécurité entre l'usager et son serveur.

Dans un second temps, nous nous sommes intéressés aux solutions permettant une sécurité bout-en-bout des appels. L'analyse des solutions applicatives comme « Future Narrow Band Digital Terminal » et « Secure Voice over IP Simple Protocol » nous a permis de formaliser les spécifications d'une architecture permettant la protection des conversations quelque soient les spécificités et l'hétérogénéité des réseaux de ToIP. Cette approche utilise le canal média pour mette en œuvre une signalisation de sécurité, ce qui rend cette solution complètement compatible avec les infrastructures existantes. Par ailleurs notre étude atteste de l'intérêt de mettre en place des entités de confiance dédiées à la sécurité des appels.

Enfin la conclusion reprend et positionne les différentes contributions relatives à ces travaux dans le contexte de la téléphonie sur IP. Notre volonté d'être interopérable avec les infrastructures sous-jacentes voire indépendantes peut être considérée comme un service à valeur ajoutée.