

# *(In)sécurité de la Voix sur IP [VoIP]*

**Nicolas FISCHBACH**

*Senior Manager, IP Engineering/Security - COLT Telecom*  
nico@securite.org - <http://www.securite.org/nico/>

version 1.0



we make business straight.forward

# Introduction

- » **Voix et téléphonie IP**
- » **Convergence des réseaux**
  - > Téléphonie et informatique
  - > PoE
- » **Mobilité**
- » **Opérateur**
  - > Circuit -> Paquet (IP)
  - > Monde fermé -> Monde ouvert
- » **Vendeurs et Time to Market**
- » **Sécurité et vie privée**
  - > IPhreakers
  - > VoIP vs 3G



# Architecture : les protocoles

## » Signalisation

- > Localisation de l'utilisateur
- > Session
  - Etablissement
  - Negociation
  - Modification
  - Fermeture

## » Transport

- > Numérisation, encodage, transport, etc.



# Architecture : les protocoles

## » SIP

- > IETF - 5060/5061 (TLS) - "HTTP-like, all in one"
- > Extensions propriétaires
- > Protocole qui devient une architecture
- > "End-to-end" (entre IP PBX)
  - Inter-AS MPLS VPNs
  - Confiance transitive
- > Extensions IM (SIMPLE)

## » H.323

- > Famille de protocoles
- > H.235 (sécurité), Q.931+H.245 (gestion), RTP, CODECs, etc.
- > ASN.1



# Architecture : les protocoles

## » RTP (Real Time Protocol)

- > 5004/udp
- > RTCP
- > Pas de réservation/QoS
- > Réordonnancement
- > CODECs
  - Historique: G.711 (PSTN/POTS - 64Kb/s)
  - G.729 (8Kb/s)



# Architecture : le réseau

## » LAN

- > Ethernet (routeurs et commutateurs)
- > xDSL/cable/WiFi
- > VLANs (données/voix+signalisation)

## » WAN

- > Internet
- > VPN
  - Ligne louée
  - MPLS



# Architecture : le réseau

## » QoS (Qualité de service)

- > Bande Passante
- > Latence (150-400ms) et Gigue (<<150ms)
- > Perte de paquets (1-3%)



# Architecture : les systèmes

## » Les systèmes

- > Proxy SIP
- > Call Manager/IP PBX
  - Gestion des utilisateurs et reporting (HTTP, etc)
  - Off-path en IP
- > H.323: GK (GateKeeper)
- > Serveurs d'authentification (Radius)
- > Serveurs de facturation (CDR/billing)
- > Serveurs DNS





# Architecture : les systèmes

## » Voice Gateway (IP-PSTN)

- > Ensemble d'éléments (Gateway Control Protocols)
- > Signalisation: interface SS7
  - Media Gateway Controller
    - . Contrôle la MG (Megaco/H.248)
    - . Interface SIP
  - Signaling Gateway
    - . Interface entre le MGC et SS7
    - . MxUA, SCTP - ISUP, Q.931
- > Transport
  - Media Gateway: conversion audio



# Architecture : le pare-feu/VPNc

## » Le pare-feu

- > Filtrage "non-stateful"
- > Filtrage "stateful"
- > Filtrage applicatif (ALG)
- > NAT / "firewall piercing"
  - (H.323 : 2xTCP, 4xUDP dynamique - 1719,1720)
  - (SIP : 5060/udp)

## » VPN chiffré

- > SSL/TLS
- > IPsec
- > Sur quel segment (LAN-LAN, téléphone-téléphone, etc) ?

## » Impact sur la QoS

## » Apports d'IPv6 ?



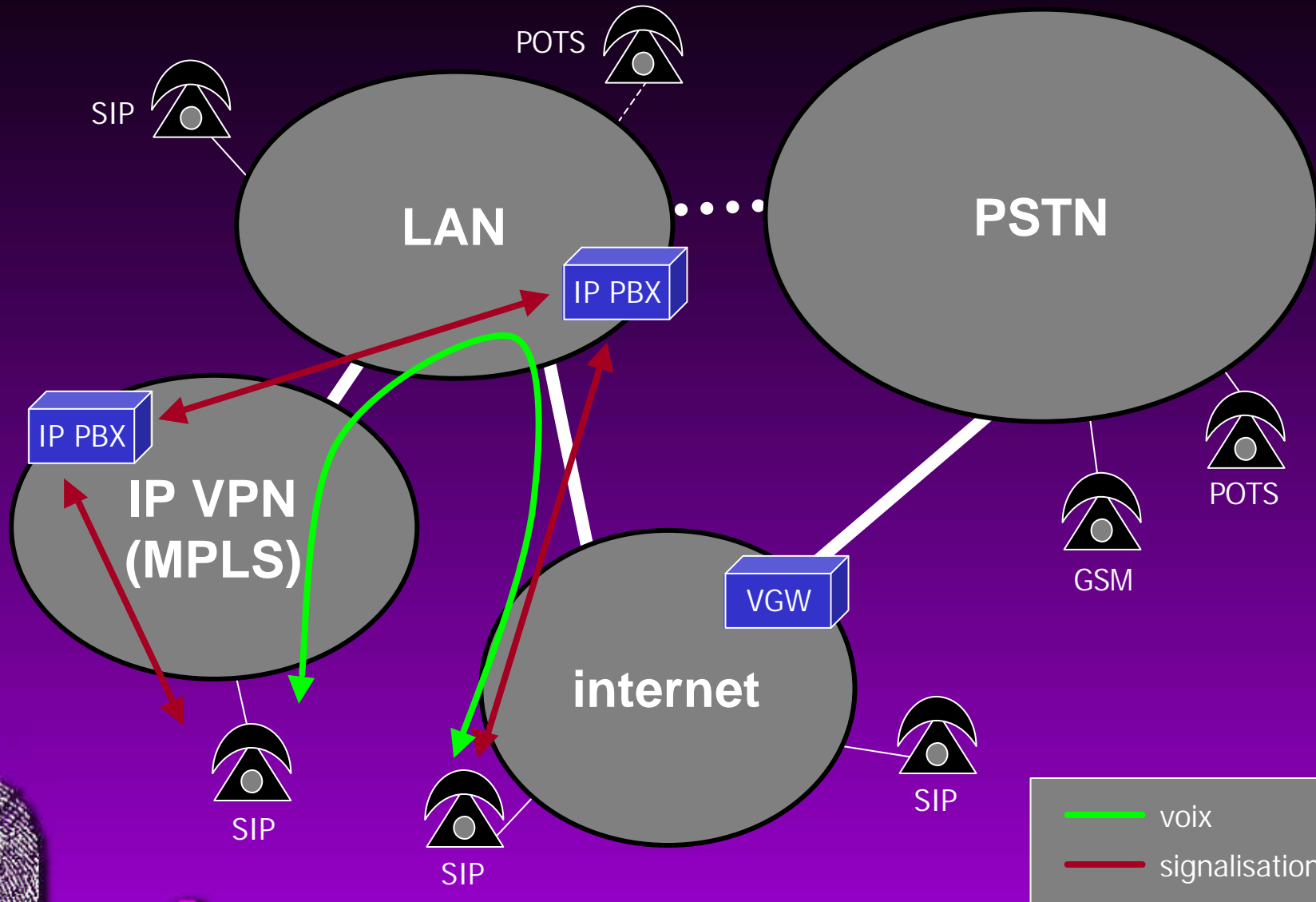
# Architecture : les téléphones

## » Les téléphones IP

- > Softphone et Hardphone
- > "Grille pain"
  - mise à jour
  - intelligence
- > Intelligence sort du réseau pour se greffer sur l'élément terminal
- > Flux téléphone -> autres éléments
  - SIP
  - RTP
  - (T)FTP
  - CRL
  - etc.



# Architecture : exemple



# Les réseaux "classiques"

- » POTS/PSTN [TDM]
- » "Sans Fil"/DECT
- » GSM
- » Satellite
- » Signalisation (SS7)



# Attaques

## » IPhreakers

- > Connaissance du monde IP
- > Faiblesses "connues"
- > Evolution 2600Hz -> voicemail/int'l GWs -> IP telephony
- > Interne ou Externe ?
- > Cible: particulier, entreprise, gouvernement, etc ?

## » Implémentation des protocoles

- > PROTOS

## » Facteur humain



# Attaques : déni de service

## » Les dénis de service

- > Réseau
- > Protocole (SIP INVITE)
- > Systèmes / Applications
- > Téléphone

## » Non-disponibilité (BC/DR)

- > Dépendance: électricité
- > Quelles alternatives (Continuité de Service/Reprise sur Incident) ?
- > E911 (lois et localisation)
- > GSM
- > PSTN-vers-GSM



# Attaques : fraude

- » **Modification du Call-ID**
  
- » **Récupération des droits**
  - > Faux serveur d'authentification
  
- » **Effets**
  - > Accès boîte vocale
  - > Numéros spéciaux
  - > Ingénierie sociale
  - > Rejeu





# Attaques : interception

## » Interception

- > Conversation
- > "Qui téléphone avec qui"
  - Ecoute réseau
  - Serveurs (SIP, CDR, etc)

## » LAN

- > Accès physique au réseau
- > Attaques ARP
- > Insertion d'éléments (pas d'authentification)
- > Différents éléments à différents niveaux (MAC, utilisateur, localisation physique, etc)



# Attaques : interception

## » Où intercepter ?

- > Localisation de l'utilisateur
- > Réseaux traversés

## » Interception légale (Lawful Intercept)

- > CALEA
- > Standard ETSI
- > Architecture et risques



# Attaques : systèmes

## » Les systèmes

- > Plate-forme non sécurisée
- > Vers, exploit, chevaux de Troie



# Attaques : téléphone

## » Téléphones (S)IP

- > Séquence de démarrage
  - DHCP, TFTP, etc.
- > Accès physique
  - Menus "cachés"
- > Pile TCP/IP
- > Firmware/configuration
- > Cheval de Troie/rootkit



# Défense

- » **Signalisation: SIP**
  - > Secure SIP vs SS7 (sécurité physique)
- » **Transport: Secure RTP (avec MIKEY)**
- » **Réseau: QoS [LLQ] (et rate-limit)**
- » **Pare-feu: applicatif**
- » **Téléphone: images signées**
- » **Identification: TLS**
  - > Clients par le serveur
  - > Serveurs par le client
- » **3P: projet, processus et politique [de sécurité]**



# Conclusion

## » Conclusion

## » A lire également

- > Backbone and Infrastructure Security
  - <http://www.securite.org/presentations/secip/>
- > (Distributed) Denial of Service
  - <http://www.securite.org/presentations/ddos/>

## » Q&R



Image: [www.shawnsclipart.com/funkycomputercrowd.html](http://www.shawnsclipart.com/funkycomputercrowd.html)