



HERVÉ SCHAUER CONSULTANTS

Network Security Agency since 1989

Specialized in Unix, Windows, TCP/IP and Internet

Sécurité Voix sur IP



Franck Davy <Franck.Davy@hsc.fr>

Nicolas Jombart <Nicolas.Jombart@hsc.fr>

Alain Thivillon <Alain.Thivillon@hsc.fr>

Enjeux et risques de la Voix sur IP

Protocoles de signalisation VoIP

- Famille de protocoles H.323
- Protocole SIP

Protocoles de transport Media (RTP/RTCP)

Sécurité de (quelques) protocoles propriétaires

Réseaux GSM et VoIP

Bilan / Conclusion

Adaptation de la téléphonie traditionnelle à un transport IP, en terme de signalisation (signalisation/contrôle d'appel), et de transport

Principales entités :

- Terminaux IP (Téléphones IP, Soft-Phones)
- Passerelles VoIP – Interfonctionnement avec les réseaux commutés ou mobiles
- Gestionnaires d'appels – Enregistrement, authentification et adressage des terminaux/passerelles/gestionnaires voisins, facturation
- Serveurs d'application divers ...

→ **Synthèse/Retour d'expérience sur la sécurité d'architectures VoIP, à partir d'exemples inspirés de situations réelles**

Deux grandes familles de risques pour les protocoles de Voix sur IP, principalement :

Risques au niveau IP

Interception des communications (écoute...) *

Déni de service (avec ou sans *spoofing*)

Sur les équipements

Sur les flux

Risques des protocoles

Surfacturation (par redirection) *

Usurpation d'identité

Modification de *Caller-ID*, utilisation de professionnels de l'imitation, ...

Insertion, re-jeu, ... *

Déni de service*

(*) Exemples cités dans la présentation

➤ **Standard H.323 = Recommandation ITU**

Ensemble de protocoles de codage de voix/vidéo, et de protocoles dits «parapluie» de synchronisation/multiplexage de flux multimedia

H.225 RAS	Signalisation H.225/Q.931	Contrôle H.245
UDP	TCP	
Couche réseau		
Couche liaison		

+ H.235 : Security and encryption for H-series
+ ...

➤ **Flux successivement constatés ... :**

...variables selon le scénario d'établissement d'appel

Enregistrement/Admission entre téléphone et *Gatekeeper* :

H225/RAS – Flux de datagrammes UDP sur un port identifié (1719/UDP) ;

Signalisation d'appel, entre téléphones, ou entre téléphone et *Gatekeeper* :

H225/Q.931 – Connexion TCP sur port identifié (1720/TCP);

Contrôle d'appel, entre téléphones, ou entre téléphone et *Gatekeeper* :

H.245 – Connexion TCP sur un port négocié dynamiquement (>1024/TCP)

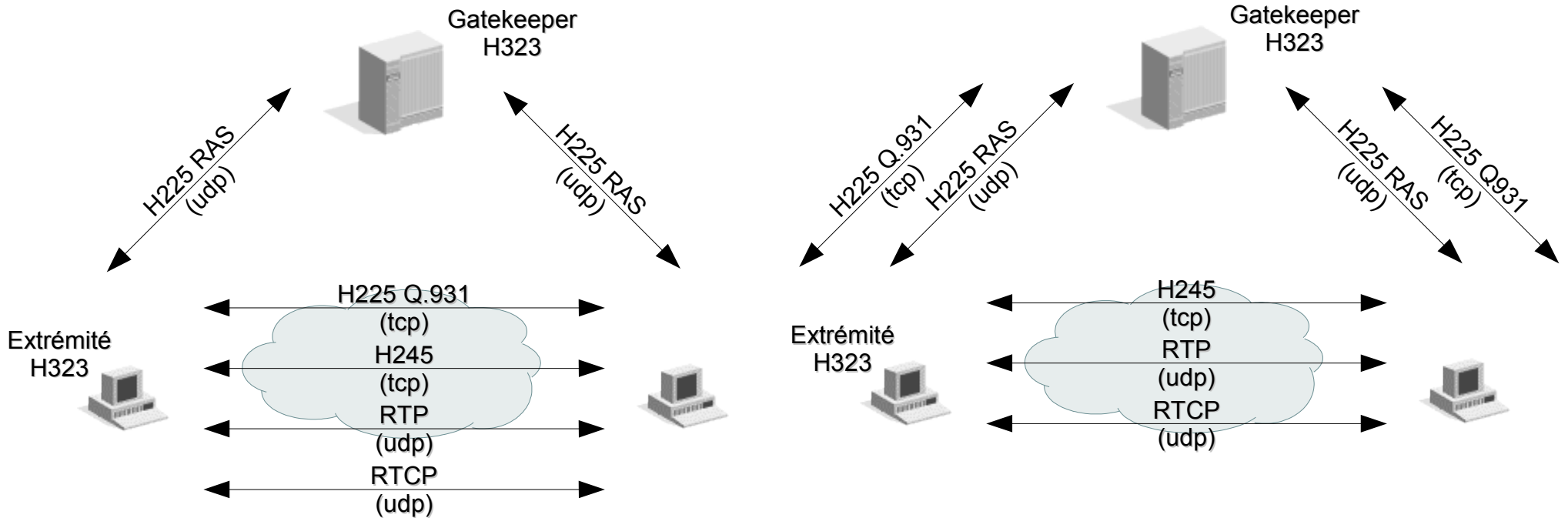
Flux de données, entre téléphones, ou entre téléphone et *Gatekeeper/Media Gateway*

Voie(s) logique(s) RTP/RTCP – Flux de datagrammes UDP sur port dynamique >1024/UDP

Protocole H.323 : Gatekeeper & établissement(s) d'appel

Mode «signalisation directe»

Mode «signalisation routée»

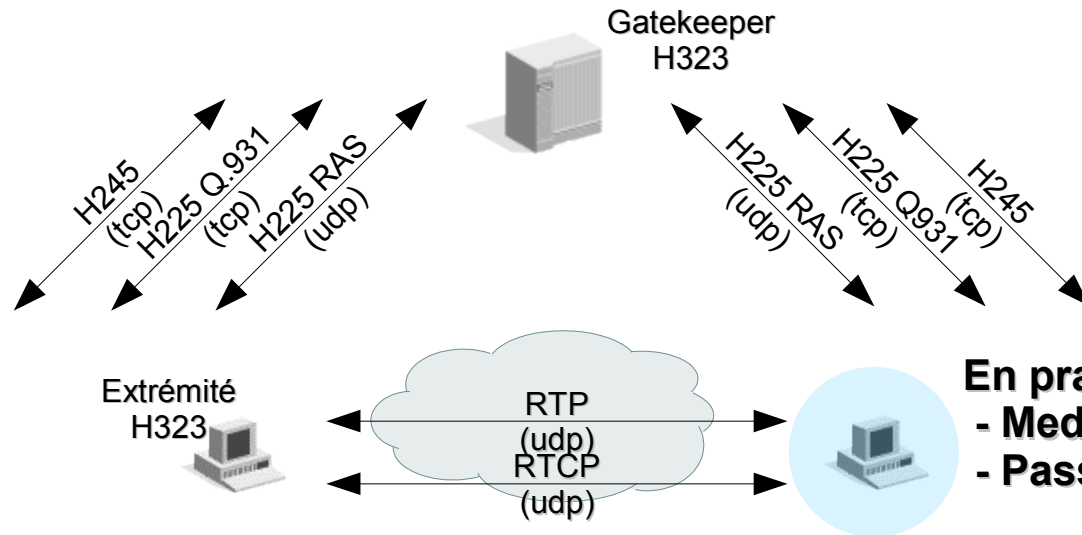


Quelques fonctionnalités du Gatekeeper H.323 :

- Gestion des terminaux et passerelles VoIP (enregistrement/authentification, statut)
 - Routage des appels (éventuellement entre GK)
 - Interface avec les systèmes de facturation ...
- **Serveur extrêmement sensible !**

Protocole H.323 : Établissement(s) d'appel

Établissement d'appel en mode signalisation et contrôle routés



En pratique, peut être scindé en deux entités :

- Media Gateway, pour les flux RTP/RTCP (côté client)
- Passerelle SS7, pour la signalisation (côté GK)

Sans oublier le mode proxy, pour lequel flux RTP/RTCP transitent à travers le GateKeeper

Gare aux temps de latence !

<150 ms ?

Time	Source	Destination	Protocol	Info	
82	*PEF*	192.70.106.105	192.70.106.69	RTP	Payload type=ITU-T G.711 PCM
83	0.030100	192.70.106.105	192.70.106.69	RTP	Payload type=ITU-T G.711 PCM
84	0.050054	192.70.106.105	192.70.106.69	RTP	Payload type=ITU-T G.711 PCM
85	0.080103	192.70.106.105	192.70.106.69	RTP	Payload type=ITU-T G.711 PCM
86	0.100406	192.70.106.105	192.70.106.69	RTP	Payload type=ITU-T G.711 PCM
87	0.130390	192.70.106.105	192.70.106.69	RTP	Payload type=ITU-T G.711 PCM
89	0.164476	192.70.106.105	192.70.106.69	RTP	Payload type=ITU-T G.711 PCM
90	0.190404	192.70.106.105	192.70.106.69	RTP	Payload type=ITU-T G.711 PCM
91	0.209031	192.70.106.69	192.70.106.98	RTP	Payload type=ITU-T G.711 PCM
92	0.209196	192.70.106.69	192.70.106.98	RTP	Payload type=ITU-T G.711 PCM

Complexité du filtrage H.323

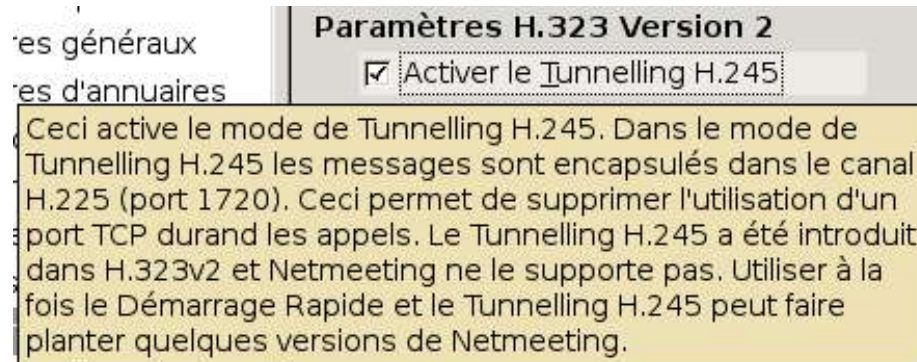
Protocole ASN.1 / Encodage PER

Sensibilité aux dénis de service

Ex: Voie RAS non fiable (1719/UDP)

Multitude de flux, de mécanismes d'établissement d'appel ou encore d'extensions à la norme (ex: *FastStart*, ou encore *H245Tunneling*, qui permet d'établir le canal de contrôle d'appel sur la connexion TCP du canal de signalisation d'appel)

*Configuration
GnomeMeeting*



Quid de la traduction d'adresses ? Les adresses IP des extrémités sont transmises au niveau applicatif ...

→ **Nécessité d'un filtrage applicatif (très) évolué**

IP Stack Integrity Checker (Ethernet, IP, UDP, TCP et ICMP)
Outil permettant l'envoi de paquets aléatoires pour éprouver la robustesse :

→ Des piles TCP/IP

→ Des applications lors de la réception de données *aléatoires*

Spoofing d'adresse

```
% sudo udpsic -s rand -d 192.168.0.1,180 -m 100
```

```
Using random source IP's  

Compiled against Libnet 1.0.2a  

Installing Signal Handlers.
```

```
Seeding with 23290
```

```
Using random source ports.
```

```
Maximum traffic rate = 100.00 k/s
```

Bad IP Version	= 10%	IP Opts Pcnt	= 50%
Frag'd Pcnt	= 30%	Bad UDP Cksm	= 10%

```
1000 @ 863.9 pkts/sec and 95.4 k/s  

2000 @ 11170.8 pkts/sec and 9.8 k/s  

3000 @ 13432.6 pkts/sec and 2.6 k/s  

(...)
```

```
Used random seed 23290
```

```
Wrote 51004 packets in 7.59s @ 6722.79 pkts/s
```

Mécanisme de graine, pour reproduire les flux et isoler les paquets posant problème

Gestion de la bande passante

Contrôle des « effets » envoyés

Indispensable de valider les équipements avec des programmes évaluant la robustesse des implémentations – et non simplement des tests en charge

Tests préliminaires avec ISIC ...

Exemples de suites de tests spécifiques :

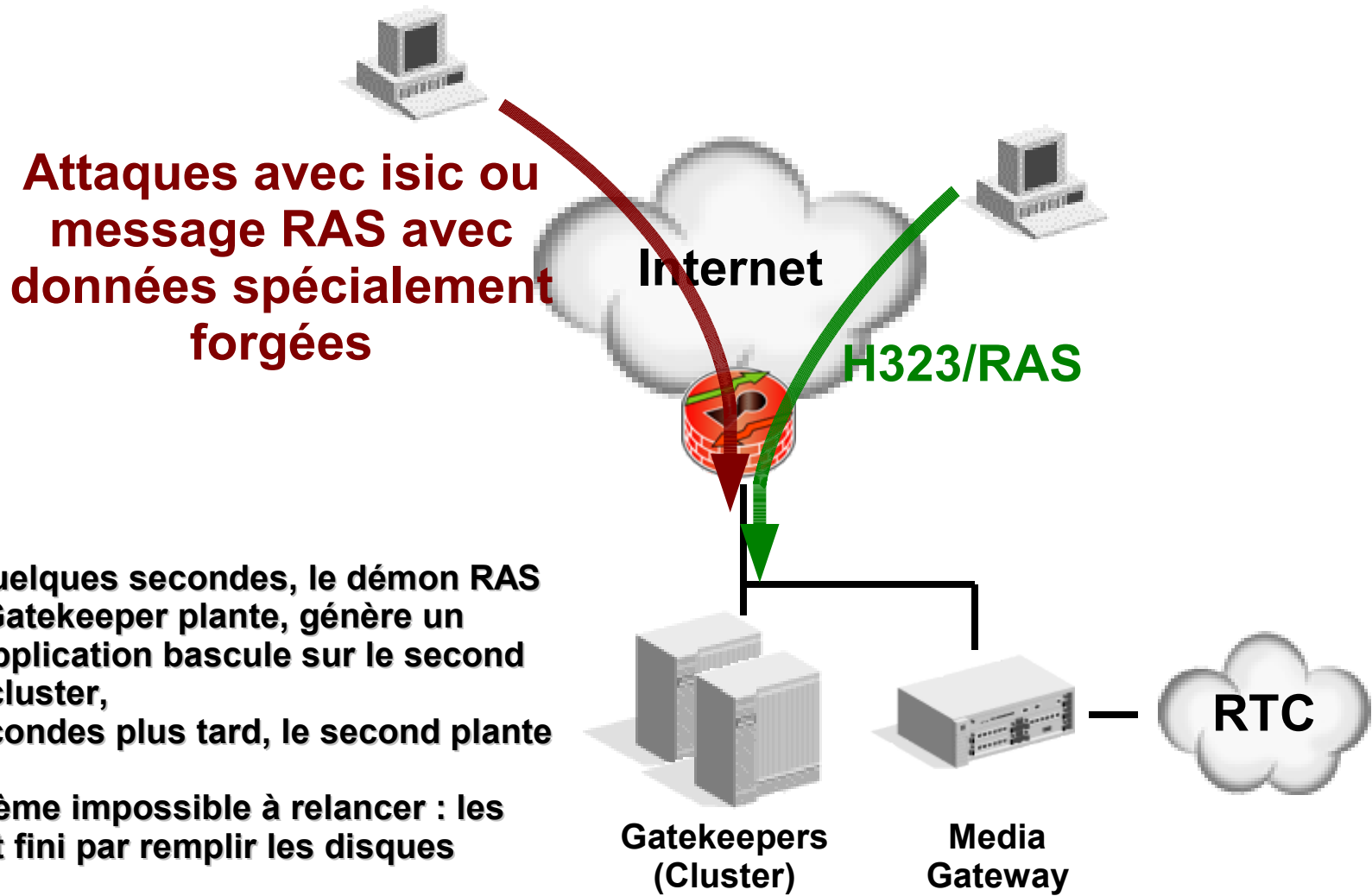
SIPSAK (<http://sipsak.org>)

CODENOMICON (commercial – non évalué <http://www.codenomicon.com>)

« Our goal is to support pro-active elimination of software faults with information security implications. [...] Codenomicon is currently working on ensuring the robustness and reliability of, e.g., 2.5/3G telecommunications networks and systems relying on Voice over IP (VoIP) protocols. »

+ Certains équipements de filtrage applicatif réalisent une inspection satisfaisante sur quelques protocoles VoIP (Ex: CheckPoint FW-1 et le filtrage H.225 RAS – avec la bonne configuration)

Filtrage H.323 : Déni de service RAS (1719/UDP)



Basiquement, gestion des sessions entre différents participants

Voix mais aussi multimédia, messagerie instantanée, ...

Analogie avec HTTP
(méthode, URI)

Relayage

Adresses SIP

Description de la session
(SDP)

```

INVITE sip:test@192.70.106.102 SIP/2.0
Via: SIP/2.0/UDP 0.0.0.0:5063;branch=z9hG4bK894348304
Route: <sip:192.70.106.104;lr>
From: <sip:at@192.70.106.104>;tag=7116539;tag=7648279
To: <sip:test@192.70.106.102>
Call-ID: 4173170638@192.70.106.104
CSeq: 21 INVITE
Contact: <sip:at@192.70.106.104:5063>
max-forwards: 10
user-agent: oSIP/Linphone-0.12.1
Content-Type: application/sdp
Content-Length: 371
    
```

1 0,000000 172,20,0,4	silver	SIP/S Request: INVITE sip:fd@hsc.fr;user=phone,
2 0,004148 silver	172,20,0,4	SIP Status: 100 trying -- your call is importa
3 0,014081 silver	172,20,0,4	SIP Status: 180 Ringing
4 17,01575 silver	172,20,0,4	SIP/S Status: 200 OK, with session description
7 17,06774 172,20,0,4	silver	SIP Request: ACK sip:fd@hsc.fr;user=phone
962 35,93460 silver	172,20,0,4	SIP Request: BYE sip:ecu@172,20,0,4:5060;user=

SDP : Échange des informations du canal voix :

Adresses IP et ports

Codecs, bande passante

Gestion des clefs pour le chiffrement (MIKEY)

Etc.

Messagerie instantanée : méthode MESSAGE

Utilisation du DNS

Sécurité :

Authentification sur les proxies SIP (~ Gatekeepers)

Une URI SIPS demande que tous les noeuds fassent de la sécurité (TLS)

Exemple d'attaques sur SIP

<http://blackhat.com/presentations/bh-usa-02/bh-us-02-arkin-voip.ppt>

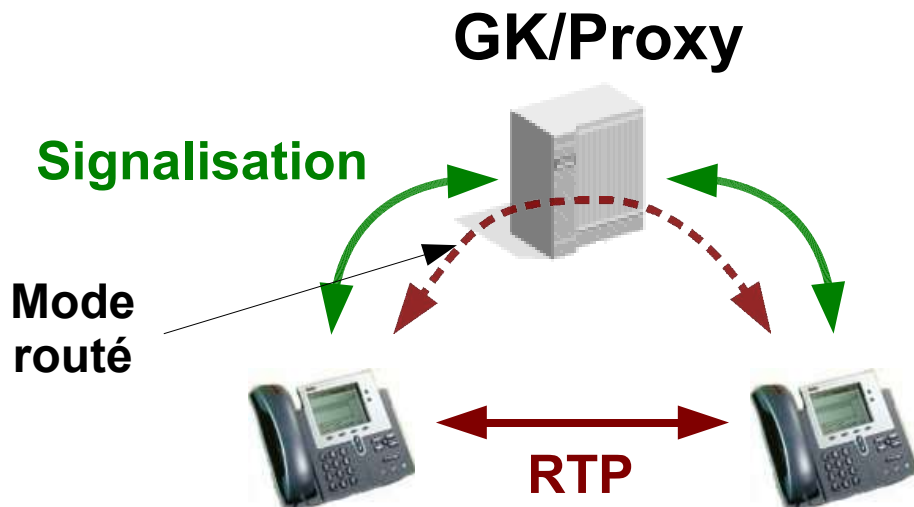
Protocoles de distribution de média type Voix/Vidéo

- Protocoles RTP/RTCP pour la voix et la vidéo
- + RTSP pour la diffusion type client(s)/serveur,

avec **RTP = flux de données (UDP, Port n – dynamique)**
RTCP = paquets de contrôle (UDP, Port n+1)

```

192.70.106.105 192.70.106.98 RTP Payload type=ITU-T G.711 PCMU, SSRC=300
192.70.106.105 192.70.106.98 RTP Payload type=ITU-T G.711 PCMU, SSRC=300
192.70.106.105 192.70.106.98 RTP Payload type=ITU-T G.711 PCMU, SSRC=300
192.70.106.105 192.70.106.98 RTP Payload type=ITU-T G.711 PCMU, SSRC=300
192.70.106.105 192.70.106.98 RTCP Sender Report
192.70.106.105 192.70.106.98 RTP Payload type=ITU-T G.711 PCMU, SSRC=300
    
```



```

Real-Time Transport Protocol
> [Stream setup by H245 (frame 46)]
10.. .... = Version: RFC 1889 Version (2)
..0. .... = Padding: False
...0 .... = Extension: False
.... 0000 = Contributing source identifiers count: 0
0... .... = Marker: False
Payload type: ITU-T G.711 PCMU (0)
Sequence number: 11010
Timestamp: 49240
Synchronization Source identifier: 3009141930
Payload: C2C2C2C2C3C4C5C6C7C8C9CACBCBCDCDCECFD1D2D4D
    
```

```
# ./voipong -d4 -f
# EnderUNIX VOIPONG Voice Over IP Sniffer starting...
Release 1.1, running on nupsy.hsc.fr

(c) Murat Balaban http://www.enderunix.org/
14/06/05 18:15:20: EnderUNIX VOIPONG Voice Over IP Sniffer starting...
14/06/05 18:15:20: eth0 has been opened in promisc mode, data link: 14
14/06/05 18:15:46: [2088] VoIP call has been detected.
14/06/05 18:15:46: [2088] 192.168.106.69:5004 <--> 192.168.106.98:5000
[...]
$ cat ./output/20050614/session-enc8-PCMA-8KHz-192.1(...).68.106.69,5004.raw
```

Ettercap/arp-sk/etc.
+
Ethereal/Vomit/Voipong/etc.

Interception



Attaque active par insertion

Flux RTP (Adresses/ports identiques)
Contenant des données aléatoires
Contenant un message enregistré avec le bon codec
Nécessite de connaître/prédire les numéros de séquence

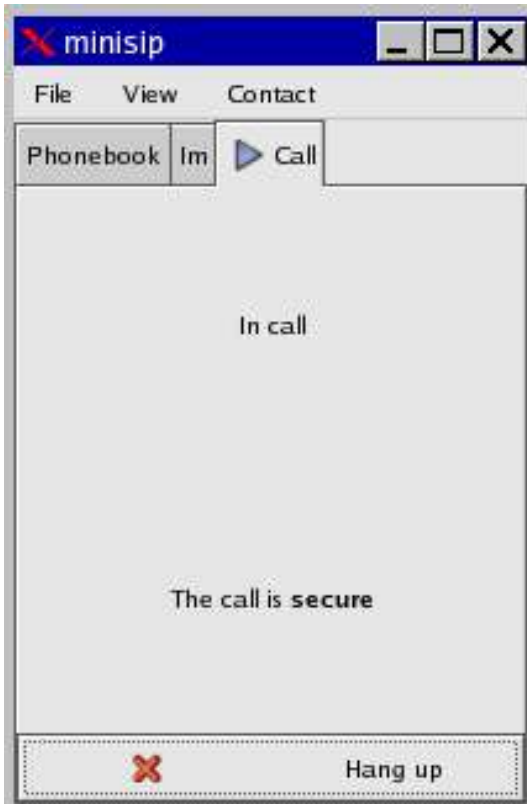
Solution : Sécurisation des flux de bout-en-bout

Chiffrement du *payload* RTP + authentification du paquet

Mikey (RFC 3830) = Protocole de gestion de clés pour SRTP

→ Disponible dans SIP et H.323 (Annexe G – rec. ITU-T H.235)

→ Authentification par clé partagée, *Diffie-Hellman* ou certificats X.509



```

▼ Media Description, name and address (m): audio 1055 RTP/AVP 0
  Media Type: audio
  Media Port: 1055
  Media Proto: RTP/AVP
  Media Format: ITU-T G.711 PCMU
▶ Media Attribute (a): rtpmap:0 PCMU/8000/1
▼ Media Attribute (a): key-mgmt:mikey AQAfGc1NKY8CAAAX1++LAAAAAF
  Media Attribute Fieldname: key-mgmt
  Media Attribute Value: mikey AQAfGc1NKY8CAAAX1++LAAAAAAAAAAAF
    
```

Tests avec minisip, configuré en secret partagé
<http://www.minisip.org>

VoIP : Sécurité des protocoles propriétaires (Cisco, Alcatel, etc.)

CISCO SCCP (*SKINNY Client Control Protocol*)

Version «historique» encore largement déployée, sans les mécanismes de sécurité plus robustes

Depuis Call Manager version 4.1 :

- SSL/TLS, pour la signalisation SKINNY
- SRTP, pour les flux RTP

Problèmes de sécurité documentés, notamment :

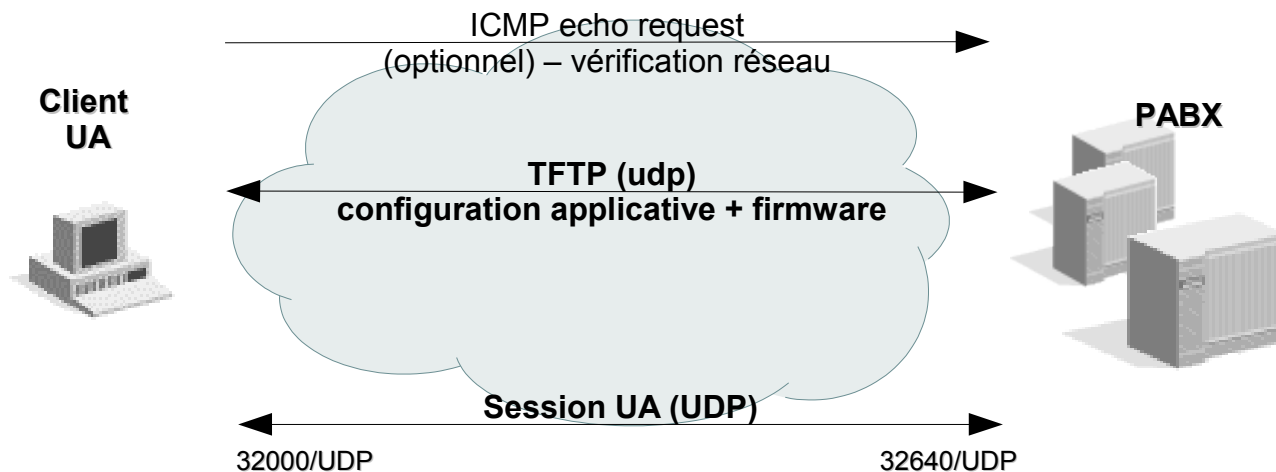
- « *The Trivial CISCO IP Phones compromise: Security analysis of the implications of deploying Cisco Systems' SIP-based IP Phones model 7960* » (Ofir Akin, 2002)
- « *Projet Ilty : I'm Listening to You (via VoIP)!* » (Nicolas Bareil, SSTIC05)

Autre exemple : Alcatel UA

Dans la version rencontrée Mi-2003

Alcatel UA :

Processus de démarrage du téléphone

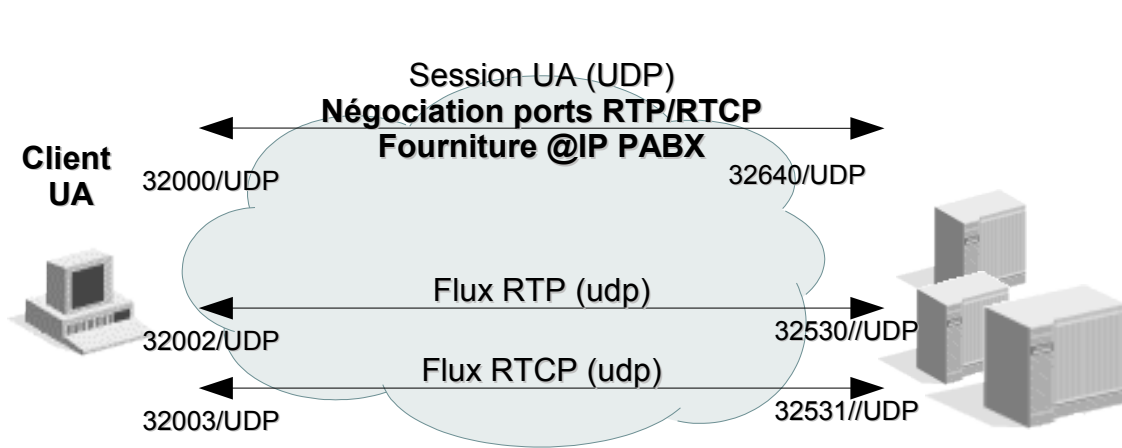


Client UA sans mémoire

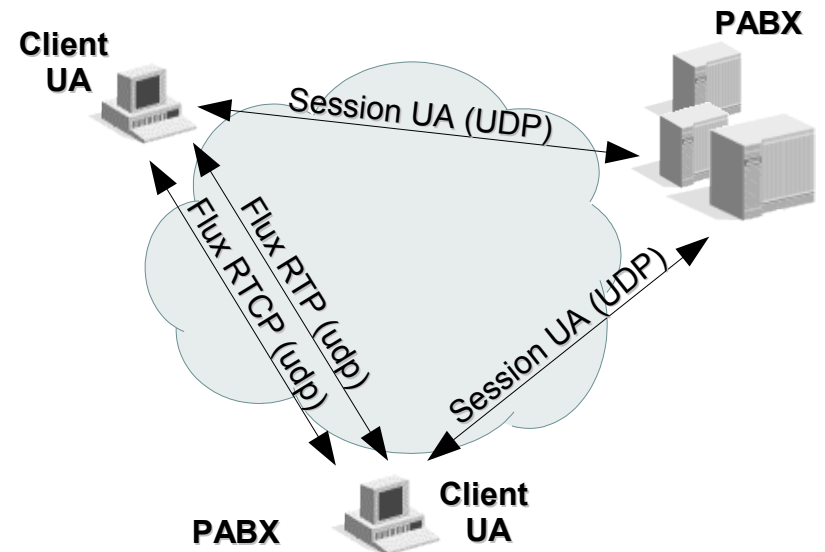
- Récupération des fichiers de configuration depuis un PABX de téléchargement pré-configuré
- Identification du téléphone par son adresse MAC transmise via une extension TFTP
Si l'adresse MAC n'est pas reconnue, l'utilisateur configure son numéro et un code secret
- Initialisation du téléphone – session UA (signalisation, sur UDP) entretenue par un *Keep-Alive* toute les 3 secondes ; au delà :ré-initialisation du téléphone

VoIP : Sécurité des protocoles propriétaires (Cisco, Alcatel, etc.)

Client UA ↔ Autre



Inter-Clients UA



Exemple d'attaques :

Désynchronisation du client UA (insertion de datagrammes UDP, avec l'adresse IP du PABX)
 → Dénis de service et réinitialisation, ou blocage du téléphone jusqu'à remise sous tension suivant le scénario

Usurpation d'identité : déni de service sur un poste, puis rejeu de son adresse MAC via une extension DHCP – possibilité de balayer le réseau à la recherche des adresses MAC des téléphones via SNMP

+ *Attaques classiques d'interception sur les réseaux locaux*

Alcatel UA



Potentiellement : résultats à généraliser à tout protocole (VoIP ou non) n'implémentant pas un minimum de sécurité applicative – dans un environnement ne fournissant pas de sécurité à un plus bas niveau (liaison/réseau/transport)

Évolution des réseaux GSM :

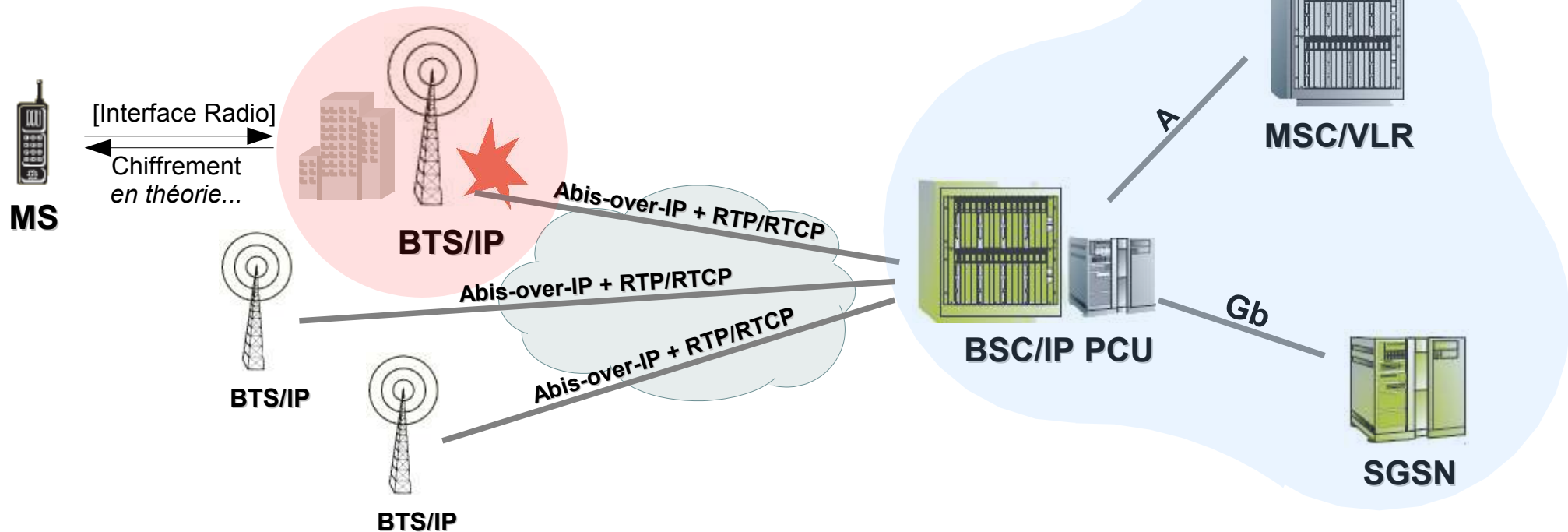
Adaptation du réseau d'accès au protocole IP

→ Utilisation des protocoles de VoIP sur des segments de réseaux

Exemple de l'interface *Abis* entre les équipements BTS (*Base Transceiver Station*, ou « Station de Base ») et BSC (*Base Station Controller*) sur IP : Signalisation propriétaire (*Abis-over-IP*) et flux de datagramme RTP/RTCP pour la Voix

→ Objectif pour un opérateur : implanter des BTS dans des endroits potentiellement hors couverture (parkings souterrains, étages supérieurs etc.), afin de densifier le réseau, en raccordant les BTS ainsi distribuées aux BSC via des liaisons IP

Architecture avec BTS/IP



Dans la version initiale : absence de mécanismes de sécurité fondés sur la cryptographie dans l'adaptation du protocole Abis sur IP :

- **Flux TCP (propriétaire) pour la signalisation** – sans authentification mutuelle ou unilatérale entre BTS et BSC, ni chiffrement ou contrôle d'intégrité,
- **Flux UDP (RTP/RTCP) pour la voix** – à destination d'une passerelle MGW (Media Gateway)
Même constat : absence complète de sécurisation

Sécurité (physique/logique) des équipements BTS/IP ?

Réseaux GSM & Protocoles de VoIP Falsification d'appel entrant

BSC (.105) ↔ BTS (.106)

Signalisation GSM

10.0.0.105	10.0.0.106	GSM	PAGING_CMD(TS=0,CCCH,)	# Appel Entrant
10.0.0.106	10.0.0.105	GSM	CHAN_RQD(TS=0,RACH,)	
10.0.0.105	10.0.0.106	GSM	CHAN_ACTIV(TS=0,SDCCH4/0,)	# Alloc. Canal Sig.
10.0.0.106	10.0.0.105	GSM	CHAN_ACTIV_ACK(TS=0,SDCCH4/0,)	
10.0.0.105	10.0.0.106	GSM	IMM_ASS(TS=0,CCCH,RR:Immediate Assignment)	
10.0.0.106	10.0.0.105	GSM	EST_IND(TS=0,SDCCH4/0,RR:Paging Response)	
[...] Mécanismes d'authentification + chiffrement (MS + BTS)				
10.0.0.105	10.0.0.106	GSM	DATA_REQ(TS=0,SDCCH4/0:MM:Identity Request)	# IMEI
10.0.0.105	10.0.0.106	GSM	DATA_REQ(TS=0,SDCCH4/0:CC:Setup)	
10.0.0.106	10.0.0.105	GSM	DATA_IND(TS=0,SDCCH4/0:MM:Identity Response)	
10.0.0.106	10.0.0.105	GSM	DATA_IND(TS=0,SDCCH4/0:CC:Call Confirmed)	
10.0.0.105	10.0.0.106	GSM	CHAN_ACTIV(TS=1,Bm,)	
[...]				
10.0.0.106	10.0.0.105	GSM	CHAN_ACTIV_ACK(TS=1,Bm,)	
10.0.0.105	10.0.0.106	GSM	DATA_REQ(TS=0,SDCCH4/0:RR:Assignment Command)	
10.0.0.203	10.0.0.106	RTP	Payload type=Unknown (84), SSRC=168645406, Seq=50107, Time=790508536	
10.0.0.106	10.0.0.203	RTCP	Receiver Report	
[...]				

Flux Audio (RTP)

MGW (.203) ↔ BTS (.106)



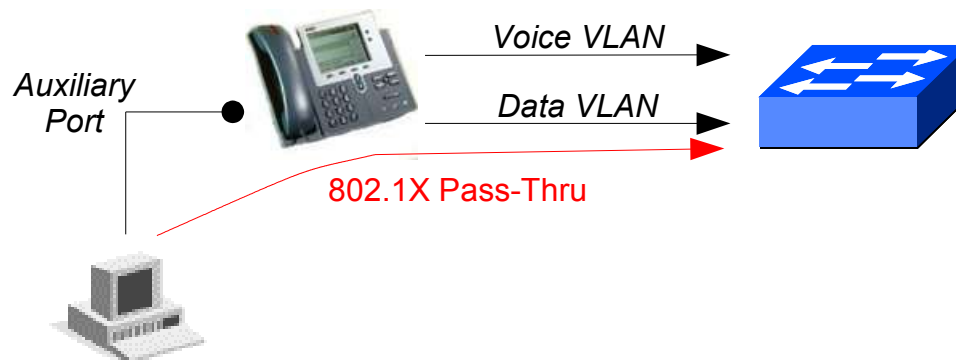
Message CALL SETUP qui comporte le numéro appelant, falsifiable :
→ Réécriture en ::;;<<05522

Risques : Atteinte à la confidentialité des conversations, fraudes diverses (détournement d'appels, redirection vers des numéros surfacturés pour les appels sortants etc.)

À propos du cloisonnement par VLAN, en environnement 802.1X

« **Voice VLAN Access/Abuse Possible on Cisco voice-enabled, 802.1x-secured Interfaces Vulnerability** » (06/08/2005)

<http://www.fishnetsecurity.com>



Poste client sur le port auxiliaire positionné dans le VLAN

Data : relayage des trames 802.1X par téléphone VoIP

Absence de Supplicant 802.1X dans les CISCO IP-Phones ...

→ « *It has been found that a specifically crafted Cisco Discovery Protocol (CDP) message is sent from the Cisco IP Phone to the switch which opens access to the voice VLAN for frames originating from that Cisco IP Phone's MAC address.*

Although 802.1x port-security may be configured on the switch port voice VLAN access is trivially gained by spoofing a CDP message. »

Avis du CERT 13 janvier 2004

Vulnérabilités multiples dans H.323 (tous constructeurs)

Téléphones, *Gatekeepers*, *Firewalls*

Du déni de service à l'exécution arbitraire de code

Avis du CERT 21 février 2003

Mêmes types de vulnérabilités dans les messages SIP INVITE

Dans des équipements de filtrage :

Déni de service distant dans Netscreen (25 novembre 2002)

Dans des outils d'analyse :

Exécution de code dans le dissecteur SIP d'Ethereal (8 mai 2005)

Dans des produits libres :

Exécution de code dans Asterisk via SIP (4 septembre 2003)

Les mécanismes de sécurité implémentés de bout-en-bout existent chez de nombreux constructeurs, mais restent très rarement mis en oeuvre

Mais restent les seules réponses satisfaisantes aux problèmes soulevés

Le succès de la ToIP/VoIP relance des problèmes de sécurité qui n'ont jamais cessé d'exister

Quid des attaques sur les réseaux locaux vis-à-vis des protocoles de messagerie utilisés en entreprise ?

Les solutions de sécurisation aux niveaux liaison (cloisonnement par VLAN, protection contre les attaques sur ARP)/réseau (filtrage IP, VPN IPsec)/transport (SSL/TLS, et prochainement DTLS etc.) apportent un élément de réponse mais restent difficiles à mettre en oeuvre

HSC tips and presentations

<http://hsc.fr>

Ethereal – A Network Protocol Analyzer

<http://ethereal.com>

VoMIT – Voice over Misconfigured Internet Telephones

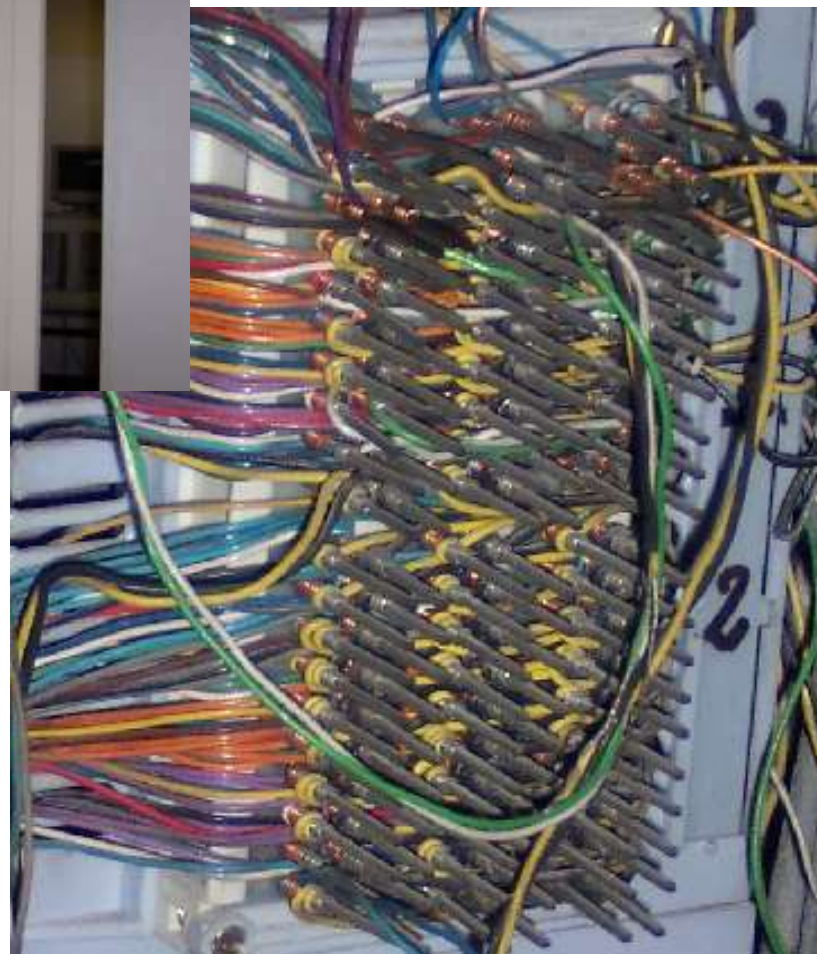
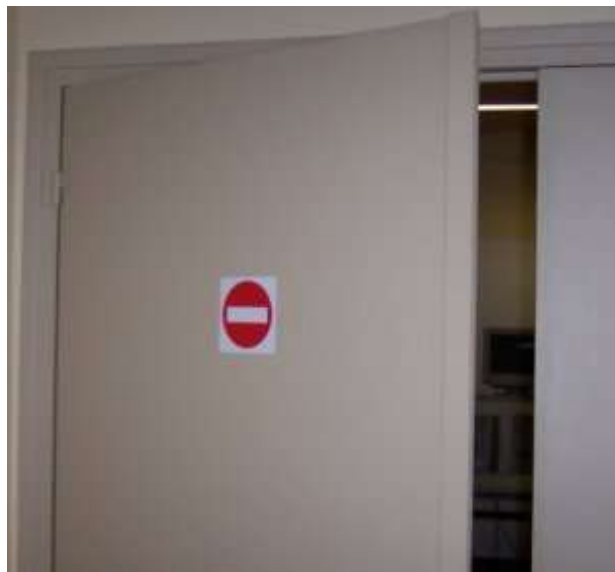
<http://vomit.xtdnet.nl/>

VoIPong – Voice over IP sniffer and Call detector

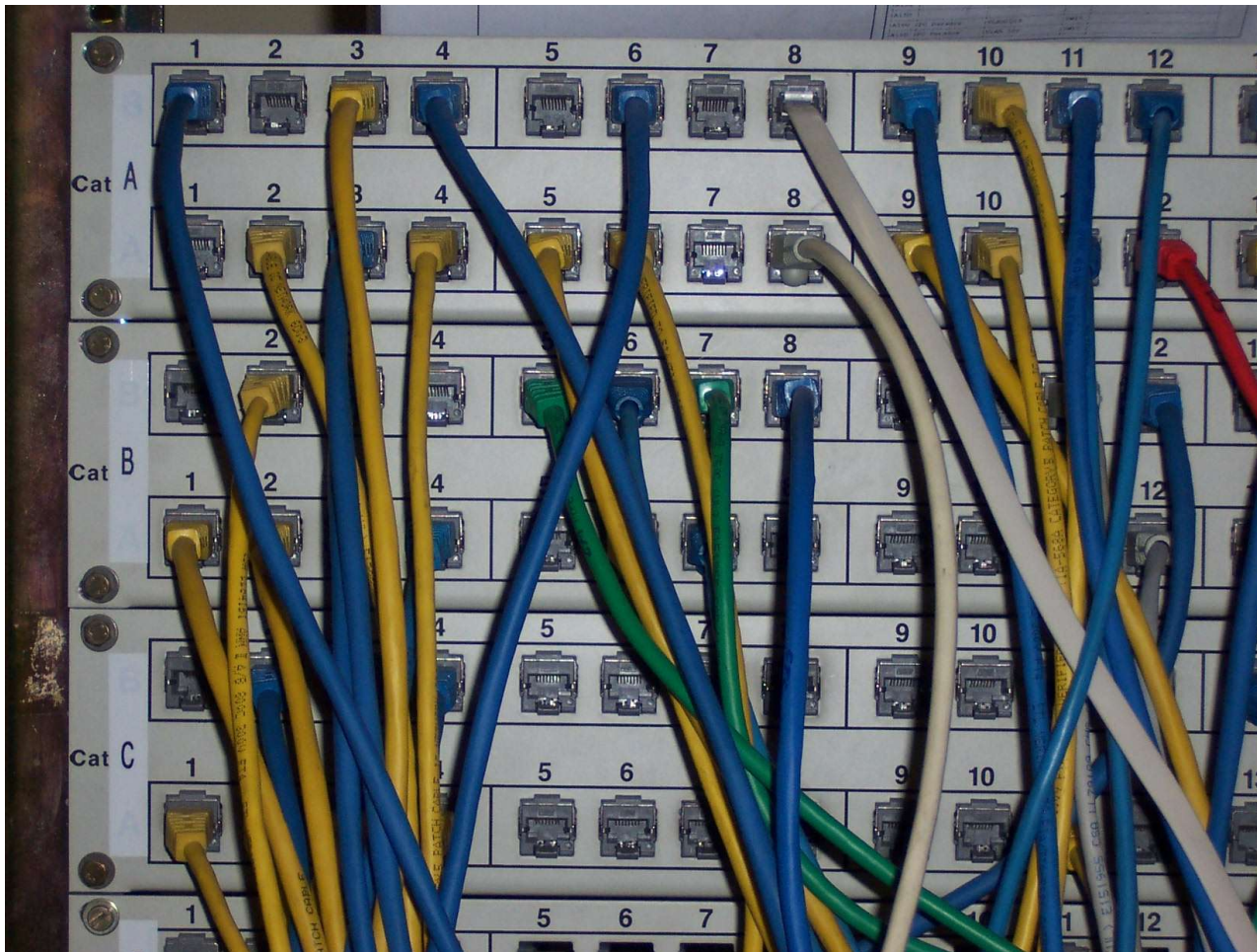
<http://www.enderunix.org/voipong/>

VOIPSA VoIP Security Alliance

<http://www.voipsa.org>



Téléphone non sécurisé ?



Questions ?

➤ **Formation DNS : 21 juin, Postfix et anti-spam : 22 juin**

➤ <http://www.hsc.fr/services/formations/>

➤ **Formations SecurityCertified : 5-9 & 19-23 septembre**

➤ **Permettant de passer la certification SCNP**



➤ <http://www.hsc.fr/services/formations/>

➤ **Formation BS7799 Lead Auditor : octobre 2005**

➤ **Certifiée par LSTI et reconnue par l'IRCA**



➤ <http://www.hsc.fr/services/formations/>

Sur www.hsc-news.com vous pourrez vous abonner à la newsletter HSC