VoIP et sécurité

Retour d'expérience d'audits de sécurité

6 avril 2006

Hervé Schauer
CISSP, ProCSSI, ISO 27001 Lead Auditor
<Herve.Schauer@hsc.fr>

Hervé Schauer Consultants

- Société de conseil en sécurité des systèmes d'information depuis 1989
- Prestations intellectuelles d'expertise en toute indépendance
  - Pas de distribution, ni intégration, ni infogérance, ni investisseurs, ni délégation de personnel
- Prestations : conseil, études, audits, tests d'intrusion, formations
- Domaines d'expertise
  - Sécurité Windows / Unix et linux / embarqué
  - Sécurité des applications
  - Sécurité des réseaux
    - TCP/IP, téléphonie, réseaux opérateurs, réseaux avionique, ...
  - Organisation de la sécurité
- Certifications
  - CISSP, BSI BS7799 Lead Auditor, LSTI ISO27001 Lead Auditor, IRCA, ProCSSI

Sommaire

- Introduction
- Technologies et risques
- Terminaux et infrastructure
- Bilan
- Solutions
  - Dont le calcul du retour sur investissement
- Conclusion
- Références et ressources

Les transparents seront disponibles sur www.hsc.fr

Introduction

- Exemples d'usages
  - Visioconférence, télésurveillance
  - Téléphonie d'entreprise
  - Télécopie
  - Téléphonie sur internet
  - Télévision & radio
- Terminaux
  - Ordinateur + logiciel
  - Téléphone de bureau
  - Téléphone sans fil WiFi
  - Freebox, Livebox, ...
- Serveurs

Technologies

- Voix sur IP → multitude de protocoles
- H323
- SIP
- SCCP (Cisco)
- MGCP
- GSM

- Signalisation : la gestion des appels, passe par des serveurs
- Données : la voix, peut passer par le chemin le plus court

H323

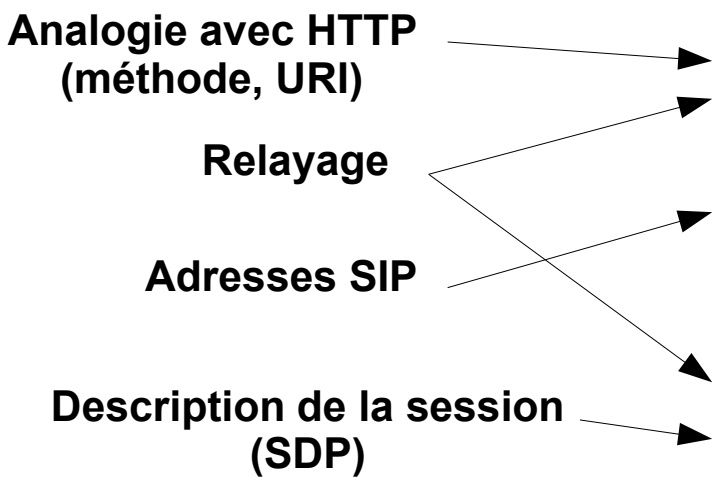
- Normalisé par l'ITU
- Transcription IP de l'ISDN
- Protocole similaire au fonctionnement des réseaux téléphonique commutés
- Complexe
  - Pleins de protocoles sous-jacents
- Encore utilisé en coeur de réseau
- En voie de disparition

H323

- Risques
  - Intrusion
    - Filtrage quasi-impossible : multiplication des flux, des mécanismes d'établissement d'appel, des extentions à la norme, et transmission des adresses IP au niveau applicatif
  - Ecoute
  - Usurpation d'identité
  - Insertion et rejeu
  - Dénis de service
    - De par la conception du protocole, pas de détection des boucles, signalisation non fiable, etc

SIP

- Normalisé par l'IETF (RFC3261)
- Protocole similaire à HTTP

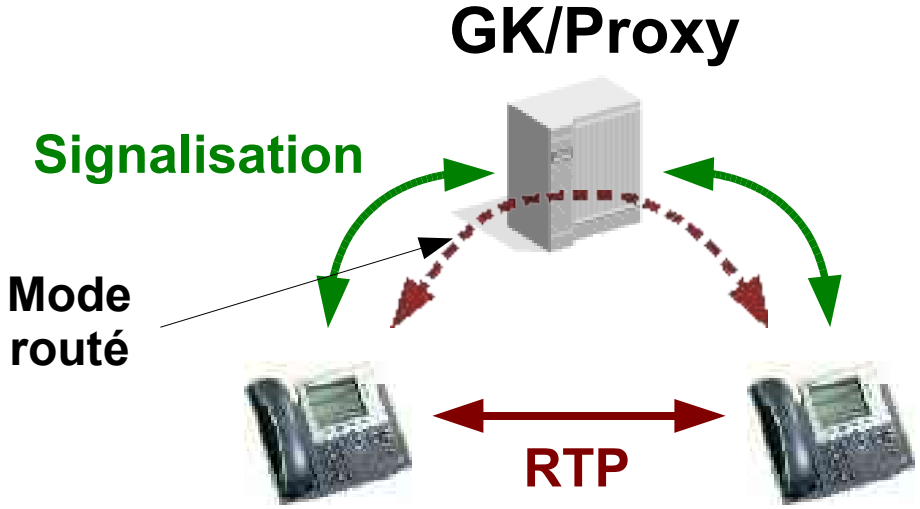



```
INVITE sip:test@192.70.106.102 SIP/2.0
Via: SIP/2.0/UDP 0.0.0.0:5063;branch=z9hG4bK894348304
Route: <sip:192.70.106.104;lr>
From: <sip:at@192.70.106.104>;tag=7116539;tag=7648279
To: <sip:test@192.70.106.102>
Call-ID: 4173170638@192.70.106.104
CSeq: 21 INVITE
Contact: <sip:at@192.70.106.104:5063>
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 importe
  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 descriptio
  7 17.05774 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=
```

SIP

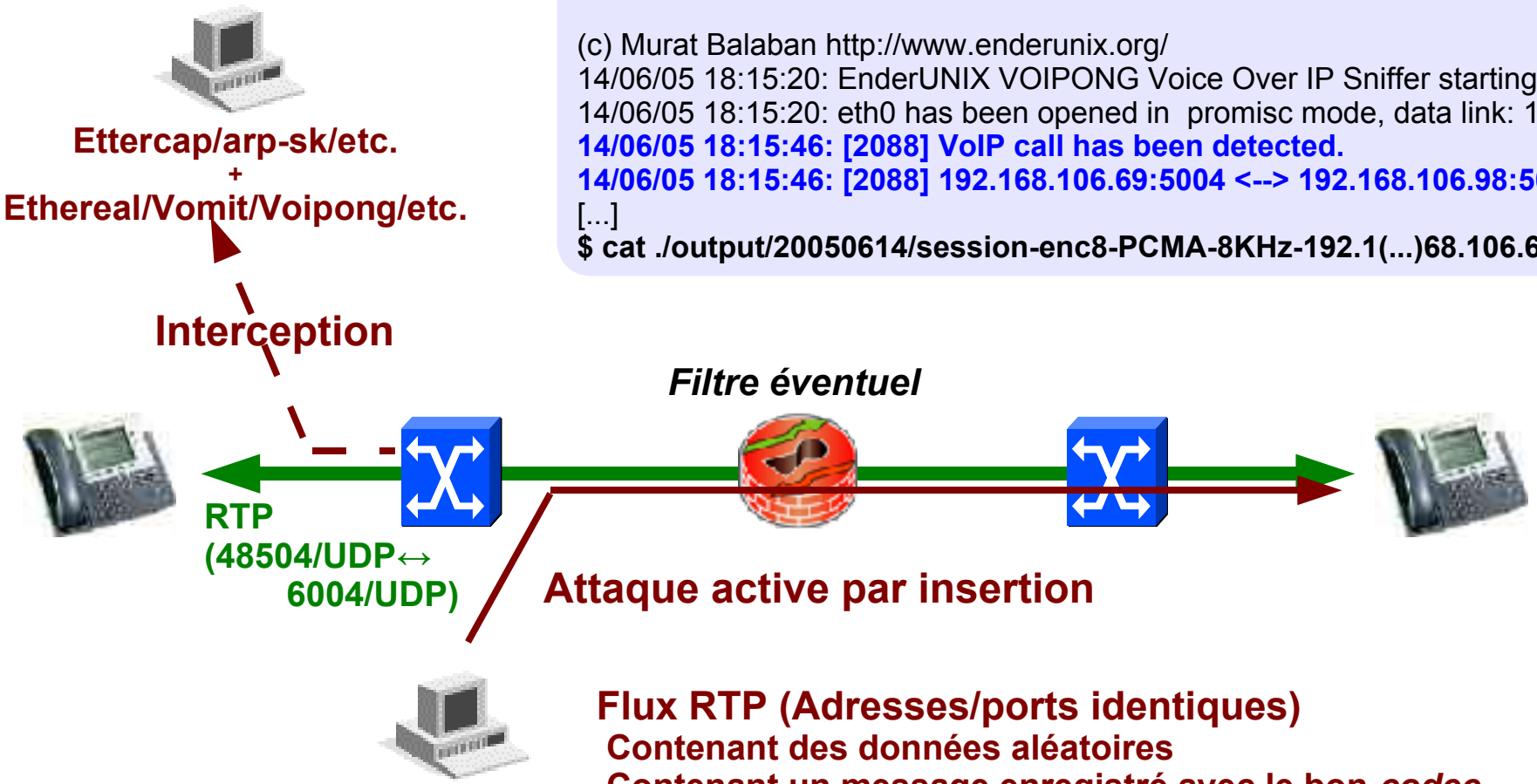
- Protocole similaire à HTTP
  - Gestion de sessions entre participants
  - SIP : signalisation, et RTP/RTCP/RTSP : données
  - Données transportées de toute nature : voix, images, messagerie instantanée, échanges de fichiers, etc
- Risques :
  - Ecoute
  - Usurpation d'identité
  - Insertion et rejeu
  - Déni de service



SIP : écoute et insertion de flux RTP

```
# ./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
```



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

SCCP

- SCCP : Skinny Client Control Protocol
- Propriétaire à Cisco
- Risques :
  - Ecoute
  - Usurpation d'identité
  - Insertion et rejeu
  - Déni de service
  - 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 Arkin, 2002)
    – *«Projet Ilty : I'm Listening to You (via VoIP)! »* (Nicolas Bareil, SSTIC05)
- Risques identiques avec les autres technologies propriétaires
  - Alcatel, Avaya, etc

MGCP

- MGCP : Multimedia Gateway Control Protocol
- Normalisé par l'IETF (RFC3435)
- Chaque paquet défini une action
- Utilisé lorsqu'il y a une intelligence centrale
  - En entreprise
  - Par les opérateurs sur l'ADSL
- Risques
  - Identiques aux autres en entreprise *(pas d'expérience d'audit sécurité)*
  - Dépendants de la sécurité du boitier ADSL
  - Moins de risques de surfacturation et de déni de service sur le serveur central

GSM sur IP : NanoBTS

- NanoBTS :
  - Borne GSM de proximité reliée par internet à l'opérateur (BTS → BSC)
    - Pour zônes hors de couverture ou à forte densité d'usage : sous-sols, centres de congrès, parkings, etc
  - Protocole propriétaire à chaque fabricant
    - Signalisation : Abis-over-IP; Données : flux RTP/RTCP
- Risques :
  - Surfacturation
  - Ecoute des communications
  - Usurpation d'identité
  - Insertion et rejeu
  - Déni de service

GSM sur IP : UMA

- UMA : Unlicensed Mobile Access
- Le téléphone portable GSM via Internet
- Permet aux opérateurs de lutter face à Skype & équivalents
- Normalisé par le 3GPP
- GSM au dessus d'IPsec avec IKE v2
- Authentification EAP-SIM
- Risques :
  - Exposition du réseau opérateur sur internet
  - Déni de service

Terminaux

- Peu de sécurisation des terminaux, peu de fonctions de sécurité
  - Pas de 802.1X
- Exemple à *ShmooCon* : test de téléphones VoIP (SIP) sur WiFi
  - 15 Téléphones testé de 8 fournisseurs
    - Cisco, Hitachi, Utstarcom, Senao, Zyxel, ACT, MPM, Clipcomm
  - Connexion interactive avec telnet ouverte
  - SNMP read/write avec *community name* par défaut
  - Ports de debogage VXworks ouverts en écoute sur le réseau WiFi
  - Services echo et time ouverts
  - Connexion interactive rlogin avec authentification basique
  - Exemple Cisco 7920
    - port 7785 Vxworks wdbrpc ouvert
    - SNMP Read/Write
    - Réponse de Cisco : les ports ne peuvent pas être désactivés, la communauté SNMP ne pas être changée : tout est codé en dur dans le téléphone...

Infrastructure

- Exemple vécu lors d'un audit qui n'était pas un audit de sécurité de la VoIP
  - Coupure de courant
  - Téléphone (Mitel) branché sur le secteur (pas PoE, pas secouru) ☞ plus de téléphone
  - Serveurs branchés sur le courant secouru mais pas le commutateur devant
  - Retour du courant
  - Serveur de téléconfiguration des téléphones injoignable (DHCP, BOOTP pour le *firmware*, etc.) car commutateur pas encore redémarré
  - Les téléphones ont redémarré plus vite que le commutateur et se sont trouvés sans adresse IP, etc. et restent bloqués sur l'écran "*Waiting for DHCP ...*"
  - Pour une raison inconnue, une fois le serveur de téléconfiguration à nouveau joignable, les téléphones n'ont pas fonctionné
  - Seule solutions trouvée : débrancher/rebrancher chaque téléphone un par un pour qu'ils se remettent en service

Bilan de la VoIP/ToIP

- N'est pas équivalent à la téléphonie classique
  - Signalisation/contrôle et transport de la voix sur le même réseau IP
  - Perte de la localisation géographique de l'appelant
- N'offre pas la sécurité à laquelle les utilisateurs étaient habitués
  - Fiabilité du système téléphonique
    - Combien de pannes de téléphone vs pannes informatique ?
  - Confidentialité des appels téléphoniques
  - Invulnérabilité du système téléphonique
    - Devenu un système suceptible d'intrusions, vers, etc

Bilan de la VoIP/ToIP

- N'est pas juste "une application IP en plus"
  - Pas d'authentification mutuelle entre les parties
  - Peu de contrôles d'intégrité des flux, pas de chiffrement
    - Risques d'interception et de routage des appels vers des numéros surfacturés
    - Falsification des messages d'affichage du numéro renvoyés à l'appelant
  - Attaques accessibles à tout informaticien et pas juste aux spécialistes de la téléphonie numérique

Solutions

- Sécurité dans le réseau IP
- Sécurité propre à la solution de VoIP / ToIP
- Calcul du retour sur investissement de la VoIP

Sécurité dans le réseau IP

- Sécurité dans le réseau
  - Liaison
    - Cloisonnement des VLAN
    - Filtrage des adresses MAC par port
    - Protection contre les attaques ARP
  - Réseau
    - Contrôle d'accès par filtrage IP
    - Authentification et chiffrement avec IPsec
  - Transport
    - Authentification et chiffrement SSL/TLS

Sécurité propre à la solution VoIP/ToIP

- SIP, MGCP, et les protocoles propriétaires incluent des fonctions de sécurité
- Limite des terminaux qui n'ont pas le CPU nécessaire à des calculs de clefs de session en cours de communication
- Mise en oeuvre de la sécurité → perte des possibilité d'interopérabilités entre fournisseurs

Retour sur investissement

- Mettre à jour son PABX apporte les mêmes service avec ou sans VoIP
  - Aucun service disponible en VoIP n'est pas disponible en téléphonie classique
  - Aucun calcul de retour sur investissement ne peut se justifier par la disponibilité de nouveaux services

Retour sur investissement

- Intégrer les coûts de la VoIP
  - Coûts de cablage
    - Poste téléphonique IP => prise ethernet supplémentaire
    - Plusieurs clients ont eu des difficultés avec le PC connecté sur le téléphone et le téléphone dans la prise Ethernet du PC
    - Aucun client HSC n'a survécu sans VLAN, avant même les considérations de sécurité
    - Service téléphonique doit savoir dans quel pièce et sur quelle prise est chaque numéro de téléphone
      - N° de téléphone, @MAC, @IP et n° de prise Ethernet sont liés
    - Très vite il faut cabler des prises spécifiques avec le courant électrique sur le cable Ethernet (PoE)
  - Onduleurs supplémentaires et spécifiques
  - VoIP/ToIP impose des coûts de cablage élevés

Retour sur investissement

- Intégrer les coûts de la VoIP
  - Services du réseau informatique deviennent des services **critiques**
    - DHCP
    - DNS
    - Commutateurs
    - ...
  - Coûts de mise en oeuvre de la haute-disponibilité devenue obligatoire
  - Coûts d'exploitation au quotidien bien plus élevés
    - 24/7, etc

Retour sur investissement

- Intégrer la dégradation du service due à la VoIP
  - Taux d'indisponibilité téléphonie classique : 5 à 6 minutes d'interruption par an, 99,99886 %
  - Taux de disponibilité téléphonie sur IP : ??
    - Nous avons vu des gens sans téléphone pendant plusieurs jours...
  - Support téléphonique hors-service
    - « Quand le réseau est panne il n'y a plus non plus de téléphone comme ça on est dérangé que par ceux qui utilisent leur mobile »
  - Téléphone : principal système d'appel au secours pour la sécurité des personnes

Retour sur investissement

- Valider au préalable la réalité des fonctionalités
  - Systématiquement il y a les fonctionalités d'un coté et le prix du poste téléphonique entrée de gamme de l'autre
  - Fonctionalités de sécurité imposant un changement de tous les postes téléphoniques
- Valider au préalable la robustesse de tous les équipements choisis
  - Cf ISIC, SIPSAK, CODENOMICON, etc
- Analyser les risques
  - Pourquoi si peu de gens font une analyse de risques sur leur projet VoIP ?

Organisation

- Téléphonie doit entrer dans le giron de la Direction des Systèmes d'Information (DSI)
  - Ne peut rester aux services généraux
- Téléphonistes doivent intégrer la DSI
  - Leurs compétences en téléphonie sont indispensables au déploiement de la VoIP
- La VoIP / ToIP vous est imposé par les fournisseurs dans leur intérêt : vous devrez y passer un jour de gré ou de force

Conclusion

- La VoIP / ToIP relance l'insécurité, vous devez vous y préparer
- Sécurité au niveau réseau
  - Réponse partielle mais nécessaire
  - Difficile à mettre en oeuvre
- Mécanismes de sécurité propriétaires proposés par les constructeurs :
  - Seule réponse satisfaisante en matière de sécurité
  - Très rarement mis en oeuvre
- ROI : calculez le vous-même !

Questions ?

Herve.Schauer@hsc.fr
www.hsc.fr

Prochains rendez-vous

- **Formation ISO27001 Lead Auditor** :
  - Certification ISO27001 Lead Auditor par **LSTI**
  - **`http://www.hsc.fr/services/formations/`**

Genève : 8-12 mai
Paris : 15-19 mai
Toulouse : 5-9 juin

Références

- Two attachs against VoIP, 04/06, Peter Thermos, Palindrome
  - http://www.securityfocus.com/infocus/1862
- VoIP et sécurité pour l'entreprise,11/05, Stefano Ventura, IICT
  - http://www.aud-it.ch/VoIP&SEC.grifes.off.zip
- Sécurité de la VoIP, 06/05, Franck Davy, Nicolas Jombart, Alain Thivillon, HSC
  - http://www.hsc.fr/ressources/presentations/csm05-voip/
- Security considerations for VoIP systems, 01/05, Richard Kuhn, Thomas Walsh, Steffen Fries, NIST
  - **http://www.csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf**

Ressources

- Sur **www.hsc.fr** vous trouverez des présentations sur
  - Infogérance en sécurité
  - Sécurité des réseaux sans fil
  - Sécurité des SAN
  - Sécurité des bases de données
  - SPAM
  - ISO27001 / ISO17799
  - Sécurité de la voix sur IP
  - etc

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