



Sécurité de la ToIP

Mercredi 16 Décembre 2009

CONIX Telecom

eric.assaraf@conix.fr

Téléphonie sur IP vs téléphonie classique



Quel est le niveau de sécurité de la téléphonie classique ?

Vomit – Voice of Misconfigured Internet Telephone (Publicly Available)

Freely downloadable

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

Decodes G.711 to .WAV file

VoipCrak (Not Publicly Available)

Near Real Time VoIP/RTP Recorder/Decoder

Uses Freeware WinPcap, “The Free Packet Capture Architecture for Windows” – Promiscuous Packet Capture

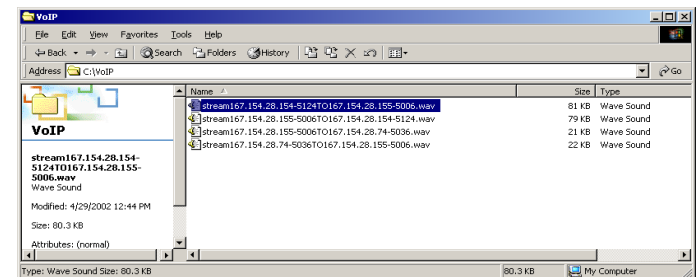
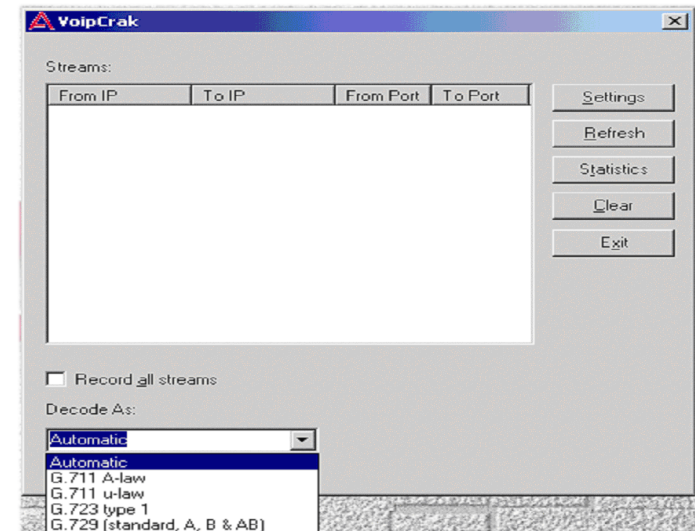
<http://winpcap.polito.it/>

Decodes:

G.711 A-law / u-law

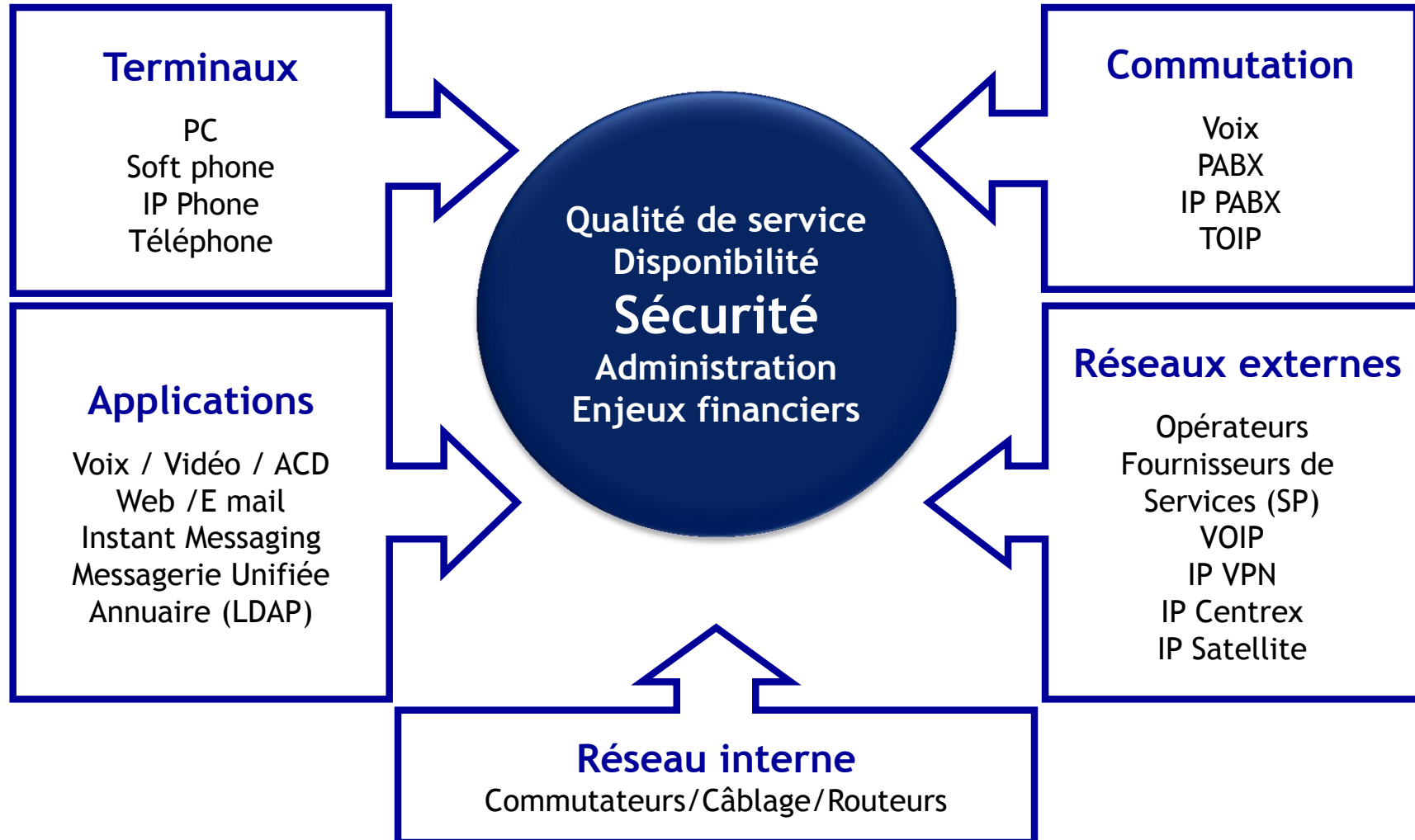
G.723

G.729



Conversations au format .WAV

Le modèle IP : Nécessite une approche globale c'est un système



La TOIP une brique applicative : La voix et la messagerie vocale essentielles, les autres sont en devenir



Téléphoniques



- Terminaux
- SIP
- Self care
- Qualité Voix
- Chiffrement

Vocales



- Messagerie
- SVI
- Standard automatique
- Reconnaissance vocale

Data



- Messagerie unifiée
- Base annuaire
- Outils collaboratifs

Vidéo



- Visiophonie
- Vidéo mail
- Diffusion vidéo
- SVVI
- IP Télévision

La TOIP besoin de la vision systémique :

Authentication

Are you who you claim to be?

Authorization

Are you allowed to do it?

Confidentiality

Is this unavailable to the unauthorized?

Non-repudiation

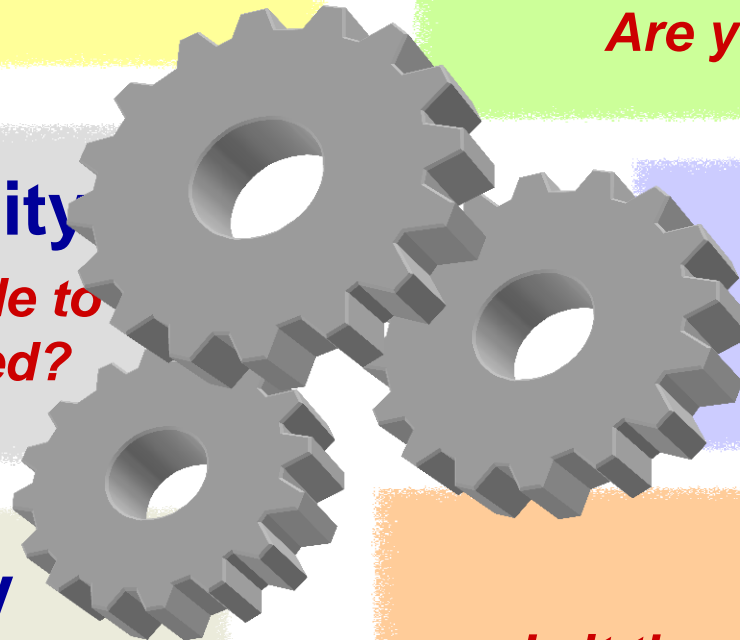
Could no other have done it but you?

Integrity

Does it remain intact?

Availability

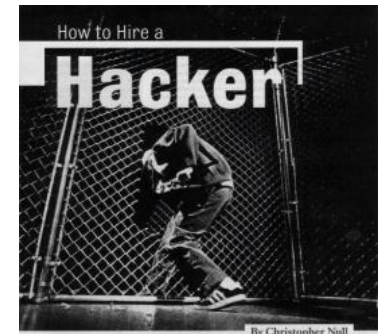
Is it there when needed?



La disponibilité : la référence et les attentes des utilisateurs ceux de la téléphonie fixe 99,999 %

- **La résilience** de la plate forme
 - Calcul du MTBF pour chaque équipement (infrastructures et téléphonie IP)
 - Calcul du MTTR pour chaque domaine (Backbone, Wan, système de téléphonie)
- **L'architecture** du système
 - Redondance et design des infrastructures
 - Plan de reprise
- **La disponibilité** des infrastructures internes et opérateurs
 - Qualification du câblage
 - Contrats de service
- **Les facteurs environnementaux et énergétiques**
 - Climatisation des locaux
 - Protection contre les surtensions
 - Sources redondées, alimentations redondées, batteries, générateur

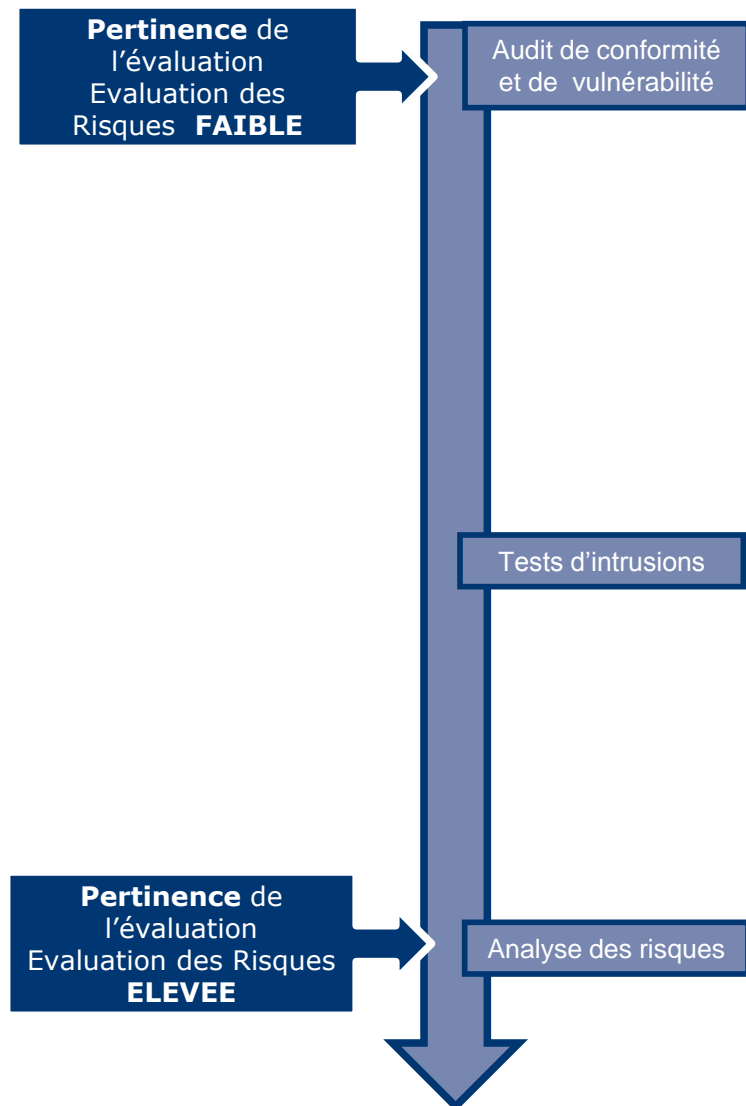
- **Attaques physiques** (systèmes d'écoute)
- **Attaques sur les couches basses**
 - ARP spoofing / ARP cache poisoning
 - MIM : écoute passive ou modification de flux
- **Attaques sur les implémentations**
 - Interface d'administration HTTP, de mise à jour TFTP, etc.
 - Exploits, Vols de session (XSS), Scripts / injections, Piles TCP/IP
 - Dénis de services (DoS)
- **Attaques sur les protocoles VoIP/SIP**
 - Spoofing SIP :Call-ID, Tags des champs From et To
 - DoS : Envois illégitimes de paquets SIP INVITE ou BYE
 - Modification « à la volée » des flux RT
- **Attaques sur les protocoles secondaires**
 - DNS : DNS ID spoofing ou DNS cache poisoning
 - DHCP : DoS, MITM
 - TFTP : upload d'une configuration (DoS, MITM...)



Exemples de mécanismes de sécurisation d'une architecture IP

- **Sécurisation physique** des équipements dans des locaux badgés, des baies fermées s'ils sont hébergés dans les centres
- Mécanismes **Authentication, Authorization, Accounting** sur tous les équipements du système, incluant les équipements d'infrastructure
- Mise en œuvre de **Firewalls** possédant des fonctions de proxy
- **Nat** (Transposition d'adressage)
- **Mise en œuvre de plans d'adressage privés** et de fonctions de translation pour l'interconnexion avec Internet
- **Durcissement des OS des serveurs du système de téléphonie**
 - Serveur Windows (patches, arrêt des services inusités, disques en NTFS, nettoyage des comptes, audit système)
 - Serveur Web
 - Serveur de base de données





- Analyse orientée « audit de conformité et de vulnérabilité »
 - Identifier de façon la plus exhaustive possible les vulnérabilités présentes sur les infrastructures, applications et processus, et estimer le niveau de risque

- Analyse orientée « test d'intrusions », consistant à tenter de prendre le contrôle des différents composants
 - Améliorer la complétude des analyses (identification de vulnérabilités)
 - Confirmer ou infirmer une vulnérabilité préalablement identifiée
 - Identifier et illustrer les vulnérabilités théoriques par des exemples concrets

- Valorisation de chacun des constats d'audit et / ou de test d'intrusion par une approche par le risque
 - Faciliter la prise de décision
 - Permettre l'identification immédiate des priorités concernant la SSI grâce à l'établissement d'une matrice de risques

- **Analyseurs Ethernet :**
 - Wireshark/Ethereal, Ethercap...
- **Outils de diagnostics**
 - NESSUS (pour vérifier la stack IP du SBC)
 - ISIC - IP Stack Integrity Checker (pour vérifier la stack IP du SBC)
- **Tests et intrusion** (RFC4475 SIP Torture Test Messages)
 - PROTOS suite de tests développé par université d'Oulu
 - Sivos Sip vulnerability scanner
 - VoiPong : Injection de trame RTP
 - SIPp : Il permet de simuler le comportement de user agent
 - HPING : à utiliser de manière combiner avec un outil réalisant des attaques Man in the Middle



Exemple des outils de l'audit : VoiPong Analyse, réinjection de trafic RTP

Ethereal, VoiPong, WinEyeQ, etc. : comprennent le trafic RTP qui est utilisé par le VoIP

Format: **GSM** (ulaw, 8 bit, 8000 Hz, mono)

Channels: forward reversed both

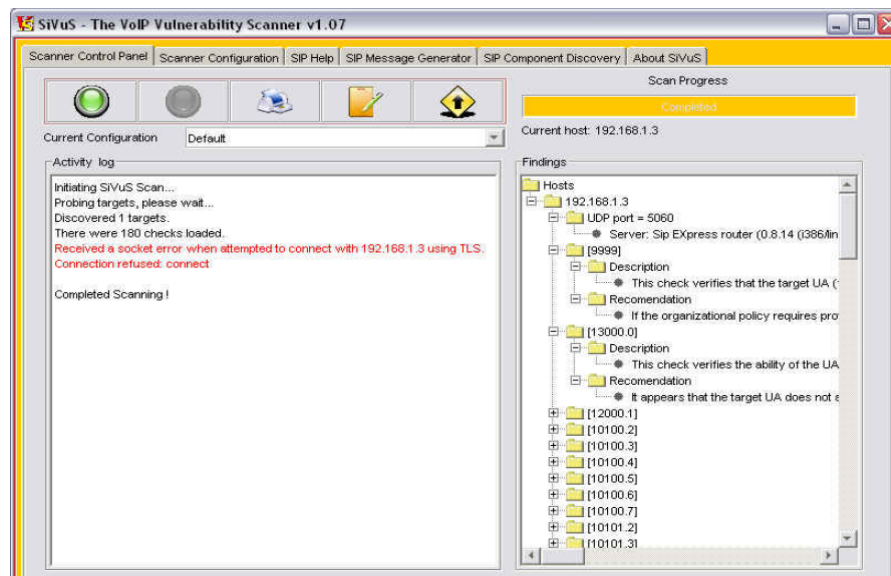
Ethereal RTP Stream Analysis

Packet	Sequence	Delay (s)	Jitter (s)	Marker	Status
17	521.01	0,000000	0,000000	SET	[ok]
18	521.02	0,000634	0,001835		[ok]
19	521.03	0,000317	0,000571		[ok]
20	521.04	0,000344	0,000204		[ok]
21	521.05	0,013589	0,005905		[ok]
22	521.06	0,000307	0,007306		[ok]
23	521.07	0,000323	0,006779		[ok]
24	521.08	0,019402	0,008858		[ok]
25	521.09	0,000330	0,010192		[ok]
26	521.10	0,000313	0,011110		[ok]
27	521.11	0,027175	0,010673		[ok]
28	521.12	0,000396	0,012044		[ok]
29	521.13	0,000335	0,013145		[ok]
30	521.14	0,029300	0,012003		[ok]
31	521.15	0,030130	0,011958		[ok]
32	521.16	0,020015	0,010000		[ok]

Max delay = 0,030677 sec at packet no. 189
Total RTP packets = 375 (expected 375) Lost RTP packets = 0 Sequence errors = 0

Save payload ... Save as CSV ... Refresh Jump to Next non-OK Close

Les outils de l'audit : SIVUS (Sip Vulnerability Scanner) Un des outils les plus utilisés avec Protos



Des fonctions de :

- Génération de messages SIP
- Découverte des éléments réseaux
- Scanne et reporting des vulnérabilités

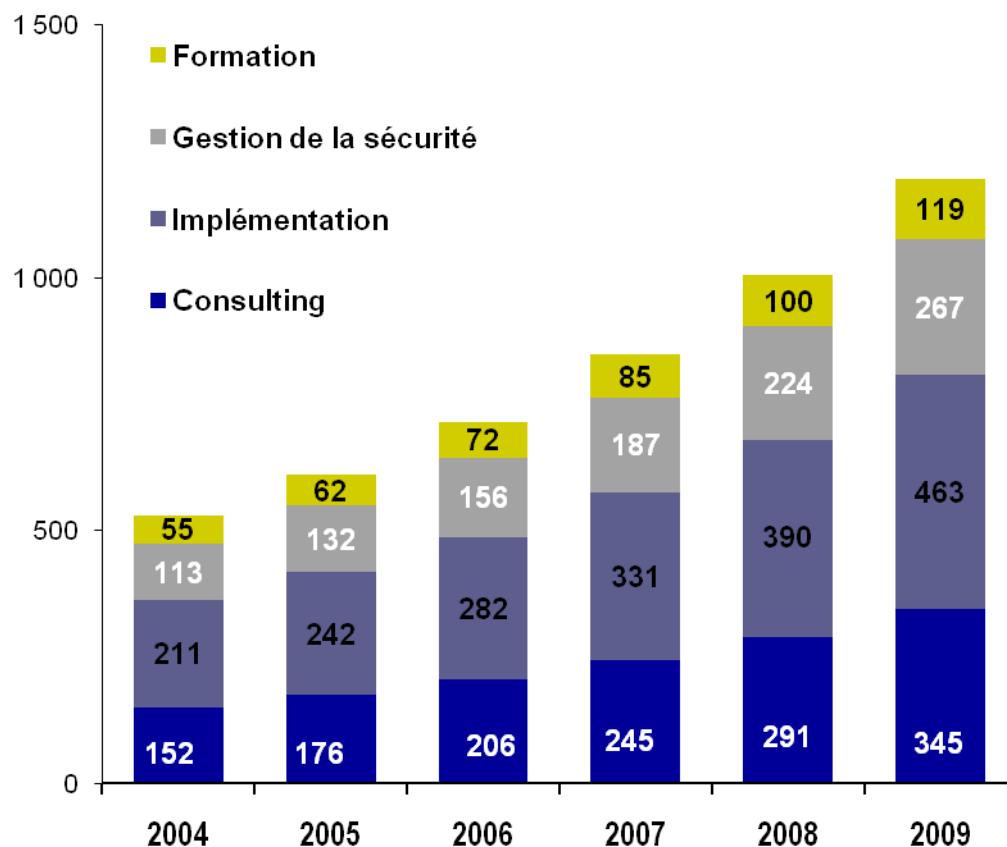
Summary of Findings

Risk Level	Number of Findings
High	24
Medium	0
Low	0
Informational	0

Findings Detail

[Informational] : Check No [0001]	
Description	
Recommendation	Server: Sip Express router (0.8.10 (386/linux))
[Informational] : Check No [0001]	
Description	
Recommendation	Server: Sip Express router (0.8.10 (386/linux))
[High] : Check No [10002.5]	
Description	This check verifies the ability of the UA to handle 5000 as the username in a URI using the REGISTER request over UDP.
Recommendation	It appears that the target UA could not handle SIP requests (over UDP) of 5000 as the username in the URI in a REGISTER request. Ensure that the UA can accept malicious requests that contain 5000 characters as the username.
[High] : Check No [10003.0]	

- La Téléphonie sur IP une application qui nécessite **une vision de la sécurité systémique**.
- Des attentes fortes des utilisateurs notamment en terme de **disponibilité**.
- **Un nombre d'applications de communications en croissance** avec l'IP en réseau fédérateur.
- **Les phases de tests et d'audit** à prendre en compte aussi bien dans les phases de mise en œuvre que dans les phases de production.
- **Une technologie mature** qui nécessite une bonne ingénierie dans son installation et dans sa sécurisation.



Une croissance de l'ordre de 20 % par an