



# Journées SSI 2006

## Sécurité et convergence voix-données

*Mardi 28 novembre 2006*

### *1. Introduction (problématique sécurité VoIP, ToIP, IMS)*

#### **Philippe Duluc**

Secrétariat général, Directeur de la sécurité groupe, France Télécom, Paris

#### **Ouverture des journées**

Révolution de la connectivité, révolution des usages, convergence de la voix sur IP, enjeux de sécurité, défis à relever.

#### **Carlos C. Solari**

Vice-President, Security Solutions, Bell Laboratories

#### **Security in a Converged World**

The threat, the challenge: secure the network; current approach is insufficient; convergence stresses the security further; a new model for security, the Bell Labs security framework; synergy in standards, the bottom line of security.

#### **Eric Wiatrowski**

Chief Security Officer, Orange Business Services (France Telecom Group) Rennes

#### **Voice over IP : Impact on security**

VoIP is going to be generalized within enterprises and public organizations.

Its implementation requires specific actions to guarantee the availability of the service and to protect communications integrity. Those actions are sometimes technical ones but organization is going to be a key factor for a successful implementation. Furthermore, the specificities of VoIP have to be taken into account: Complex architectures; Close relationships with data infrastructure; Physical environment constraints (power supply); Standards and equipments not mature enough; Etc

Not being exhaustive, the talk is going to present some risks and some possible remediative actions.

**Philip R. Zimmermann**

Special advisor and consultant, PGP Corporation; president, OpenPGP Alliance

**Securing VoIP phones**

Zfone is a new secure VoIP phone software product and protocol which lets you make encrypted phone calls over the Internet. Zfone uses a new protocol called ZRTP, which is better than the other approaches to secure VoIP, because it achieves security without reliance on a PKI, key certification, trust models, certificate authorities, or key management complexity that bedevils the email encryption world. It also does not rely on SIP signaling for the key management, and in fact does not rely on any servers at all. It performs its key agreements and key management in a purely peer-to-peer manner over the RTP media stream. It interoperates with any standard SIP phone, but naturally only encrypts the call if you are calling another ZRTP client. This new protocol has been submitted to the IETF as a proposal for a public standard, to enable interoperability of SIP endpoints from different vendors. Zfone is available as a universal "plugin" for a wide variety of existing VoIP clients, effectively converting them into secure phones. It's also available as an SDK to allow VoIP product vendors to integrate encryption into their products.

## **2. Architectures (architecture des réseaux, qualité de service, sécurité)**

**Nicolas Fischbach**

Senior Manager, Network Engineering Security, COLT Telecom, Zurich

**Carrier VoIP Security**

VoIP, IMS, FMC, NGN, PacketCore, MPLS. Put those together and you are looking at the next security nightmare when it comes to Service Provider infrastructure security. Carriers are already moving away from basic data and VoIP services towards the Next Generation Network, where you have one Packet-based Core network which is going to carry "junk" Internet traffic, "secure" Multi-Protocol Label Switching VPNs, "QoS guaranteed" voice, etc. And soon, thanks to new handhelds you'll see more and more Fixed and Mobile Convergence which enables you to roam anywhere inside and outside of the enterprise and access new interactive content thanks to the IP Multimedia Subsystem.

During this talk we will present such an architecture (based on a real large scale deployment with 4 major vendors), the security and architecture challenges we ran (and still run) into, and how we mitigate the risks (denial of service, interception, web apps security, fraud, etc).

**Olivier Seznec**

Chief Technology Officer France, Cisco France, Issy-les-Moulineaux

**Network Evolution : How to cope with new applications?**

IP convergence and new communication applications, infrastructure dependencies, Cisco's vision for the future; technology for the intelligent information network.

**Fabrice Lieuvain**

Senior Security Solutions Manager, Lucent Technologies, Le Plessis-Robinson

**Securing VoIP Networks**

On assiste à un développement rapide de la convergence des réseaux voix, données et images. Ces solutions, basées sur IP, partagent un objectif commun de simplifier la

communication, d'augmenter l'efficacité et la productivité de leur utilisateurs. Cependant, les améliorations et les services nouveaux offerts ne doivent pas être synonyme de plus de risque et moins de qualité de service. Aujourd'hui pour tirer le maximum de profit de la convergence, les problématiques de sécurité, de disponibilité du réseau et de ces nouvelles applications sont trop souvent négligées. Par exemple, le déploiement d'une solution de VoIP peut mettre le système d'information et son réseau en réel danger, soit par manque de moyen ou simplement par ignorance.

*Mercredi 29 novembre 2006*

### **3. Menace (analyse de la menace VoIP –voix et données-)**

#### **Olivier Dembour, Guillaume Lehembre**

consultants sécurité, Hervé Schauer Consultants, Levallois-Perret

#### **Exemples d'intrusion sur les réseaux VoIP**

Suite aux audits effectués par HSC, Olivier Dembour et Guillaume Lehembre présentent des exemples d'attaques menées sur les réseaux voix sur IP, ainsi que les menaces existantes sur les différentes solutions "entreprise" et "opérateur".

#### **Philippe Bourcier**

consultant sécurité, CITALI, Louveciennes

#### **Olivier Geoffre**

consultant senior, directeur de projets, CITALI, Louveciennes

#### **Démonstration d'interception VoIP**

La démonstration a pour but de montrer qu'il est aujourd'hui trivial avec des outils standards du monde open-source d'intercepter les communications émises depuis un téléphone VoIP classique et de consulter ces conversations à distance depuis Internet, si l'architecture VoIP n'a pas été correctement sécurisée.

Cette démonstration utilisera une micro plate-forme Linux à faible coût fabriquée et conçue en Europe.

#### **Michel L'Hostis**

Netcentrex – Comverse, Lannion

#### **Sécurité et Voix sur IP, Synthèse conférence VoIPSA de juin 2006**

Les urgences, Firewall/SBC, l'attaque des réseaux VoIP, les interceptions légales, le SPIT, le SPIM, Skype, le chiffrement.

#### **Nicolas Bareil**

ingénieur R&D Sécurité des Systèmes d'Information, EADS – CCR, Suresnes

#### **Sécurité des systèmes VoIP: Comment les tester?**

Aujourd'hui, les entreprises se voient proposer un nombre élevé de solutions VoIP, or seules quelques unes ont subi un audit de sécurité approfondi.

Quelles sont les possibilités offertes aux entreprises ? Missionner un audit à un prestataire, faire confiance au constructeur ou auditer soit-même l'équipement ?

Cette présentation se penchera sur cette dernière option. Pas à pas, à partir d'un équipement totalement inconnu, nous essaierons de récupérer le maximum d'information sur

le système utilisé, le mécanisme de démarrage, le chargement des firmwares, les protections mises en oeuvre, ainsi que les protocoles de communication.

### **Christophe Mangin**

Mitsubishi Electric ITE-TCL Rennes

#### **Attacks against SIP servers in a telco environment: Some directions to explore**

SIP a été choisi comme protocole de signalisation pour les futurs réseaux de télécommunications (NGN). Il est la base de l'IMS (Internet Multimedia Subsystem), l'architecture de contrôle, clé de voûte des NGNs, permettant de mettre en oeuvre du concept de convergence des services. Parmi ceux-ci, la voix devrait être la première application à bénéficier de cette nouvelle architecture.

Développé dans une philosophie de souplesse et d'ouverture propre à l'IETF, SIP n'a pas été nécessairement pensé pour faire face à un environnement hostile.

Dans un premier temps, la présentation passe en revue les menaces potentielles dont peut être victime un service de voix sur IP, ainsi que les mécanismes classiquement préconisés pour la sécurisation de SIP. On s'attache ensuite à lister un ensemble de vulnérabilités inhérentes à SIP et à l'architecture IMS et à évaluer les moyens à mettre en oeuvre pour les exploiter. Enfin, les résultats d'une étude d'un type particulier de vulnérabilités sont présentés : les vulnérabilités d'implémentation. Celles-ci ont été recherchées, via une revue des codes sources de différentes implémentations publiques de parser et de proxy SIP. Un exemple d'attaque par épuisement des ressources de calcul d'un proxy vient finalement illustrer ces résultats.

### **Franck Veysset**

expert sécurité internet/intranet, France Telecom R&D, MAPS/NSS, Issy-les-Moulineaux

#### **UMA, WiFi SIP, and FMC (Fixed Mobile Convergence) What about security?**

Depuis quelques mois, de nombreuses offres dans le domaine de la convergence téléphonique (FMC : Fixed Mobile Convergence) ont fait leurs apparitions. Deux grandes technologies semblent dominer le marché, le "WiFi SIP" et les solutions UMA (Unlicensed Mobile Access). Après avoir présenté le principe de ces solutions, nous détaillerons leurs éléments sécurité propres.

### **Radu State**

Madynes group, LORIA INRIA Lorraine, Nancy

#### **VoIP Security assessment and intrusion detection**

The objective of this presentation is to show the conceptual approach and the implementation of a VoIP assessment tool. The security assessment of a VoIP infrastructure allows to identify potential vulnerabilities and to validate their exploitation by an automatic penetration test. Vulnerabilities can range from miss-configured devices, protocol and deployment detour and up to software level vulnerabilities. We will present a methodology based on automatic attack tree construction adapted to the VoIP signalling and transport plane. We will show how attacks done both at a signalling plane (SIP) and IP layer 2 can lead to the compromise of a VoIP network. The described work will be illustrated with examples of a prototyped tool that is under development in the Madynes group.

## **4. Déploiement (problèmes pratiques et techniques du déploiement des réseaux VoIP)**

**Luc Delpha, Gabriel Caudrelier**

Cyber-Networks, Paris

**Convergence voix-données, conséquences pour l'entreprise, son organisation et la sécurité, retours d'expériences**

Périmètre, convergence, caractéristiques et besoins de la voix et des données, comparaison, conséquences financières, organisationnelles, fonctionnelles et techniques pour l'entreprise, exemples, conclusions.

**Jean Davodeau**

Cisco France, Issy-les-Moulineaux

**Déploiement téléphonie sur IP**

Déploiement d'un réseau de téléphonie sur IP chez Renault: contexte, besoin, architecture, sécurité.

**Bernard Minier**

DGA / Centre d'électronique de l'Armement, Bruz

**Démarche pour l'implémentation de la voix sur IP au sein des réseaux du Ministère de la Défense**

Le développement de la Voix sur IP dans les réseaux de la Défense présente l'intérêt majeur d'envisager une convergence voix et données permettant d'une part une économie d'échelle au niveau des réseaux, et d'autre part l'introduction de nouveaux services aux utilisateurs. Elle permet la convergence et l'interaction des services (voix, messagerie, chat, travail « collaboratif », gestion de présence ...) sur une même infrastructure, voire sur des postes communs.

Cependant, ce développement de la Voix sur IP présente deux risques majeurs :

L'introduction de vulnérabilités supplémentaires sur la sécurité des réseaux .

La limitation de l'interopérabilité des solutions.

Un déploiement non coordonné de solutions VoIP au sein du Ministère de la Défense ferait peser un risque fort sur la capacité d'interconnexion des réseaux utilisant la technologie de Voix sur IP et sur une offre de service sécurisée aux utilisateurs.

Afin de permettre un développement de la Voix sur IP évitant ces deux écueils, cet exposé a pour but de présenter les premières réflexions sur l'implémentation d'une solution VoIP au sein des réseaux du Ministère de la Défense.

*Jeudi 30 novembre 2006*

## **5. Technologies (sécurité VoIP: points techniques)**

**Philippe Rondel**

Check Point Software,

**Problèmes posés par l'intégration de la sécurité VoIP**

Complexité de la VoIP (protocoles, besoins, architectures); ses trois aspects: Sécurité, Connectivité, Qualité de Service.

## **Vincent Cottignies**

Head of the Communication System Architecture Department, within the Battlespace Transformation Centre of THALES, Colombes

## **Sandrine Masson**

Network System Engineer, Responsible for the ETNA Eurofinder Project, THALES Colombes

### **Military Security & QoS: Secure QoS Signalling Gateway**

The presentation deals with Military QoS and associated Security issues.

In the first part, the requirements and issues regarding military QoS are compared to civilian systems. The analysis concludes that for mobile tactical systems, with scarce resources and little number of users, the simple DiffServ model is not sufficient to provide the requested "Guaranteed QoS".

Indeed, additional IntServ mechanisms are required, with extensions to handle the Military Operational Importance to be taken into account for the delivery of competing services.

However, there is then a security issue because of the Security Architecture of Military Systems based on IPSec VPN with strict separation between Red & Black sides of the IPSec Cryptos.

The second part of the presentation introduces the work achieved by the ETNA Eurofinder program from 09/2004 to 09/2006 to tackle this issue of Military QoS & Security.

It consists in an architecture, a technical solution and a prototype for demonstration including:

- An RSVP Signalling and Call Admission Control to reserve resources for RT flows

- A preemption capability based on MLPP (Multi-Level Priority & Preemption)

- A QoS Routing & Route Pinning capability able to ensure a stable guaranteed QoS for whole duration of a session through a routed IP network

- A QoS Security Gateway function able to control the regeneration of controlled RSVP messages across the Red & Black sides of an IPSec Crypto.

As a conclusion, we note that similar approaches are under study in the US (HAIPIS) and that NATO is also interested. Nevertheless, we also recognize that, even if the demonstration proved that it is technically feasible to provide "Guaranteed QoS", it still requires a deeper analysis with military security authorities (FR, NATO, EU), in order to assess whether such QoS Security Gateway functions can be acceptable for operational systems on the field.

## **Philippe Leroy, Reine Essobmadje**

CheckPhone, Suresnes

### **Filtrage et contrôle des protocoles voix**

Les fraudes et détournements d'usage de la téléphonie ne cessent de croître et aucune stratégie réellement efficace, telles que celles développées pour assurer la maîtrise des flux de données n'avait à ce jour encore été proposée.

La société CHK a développé des solutions dont l'efficacité technologique et l'intérêt stratégique répondent sans conteste au besoin croissant du marché de la sécurisation de la voix, quel qu'en soit le support.

ETSS® (Expert Telecom Security System) Manager fournit aux entreprises et aux administrations une protection en temps réel de leur réseau voix. Grâce à son interface graphique, ETSS® permet à l'administrateur de superviser et de sécuriser les flux voix, tant en environnement hybride (TDM, ToIP, VoIP) qu'en environnement hétérogène multi constructeurs. ETSS® surveille les activités, automatise la mesure des risques et des vulnérabilités et produit des rapports permettant d'adapter les choix fonctionnels à cette mesure. L'intégration de la solution ETSS® est la solution idéale pour accompagner, de manière sécurisée, les projets de convergence voix vers IP. Son positionnement périmétrique rend ETSS® indépendant mais compatible à la grande majorité des solutions PABx/IPBx et autorise une surveillance permanente des réseaux voix.

## **6. Tendances (orientations technologiques, problèmes légaux)**

### **Eric Barault**

Network & Security Architect, France Telecom Research & Development, Lannion

### **Armand Vandebussche**

France Telecom Research & Development, Lannion

#### **Introduction à la sécurité pour l'IMS**

L'évolution de l'environnement des services conversationnels; la cible théorique pour une architecture de sécurité de bout en bout (principes, points clés, services IMS, intégration sécurisée); l'application théorique de cette cible à l'architecture IMS TISPAN; conclusion: nécessité d'une approche de bout en bout de la sécurité.

**Nabil Ajam**, Doctorant, **Yehia El Rakaiby**, Doctorant

**Ahmed Bouabdallah**, Maître de Conférences

GET / ENST Bretagne, Département Réseaux, Sécurité, Multimédia, Cesson-Sévigné

#### **Sécurité dans les réseaux d'opérateurs**

Nous présentons dans un premier temps les réseaux d'opérateurs dans une double perspective historique et technique. Nous introduisons dans une seconde partie la méthode d'analyse utilisée qui s'inspire principalement de la recommandation ITU-T X.805. La dernière partie présente une synthèse de notre analyse.

### **David Bénichou**

Magistrat chargé de mission du secrétaire général, Ministère de la Justice, Paris

#### **Le régime légal des interceptions**

Nous présenterons ici les grands principes et textes qui encadrent l'interception des communications électroniques, tant administratives que judiciaires, pour les resituer dans leur contexte juridique et pratique, et les mettre en perspective au regard des évolutions actuelles.

### **Carlos Aguilar Melchor**

ATER, XLIM, Université de Limoges

### **Yves Deswarte**

Directeur de Recherche CNRS, LAAS-CNRS, Toulouse

#### **Protection contre l'analyse du trafic dans la Voix sur IP**

Dans beaucoup de situations, les informations relatives à l'existence d'une communication sont des données sensibles. Pour un utilisateur donné, le fait qu'il soit en train de communiquer peut par exemple dévoiler sa localisation. Le fait de savoir qui communique avec qui, peut divulguer des relations entre les utilisateurs. Aussi, est-il souvent souhaitable que de telles informations ne puissent pas être obtenues par d'éventuels attaquants.

On dit d'un service protégeant ces informations qu'il fournit la possibilité de réaliser des communications anonymes. Les contraintes en latence qu'impose la voix sur IP ne permettent pas d'utiliser l'approche classique (l'utilisation successive de plusieurs relais) pour implémenter de tels services. Nous présenterons dans cet exposé différentes techniques classiques qui peuvent être utilisés dans le cadre de la voix sur IP pour obtenir un service permettant de réaliser des communications anonymes. Nous proposerons une nouvelle technique permettant de réduire fortement les coûts en communication, et étudierons de façon comparative les différentes approches pour implémenter un tel service.

**François Lesueur**

PhD student, Supélec Network and Information System Security Group, Rennes

**Ludovic Mé**

Professor, Head of the "Network and Information System Security" group, Supélec, Rennes

**Hervé Debar**

Senior Researcher, France Telecom Research & Development, Caen

**Annuaire distribué sécurisé pour réseau VoIP pair-à-pair**

Les systèmes de VoIP actuels, s'ils présentent un intérêt économique indéniable, demandent encore un investissement matériel et humain non négligeable. Par contraste, les environnements P2P nous paraissent particulièrement intéressants pour la VoIP en raison de leur déploiement simple et peu onéreux, ainsi que pour leur forte disponibilité. P2PSIP est pour nous un exemple intéressant de VoIP P2P. Malheureusement, P2PSIP ne propose aucun mécanisme de sécurité. En particulier, rien ne permet l'identification unique et distribuée des utilisateurs. Aussi, dans cette présentation, nous proposons un mécanisme d'annuaire distribué sécurisé pour P2PSIP. Cet annuaire offre un lien, certifié par coopération entre  $k\%$  des noeuds du réseau (mécanisme de chiffrement à seuil), entre l'identifiant SIP et l'adresse IP de l'utilisateur correspondant. En outre, nous assurons qu'aucun groupe de quelques noeuds n'est en mesure de certifier à lui seul un tel lien.

**Patrick Pailloux**

SGDN/ Directeur Central de la Sécurité des Systèmes d'Information, Paris

**Clôture des Journées SSI**