

Sécurité de la VoIP



Ludovic LECLERC
Architecte Solution

Alain YVON
Architecte PQA

Avril 2014

Agenda

1. Introduction
2. Historique: des PABX traditionnels à la communication unifiée
3. Analyse de Risque de la VoIP
4. Stratégie de Défense pour la VoIP
5. Réglementations et Certifications
6. Conclusion
7. Démo
8. Test QCM

1

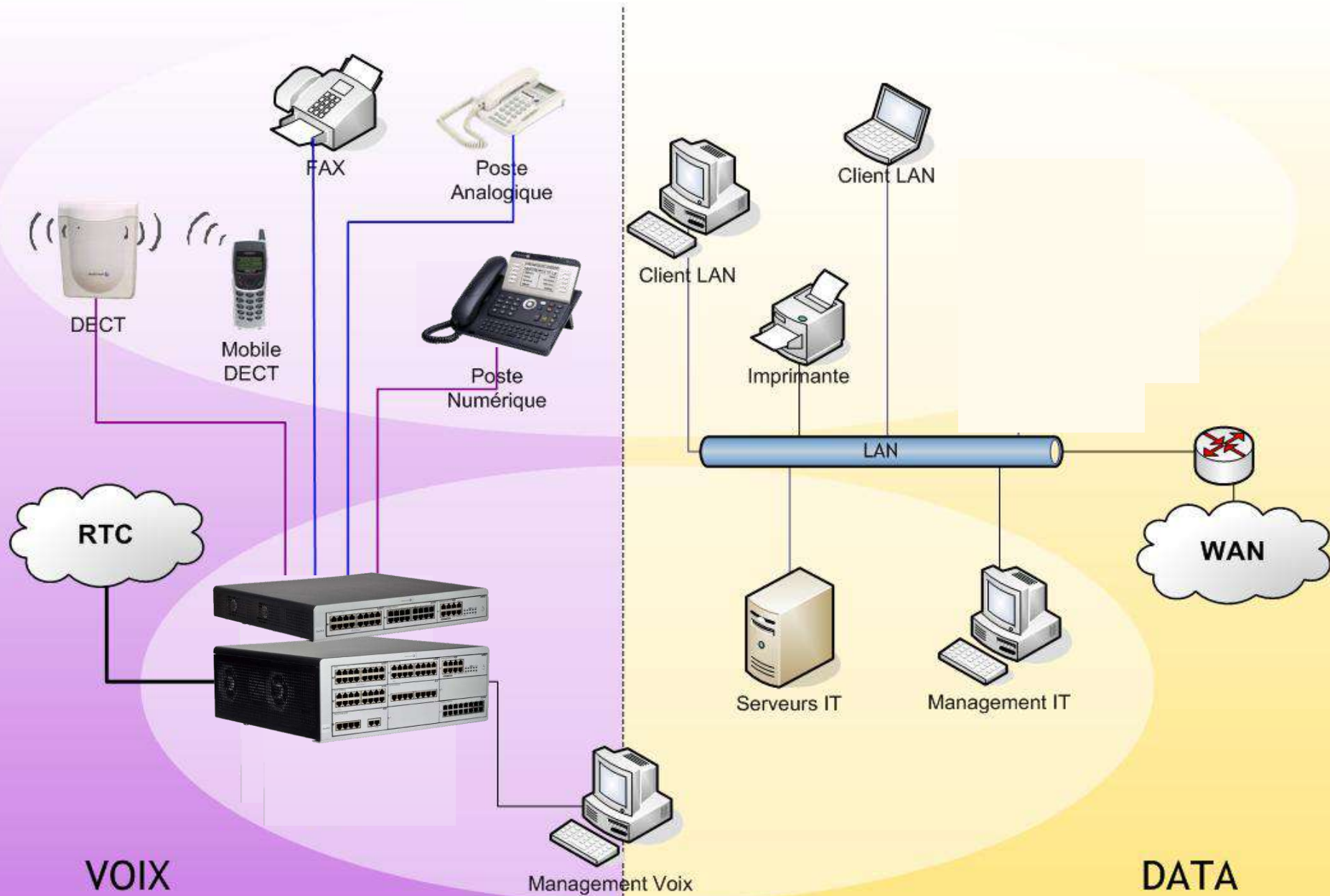
Introduction

Objectifs de cette présentation

- Comprendre les fondamentaux de la sécurité dans un environnement IT en réseau
- Comprendre les spécificités de la sécurité de la VoIP
- Avoir une vision de l'état de l'art en matière de sécurité de la VoIP

2

Historique: des PABX traditionnels à la communication unifiée



Le monde “protégé” des PABX

- Hardware propriétaire
- Etanchéité entre le réseau de données “voix” et le réseau de données “data”
- La bande passante est fixe donc la qualité de voix assurée
- Protocoles de communication en réseau standardisés et réglementation stricte
- Assurance de haute disponibilité

Le monde “protégé” des PABX

Menaces traditionnelles contre la téléphonie:

- 1) Ecoutes discrètes
- 2) Usurpation d'identité
- 3) Fraude à la taxation

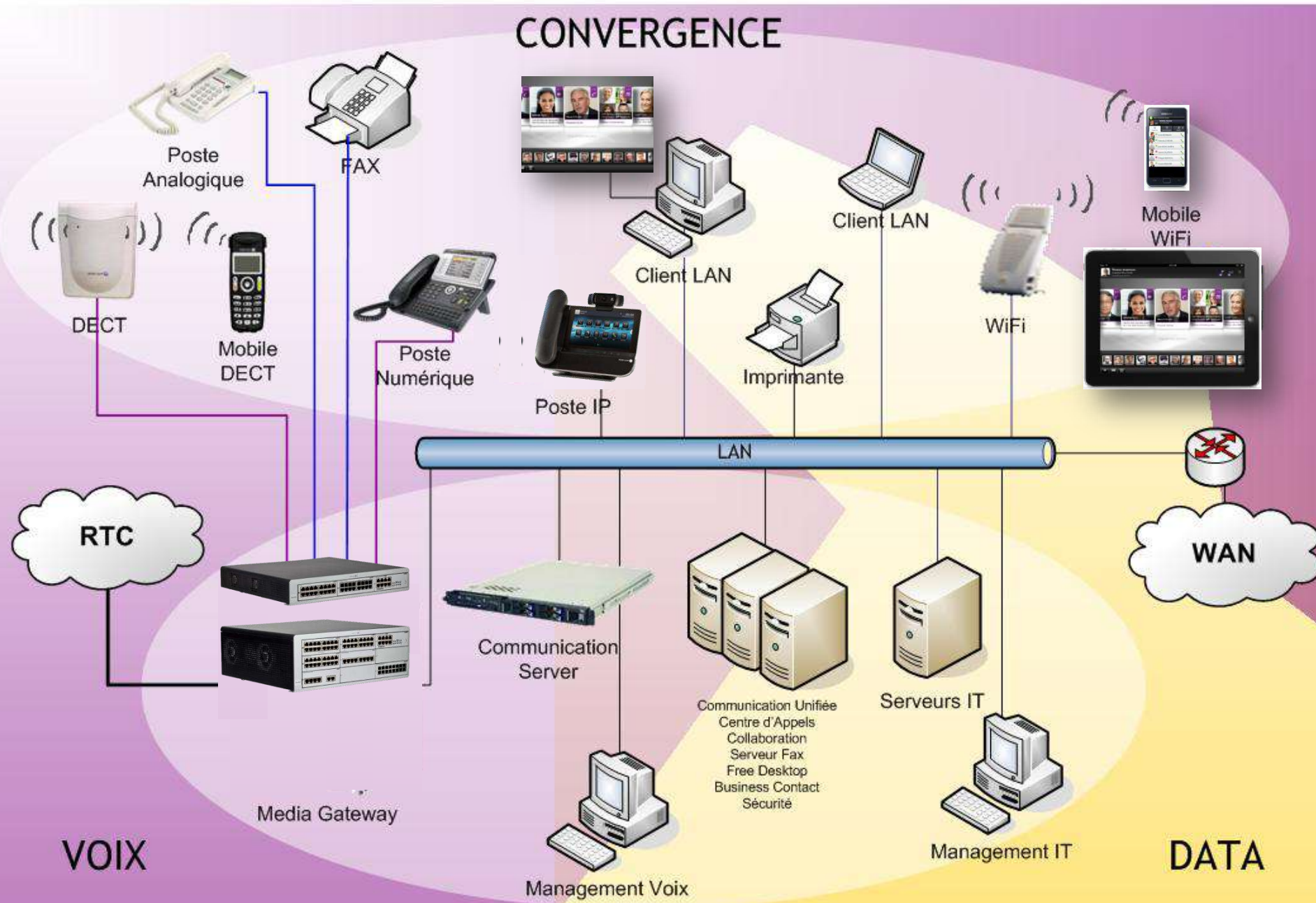
Mais...

- 1) Difficile à mettre en oeuvre (équipement, connaissances techniques)
- 2) Tracabilité aisée (intrusion physique)
- 3) Impact restreint à la fonction de téléphonie

Les systèmes de communication unifiée

- Fin des années 90: explosion d'internet, demande forte de système "IP ready"
- Evolution vers du hardware standard pour les serveurs de communication
- Postes IP avec des fonctionnalités avancées (web services)
- Services IP avancés (DHCP, LDAP, NTP...)
- Ouverture vers le monde applicatif (messagerie unifiée, softphone)





3

Analyse de Risque de la VoIP

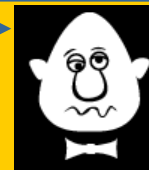
Les fondamentaux de la sécurité IT

Déni de Service (DoS)



Impact sur la Disponibilité

Ecoute Illicite



Impact sur la Confidentialité

“Man-in-the Middle”



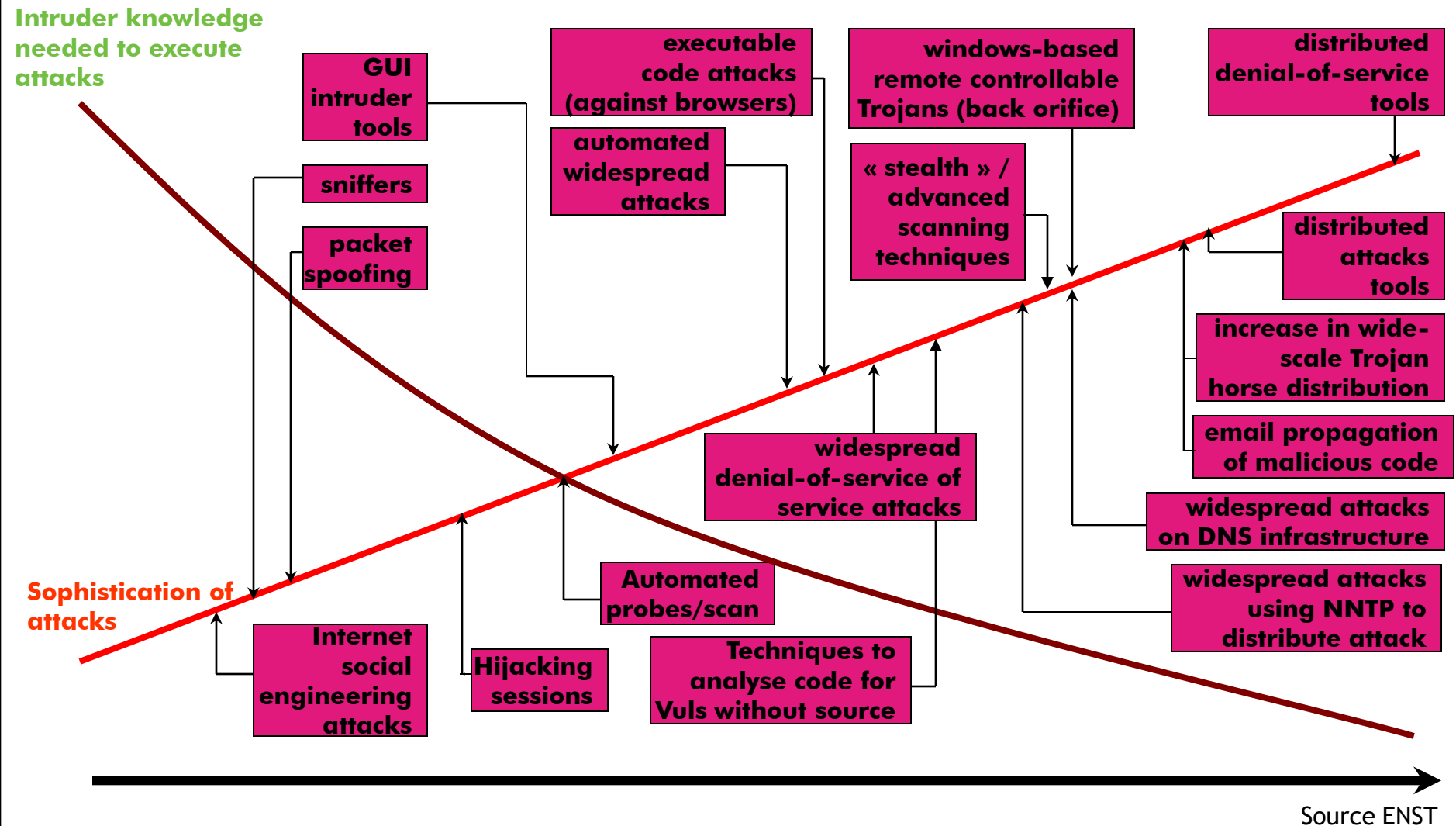
Impact sur l'Intégrité

“Spoofing”



Impact sur l'Authentification

Attaques contre les équipements IP

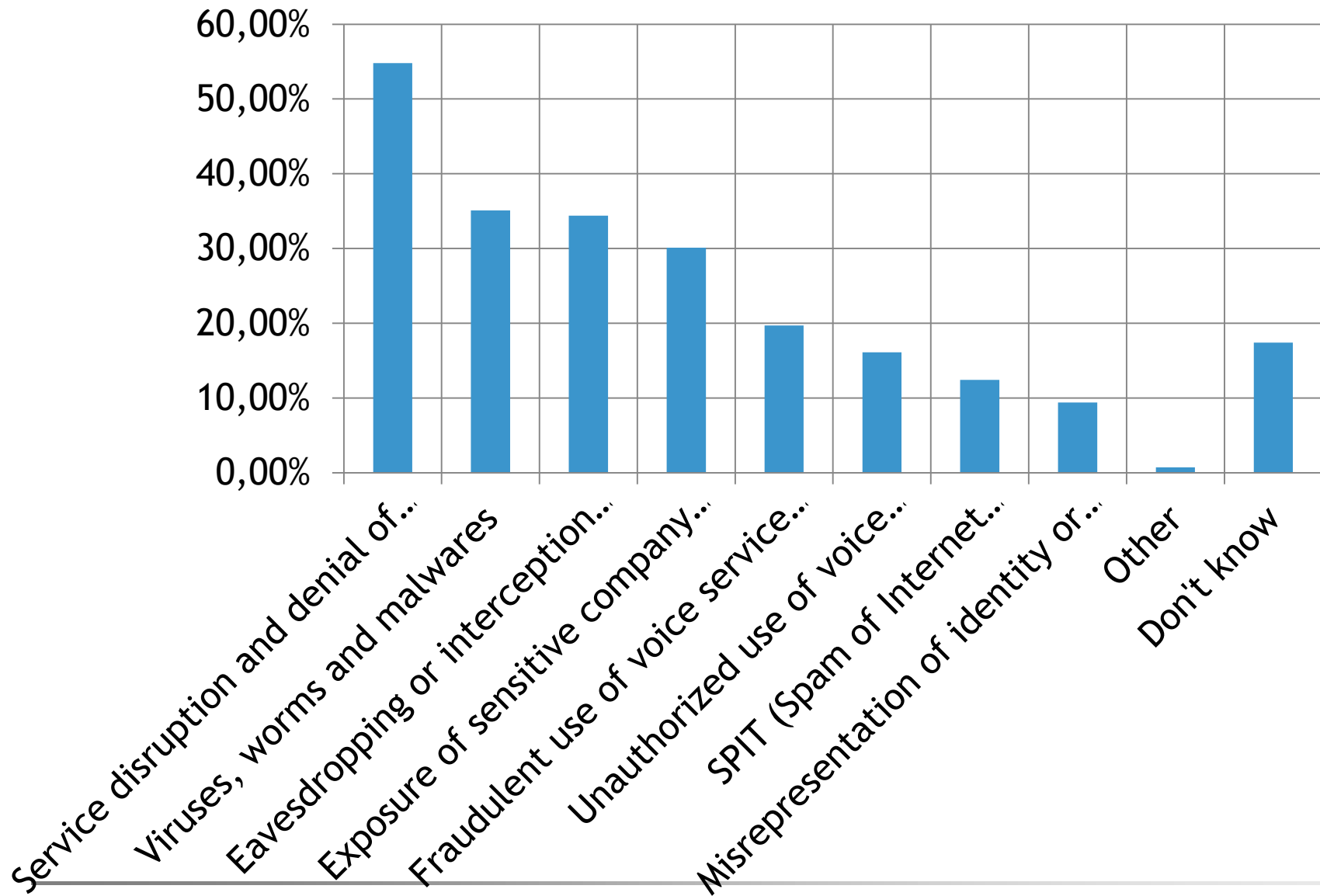


Téléphonie traditionnelle VS Téléphonie sur IP

La menace contre la VoIP est plus importante pour plusieurs raisons:

- Il suffit d'un **PC connecté au réseau IP** pour lancer des attaques
- L'utilisation de **protocoles standardisés** et utilisés dans le contexte plus général des réseaux diminue le côté « sécurité par obscurantisme »
- Les serveurs de communication vont subir les mêmes attaques que les autres **serveurs applicatifs**, de façon ciblé ou aveugle
- Intérêt des **hackers** en tant que nouvel « espace de jeu » (le besoin de haute disponibilité du service de téléphonie en fait une cible de choix pour les **attaques de déni de service**)
- De façon général, le service de téléphonie est assujetti à la **disponibilité du réseau IP** et à sa sécurisation intrinsèque

Menaces contre la VoIP vue par l'analyste In-Stat 2/08



4

Stratégie de Défense pour la VoIP

Remarques générales

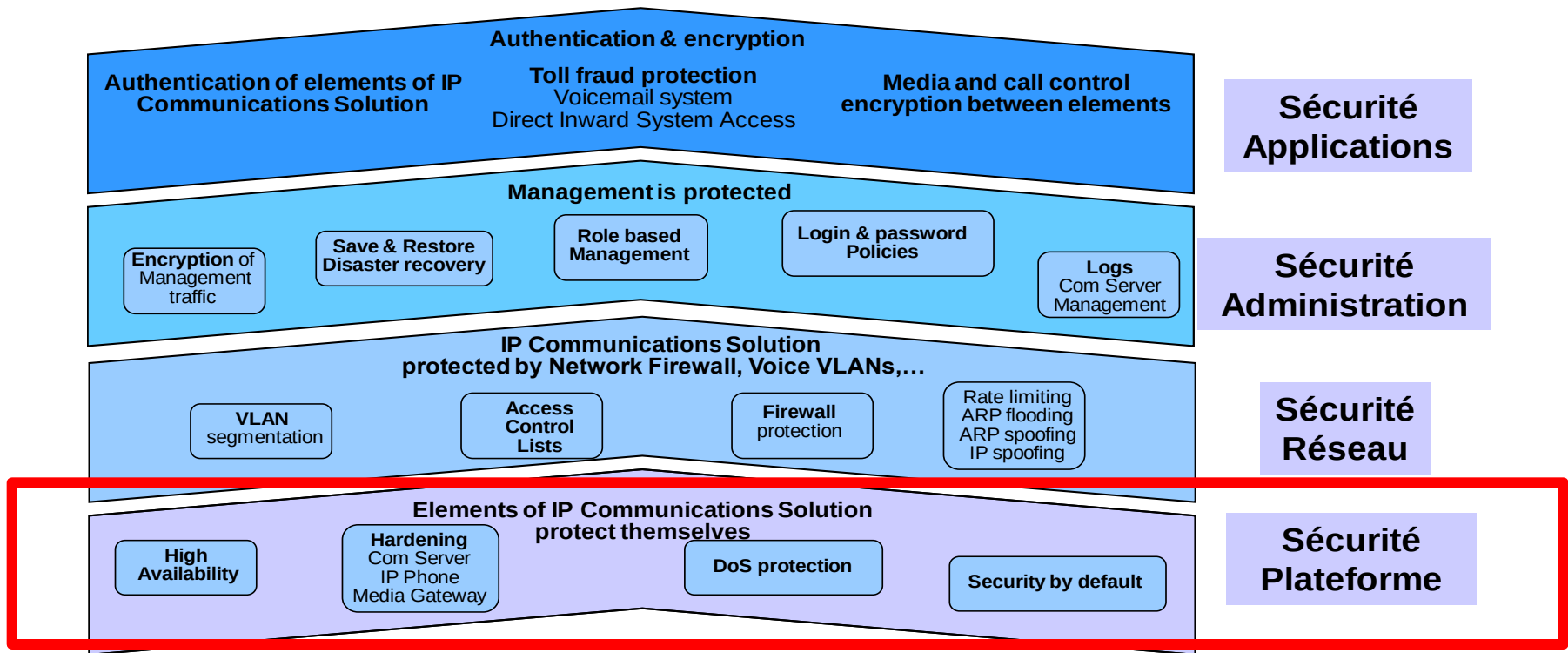
La sécurité globale du système d'information est basée sur:

- Le **durcissement individuel** de chacun des éléments de l'infrastructure (routeurs, firewall, serveurs réseau, passerelles, serveurs applicatifs, postes client).
- La sécurisation de l'**accès au réseau** et ensuite de l'accès aux différentes ressources sur ce réseau.
- La protection des plateformes de **management et de configuration** de ces équipements.
- La protection de l'**application de téléphonie** elle-même (la partie établissement d'appel et la partie média voix).

L'approche par couche permet de renforcer la sécurité globale et si un élément est corrompu il ne doit pas compromettre l'ensemble du dispositif.

Une approche de la sécurité par couche

Il est essentielle d'adresser l'ensemble des couches !



Serveur de communication

1) OS (système d'exploitation) optimisé et durci

- LINUX Kernel customisé pour les contraintes temps réel
 - Aspect QOS
 - Optimisation/disponibilité
- Empreinte réseau réduite
 - Limitation du nombre de services installés/exécutés
- **Résistance aux attaques DOS (dénî de service)**
 - **Configuration spécifique de la pile IP**



Une attaque de Dénier de Service (Denial of Service) peut être lancée contre n'importe quel équipement connecté sur un réseau à partir du moment où il offre des services réseaux

=> SERVICE = PORT (TCP ou UDP)

Service	Port
ftp	21/TCP
telnet	23/TCP
dns	53/TCP
http	80/TCP

Il existe plusieurs méthodes pour parvenir au déni de service:

- 1) consommation de bande passante (attaques type “packet storm”)
- 2) consommation de ressource (on vise un service réseau spécifique et sa saturation)
- 3) exploitation d'une **vulnérabilité** connue sur un service réseau

Il existe plusieurs modes opératoires pour exploiter une vulnérabilité:

- 1) Attaques “one shoot” (un seul paquet suffit...)
- 2) Attaques par flooding (objectif: surcharger la cible de requêtes !)

Sécurité des Plateformes

Résistance aux attaques DoS

Protocol	Denial of Service	Category	Descr.
ARP	ARP flood	flood	Net exhaust
ICMP	Ping of Death Ping flood Echo reply flood	Bug Flood Flood	>64KB echo Net exhaust Net exhaust
UDP	Teardrop attack Teardrop Timeout (opentear attack) Bad TTL flood	Bug ½ flood flood	IP fragments Mem exhaust Net exhaust
TCP	TCP flood:SYN, ACK (stream attack), FIN, URG, RST, PSH Teardrop Timeout Land attack Naphta attack	Flood ½ flood bug ½ flood	Exhaust Mem exhaust src=dest exhaust cnxQ exhaust

Ressources:

PacketStorm <http://www.packetstormsecurity.com>
Infos, scripts et programmes de test

Nessus <http://www.tenable.com/products/nessus>
Outil de test de vulnérabilité (scanner de vulnérabilité)

Serveur de communication

1) AOS (système d'exploitation) optimisé et durci

- LINUX Kernel customisé pour les contraintes temps réel
 - Aspect QOS
 - Optimisation/disponibilité
- Empreinte réseau réduite
 - Limitation du nombre de services installés/exécutés
- Résistance aux attaques DOS (dénî de service)
 - Configuration spécifique de la pile IP
- **Traitement des alertes de vulnérabilité**
 - **Suivi au quotidien et apport de correctifs**



Gestion et suivi des alertes de vulnérabilités



■ Missions du CERT-IST

(Computer Emergency Response Team-Industry, Services and Tertiary)

- Centralisation et gestion de la base des alertes de vulnérabilités sur l'ensemble des produits du monde IT
- Mutualiser les ressources et les connaissances
- Faciliter la diffusion de l'information concernant des alertes

Ressources:

CERT-IST <http://www.cert-ist.com/>

Référence officielle pour la centralisation des alertes de vulnérabilité

SecurityFocus <http://www.securityfocus.com/vulnerabilities>

Portail de suivi au jour le jour des nouvelles vulnérabilité

BugTraq <http://www.securityfocus.com/archive/1>

Mailing list traitant des dernières vulnérabilités découvertes

Sécurité des Plateformes

Traitement des alertes de vulnérabilité

- **Password par défaut** sur les comptes système

[CVE-2002-1691]

- **Compte système "Halt"** utilisable pour **arrêter le système sans posséder le niveau d'autorisation requis**

[CVE-2002-0293]

- **Problème sur les droits d'accès de certains fichiers système**

[CVE-2002-0295]

CVE-ID	
CVE-2002-1691	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
(under review)	
Description	
Alcatel OmniPCX 4400 installs known user accounts and passwords in the /etc/passwd file by default, which allows remote attackers to gain unauthorized access.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	

CVE-ID	
CVE-2002-0293	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
(under review)	
Description	
FTP service in Alcatel OmniPCX 4400 allows the 'halt' user to gain root privileges by modifying root's .profile file.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	

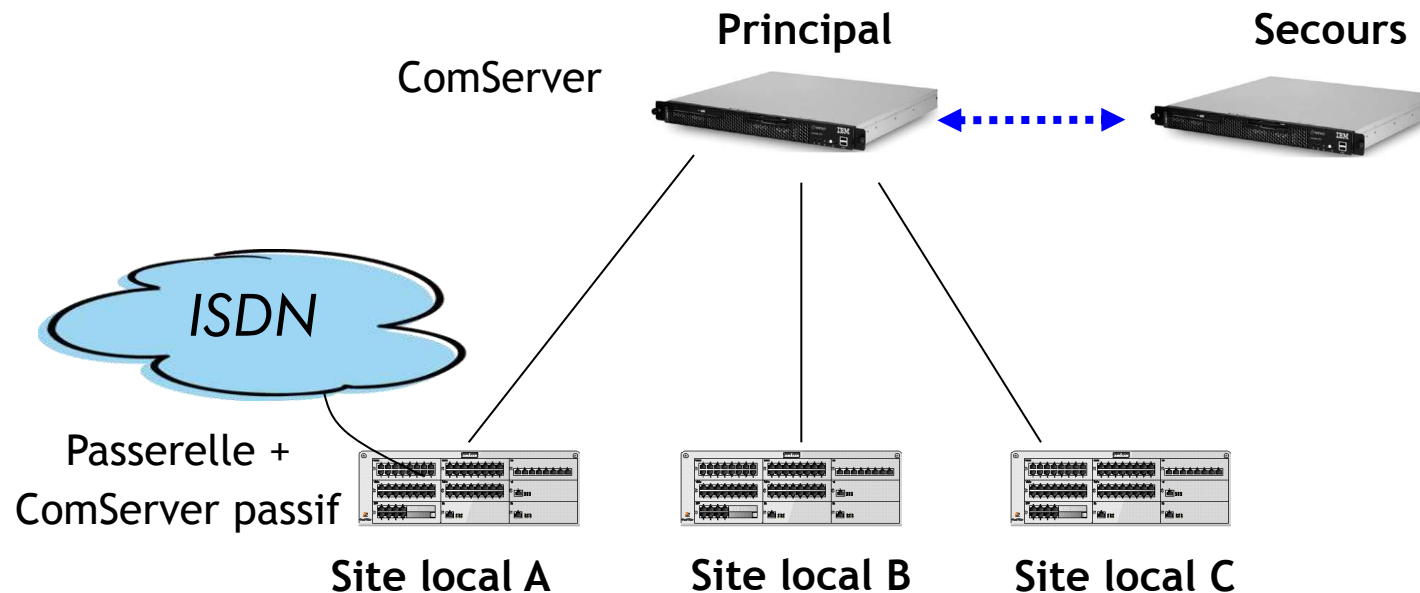
CVE-ID	
CVE-2002-0295	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
(under review)	
Description	
Alcatel OmniPCX 4400 installs files with world-writable permissions, which allows local users to reconfigure the system and possibly gain privileges.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	

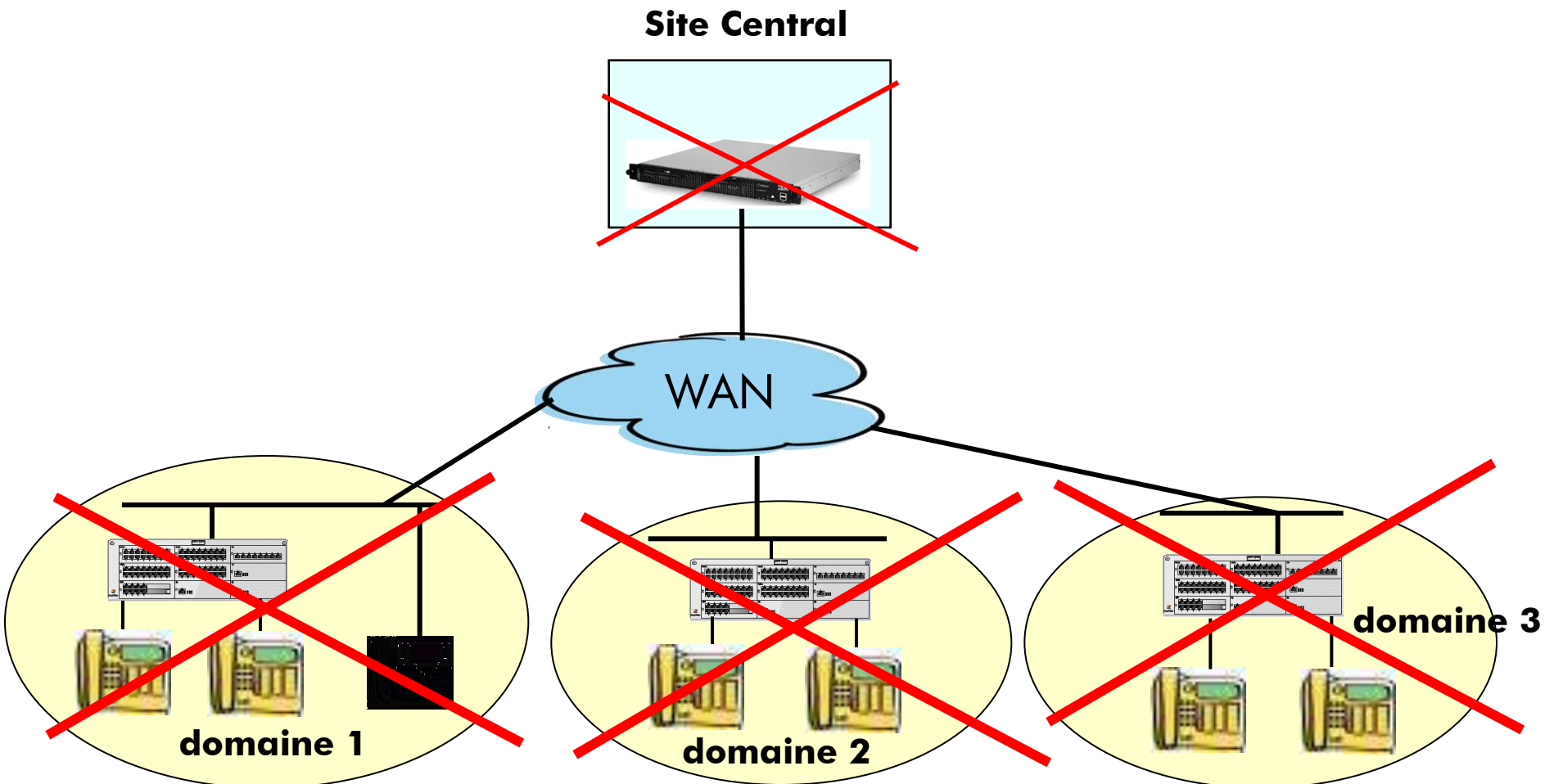
Candidate	
Phase	Proposed (20020502)
Votes	MODIFY(1) Frech NOOP(5) Christey, Cole, Cox, Foat, Wall
Comments	
Frech> XF: omnicpx-insecure-groups (8227) REASON: LIRRLY Christey> Acknowledged by Alcatel via email October 4, 2002	
Candidate assigned on 20020501 and proposed on 20020502	
SEARCH CVE USING KEYWORDS: Submit	
You can also search by reference using the CVE Reference Maps .	
FOR MORE INFORMATION: cve@mitre.org	

Serveur de Communication

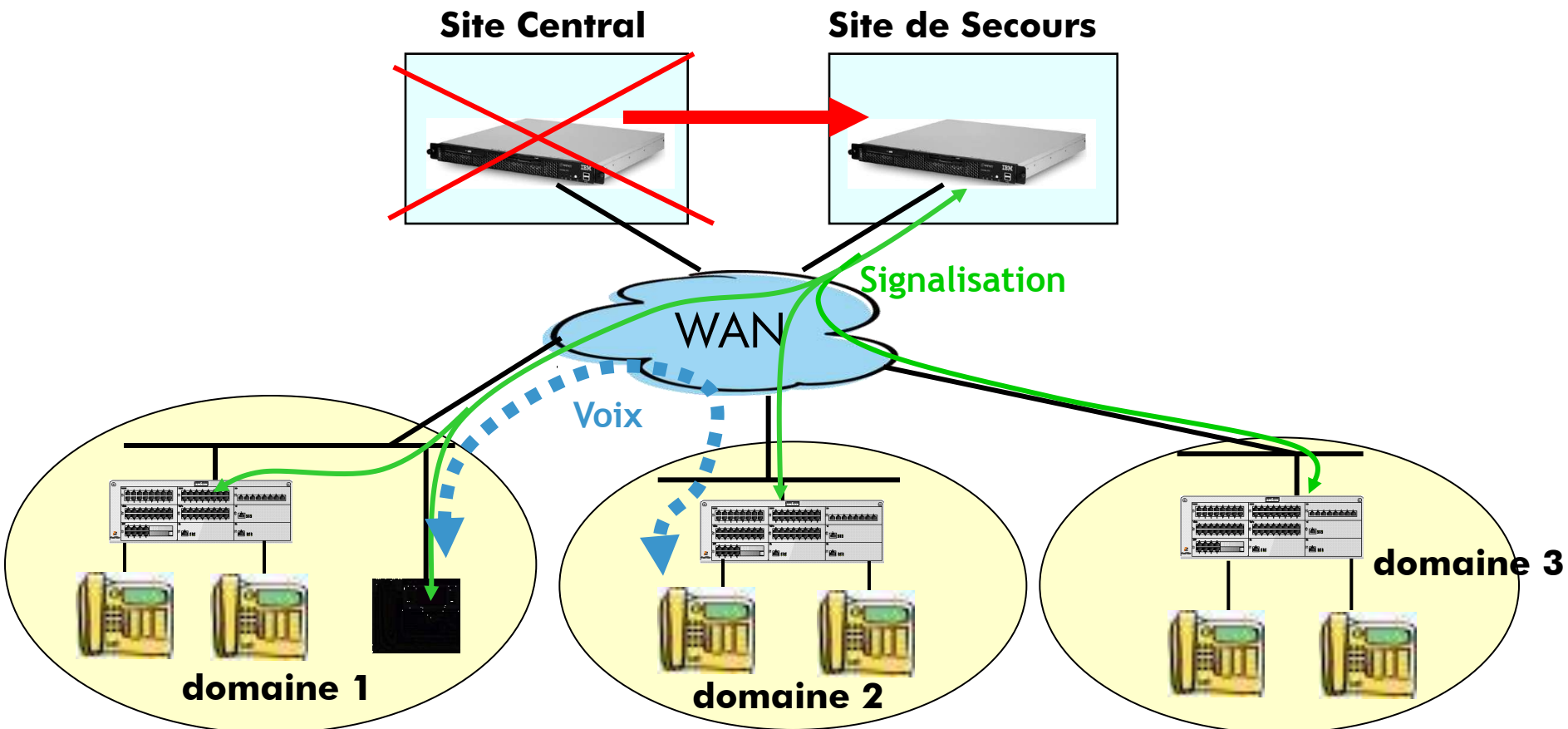
2) Mécanismes de Haute Disponibilité

- Redondance en mode Principal-Secours
- Survivabilité en local pour les sites distants via une passerelle “intelligente”

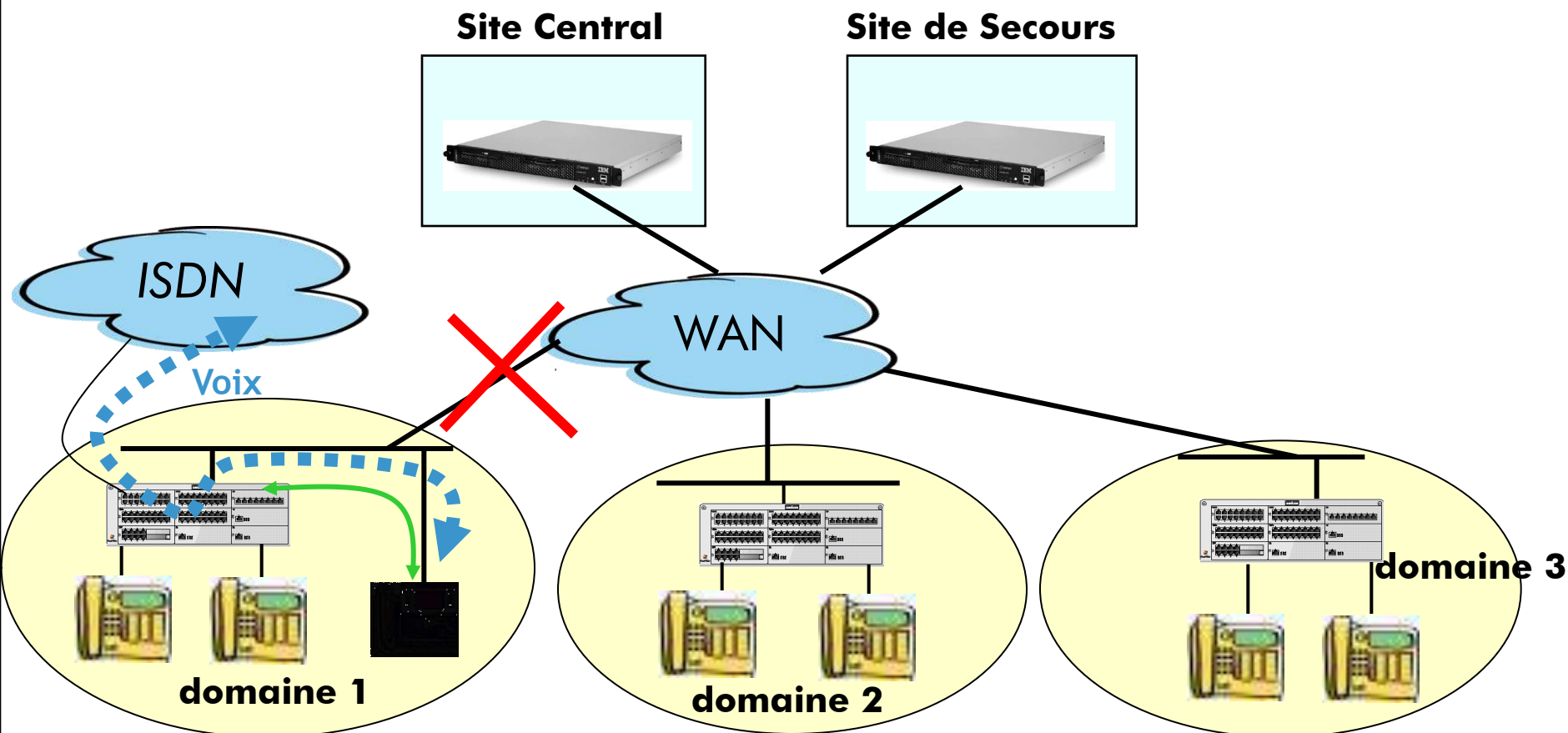




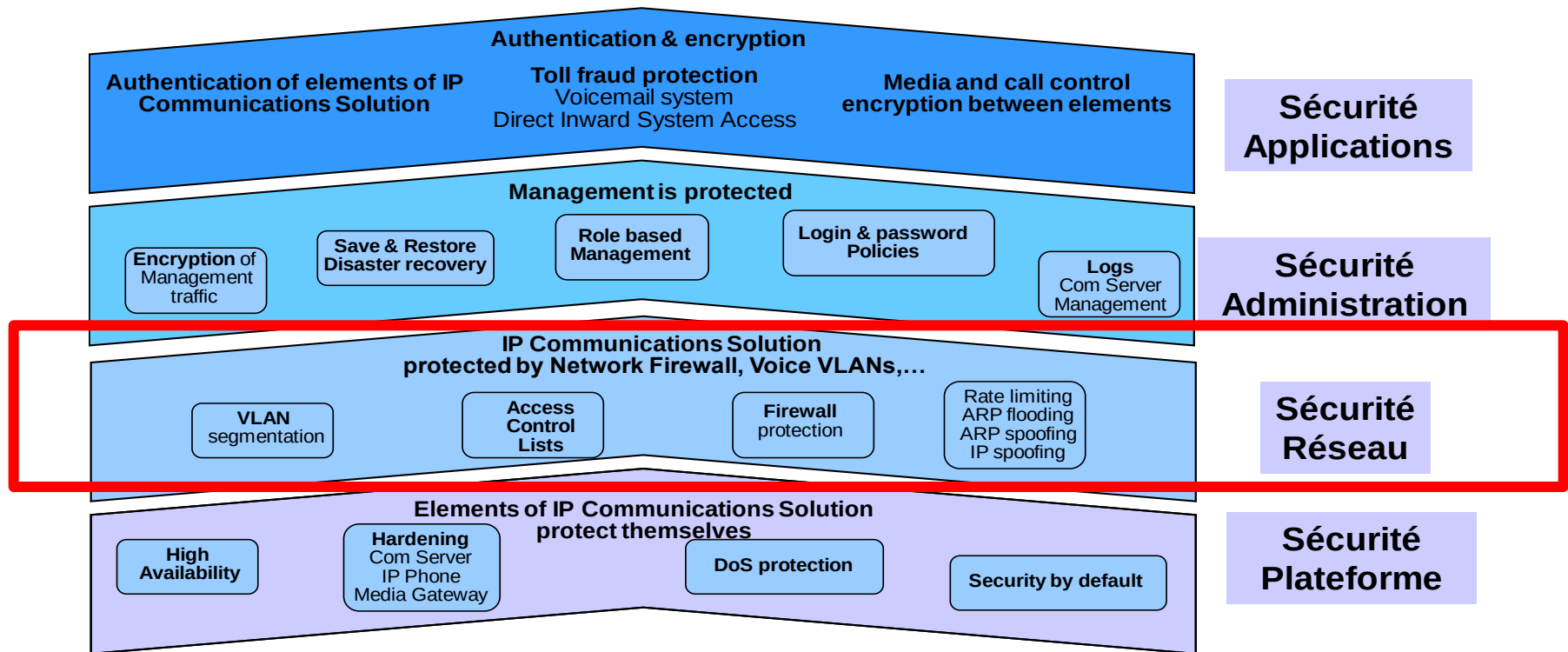
- Redondance dite spatiale (domaines IP différents)
- Pas de perte des communication en cours



- En cas de perte du lien WAN sur un site distant, la passerelle fait office de serveur de communication de secours pour la survivabilité en local.



Une approche de la sécurité par couche



Points clés de la sécurité de la couche Réseau:

- ✓ Sécuriser la configuration des switch/routeurs
 - Désactiver les ports ethernet non utilisés
 - Isoler logique avant authentification
- ✓ Authentification au niveau des équipements IP
- ✓ Penser à la ségrégation d'adressage IP
- ✓ Analyse et filtrage de la VoIP

Sécurité de la couche Réseau

Standard d'authentification 802.1X

Sécurité Application

Sécurité Administration

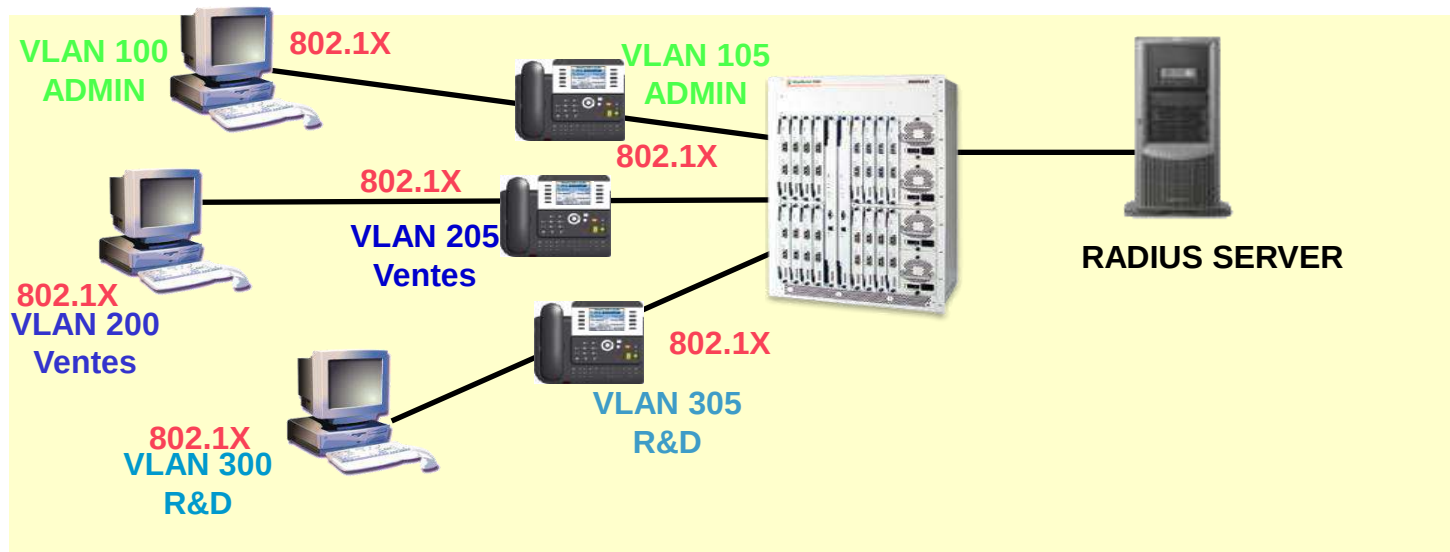
Sécurité Réseau

Sécurité Plateforme

✓ Authentification au niveau des équipements IP

Utilisation du mécanisme d'authentification 802.1X

- Standard IEEE pour les équipements du réseau
- Différentes méthodes d'authentification MD5 (Message Digest 5) et TLS (Transport Layer Security)
- Support du 802.1X multi-session: les PC derrière les postes IP seront placés dans un Vlan Data dédié



Sécurité de la couche Réseau

Standard d'authentification 802.1X

Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

IP Phone



Switch



ComServer



RADIUS server



- 1 By default, switch ports are closed to all but EAPOL traffic
- 2 IP Phone sends EAP-TLS credentials (X509 digital certificate)
- 3 Ethernet switch forwards encrypted EAP credentials to RADIUS Server for verification
- 4 RADIUS Server responds with approve or deny message
- 5 If authentication is successful, the Ethernet switch can open the blocked port
- 6 IP Touch can now perform DHCP/TFTP initializations and register with PCX
- ? User authentication via PIN code can be performed (optional)

Sécurité de la couche Réseau

Ségrégation d'adressage IP

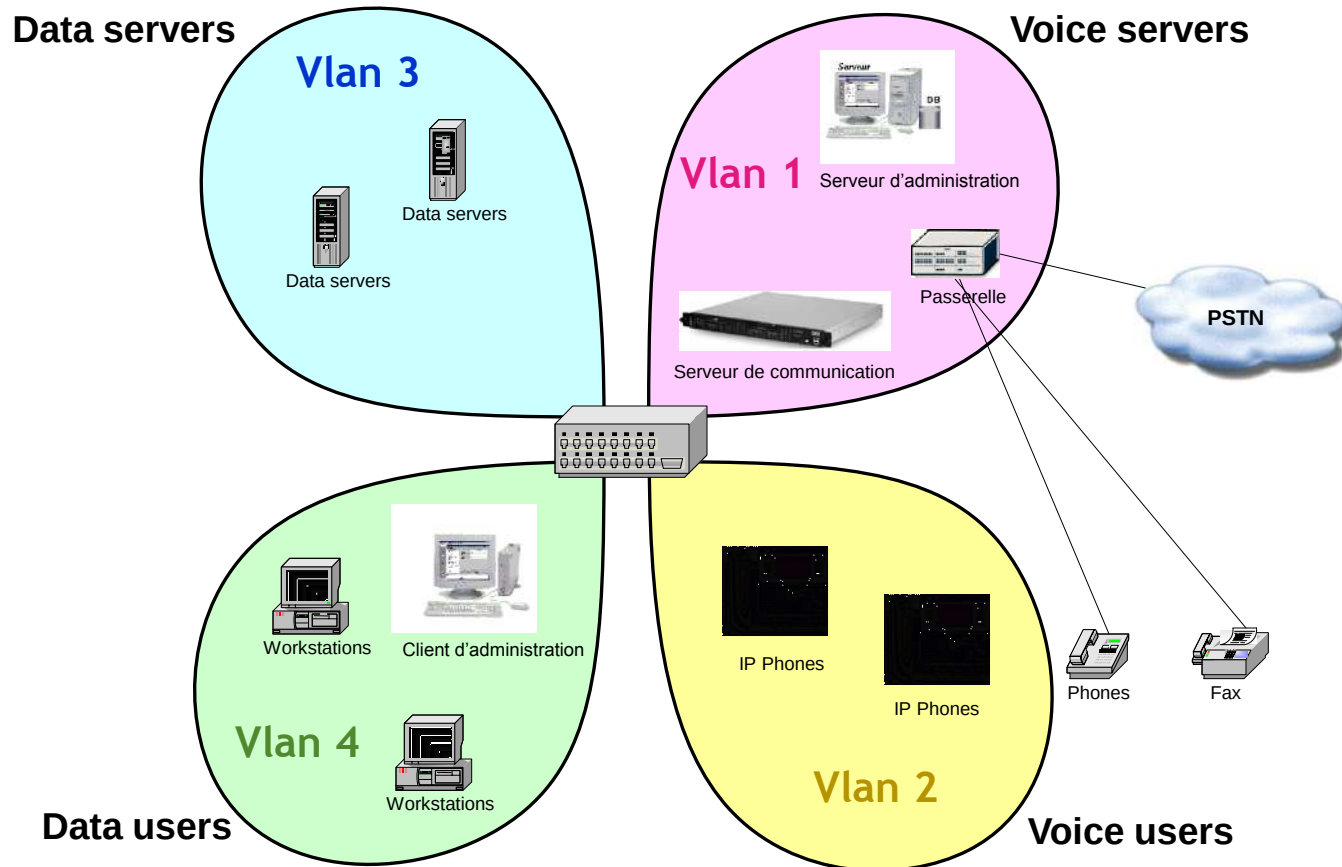
Sécurité Application

Sécurité Administration

Sécurité Réseau

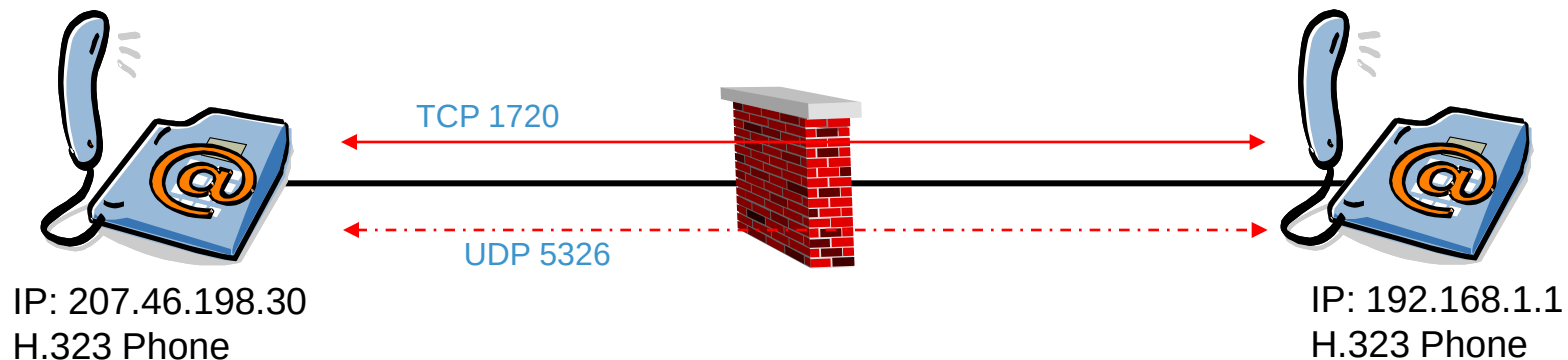
Sécurité Plateforme

✓ Ségrégation d'adressage IP



✓ Analyse des flux VoIP via ALG (Application Layer Gateway)

- Analyse protocolaire
- Vérification de la cohérence des états (Firewall Statefull)
- Ouverture des ports média: méthode statique/méthode dynamique



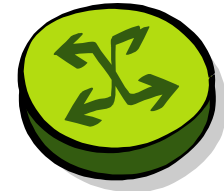
En analysant les échanges H323 (port TCP 1720), le firewall voit que le message Start RTP contient le port UDP 5326 et ouvre ce port entre les deux postes IP.

✓ Translation d'adresse pour la VoIP (NAT)

▪ NAT3 (ISO level 3 - Network)

Address/Port translation at the level of IP header:

- Source/Destination IP address and/or Port



▪ NAT5 (ISO level 5 - Session)

Address/Port translation at the level of packet payload:

- IP address and/or Port depending on protocol used



**ALG
required**

Sécurité de la couche Réseau

Analyse des flux VoIP - NAT5 ou HNAT

Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

10.31.101.20

10.31.101.50

172.20.120.50

LAN

WAN



172.20.120.30

1. Alice's phone sends an INVITE requests to Bob's phone

```
INVITE sip:BobPhone@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 10.31.101.20:5060
From: AlicePhone <sip:AlicePhone@10.31.101.20>
To: BobPhone <sip:BobPhone@172.20.120.30>
Call-ID: 314159@10.31.101.20
Cseq: 1 INVITE
Contact: sip:AlicePhone@10.31.101.20
v=0
o=AlicePhone 5462346 3332123 IN IP4 10.31.101.20
c= IN IP4 10.31.101.20
m= audio 49170 RTP 0 3
```

2. SIP ALG creates pinhole, accepting traffic on WAN with destination address: port numbers 172.20.120.22 49170 (RTP) 49171 (RTCP)

Request	SIP headers	NAT action	SIP body	NAT action
Outbound request (from private to public)	To:	None	o=	Replace local address with ALG address
	Request-URI:		c=	
	From:	Replace local address with ALG address		
	Call-ID:			
	Via:			
	Contact:			
	Record-Route:			
	Route:			

3. NAT action on the INVITE request. The SIP ALG forwards the NATed request to BobPhone

```
INVITE sip:BobPhone@172.20.120.30 SIP/2.0
Via: SIP/2.0/UDP 172.20.120.50:5060
From: AlicePhone <sip:AlicePhone@172.20.120.50>
To: BobPhone <sip:BobPhone@172.20.120.30>
Call-ID: 314159@172.20.120.50
Cseq: 1 INVITE
Contact: sip:AlicePhone@172.20.120.50
v=0
o=AlicePhone 5462346 3332123 IN IP4 172.20.120.50
c= IN IP4 172.20.120.50
m= audio 49170 RTP 0 3
```

Session

- Interaction au niveau des sessions multi-médias traversant le SBC

Border

- Localisé en général en bordure de l'entreprise dans une zone dite Démilitarisée (DMZ)

Controller

- L'entreprise a besoin de contrôler les applications entre le monde externe et le monde interne



Sécurité de la couche Réseau

Analyse des flux VoIP - SBC

Sécurité Application

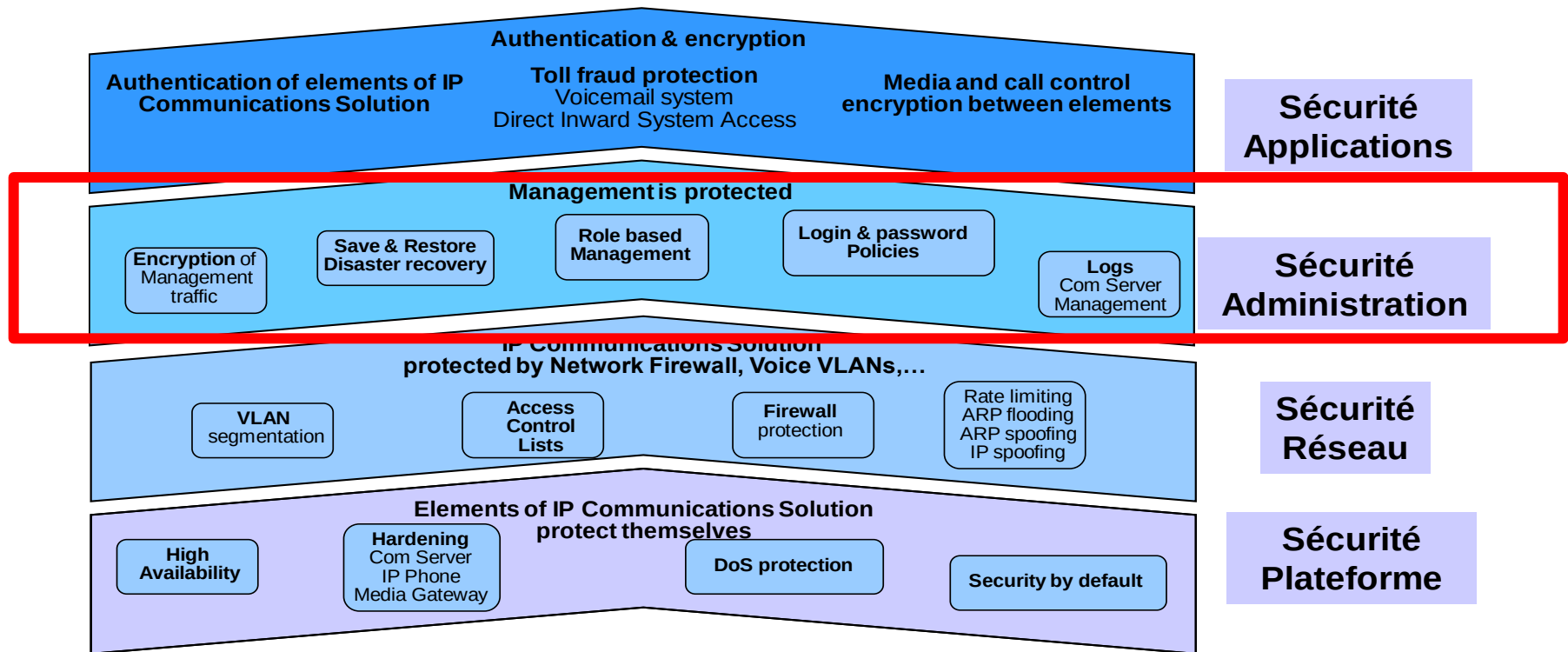
Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

Besoins	Fonctions du SBC
Interoperabilité	- SIP signaling gateway - DTMF transcoding - Codec negotiation - Media Proxy (manipulate SDP)
Connectivité	- NAT/PNAT traversal (level 5 - SIP session) - Hosted NAT Traversal (SIP end-points) - VLAN Aggregation - SIP sessions routing (multi IPPBX/multi Carriers)
QOS	- active control (Call Admission Control) - passive control (QOS Tickets) - TOS/Diffserv marking - High Availability
Sécurité	- VoIP « aware » firewall • ALG SIP • Dynamic Pinholing for voice media • DoS (Denial of Service) prevention - Hidden internal IPPBX topology - TLS encryption for SIP and SRTP for media

Une approche de la sécurité par couche



- ✓ Authentification des administrateurs
- ✓ Gestion des autorisations d'accès aux ressources
- ✓ Traçabilité des actions de configuration

Framework AAA (Authentication-Authorization-Accounting)

Sécurité de l'Administration

Points Clés

Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

Identity Management Be careful: identification (who I am) is not authentication (I prove who I am)



Access request

Authentication

Application

Accounting

Audit

Journal

Action

Authorisation

Data

AAA

Sécurité de l'Administration

Protocole RADIUS

Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

Administrateur

Communication Server

Serveur RADIUS



✓ **User:** dupont **Pass:** abcd



USER	PASS
titi	hghi
toto	efgh
dupont	abcd



Possibilité d'utiliser un système de token sécurisé (mécanisme OTP – One Time Password) afin de renforcer la sécurité de l'accès aux serveurs.

Sécurité de l'Administration

Disaster recovery (reprise d'activité)

Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

- Processus de récupération: données, matériel et logiciel critiques
- Sauvegardes synchrones et asynchrones de la base de données
 - Usagers/Equipements/Système...
 - Statistiques d'appels (Call Data Record) → facturation
 - Répertoires LDAP
 - Compteurs de performance
 - etc...
- Redondance du système de management
- Mécanisme de détection de saturation de la base de données
- Stockage disque optique / RAID 5

Sécurité de l'Administration

Encryption management

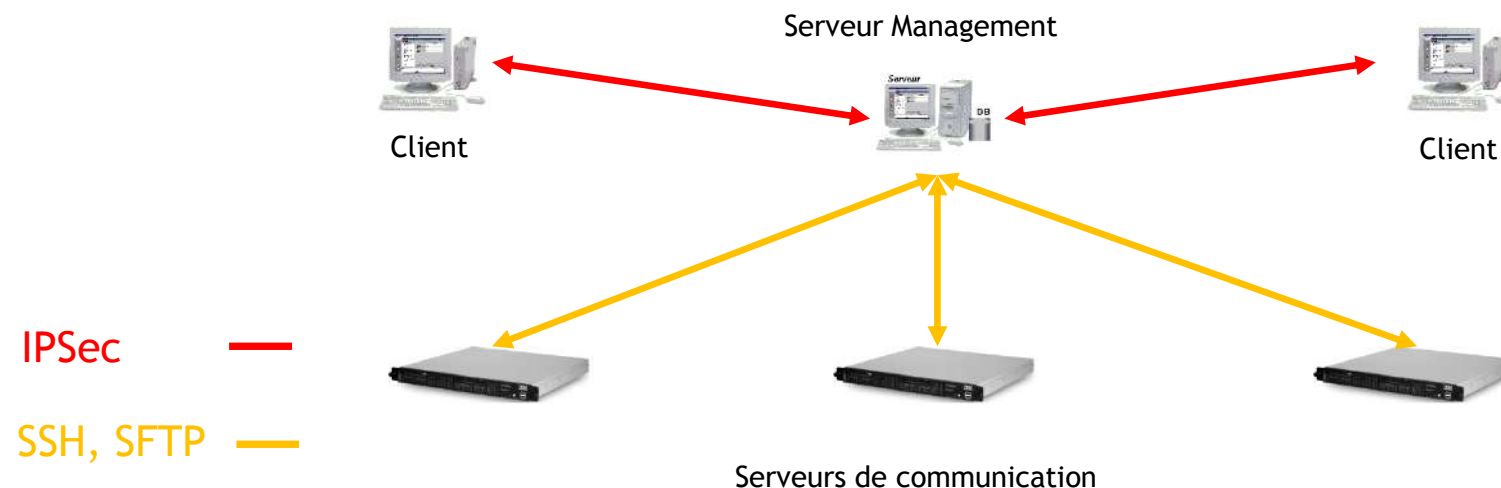
Sécurité Application

Sécurité Administration

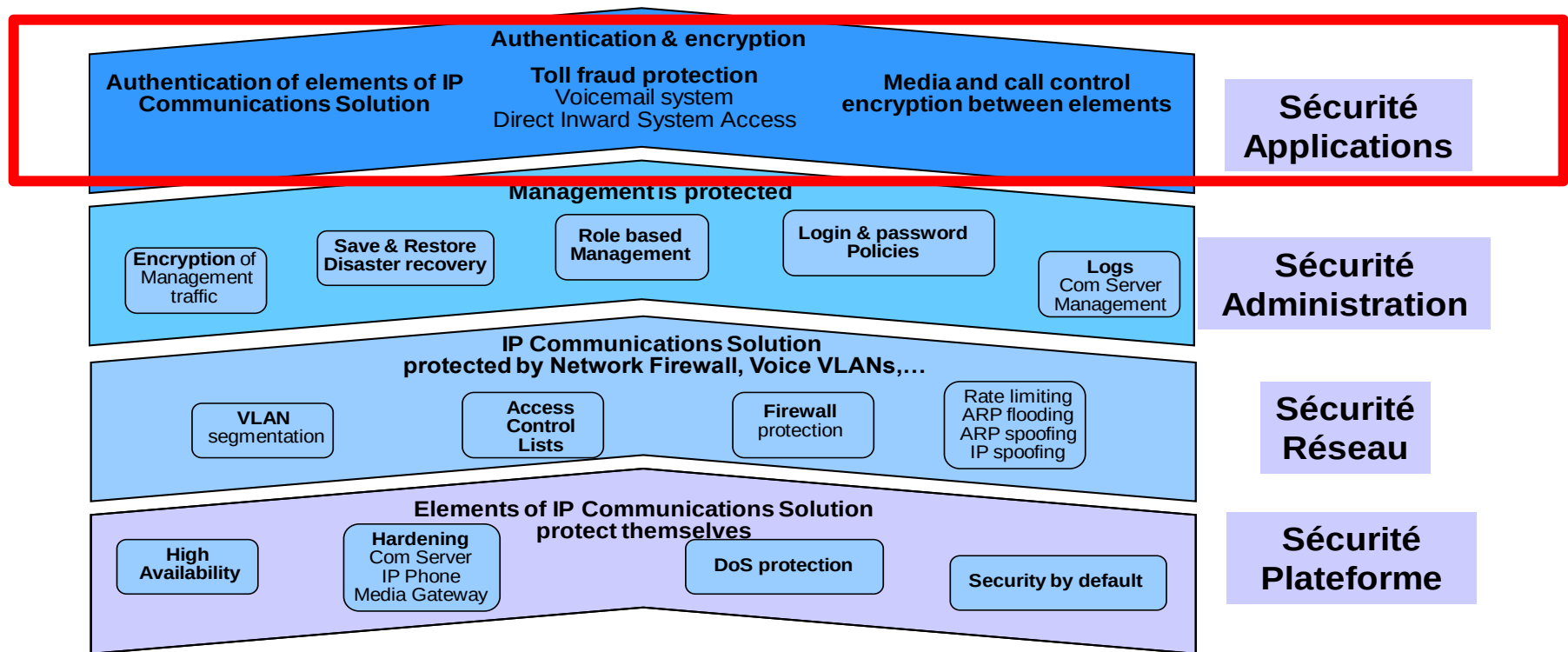
Sécurité Réseau

Sécurité Plateforme

- Authentification et chiffrement des flux de management
 - Client et serveur de management
 - IPSec: authentification mutuelle, chiffrement, mécanisme de non-corruption des données
 - Management et serveur de communication
 - SSH: gestion dans un tuyau sécurisée
 - SFTP: transfert de fichiers sécurisés (CDR)



Une approche de la sécurité par couche



Sécurité au niveau Application

Confidentialité des communications

Sécurité Application

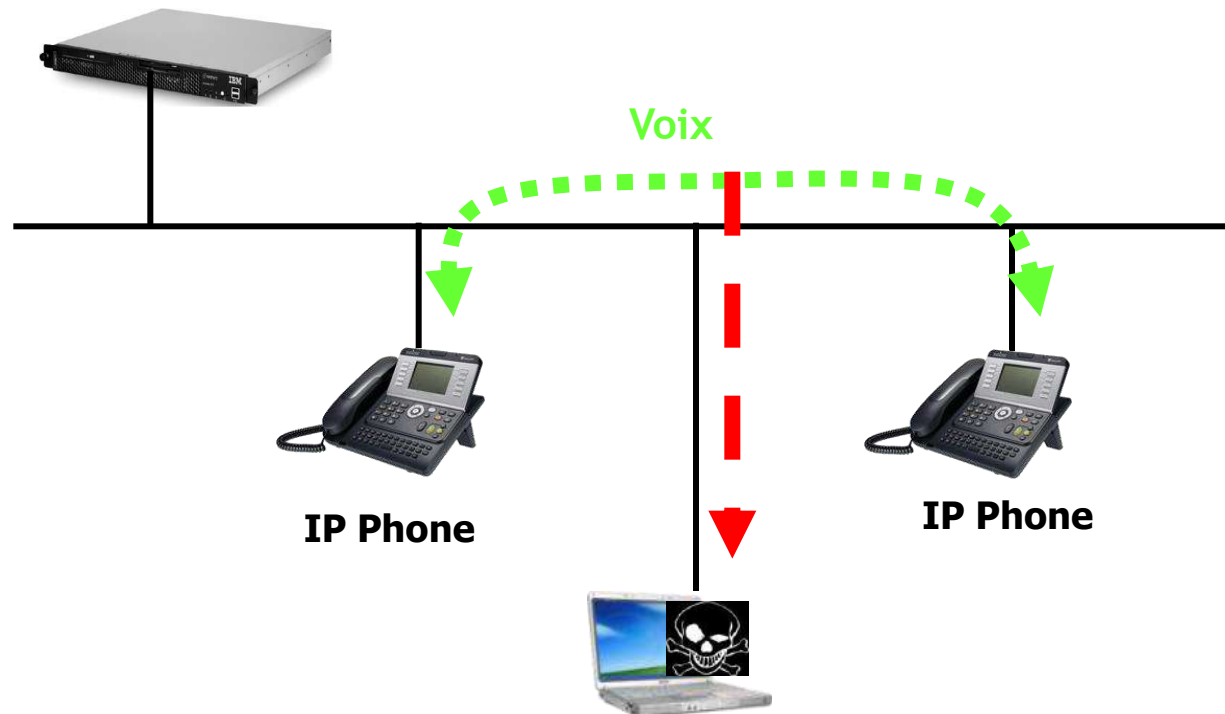
Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

Un des principaux risques d'une application de Voix sur IP est la possibilité d'écoute des communications sur le réseau.

Serveur de communication



Sécurité au niveau Application

Confidentialité des communications

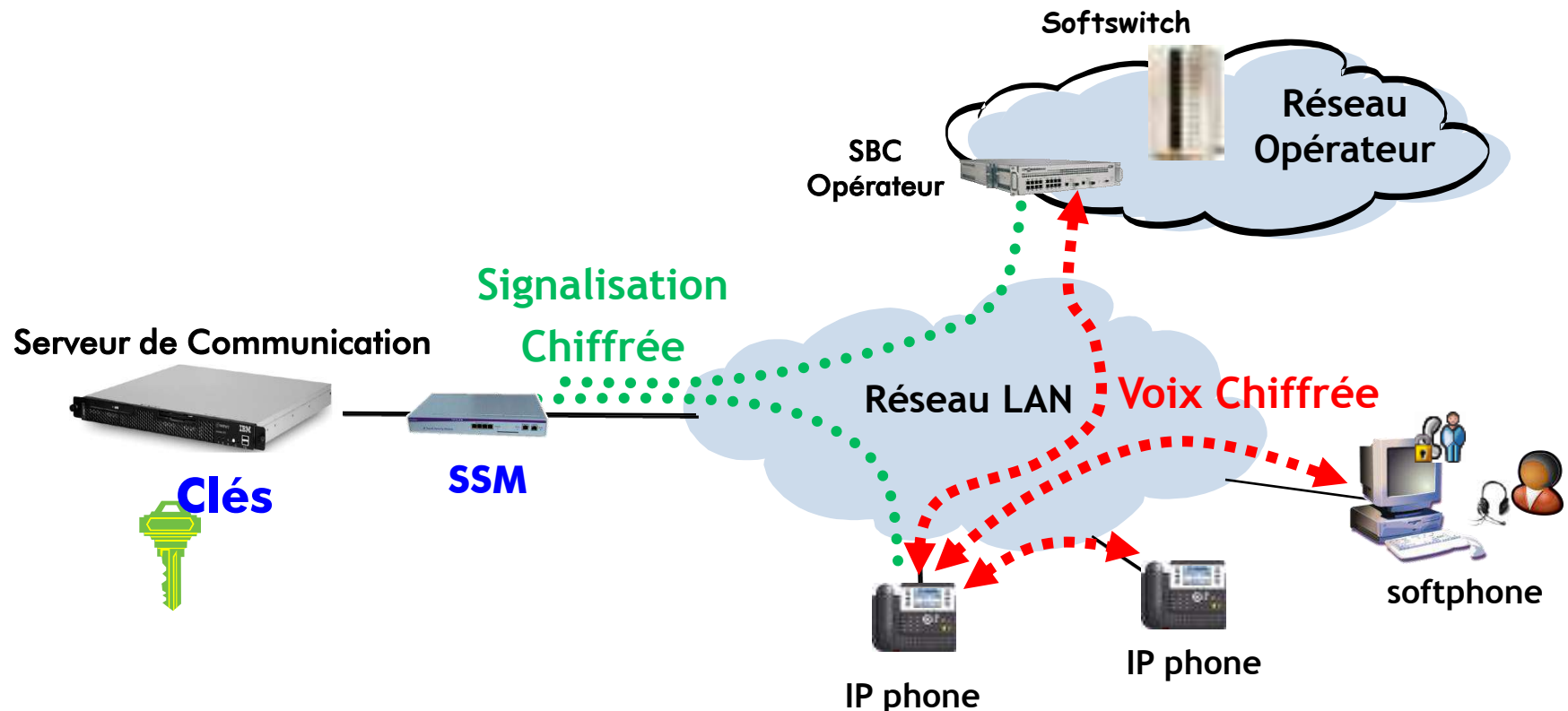
Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

- Chiffrement de la signalisation (IPSec ou TLS)
- Chiffrement du media voix (SRTP)
- Gestion centralisée ou distribuée des clés de session



Sécurité au niveau Application

Confidentialité des communications

Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

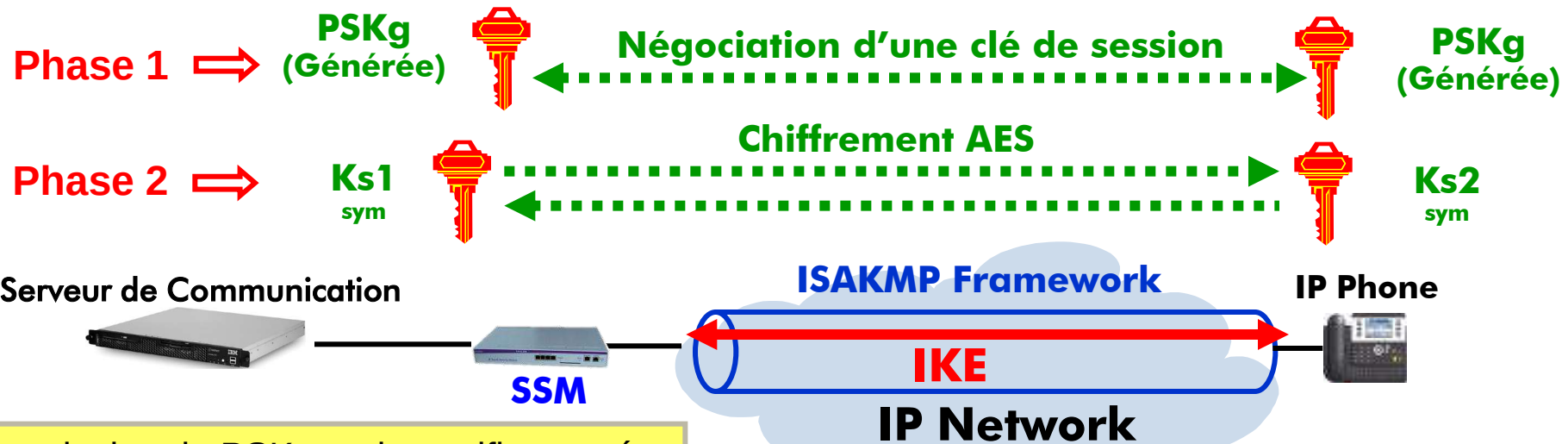
Chiffrement de la signalisation basée sur protocole IPSec

Phase 1 : phase “principale” (framework ISAKMP et protocole IKE)

- Établissement d'un canal sécurisé entre les deux éléments

Phase 2 : phase “rapide”

- Négociation IPSec à l'intérieur du canal sécurisé



Le principe de PSKg et de certificats pré-installés en usine permet un déploiement "plug and play".

Sécurité au niveau Application

Confidentialité des communications

Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

Chiffrement de la signalisation basée sur protocole TLS (Transport Layer Security)

Pourquoi TLS est plus sécurisé ?

- Basé sur des **Certificats Digitaux**:
 - **Authentification** : identifier l'originataire d'un message
 - **Intégrité** : s'assurer que message reçu et message envoyé sont identiques
 - **Non-répudiation** : l'originataire du message ne peut déclinier sa responsabilité
 - **Confidentialité** : les messages échangés sont chiffrés de bout en bout

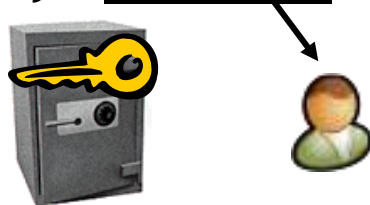
De quoi a t'on besoin pour l'implémenter ?

- Certificat Digital (X509 v3)
- Une PKI (Public Key Infrastructure) pour gérer les certificats digitaux

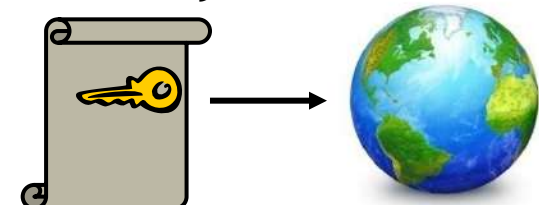
Public Key Infrastructure

- Basé sur des Public Key qui appartiennent aux principes de cryptographie asymétriques
- **Clé Publique** et **Clé Privée** sont mathématiquement liées:
 - Il est impossible de déduire la clé privée à partir de la clé publique
 - Il faut posséder la clé privée pour pouvoir répondre à la clé publique
 - La clé privée est conservée en lieu sûr et jamais partagée
 - La clé publique est diffusée largement (à travers le **certificat digital**)

Private Key + Pass Phrase

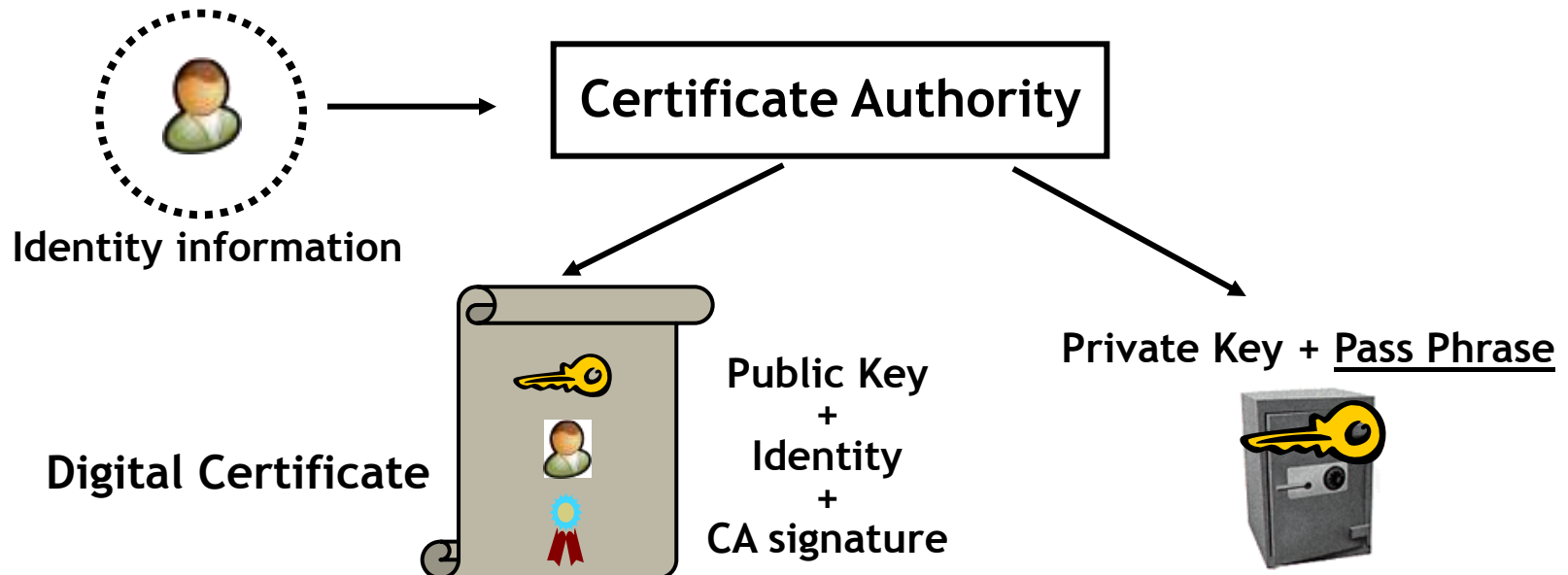


Public Key



Public Key Infrastructure

- Infrastructure dont le but est d'apporter l'élément de confiance:
 - association entre la clé publique et les éléments d'identité dans le **Certificat Digital (X509)**
 - **Certificate Authority** pour certifier cette association



Sécurité au niveau Application

Confidentialité des communications

Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

Certificate = digital document = identity card = prove who I am

- Data structure
 - Binding public keys with the identity of the public key holder
 - Signature made by a trusted authority
- Based on ITU-T X.509 international standard V3 - 1996

Data	Version	X509 standard version
	Serial number	Used to uniquely identify the certificate
	Issuer	Trusted authority
	Validity	Issue and expiration dates
	Subject	Person or entity identified
	Subject Public Key Info	Public key of the person/entity
	X509v3 extensions	<u>Optional generic extensions</u> : key information, certificate use information, user and CA attributes, co-certification constraints
Signature	Signature Algorithm	Algorithm used for the signature
	Signature	Signature made by the trusted authority

Sécurité au niveau Application

Confidentialité des communications

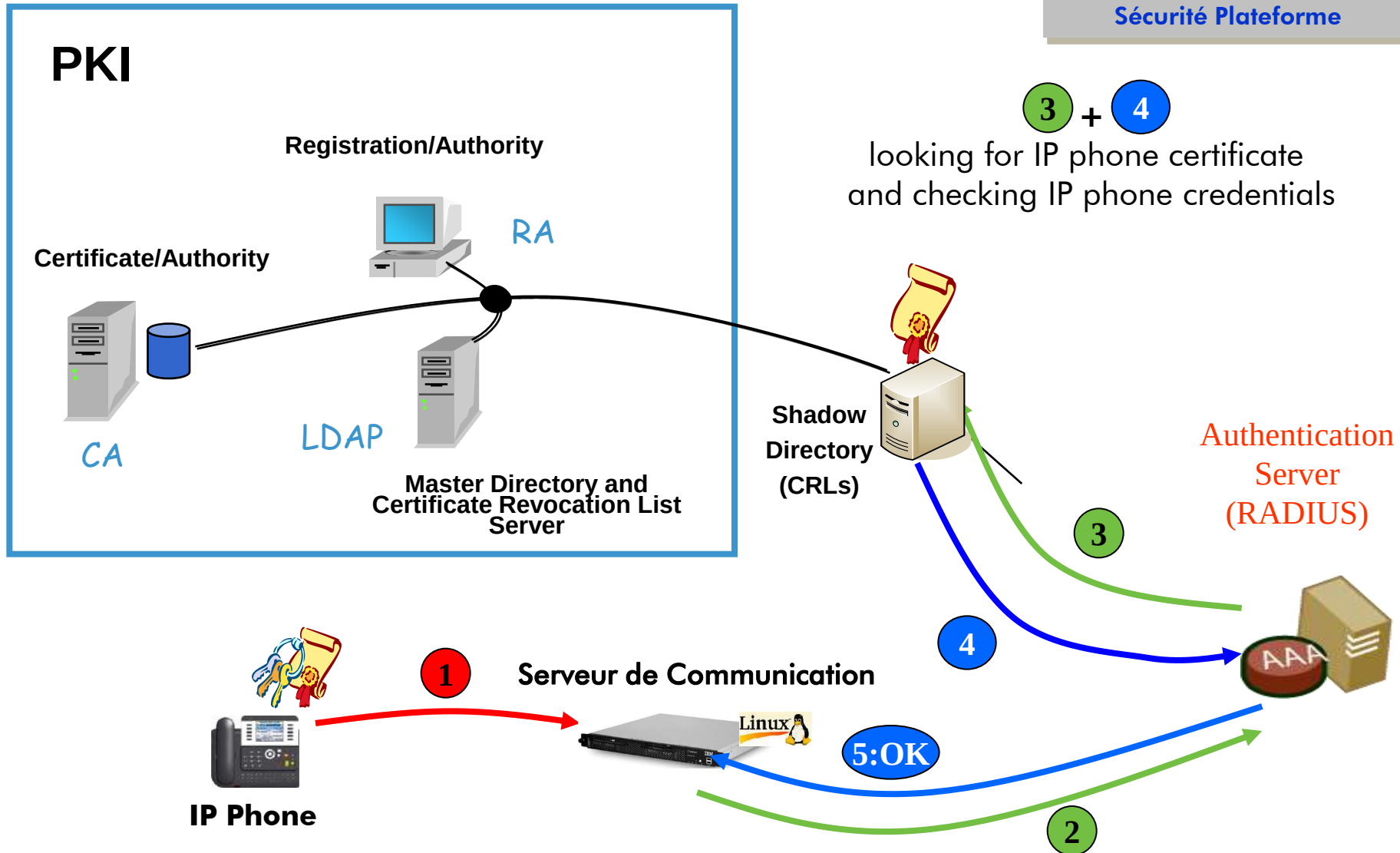
Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

PKI



Sécurité au niveau Application

Confidentialité des communications

Sécurité Application

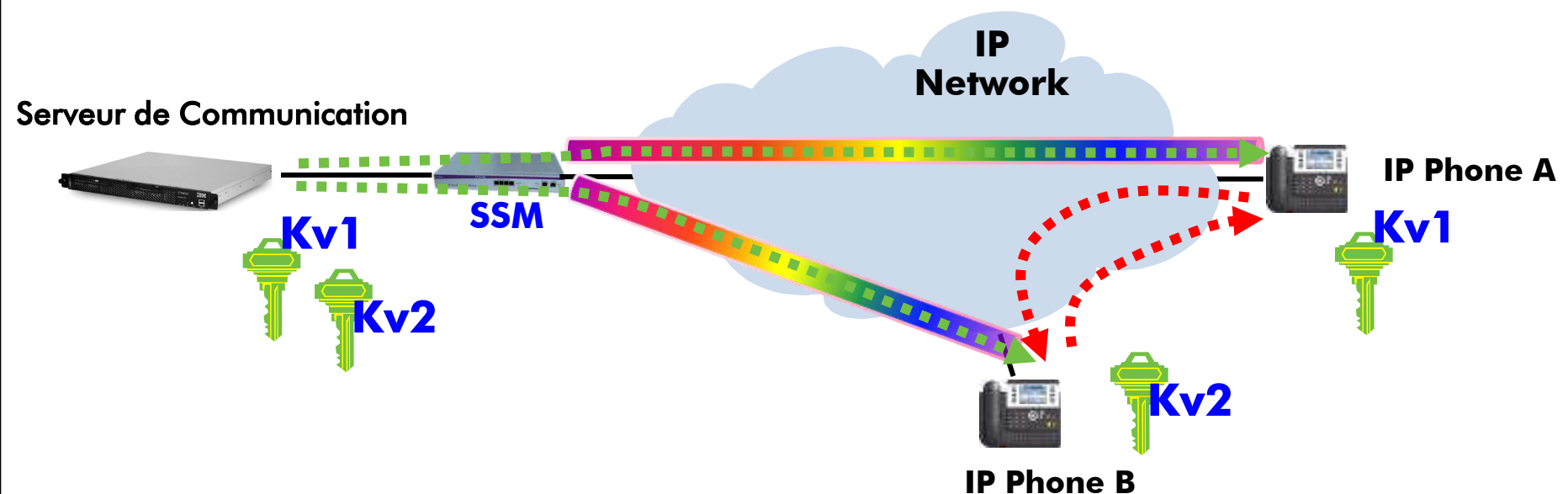
Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

Chiffrement du media Voix

- Génération des clés au niveau du Serveur de Communication
- Une clé différente pour chaque direction (A vers B, B vers A)
- Transmission sécurisée des clés Voix à travers les canaux IPSec pré-établis ou TLS
- Utilisation du protocole SRTP (Secured RTP)



Sécurité au niveau Application

Protection contre la fraude téléphonique

Sécurité Application

Sécurité Administration

Sécurité Réseau

Sécurité Plateforme

- **Restriction sur les transferts d'appels**
 - Appel entrant vers appel interne autorisé
 - Appel entrant vers appel extérieur autorisé
 - Appel sortant vers appel extérieur non autorisé
- **Restriction sur les renvois d'appels**
 - Interne uniquement
 - Appel extérieur non autorisé (international, mobile)
- **Restriction d'accès sur le poste**
 - Verrouillage/déverrouillage IHM
 - accès aux services téléphoniques par code PIN
- **Restriction d'accès distant sur le serveur de communication**
 - DISA, accès aux services téléphoniques par code PIN
- **Restriction de services des messageries vocales**
 - Consultation messages par code PIN
 - Rappel de l'appelant via le réseau public interdit (freaking)
 - Contrôle appels entrants/sortants

5

Réglementation et Certification

Réglementations

- Sectorielle:
 - **SOX (Sarbanes & Oxley)** : intégrité des opérations financières
 - **HIPAA (Health Insurance Portability and Accountability Act)**: confidentialité des données patients (médical)
- Ecoutes légales:
 - **CALEA** (Communications Assistance for Law Enforcement Act of 1994) / USA
 - **CNCIS** (Commission nationale de contrôle des interceptions de sécurité) / France
- Militaire:
 - **PRIS** (Politique de Référencement Intersectorielle de Sécurité) / France
 - **JITC** (Joint Interoperability Test Command): délivre au ministère de la défense US les attestations sur le niveau de résistance des équipements après audit et tests.

Normalisation (1/2)

Ensemble des normes ISO 270xx

- ➔ Méthodologie pour la Sécurité du Système d'Information (SI)
- ➔ Crédibilité et engagement vis à vis de ses clients et partenaires

Norme	Titre
27001	Exigences d'un Système de Management d'un Système d'Information (SMSI)
27002	Guides de bonnes pratiques de sécurité de l'information
27005	Gestion des risques
...	...

Mise en place d'un SMSI ou SGSI

Gestion des
risques

Amélioration
continue

- Plan
- Do
- Act
- Check



Approche
processus

- piloter le SMSI
- analyser les risques
- gérer le traitement des risques
- contrôler l'efficacité
- gérer les incidents et les vulnérabilités
- former et sensibiliser
- gérer la documentation et les preuves

Implication
du
management

Certifications

- **Common Criteria (ISO-15408):** certification reconnue dans de nombreux pays dans le monde. Permet de s'assurer qu'un produit répond aux exigences de sécurité induite par son contexte d'utilisation
 - USA, Canada, UK, Germany, France, Australia, New Zealand, Netherlands, Finland, Greece, Italy, Norway, Spain, Israel, Austria, Sweden, India, Singapore, Japan, Turkey, Hungary, Portugal)
 - EAL1 to EAL4: Civil use
 - EAL5 to EAL7: Military use

Common Criteria



Processus de qualification/certification:

- 1) Définition d'une cible de sécurité (périmètre)
- 2) Analyse des procédures de développement, test, installation du produit par un organisme spécialisé (CESTI - Centre d'Evaluation de la Sécurité des Technologies de l'Information)
- 3) Validation de l'analyse par un organisme d'état au niveau de chacun des pays (ANSSI en France)

OmniPCX Enterprise R9 & Certification Critères Communs



La solution OmniPCX™ Enterprise est certifiée EAL 2+
Tests réalisés par l'agence française ANSSI

THE SOURCE FOR INTERNATIONALLY
RECOGNIZED CERTIFIED
IT SECURE PRODUCTS

The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which ensures that:

- Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of Certificate

→ Produits réseau

Produit certifié	Niveau	Développeur / Commanditaire	Réf. date
OmniPCX Enterprise Solution : logiciels OmniPCX Enterprise (release 9.0) et OmniVista 4760 (release 5.0)	EAL2+	Alcatel-Lucent / Alcatel-Lucent	2010/16 07/04/2010
OmniPCX Enterprise Solution: logiciels OmniPCX Enterprise (release 9.0) et OmniVista 4760 (release 5.0)	EAL2+	Alcatel-Lucent / Alcatel-Lucent	2010/15 07/04/2010
Suite logicielle IPS-Firewall pour boîtiers appliances NETASQ, version	EAL2+	NETASQ / NETASQ	2009/30

Source: <http://www.commoncriteriaportal.org/>
<http://www.ssi.gouv.fr/> (FR)

6

Conclusion

Conclusion

- La VoIP n'est pas fondamentalement moins sécurisée que la Téléphonie traditionnelle
- Plus de facilité à mettre en œuvre les attaques
- La sécurité doit être prise en compte dans le design des produits
- La sécurité doit être prise en compte au niveau du déploiement

Responsabilité de l'architecte
Responsabilité du programmeur
Responsabilité du testeur

www.alcatel-lucent.com

Any question ?

Thank You for your attention