CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

La sécurité des PABX
Le point de vue d'un constructeur

Les mesures de sécurisation des équipements lors du développement et de l'intégration

Pierre-Alexandre FUHRMANN

AASTRA

Vice-President Global R&D

25 Avril 2013

Solution de téléphonie sécurisée

Prise en compte des aspects sécurité dès la phase de conception des logiciels

- Application téléphonique
  - Utilisation des liens opérateurs (€ € !)
  - Ecoute, enregistrement
- Gestion de la solution de téléphonie
  - Gestion des utilisateurs et droits
  - Gestion du système (local/Distant)
- Intégration dans le système d'information
  - Interaction avec le SI (Annuaire, Firewall)
  - Interaction avec le poste de travail informatique
  - Data Center, Operating System, Virus
- Intégration dans l'infrastructure de communication IP
  - Interaction avec le réseau IP
  - Etanchéité /Protection des données en IP
  - Topologie distribuée IP
  - Solutions de mobilité

Une approche globale nécessaire dès la phase d'architecture des solutions

Application téléphonique

Adaptation des logiciels pour augmenter la sécurité

- Clé logicielle nécessaire pour certaines fonctions sensibles
  - Ecoute Discrète, DISA (Substitution externe)

- Classe de facilités , catégorie d'appels pour limiter les risques
  - Interception, offre, entrée en tiers, outrepassement… soumis à droit

- Paramètrage par défaut restrictif de certaines fonctions sensibles
  - Renvois vers l'extérieur : par classe de facilité. Par défaut, pas autorisé
  - Transfert dans la messagerie intégrée : par système, Par défaut pas autorisé vers l'extérieur
  - SVI : programmable par l'exploitant uniquement (pas de SVI personnel)
  - DISA : Numéro d'appel spécifique, Droit par utilisateur
  - Ecoute discrète : paramétrage non accessible par menu simple
  - Ecoute Bébé : par classe de facilité et uniquement pour les appels locaux. Par défaut, pas autorisé.
  - Transit & Conférence réseau/ réseau : Non ouvert par défaut

Application téléphonique

Adaptation des logiciels pour augmenter la sécurité

- Prise en compte de la confidentialité des utilisateurs
  - Verrouillage de l'abonnement : journal d'appels non visible sur l'ensemble des terminaux
  - Voix et signalisation chiffrés
  - Message vocaux chiffrés et non écoutables par l'administrateur
  - Mot de passe non visible des administrateurs

- Renforcement de certains mécanismes de défense
  - Login/ gestion du poste : Abonnement gelé après 3 tentatives
  - DISA : N° du service + password du service + n° de l'abonné + password de l'abonné. Abonnement gelé après 3 tentatives
  - Mot de passe par défaut configurable par l'administrateur (et non pas 0000 pour tous)
  - Fonction anti-bavard : limiter les communications longues

- Traçabilité des communications : tickets d'appels répliquables avec stockage sécurisé

Gestion de la téléphonie

Adaptation des logiciels pour augmenter la sécurité

- Gestion des droits de configuration
  - Droits de configuration à base profil exploitant
    - Segmentation fonctionnelle, géographique, administrative
  - Possibilité de configurer la robustesse du mot de passe
    - Ex : nb caractères, nb Majuscule/minuscule, nb chiffres, nb caractères spéciaux, périodicité du mot de passe

  - Politique mot de passe constructeur modifiée récemment
    - Modifiable par l'intégrateur une fois – RAZ uniquement par intervention sur site d'Aastra

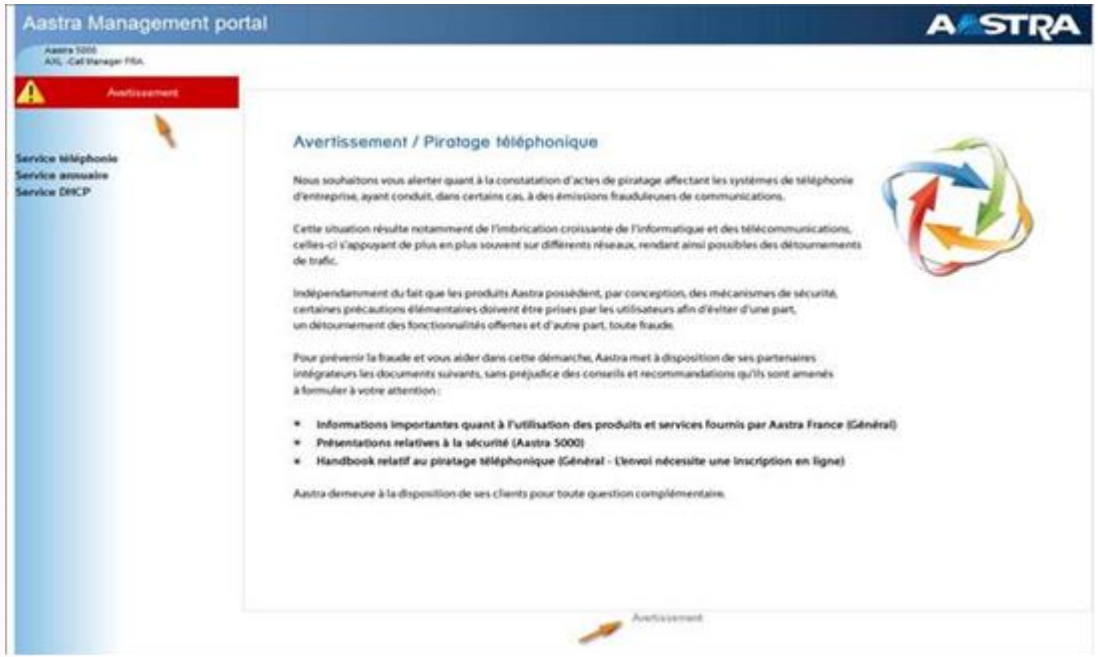
- Télégestion RNIS
  - Accès modem RNIS distant – filtrage des numéros appelants
  - Trace des tentatives de connexion journalisées- Traces non destructibles par télémaintenance

- Télégestion IP
  - Sécurisation selon les modes 'classiques' de prise à distance IP (règles d'intégration préconisées aux intégrateurs)

Gestion de la téléphonie

Adaptation des logiciels pour augmenter la sécurité

- Insertion d'un message d'information préventif lors de l'installation du système téléphonique
  - ❖ Sensibiliser l'intégrateur aux bonnes pratiques de sécurité
  - ❖ Protection juridique vis-à-vis du client final



Intégration de la téléphonie dans le système d'information

Politique d'Operating System

- PABX TDM : ex PABX sous OS iRMX
  - OS temps réel très spécialisé
  - Peu d'attaques potentielles, aucun virus connu
  - Système autonome, avec peu d'interaction avec le SI

- PABX IP, Call Manager, terminaux IP, Serveurs : Linux ou Windows
  - Distribution beaucoup plus large, risque de faille plus grand
  - Nécessité de mise à jour fréquentes
  - Intégration plus forte avec la politique informatique

- Packaging customisé des OS
  - Suppression d'éléments inutilisés (ex : 120 Mo au lieu de 2 Go)
  - Désactivation de certains services non critiques (interface graphique, partage de fichiers…)
  - Nombre minimum de ports ouverts

- Politique de suivi des évolutions des distributions Linux pour résoudre de manière continue les failles de sécurité
  - Tests des patchs de sécurité publiés et impactant la solution de téléphonie
  - Mise à jour de manière régulière (tous les 2 mois)

Recommandation : mettre à jour ses solutions de téléphonie sur IP pour réduire les failles de sécurité

Intégration de la téléphonie dans le système d'information

Interactions avec le SI

- Anti-virus
  - Tests réguliers avec les anti-virus du marché
  - Recommandations publiées sur les politiques d'activation (en heure creuses, quels fichiers scanner…)
  - Pas de scan des OS terminaux mais contrôle d'intégrité des données à chaque mise à jour des firmware

- Base annuaires
  - Interfaçage annuaire avec contrôle d'accès ACL/LDAP v3
  - Mise en place de mécanisme d'audit et de contrôle lors des mises à jours automatiques

- Poste de travail informatique/ terminaux
  - Mécanisme d'authentification (MD5) du client informatique pour éviter le déni de service
  - Sécurisation des flux (TLS) utilisés par le dialogue avec l'application de téléphonie
    - Messages vocaux envoyés en email
    - Flux XML pour dialogue interactif

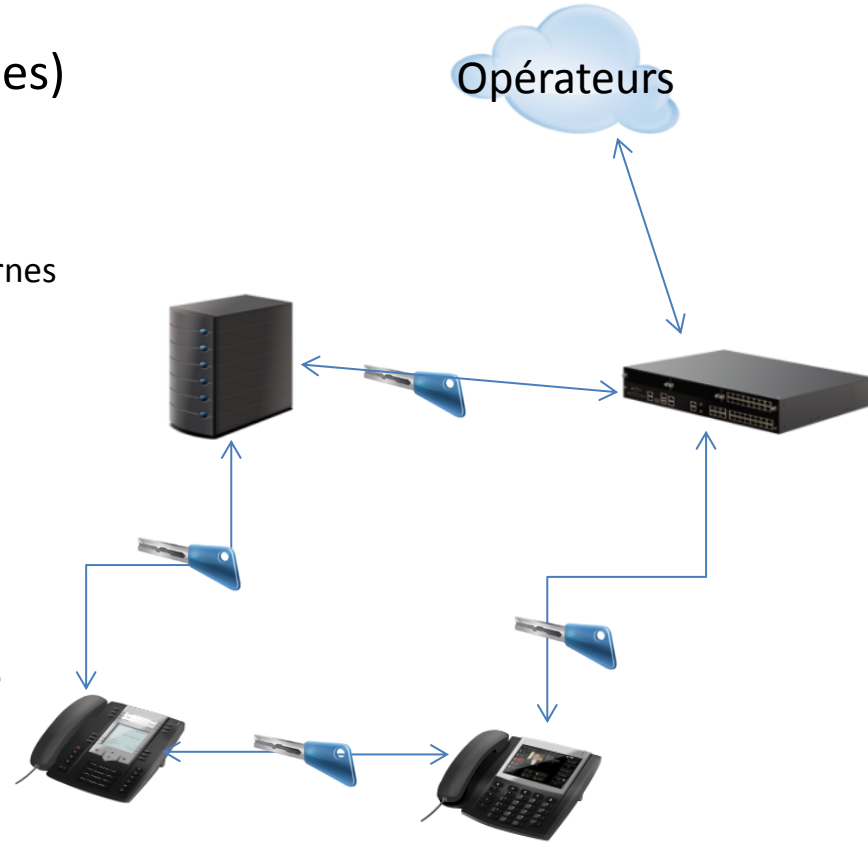
Intégration de la téléphonie dans le réseau de communication IP

- Authentification - Accès du terminal au réseau IP
  - Règles d'ingénieries préconisées : Isolation VLAN, paramétrage DHCP…
  - Mécanismes standards : 802.1X, MD5 implémentés au niveau des terminaux
  - Cas du PC connecté derrière poste : envoi d'un ordre de log-off en cas de déconnexion

- Authentification - accès de l'utilisateur au terminal
  - Lecteur biométrique sur terminal
  - Login abonné – mot de passe
  - SSO pour les applications de communications unifiées

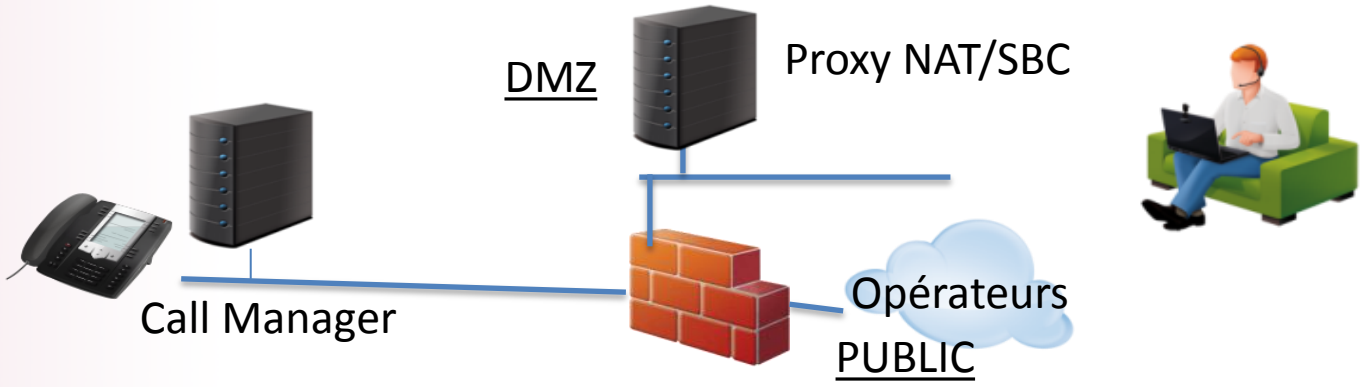
Intégration de la téléphonie dans le réseau de communication IP

- Protection des communications IP (locales)
  - Déploiement de méthode de chiffrement
    - Signalisation (TLS)
    - Media – voix/video en SRTP
    - Certificats générés automatiquement ou externes
  - Chiffrement pendant toutes les phases d'appels, ce qui complexifie le traitement d'appel (ex : conférence à 3, comm. TDM/IP…)
    - Gestion des terminaux chiffrés/ non-chiffrés
- Communication externes
  - Accès TDM non chiffrés (chiffrement sur le LAN seulement)
  - Peu d'opérateurs SIP trunk permettent le chiffrement des communications externes



Intégration de la téléphonie dans le réseau de communication IP

- Accès trunk IP sécurisé
  - Session Border Controller intégré/intégrable dans le logiciel de téléphonie et interaction avec le NAT
  - Tests de performance /résilience (ex: duplication spatiale) réalisés pour chaque version en raison des modifications d'échange de messages SIP
- Accès distant sécurisé du terminal sur Internet
  - Télé-travail :
    - Protection par VPN pour certains types de terminaux (postes, softphones)
    - Gestion par Session Border Controller avec définition des flux autorisés
  - Convergence fixe-mobile : gestion firewall intégrée avec Session Border Controller



Intégration de la téléphonie dans le réseau de communication IP

- Isolation des flux d'administration et voix
  - Possibilité de ports IP spécifiques sur Call Serveur ou PABX-IP
    - 1 port pour les flux d'administration/signalisation
    - 1 port pour la voix
  - Possibilité de double rattachement sur des switch différents

- Centralisation des flux voix – Architecture spécifique
  - Possibilité de centraliser les flux voix afin de contrôler les communications
  - Procédures de tests de performance spécifiques à ce type d'architecture
- Mécanismes de défense IP contre le déni de service
  - Catégories d'adresses IP autorisées/non autorisées
  - Blacklist auto sur tentative de flooding (envoi massif de trames)
  - Désactivation après 3 tentatives MD5 infructueuses
- Tests génériques de simulations d'attaque/défenses réalises pour chaque version logicielle

Solution de téléphonie sécurisée
En résumé

- Prendre en compte dès la phase de conception des architectures
- Prendre en compte tous les éléments qui interagissent avec la téléphonie
- Prévoir des tests spécifiques pour garantir les performances
- Les solutions de téléphonie IP peuvent être davantage 'sécurisées' que les solutions TDM traditionnelles
- Les pré-requis de déploiement et les recommandations d'exploitation doivent alors être respectés pour atteindre un niveau total de sécurité

Impératif : mettre à jour REGULIEREMENT ses solutions de téléphonie sur IP pour réduire les NOUVELLES failles de sécurité