SÉCURITÉ.ORG

EUROSEC 2005

Sécurité de la Voix sur IP

Attaques et défenses

Pierre BETOUIN
EADS CCR / ESIEA
pierre.betouin@security-labs.org

Nicolas FISCHBACH
Senior Manager, Network Engineering Security, COLT Telecom
nico@securite.org - http://www.securite.org/nico/

EADS CCR

COLT

Introduction

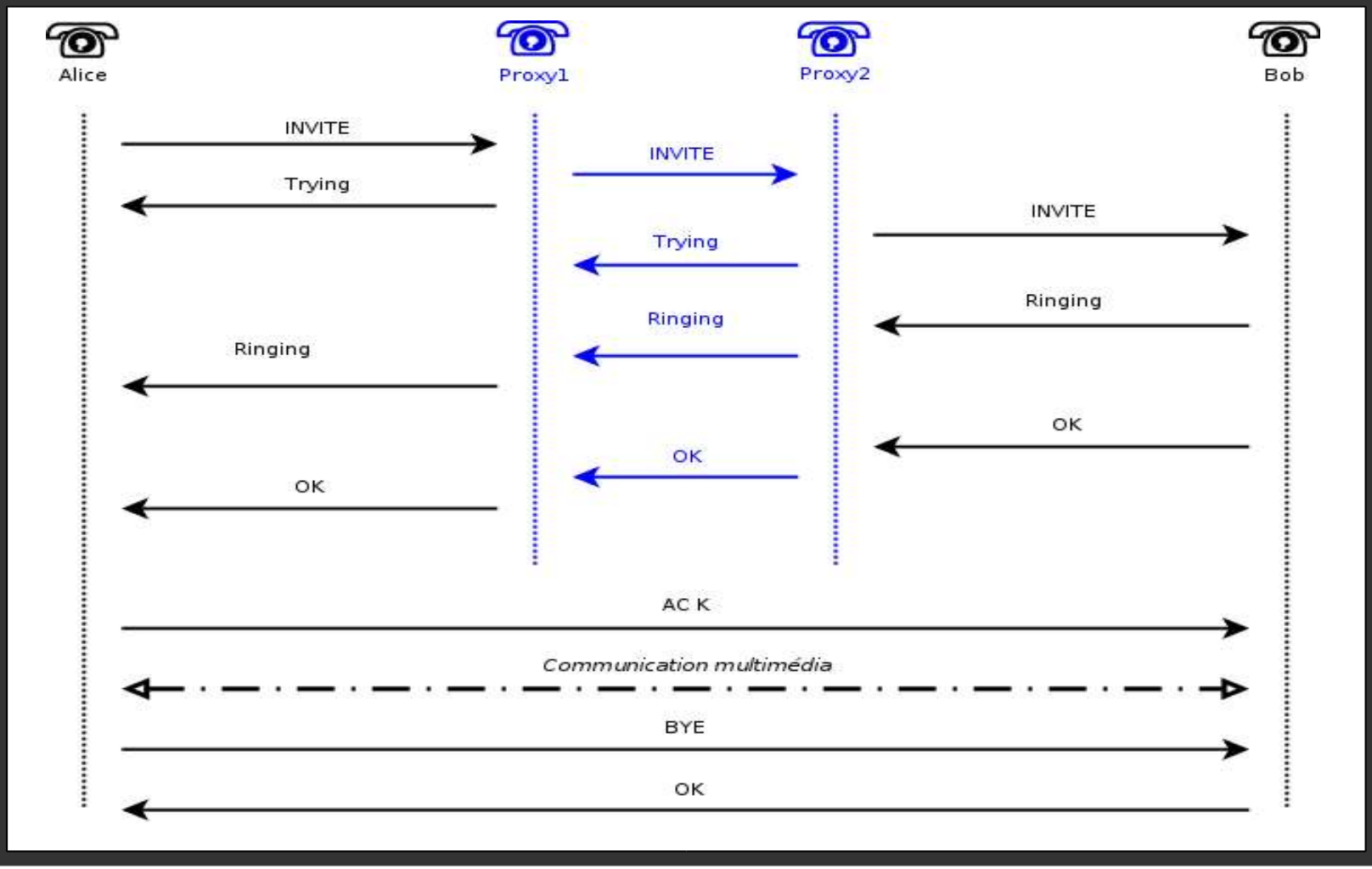
- Consolidation/convergence téléphonie / informatique
  - Complexité
  - Coûts
- Enjeux importants
  - Projet stratégique en 2005
  - Entreprises et opérateurs
  - Particuliers
- Nouveaux risques

Protocoles VoIP

- Signalisation et contrôle
  - SIP (Session Initiation Protocol)
    - HTTP-*like*
    - Adresses simples : *sip:user@domaine.com*
  - H.323
    - Complexe
    - H.235 : définit des mécanismes de sécurité
- Transport
  - RTP (Real-Time Protocol) / RTCP (Real-Time Control Protocol)
  - SRTP / SRTCP : équivalents chiffrés

Protocoles VoIP (suite)

- Exemple de session SIP



Protocoles secondaires

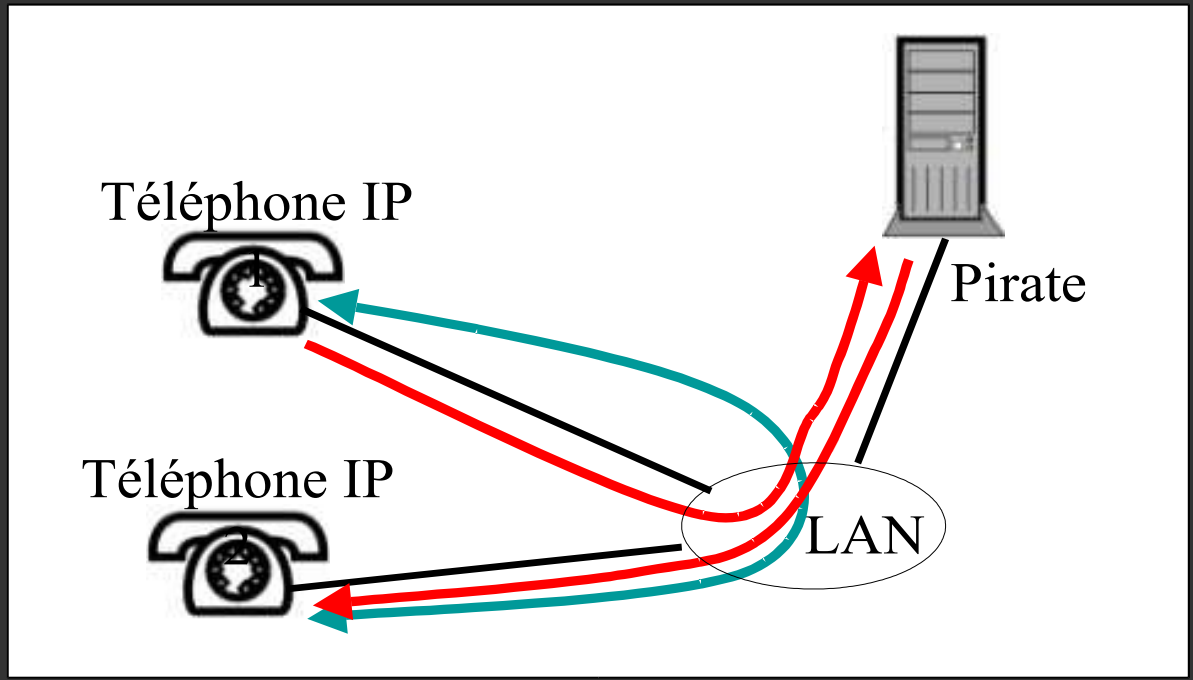
- DNS : Annuaire et localisation
- DHCP : Attribution IP/DNS/etc
- TFTP : Configuration & mise à jour
- HTTP : Administration
- ENUM : Correspondance adresses SIP / numéros E.164 en utilisant DNS

Équipements

- Téléphones *hard-phones* « classiques »
  - Propriétaires
  - Appliances
- *Soft-phones* / UA (User-agents)
  - Solutions logicielles
  - Souples

Quelques attaques envisageables

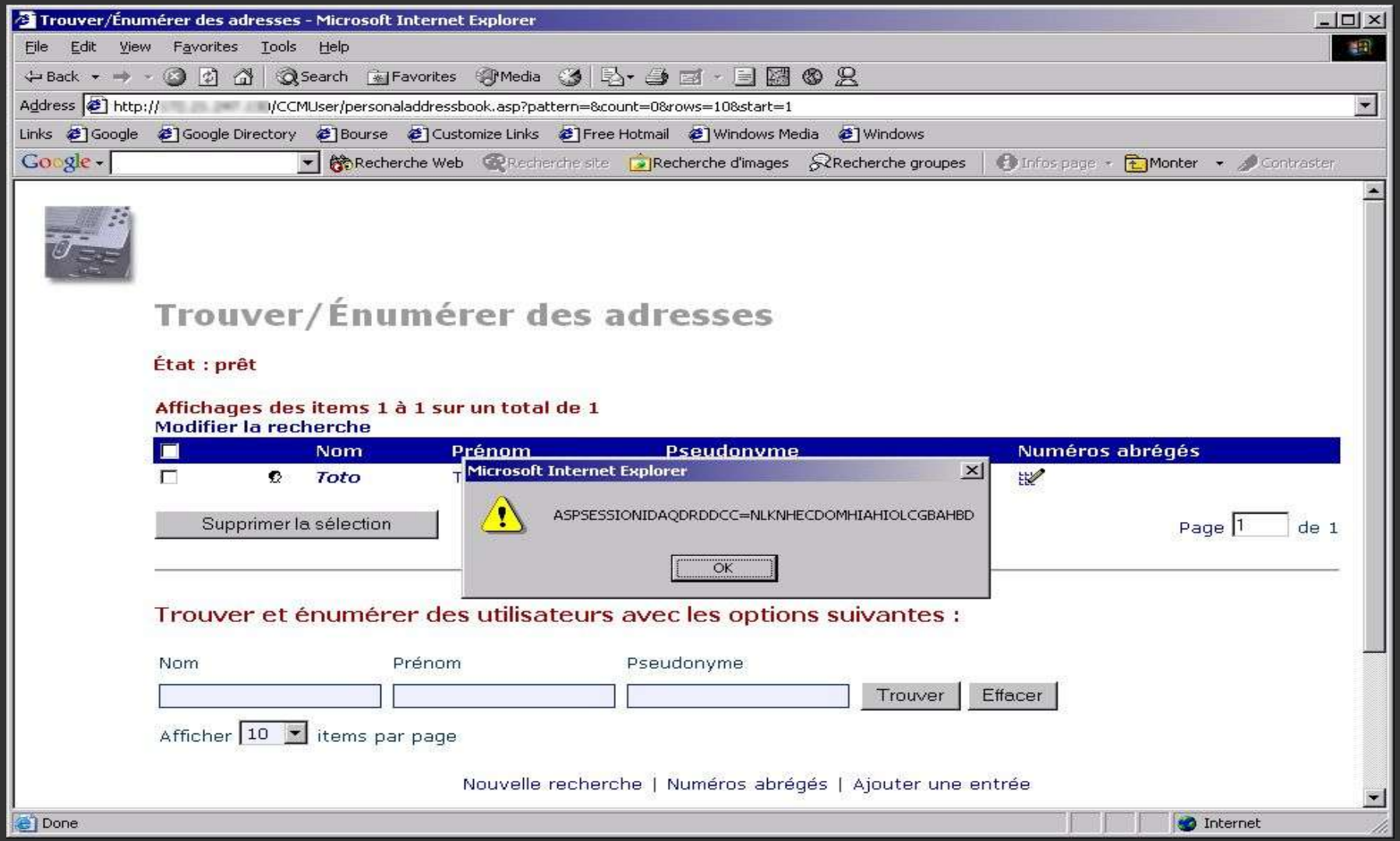
- Attaques physiques (systèmes d'écoute)
- Attaques sur les couches basses
  - ARP spoofing / ARP cache poisoning
  - MITM : écoute passive ou modification de flux



Attaques envisageables (suite)

- 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)
- Portes dérobées

Attaques envisageables (suite)



Attaques envisageables (suite)

- Attaques sur les protocoles *VoIP*
  - *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 RTP

Attaques envisageables (suite)

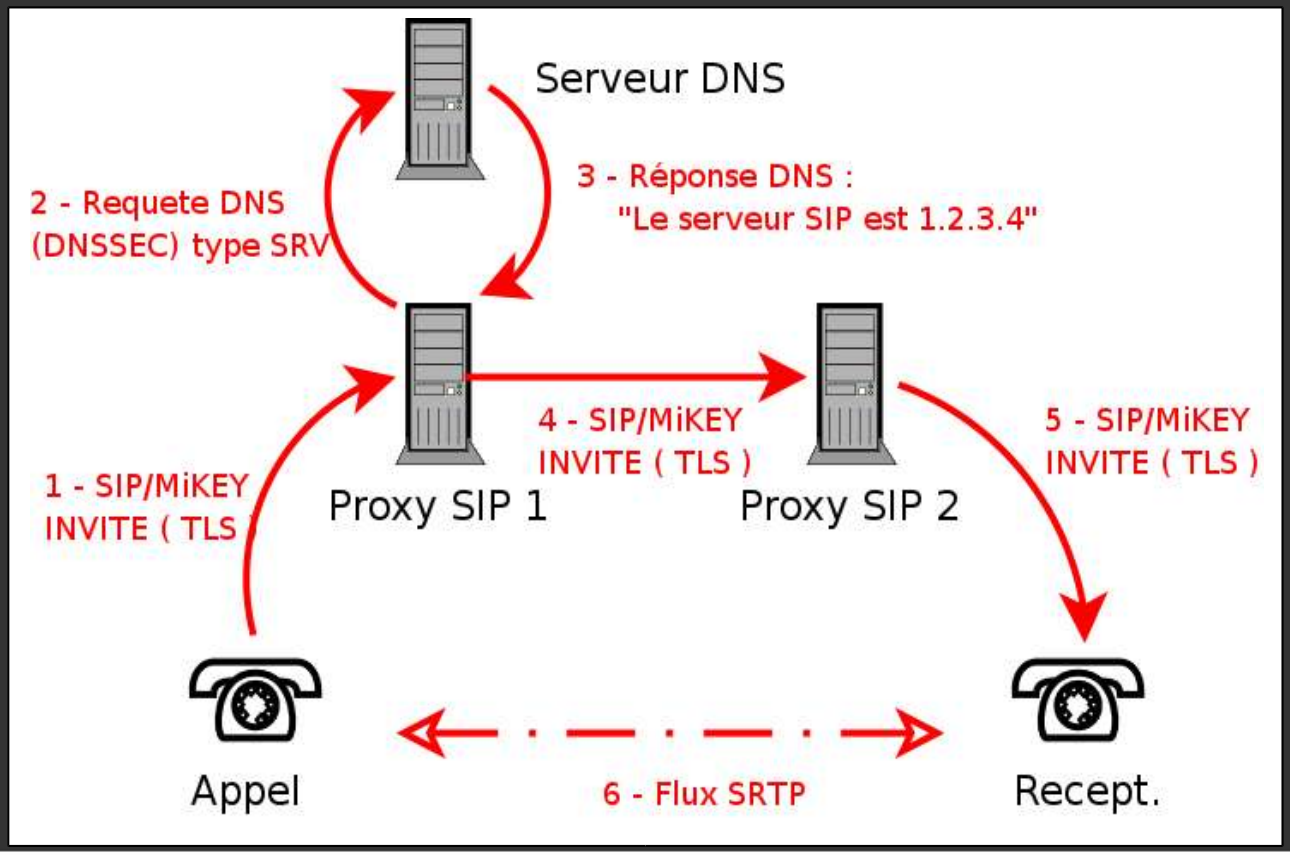
- Attaques sur les protocoles secondaires
  - DNS : *DNS ID spoofing* ou *DNS cache poisoning*
  - DHCP : DoS, MITM
  - TFTP : *upload* d'une configuration (DoS, MITM...)

Recommandations

- Mécanismes de détection
- Sécurisation des couches basses
- Utilisation de TLS pour la signalisation SIP
- Utilisation de SRTP/SRTCP
- Protocole de gestion de clefs VoIP : MiKEY
  - Encapsulé dans SIP
    - PSK (Pre-shared key)
    - Diffie-hellman
    - PKI
- Sécurisation des échanges DNS : DNSSec

Recommandations

- Utilisation de tunnels IPSec en remplacement des solutions précédentes
- Exemple de solution sécurisée :



Recommandations - Limites

- QoS, bande-passante...
- Qualité de la voix : choix important des CODECs
- Temps d'établissement
- Compromis utilisation / complexité
- IPsec parfois trop lourd : restriction possible aux protocoles utilisés
- Ne pas se limiter aux protocoles VoIP et au réseau: clients (UA), serveurs (*soft switch*, *call manager*, DHCP/TFTP), détection de fraude, etc.
- Ni aux aspects techniques: ingénierie, opérations, support, etc, comment les répartir ?

VoWLAN

- Utilisation de PDA / Laptop : téléphonie mobile
- Problèmes classiques du WiFi
- Utilisation d'un protocole de mobilité pour couvrir de grandes distances (IAPP)
- Choix judicieux des CODECs (PCM, GSM...)

Conclusion

- Technologie encore jeune
- Étude fine des solutions nécessaire avant déploiement
- Désormais accessible aux particuliers (Skype...)
- Sécurité au coeur de la problématique