La VoIP, une opportunité pour la sécurité ?

SSTIC 2007

Nicolas Dubée - Secway

Introduction (1)

- La convergence globale vers l'IP est une réalité
- La téléphonie fait partie des domaines concernés, au travers des technologies VoIP
- Le besoin de convergence est légitime, eu égard aux économies possibles, mais surtout aux nouveaux services rendus par la VoIP

Introduction (2)

- La VoIP apparaît comme un risque (cf. MISC mai-juin 2007 « Le risque VoIP »)
- La VoIP n'introduit en elle-même que peu de risques vraiment nouveaux
  - Il a toujours été possible d'intercepter une conversation (intrusion physique)
  - Il a toujours été possible de paralyser fortement la téléphonie en détruisant certains équipements clefs
- Ce qui change :
  - D'un côté l'importance de la menace (en nombre, potentiel, distance)
  - De l'autre les possibilités pour sécuriser la téléphonie, largement meilleures qu'auparavant

Introduction (3)

- Nous avons choisi de développer un boitier matériel de chiffrement bout-en-bout des conversations VoIP

- Ce projet sera l'opportunité d'une présentation sur :
  - Les protocoles et risques de la VoIP
  - Notre retour d'expérience sur la VoIP
  - Notre retour d'expérience sur un développement embarqué (carte-mère embarquée ARM + GNU/Linux)

La VoIP, une opportunité pour la sécurité ?

- Aperçu des protocoles VoIP
- Attaques et risques en VoIP
- Solutions pour la confidentialité des flux
- Notre retour d'expérience

Les protocoles de la VoIP (1)

- Les protocoles de la VoIP se classent en deux familles
  - Les protocoles de signalisation
  - Les protocoles de transport des données (audio/vidéo)
- Toute conversation VoIP fait intervenir ces deux familles
- En outre, d'autres protocoles peuvent intervenir en support
  - DHCP / TFTP pour la gestion des adresses et des configurations des téléphones
  - 802.1q pour la segmentation en VLANs
  - DNS pour la résolution des adresses distantes…

Les protocoles de la VoIP (2)

- Plusieurs protocoles de signalisation se distinguent (H.323, SIP, SCCP)
- Pour les protocoles de données, RTP est prédominant
- En général, on désigne une architecture par le protocole de signalisation qu'elle utilise

Protocoles de signalisation

- Protocoles ayant vocation à mettre en place et gérer des sessions de communication
  - Signalisation des appels
  - Mise en place d'un canal de communication (IPs + ports) pour faire circuler la voix
- Deux approches différentes pour ces protocoles
  - Monde des télécoms - H.323
  - Monde des SI
    - SIP
    - IAX2, avec l'IPBX open-source Asterisk
    - SCCP (Skinny) de Cisco

H.323

- Série de recommandations ITU-T pour véhiculer des communications audio/vidéo sur un réseau de paquets
- Contient notamment H.225.0 (RAS + Q.931) pour la signalisation des appels

➢ Protocole largement utilisé, aussi bien pour de petites applications, que sur de très gros déploiements

SIP

- *Session Initiation Protocol*, conçu dès 1996 et décrit dans sa forme actuelle par le RFC 3261
- Protocole ayant reçu une large publicité, du fait notamment de son côté « S.I. »
  - Adopté en 2000 par le 3GPP comme protocole de signalisation
  - Utilisation dans de nombreuses autres applications (anciennes messageries instantanées Exchange, souhait de google d'intégrer SIP dans GoogleTalk…)
- Déploiements importants de ce protocole dans les nouvelles infrastructures VoIP

Les composants d'une architecture SIP (1)

- *User-Agent* (UAS+UAC) : les terminaux (softphone, hardphone, ATA…)
- *Registrar* : serveur d'enregistrement (reçoit des messages REGISTER)
- *Location server* : suit les localisations des utilisateurs
- *Proxy server* : relai pour les messages SIP, notamment vers d'autres réseaux
- *Redirect server* : indique aux UA l'adresse à contacter directement

Les composants d'une architecture SIP (2)

- En pratique, ces rôles sont fonctionnels
- Ils correspondent très rarement à des serveurs différents
- Dans les petites infrastructures, l'IPBX assure généralement tous ces rôles

Les messages SIP

- Sur IP, les messages SIP sont véhiculés au travers de datagrammes UDP ou de sessions TCP (si message SIP trop gros ou TLS) sur le port 5060
- Les messages SIP sont en texte ASCII, suivant une syntaxe similaire à HTTP
- Ces messages contiennent un verbe (REGISTER, INVITE, ACK, BYE, CANCEL, NOTIFY…) suivi d'en-têtes et d'un payload optionnel en SDP

Aperçu d'un message, l'INVITE

Verbe invite

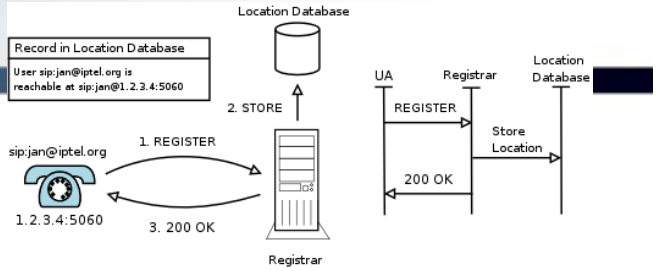
```
INVITE sip:UserB@biloxi.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl
To: LittleGuy <sip:UserB@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 1 INVITE
Contact: <sip:UserA@client.atlanta.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 143

v=0
o=UserA 2890844526 2890844526 IN IP4 client.atlanta.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

En-têtes SIP

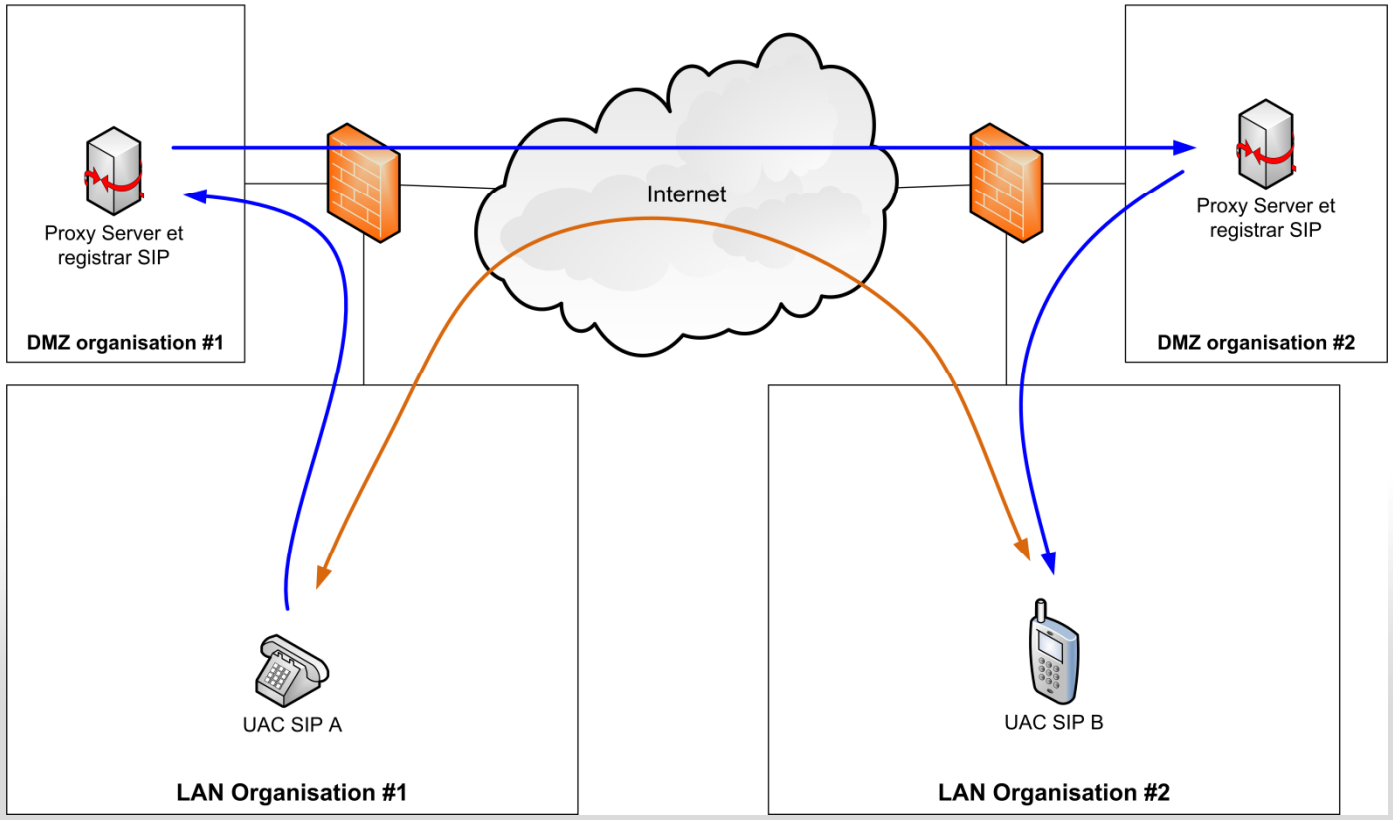
Payload SDP

Topologie réseau cible



Flux SIP d'établissement de session

Flux voix RTP



RTP

- *Real-Time Transport Protocol* est un protocole pour le transport de données temps-réel audio/video sur IP
- Défini dans le RFC 3550 (2003, remplace RFC 1889 de 1996)
- RTP est utilisé dans la plupart des applications VoIP, quelque soit le protocole de signalisation

RTP et RTCP

- L'appellation RTP identifie en fait deux protocoles
  - RTP pour le transport des données temps réel
  - RTCP pour véhiculer des informations de contrôle sur le flux (statistiques pour utilisation QoS)

- Services offerts par RTP / RTCP
  - Identification du type de contenu
  - Séquençage du flux
  - Synchronisation et calcul de gigue (*jitter*)
  - Surveillance du transfert

RTP : Format des paquets

+ Bits	0-1	2	3	4-7	8	9-15	16-31
0	Ver.	P	X	CC	M	PT	Sequence Number
32	Timestamp						
64	SSRC identifier						
96	... CSRC identifiers ...						
96+(CC×32)	Additional header (optional), indicates length "AHL"						
96+(CC×32) + (X×(AHL+16))	Data						

Source: wikipedia

Eléments actifs en RTP

- RTP introduit les éléments fonctionnels suivants :
  - Les *mixers* – systèmes faisant un mixage de flux RTP, typiquement pour les conférences
  - Les *translators* – systèmes réalisant un recodage du flux, typiquement lors de changement de codecs
- En pratique, ces éléments sont implémentés directement dans les IPBX

La VoIP, une opportunité pour la sécurité ?

- Aperçu des protocoles VoIP
- ➢ Attaques et risques en VoIP
- Solutions pour la confidentialité des flux
- Notre retour d'expérience

Taxonomie des risques VoIP

- Disponibilité de l'infrastructure
  - Dénis de service affectant l'ensemble de l'infrastructure
  - Coupure des communications
- Confidentialité de l'infrastructure
  - Ecoute de conversations, des VMB (boites vocales)
  - Accès aux informations de signalisation (appels, taxation)
  - Récupération de l'annuaire d'un poste, de l'ensemble de l'entreprise
- Intégrité de l'infrastructure
  - Création de fausses lignes / faux utilisateurs, ingénierie sociale via ces faux
  - Redirections de lignes
- Abus de service
  - Utilisation frauduleuse des services pour appeler gratuitement
- Utilisation des infrastructures VoIP comme porte d'entrée

Disponibilité

- De loin le risque le plus traité actuellement en VoIP
- Les utilisateurs se sont habitués avec le POTS à des taux de service très élevés
- La VoIP introduit une très grande sensibilité à un certain nombre de services / d'équipement
  - L'énergie
  - Les serveurs registrar, les gateways
  - Ces équipements sont des équipements informatiques, peut-être plus sujets à des bugs que des PBX POTS ?

Intégrité

- La taxation, les journaux sont présent sur le réseau (serveurs SIP), ces informations sont critiques et sont à considérer comme des logs de serveurs sensibles

- L'intégrité des bases registrar doit être protégée, afin d'éviter toute déclaration frauduleuse de ligne
  - Sur des WAN d'entreprises, nous avons vu des registrars avec interface Web pour se déclarer
  - ➢ Il était alors possible i) d'abuser des services de téléphonie de l'entreprise, ii) de mener des attaques de type ingénierie sociale / phishing en se déclarant certaines lignes non prises telles que « admin » ou « CEO »
  - ➢ En somme, le bon vieux coup de l'enregistrement d'une belle adresse admin_hotmail@hotmail.com

Abus de service

- L'ensemble des bonnes vieilles attaques classiques de phreaking sont :
  - Possibles sur la VoIP
  - Automatisables sur la VoIP
- Exemple : les outdials
  - Années 90, utilisation par les phreakers d'outdials, numéros spéciaux sur un PBX permettant de renuméroter vers l'extérieur (appel du PBX via numéro vert 0800.., puis renumérotation gratuite)
  - Maintenant, scan des ports 5060 pour découvrir des proxy SIP utilisables (register blanc, register 1234/1234, pas de register…)
  - Sur Internet, nombreux proxy dans ce cas, certains avec passerelles POTS
  - Exploitation financière en appelant des numéros surtaxés contrôlés par le pirate (*partylines* ou similaire)

Dommages collatéraux

- Les *best practices* recommandent une ségrégation forte entre infrastructures VoIP et reste du réseau
- Cette ségrégation a vocation à limiter la casse à la seule VoIP en cas d'intrusion par là
  - Déjà assez grave comme cela
- En pratique, difficile d'atteindre une ségrégation complète
  - Nécessité de certaines interactions pour pouvoir bénéficier de tous les services de la VoIP (ex: réutilisation de l'Active Directory comme annuaire)
  - La segmentation en VLAN recommandée a comme limite le fait que les téléphones ont souvent un switch interne, et nécessitent donc un port trunk

En pratique

- La ségrégation interne est faite par VLAN
- Les services communs sont placés dans des DMZ
- Des SBC (*Session Border Controllers*) sont placés au niveau des interconnexions VoIP
  - Agissent comme proxy de signalisation et de données
  - Assurent des fonctions avancées de sécurité pour la signalisation et les données (ACL, monitoring…)

La VoIP, une opportunité pour la sécurité ?

- Aperçu des protocoles VoIP
- Attaques et risques en VoIP
- ➢ Solutions pour la confidentialité des flux
- Notre retour d'expérience

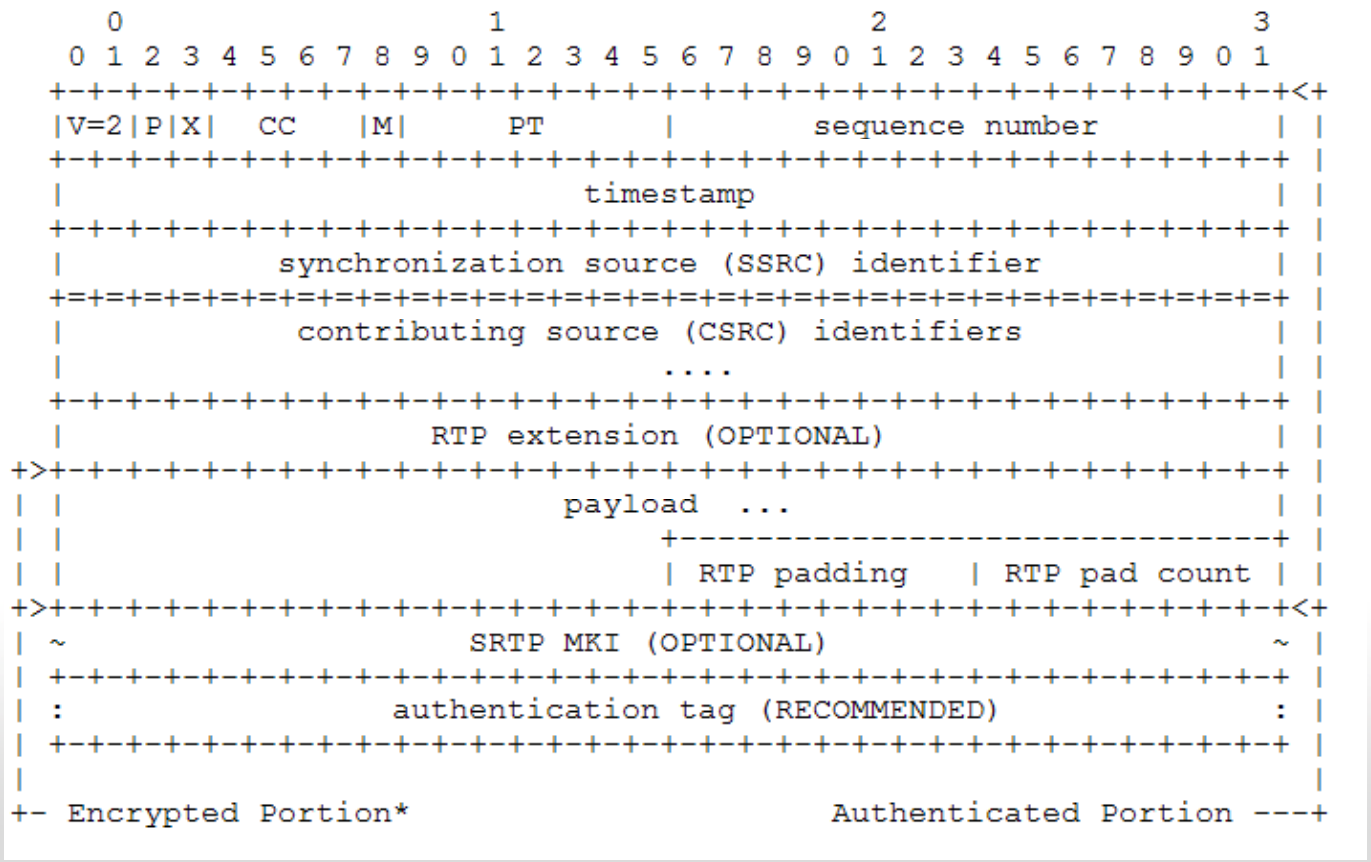
Le besoin de confidentialité

- Les protocoles de signalisation ou de données n'assurent pas la confidentialité des échanges VoIP
- Des extensions existent cependant pour :
  - La sécurisation (=confidentialité, intégrité) des données (SRTP)
  - La sécurisation de la signalisation (SIP + TLS)
- Le SRTP a été le premier protocole développé pour l'occasion

SRTP

- Protocole IETF défini dans le RFC 3711
- Apporte à RTP / RTCP des services de sécurité
  - Chiffrement du flux
  - Authentification des paquets
  - Vérification d'intégrité
  - Anti-rejeu
- Se base essentiellement sur AES, utilisé en mode Counter ou F8 (transforment AES en un *stream cipher*)

SRTP : Format des paquets



Source: RFC

L'établissement de la clef

- Les différentes clefs sont dérivées à partir d'une clef maître
- L'établissement de cette clef maître n'est pas du ressort de SRTP
- La négociation des autres paramètres (algorithmes…) n'est pas non plus du ressort de SRTP

➢ Des protocoles de négociation hors SRTP sont nécessaires pour établir les associations de sécurité

Négocier les SA

- Délicat à concevoir
  - Où placer cette négociation (signalisation, données…)
  - Comment établir ces SA avec le minimum de messages et de latence…
- Solutions diverses, souvent propriétaires
- Quelques-unes se détachent :
  - Tout hardcodé dans la config des téléphones : ne sera même pas décrit… !
  - SDES (SDES ou sdescriptions) : passage des paramètres cryptographiques, y compris la master key, dans le flux SDP
  - MIKEY : protocole d'échange de clef dans le flux de signalisation (SDP)
  - ZRTP : protocole de négociation de clef dans le flux de données RTP

SDES (1)

- RFC 4568 : « Security Descriptions for Media Streams »
- Nouveaux attributs et paramètres SDP pour véhiculer les informations de sécurité SRTP
- Clef transportée en base64 dans l'attribut « crypto » des payloads SDP des messages SIP

```
a=crypto:1 AES_CM_128_HMAC_SHA1_80
  inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9C
  nVubGVz|2^20|1:4 FEC_ORDER=FEC_SRTP
```

SDES (2)

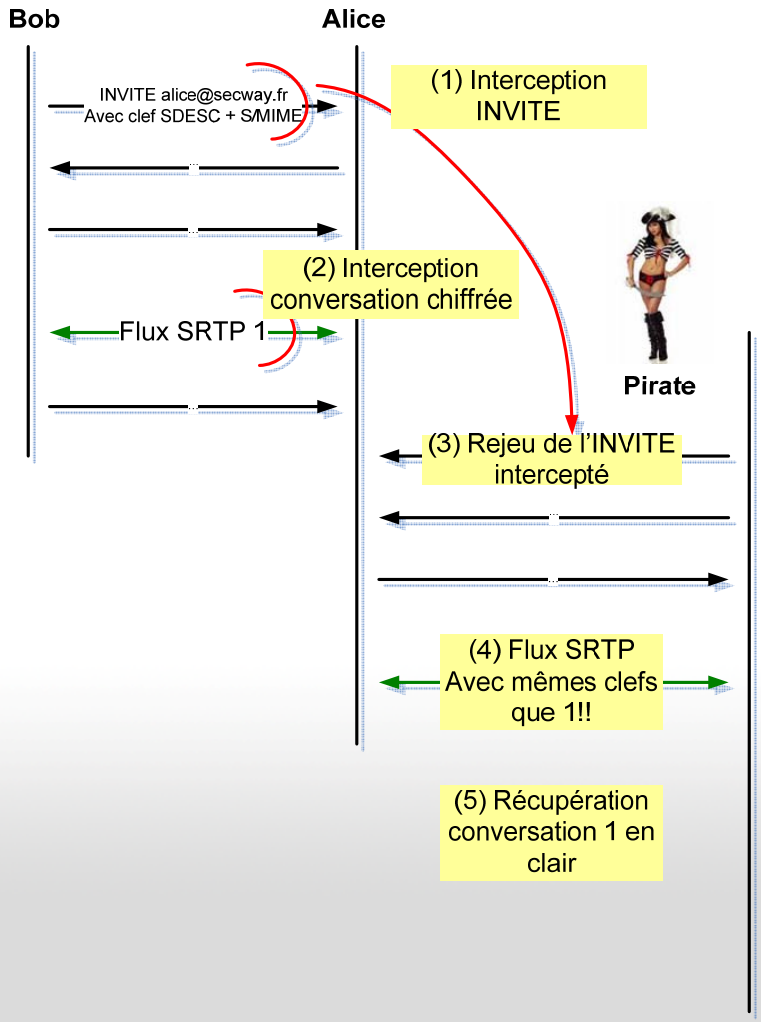
- Nécessité de protéger l'échange SDP (=le flux de signalisation)
- Utilisation courante de TLS pour ce faire -> SIPS
  - Mise en place impossible sans reconfigurer les éléments finaux et centraux
  - SIPS + SDESC offrent une sécurité de proches en proches, non de bout en bout
  - Nécessité d'équipements puissants pour gérer TLS

SDES (3)

- Possibilité d'utiliser S/MIME pour la sécurité de bout en bout

- Si TLS non employé, pas de protection anti-replay, ni sur S/MIME, ni sur SDESC
  - Attaque par rejeu d'un échange S/MIME intercepté, forçant la réutilisation de la même clef maître SRTP
  - Récupération du plaintext original et de la clef (cf. WEP)

SDES (4)



SDES (5)

- Malgré ses problèmes, SDES est largement utilisé, principalement avec TLS :
  - SNOM
  - Broadcom
  - Cisco
  - Counterpath
  - GrandStream
  - Ingate
  - Mitel
  - Covergence
  - …

MIKEY

- Protocole très rapide pour l'établissement de SA dans le cas de flux multimédias.
- Conçu par Ericsson en 2004, décrit dans le RFC 3830
- Dans le cas de SIP, protocole véhiculé au travers de SDP (interfaçage décrit dans RFC 4567 « *Key Management Extensions for SDP and RTSP* »)

Modes de fonctionnement de MIKEY

- Mode PSK (*Pre Shared Key*)
  - Secret partagé établi entre les correspondant préalablement à la conversation
  - La compromission de la PSK amène à la compromission de toutes les conversations précédentes
- Mode *public key*
  - Transmission des paramètres de sécurité via une clef de session, elle-même transmise chiffrée par la clef publique du destinataire
  - Nécessite obligatoirement une PKI
- Mode Diffie-Hellmann authentifié
  - Key agreement par DH authentifié, nécessite là aussi une PKI
  - Par rapport au mode *public key*, permet d'atteindre un PFS
- Nouveau mode DH non authentifié ? (récent, pas étudié)

Merci MIKEY

- MIKEY nécessite dans ses modes intéressants une PKI

➢ Côté vendeurs, complexité dans l'implémentation
  – Gestion par le téléphone de toutes les fonctions d'un 'client PKI'
  – Interaction avec l'utilisateur

➢ Côté utilisateurs, complexité dans la mise en œuvre et l'utilisation

ZRTP

- Protocole pour l'établissement d'une SA SRTP, indépendant du flux de signalisation
- Draft déposé à l'IETF (draft-zimmermann-avt-zrtp-03)
- Implémentation de référence disponible sous licence (libzrtp), mise en œuvre dans logiciel ZFone
- Auteurs :
  - Phil Zimmermann (créateur de PGP)
  - Jon Callas (CTO de PGP Corp)
  - Alan Johnston (co-auteur du RFC3261 (SIP))

Aperçu de ZRTP

- Chiffrement :
  - Utilisation d'un arrangement Diffie-Hellmann pour la négociation de la master key SRTP
  - Pas d'authentification, mais protection anti-MITM par *short authentication string* (SAS)

- Réseau :
  - Multiplexage sur les mêmes numéros de ports que l'échange RTP
  - Protocole clairement différenciable de RTP/STUN, mais possibilité d'envoyer le premier paquet (Hello) dans extension d'un paquet RTP
  - Négociation rapide, 7 paquets avant l'établissement d'une session SRTP

Caractéristiques de sécurité de ZRTP (1)

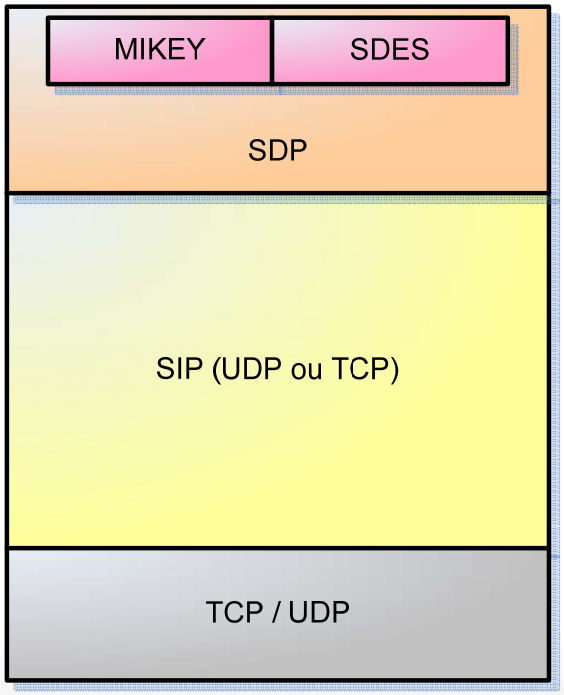
- Négociation en vue d'un SRTP avec :
  - Authentification 32 bits HMAC-SHA1
  - Chiffrement AES-CM, 128 out 256 bits, salt de session 112 bits
- *Perfect Forward Secrecy* – clefs détruites après utilisation
- Structure des messages posée pour limiter bugs de type *overflow*…
  - Tiens, des messages binaires !
  - Partie en ASCII de longueur fixe à 8 octets pour le type de message (spécial Wireshark)

Caractéristiques de sécurité de ZRTP (2)

- Mécanisme anti-MITM : le SAS
  - SAS = base32(cut$_{64bits}$(hash(Hello | Commit | DHPart1 | DHPart2)))
  - Vérification orale par les utilisateurs, le SAS doit matcher des deux côtés
  - Possible système de « cache » pour ne pas avoir à revérifier le SAS à chaque conversation avec correspondant x

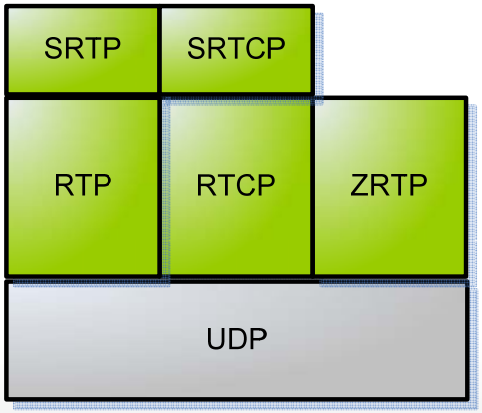
- Attention, ce n'est pas une authentification de l'utilisateur !!!

Stack avec protocoles de sécurité



Stack protocolaire signalisation

- SIP établit une session
- SDP décrit cette session (numéros de ports utilisés…)
- RTCP, RTP, ZRTP, SRTP vont utiliser ces ports
- MIKEY, SDES, ZRTP négocient les algorithmes et clefs pour SRTP



Stack protocolaire données

La VoIP, une opportunité pour la sécurité ?

- Aperçu des protocoles VoIP
- Attaques et risques en VoIP
- Solutions pour la confidentialité des flux
- ➢ Notre retour d'expérience

Le constat

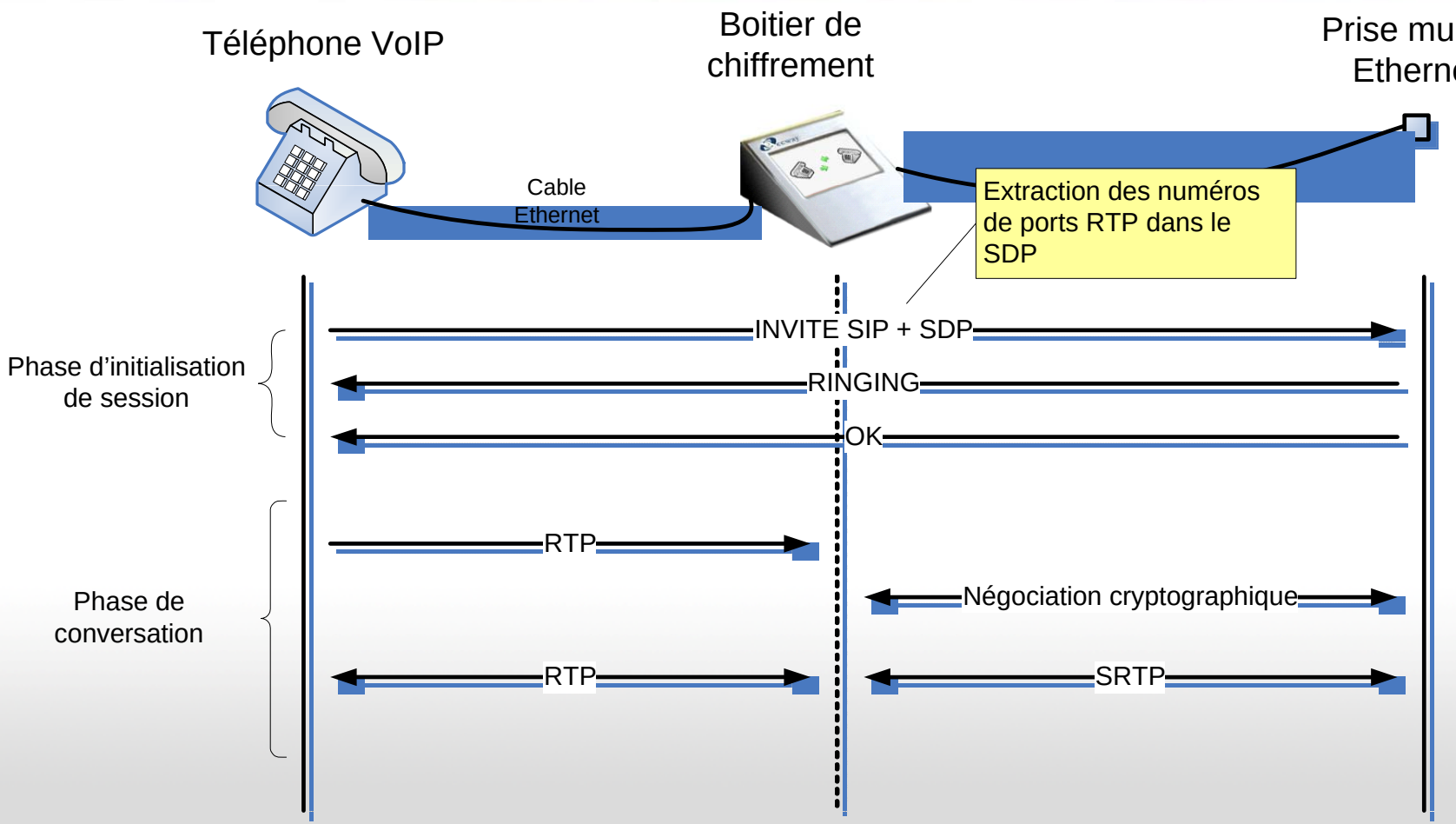
- Nécessité pour certains postes clefs d'une confidentialité forte des échanges
  - Postes de VIP lors d'opérations financières
  - Postes de personnes clefs dans les administrations, entreprises…
- Ce besoin peut surgir rapidement, devant être mis en place sans grand changement de topologie
- Un besoin peut aussi exister pour un dispositif de protection externe, meilleur que le chiffrement natif du téléphone (« qui fait confiance au chiffrement de xxx ?»)

Remplacer par nom de vendeur VoIP américain de votre choix

Notre idée, le cahier des charges

- Réalisation d'un boitier de chiffrement bout-en-bout des conversations VoIP
- Boitier de petite taille (13x7 cm), destiné à être installé sur le bureau de l'utilisateur
- Boitier ne nécessitant aucune configuration
  - Peut être mis en place par un utilisateur non technique, sans intervention des techniciens
  - Le moins intrusif possible, supportant une majorité des protocoles VoIP usuels (SIP, SCCP, H.323, RTP…)
- Affichage de l'état cryptographique via un écran LCD ou similaire

Topologie cible



Réalisation pratique : le matériel

- Nous avons opté pour un développement sur une plateforme embarquée à base de processeur ARM

- Caractéristiques :
  - Carte mère sur étagère, dotée d'un Intel Xscale PXA255, 64 Mo RAM, 16 Mo StrataFlash
  - Deux interfaces Ethernet 10/100
  - La connectique pour un écran LCD (contrôleur inclus dans le CPU)
  - Quelques GPIO pour diverses applications (LED et boutons)
  - Un lecteur MMC pour les mises à jour

- Version CPU 200 MHz abandonnée au profit d'une 499 MHz, car pas assez performante pour soutenir la négociation DH

Le logiciel

- Utilisation d'un OS Linux (kernel 2.6)
- Configuration des interfaces en bridge, pas d'IP
- Utilisation de libnetfilter_queue pour récupérer en userland les paquets de signalisation et de data
- Cœur entièrement en userland

Choix d'architecture

- Nous avons choisi de supporter la signalisation SIP et SCCP
  - Extension possible à H.323… un jour !
- Pour les data, RTP / SRTP étaient incontournable
- Seuls restaient à choisir :
  - Le chiffrement de la signalisation, si besoin
    - Complexité de mise en œuvre d'une solution TLS, qui aurait nécessité potentiellement des changements au niveau des serveurs SIP
    - Si le téléphone parle déjà en TLS, le boitier ne fonctionne plus
  - L'échange de clef pour le SRTP
    - Implémentation de MIKEY et ZRTP

Spécifications techniques

- Support signalisation SIP et SCCP
- Support data RTP en entrée
- Chiffrement en SRTP en sortie
- Négociation de clef par MIKEY ou ZRTP

Les problèmes…

- … car la VoIP, c'est beaucoup de problèmes.
- De nombreux problèmes sont apparus lors des tests
- Ces problèmes sont dus :
  - A la complexité des protocoles, et leur enchevêtrement
  - Au fait que personne (sauf peut-être N. Fischbach?) ne semble avoir de vision globale des protocoles et implémentations VoIP
  - A l'absence de vrai interopérabilité, dès qu'on parle de fonctions avancées

SIP (1)

- SIP est un protocole en texte, similaire à HTTP
- SDP est aussi en texte
- Le nombre d'en-têtes, la variété des extensions et des payloads différents font du parsage de paquet SIP un vrai cauchemar
  - Spécifications SIP : 269 pages
  - 25 pages pour le modèle SDP
  - Plus de 150 drafts pour compléter SIP

SIP (2)

- Exemple d'en-têtes SIP parfaitement équivalents, on notera le nombre de strstr(), strtok(), strcpy(), sscanf(), sprintf() en puissance…

```
Route: <sip:alice@atlanta.com>
Subject: Lunch
Route: <sip:bob@biloxi.com>
Route: <sip:carol@chicago.com>

Route: <sip:alice@atlanta.com>, <sip:bob@biloxi.com>
Route: <sip:carol@chicago.com>
Subject: Lunch

Subject: Lunch
Route: <sip:alice@atlanta.com>, <sip:bob@biloxi.com>,
 <sip:carol@chicago.com>
```

Citation: *today, SIP stands in the market as a 'HTTP similar expandable protocol' but to the developer, stands as a 'Massive hack of spaghetti headers and rules".*

Problèmes avec MIKEY

- MIKEY nécessite une PKI
  - C'est a contrario du caractère simple à mettre en œuvre que nous souhaitions
- MIKEY fait passer l'échange dans le flux de signalisation (dans *offer-answer* SDP du flux SIP)
- Sur certains PABX testés, l'échange MIKEY était enlevé des messages SIP
- La taille des données échangées par MIKEY impliquait d'autre part une utilisation de TCP (et donc un changement de transport UDP -> TCP en cours de négociation SIP)

ZRTP

- ZRTP représente une alternative très alléchante pour son côté léger
- Cependant, tous les problèmes ne sont pas résolus
  - Quid du flux de signalisation, certaines informations pouvant y être utiles pour l'agresseur?
  - Quid de la compatibilité très restreinte, pour l'instant?
  - Quid de l'authentification?

Problèmes avec ZRTP

- Pas d'authentification
  - Est-ce bien grave ?
  - Veut-on une authentification du poste, ou de l'utilisateur ?

➢ Problème principal : la traversée des MG

➢ Ce problème n'est pas uniquement lié à ZRTP, il touche aussi SRTP

Problèmes avec SRTP

- Outre la nécessité d'avoir un *peer* qui parle SRTP, nombreux problèmes liés à SRTP
- Un très important est celui lié aux mixers et translators
- D'un point de vue fonctionnel, l'utilisateur distant est le peer; d'un point de vue technique, le peer peut être une media gateway (mixer, un translator…)

➢ Il est alors impossible de chiffrer, ou alors il faut chiffrer à l'attention de la media gateway

➢ Il faut ensuite faire confiance à la MG

Conclusion

- La VoIP, un domaine complexe de par les protocoles en jeu
- La VoIP présente des risques importants, notamment dus à la menace déjà existante sur les réseaux IP
- Des opportunités de sécurité existent pourtant; les technologies SSI classiques peuvent enfin bénéficier à la voix

Questions ?

Merci pour votre attention !