SÉCURITÉ.ORG

JSSI 2006

Sécurité de la VoIP chez un opérateur

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

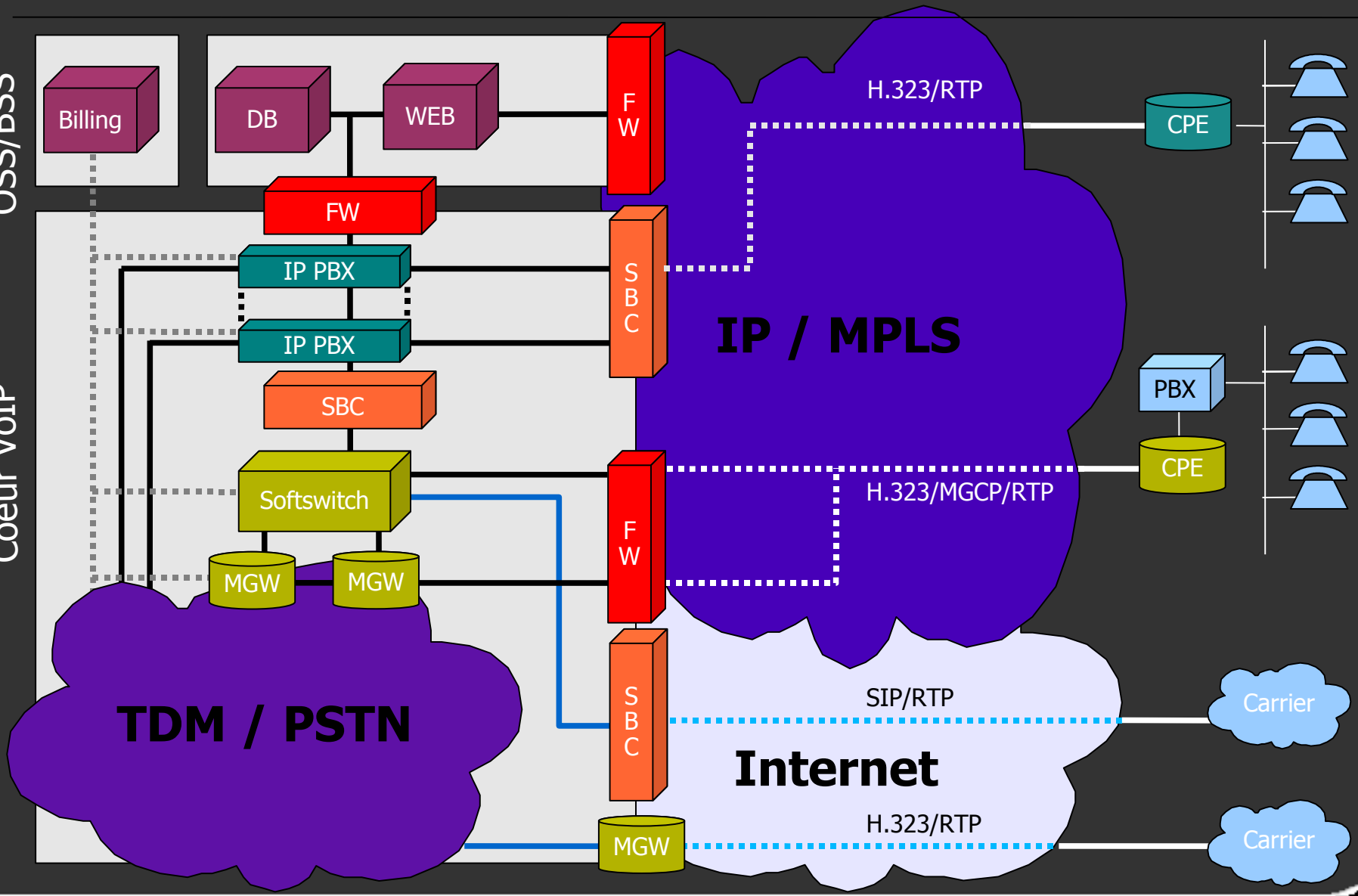
COLT

COLT et la VoIP

- COLT Telecom
  - Services Managés, Voix et Données. FAI “Tier1” en EU
  - 14 pays, 60 villes, 50k clients business
  - 20 000 km de fibre en Europe + DSL
- “Expérience” VoIP
  - 3 vendeurs majeurs:
    - Un “nous venons du monde TDM”
    - Un “nous venons du monde IP”
    - Un “nous sommes une société spécialisée VoIP”
  - VoIP via de l'accès Internet et des VPN MPLS
  - Réseau propre (fibre + DSL) et wDSL
  - Futur PacketCore + NGN + IMS

SÉCURITÉ.ORG

Architecture de réseau VoIP



Protocoles VoIP

- H.323
  - ITU, ASN.1, CPE/Téléphone<->Gatekeeper
  - H.225/RAS (1719/UDP) pour l'enregistrement
  - H.225/Q.931 (1720/TCP) pour la signalisation d'appel
  - H.245 (>1024/TCP – ou via le canal de signalisation d'appel) pour la gestion de l'appel
- MGCP (Media Gateway Control Protocol)
  - IETF, Softswitch (CallAgent)<->MediaGateWay
  - CallAgents->MGW (2427/UDP)
  - MGW->CallAgents (2727/UDP)
  - Utilisé pour contrôler les MGWs
  - AoC (Advise Of Charge) en direction du CPE

Protocoles VoIP

- SIP
  - IETF, “ressemble” à HTTP
  - Voir http://www.securite.org/presentations/voip/EUROSEC2005-SecuriteVoIP-PB-NF-v1.{ppt,pdf}
- RTP
  - Flux multimédia (un dans chaque direction)
  - RTCP: protocole de contrôle pour RTP
  - SRTP: Secure RTP (avec MiKEY)
  - Généralement 16000+/UDP ou plage NAT, mais tout UDP>1024 est possible
  - Soit UA<->UA (risque de fraude), soit UA<->MGW<->UA

Session Border Controller

- Quel est le rôle d'un SBC ?
  - Securité
  - Hosted NAT traversal (mise en conformité de l'en-tête IP et de la signalisation)
  - Convertir la signalisation
  - Convertir le flux multimédia (CODEC)
  - Autoriser RTP de manière dynamique
- Il peut être localisé à différents endroits: client/opérateur, au sein du réseau client, à l'interface entre deux opérateurs (Peering VoIP)
- Que peut-on réaliser avec un pare-feu applicatif ?
- Que peut-on réaliser au niveau système ?
- Existe-t-il un besoin pour un NIDS VoIP (ex: si SIP-TLS)?

Equipement VoIP

- Combinaison matériel+logiciel (surtout des DSPs)
  - Softswitch: généralement dédié à la signalisation
  - MGW (Media Gateway): RTP<->TDM, SS7oIP<->SS7
  - IP-PBX: Softswitch+MGW
- Systèmes d'exploitation
  - OS temps réel (QNX/Neutrino, VxWorks, RTLinux)
  - Windows
  - Linux, Solaris
- Sécurisation par défaut souvent quasi inexistante
- Gestion des mises-à-jour:
  - Les OS sont rarement à jour
  - Les mises-à-jour ne sont pas “autorisées”

Sécurité VoIP: challenges

- Protocoles VoIP
  - La VoIP ne se limite pas à SIP
  - SIP est porteur (services IMS et nouveaux CPEs)
  - H.323 et MGCP dominent le monde des opérateurs
- Quelles problématiques ?
  - Les dialectes VoIP
  - Il existe que quelques piles VoIP (OEM/vulnérabilités)
  - Les pare-feux et SBCs résolvent-ils des problèmes ou introduisent-ils de la complexité ?
  - Créons-nous des portes dérobées dans les réseaux de nos clients ?
  - CPS et QoS

Impact des dialectes VoIP

- Impossible de sécuriser le traffic (tout particulièrement sans gestion de session) en fonction de l'inspection du protocole de signalisation
- Certains vendeurs n'ont jamais entendu parler de gestion de *timeouts* et n'envoient pas de *keep-alives*
- Résultat :
  - Intelligent:
    `permit UDP <plage de ports> <systèmes identifiés>`
  - A moitié: `permit UDP <ports>1024> any`
  - Pas du tout: `permit UDP any any`
- Résultat final :
  - Compromission via des services UDP exposés
  - Besoin de services RPC (>1024/UDP) ?

Interception (légale) de trafic

- Lawful Intercept
  - Réutilisation de solutions existantes: TDM break-out
  - Déployer un *sniffer* (flux signalisation et média)
  - Rerouter les appels (en le masquant dans la signalisation)
- Interception/Ecoute
  - Risque faible (réseau propre)
  - Réseau d'entreprise : stratégie globale
    - E-mail en clair
    - Protocoles non chiffrés (HTTP, Telnet, etc)
    - VoIP non chiffrée
    - Etc
  - vomit, YLTI, VOIPONG, scapy (VoIPoWLAN) : relativement facile de démontrer l'insécurité

Les téléphones

- Faire “planter” des téléphones IP
  - Ce n'est pas une nouvelle :)
  - Relativement facile (pile TCP/IP peu résistante et implémentations pleines de failles)
  - Attaquant interne:
    - Serveur DHCP
    - Serveur TFTP (configuration du téléphone)
    - Identifiants (login + PIN)
- La VoIP n'implique pas une migration vers des IPPhones
  - PBX avec une E1 (PRI/BRI) avec le routeur puis VoIP
  - PBX avec une interface IP vers le monde extérieur (est-ce sérieux de connecter son PBX à l'Internet) ?
  - Implique de maintenir deux réseaux, mais solution pour la QoS sur le LAN
  - Et les clients logiciels ?

A tenter à la maison :)

- Beaucoup de téléphones avec PoE
- Echange CDP: VLAN + information PoE
- Que se passerait-il avec un vers qui dirait au commutateur d'envoyer 48V à une interface Ethernet non PoE ?

Risque de déni de service

- DDoS génériques
  - Pas vraiment un problème, notre coeur VoIP n'est pas atteignable depuis l'extérieur
  - Eviter des ACLs, préférer "*edge-only BGP blackholing*"
  - Nous avons l'habitude des "gros" DDoS :)
- Les dénis de services plus problématiques:
  - Générés par les clients: bonne traçabilité
  - DoS applicatif : H.323 / MGCP / SIP
    - Remplacer le CPE / utiliser un client logiciel
    - Injecter du bruit dans la signalisation en-bande (commandes MGCP, messages TKIPs H323, etc)
    - Forcer la machine d'état du mécanisme d'inspection dans un état instable ou bloquant: par chance pour les adresses serveurs et non le client

La sécurité applicative

- Services en ligne
  - Call Management (console opérateur)
  - IN routing
  - Reporting / CDRs
- Risques de sécurité
  - Fonctionnalités "*Multi-tenant*"
  - Beaucoup de vendeurs n'ont jamais entendu parler de sécurité applicative
  - Pourquoi tenter de sécuriser ou de déployer des plates-formes d'interception légale si un gamin peut rerouter vos appels par injection SQL
- Réel besoin de pare-feux pour applications web

Sécurité VoIP: deux mondes

- TDM / VoIP : deux mondes, deux royaumes, un futur ?
  - Sécurité par obscurité / complexité vs le monde IP
  - Détection de fraude
- Nouveaux risques
  - Nouvelle surface d'attaque pour les réseaux historiques
  - Pas de fonctionnalités de sécurité dans les vieux commutateurs
  - Pas de journaux, pas de fonctions d'audit, plus de lignes physiques
  - Les gens: Voice Engineers vs Data Engineers vs Security engineers. Engineering vs Operations. Marketing vs Engineering. Conflits et Time-to-Market

Attaquer les NMS/Opérations

- La VoIP est très complexe
- Le seul moyen de résoudre la majorité des problèmes: ingénieur Voix + ingénieur IP/Données + ingénieur Sécurité sur le même pont téléphonique / chat en ligne
- Pré-requis: pouvoir *sniffer* le trafic
- Outil: Ethereal (ou équivalent)
- Attaquant: utiliser une faille dans un des décodeurs
- Sniffer sur port mirroir en R/O dans une DMZ dédiée avec uniquement VNC/SSH
- Si l'attaquant arrive à télécharger un rootkit via RTP: offrez lui un poste d'administrateur système ;-))

Sécurité VoIP entre opérateurs

- Aka “VoIP peering” / Carrier interconnect
- Existe déjà (connectivité TDM pour des opérateurs VoIP/Skype{In, Out})
- Connectivité: Internet, IX (public/private), VPN MPLS ou VPLS (Ethernet)
- Pas de service VPN MPLS de bout-en-bout, pensez à “casser” le VPN et utiliser une interface IP-IP
- Masquez votre infrastructure (*topology hiding*), utilisez le {white, black}listing et vérifiez que seul l'autre opérateur peut s'interfacer avec vous
- Conversion de la signalisation et du flux multimédia (SBC)

Chiffrement / Authenfication

- Devons nous l'introduire ?
- Vendeur X: “Compliant”. Bien sûr.
- Vendeur Y: “C'est sur notre roadmap”. Q1Y31337 ?
- Vendeur Z: “Pourquoi en avez-vous besoin ?”. Hmmm...
- IPsec entre le CPE et le coeur VoIP
  - Envisageable (CPE avec CPU récente ou carte de chiffrement)
  - Comment traiter le traffic RTP CPE<->CPE ?
  - RTT reste correct et dans la fenêtre de gestion d'écho
- Solution plus probable: nomade <- IPsec -> coeur VoIP
  - L'attaquant ne peut se focaliser que sur le VPNC
  - Pas d'impact sur les clients connectés directement

Futur : Services IMS

- IMS = IP Multimedia Subsystem
- (Mauvais) souvenir: les opérateurs GSM et leurs réseaux WAP et 3G
- Très/trop ouverts (le téléphone est considéré sûr)
- Interconnexion avec leur réseau interne voire IT
- Services IMS avec les MVNOs, 3G/4G: architecture d'une complexité incroyable avec beaucoup d'interfaces
- Mise en place de pare-feux: complexe voire impossible

Sécurité VoIP chez un opérateur

- Conclusion
- Q&R