Sécurité des architectures de Convergence Fixe-Mobile (FMC)

Symposium sur la Sécurité des Technologies de l'Information et des Communications

Laurent BUTTI
Orange Labs

Agenda

- Direction tout-IP et convergence fixe-mobile (FMC)
- Les technologies FMC et leurs mécanismes de sécurité
  - Unlicensed Mobile Access (UMA)
  - Interworking Wireless Local Area Network (I-WLAN)
  - IP Multimedia Subsystem (IMS)
- Déployer au mieux ces nouvelles architectures
  - Normalisation, audits de sécurité, recherche de vulnérabilités...

Contexte

Contexte

- Recherche de nouveaux usages (et donc de services)
  - Messagerie unifiée
  - Messages multimédias
  - Softphones
- Convergence des équipements
  - PDAs, téléphones, lecteurs multimédias...
- Nouveaux acteurs privilégiant les solutions « IP »
  - Moins coûteuses au déploiement (?)
  - Moins coûteuses à l'appel (?)
  - Évolutives sur les services (?)

Fixed Mobile Convergence (FMC)

- Mutualiser les accès et services (fixes et mobiles) sur un même terminal (mobile !)
  - Messagerie unifiée, facture unique
- Les buts sont (toujours) les mêmes
  - Apport de nouveaux services (source de revenus)
  - Réduction des coûts de déploiement et d'exploitation
  - Extension de la couverture radioélectrique
  - Unicité du terminal

Fixed Mobile Convergence (FMC)

- Nombreuses opportunités techniques pour les opérateurs
  - Extension de la couverture radioélectrique GSM / UMTS
    - PicoBTS et FemtoCell
  - Unlicensed Mobile Access (UMA)
  - Interworking Wireless Local Area Network (I-WLAN)
  - IP Multimedia Subsystem (IMS)
- Un support naturel est le Wi-Fi
  - Ubiquité de la technologie
  - Bas coûts

Fixed Mobile Convergence (FMC)

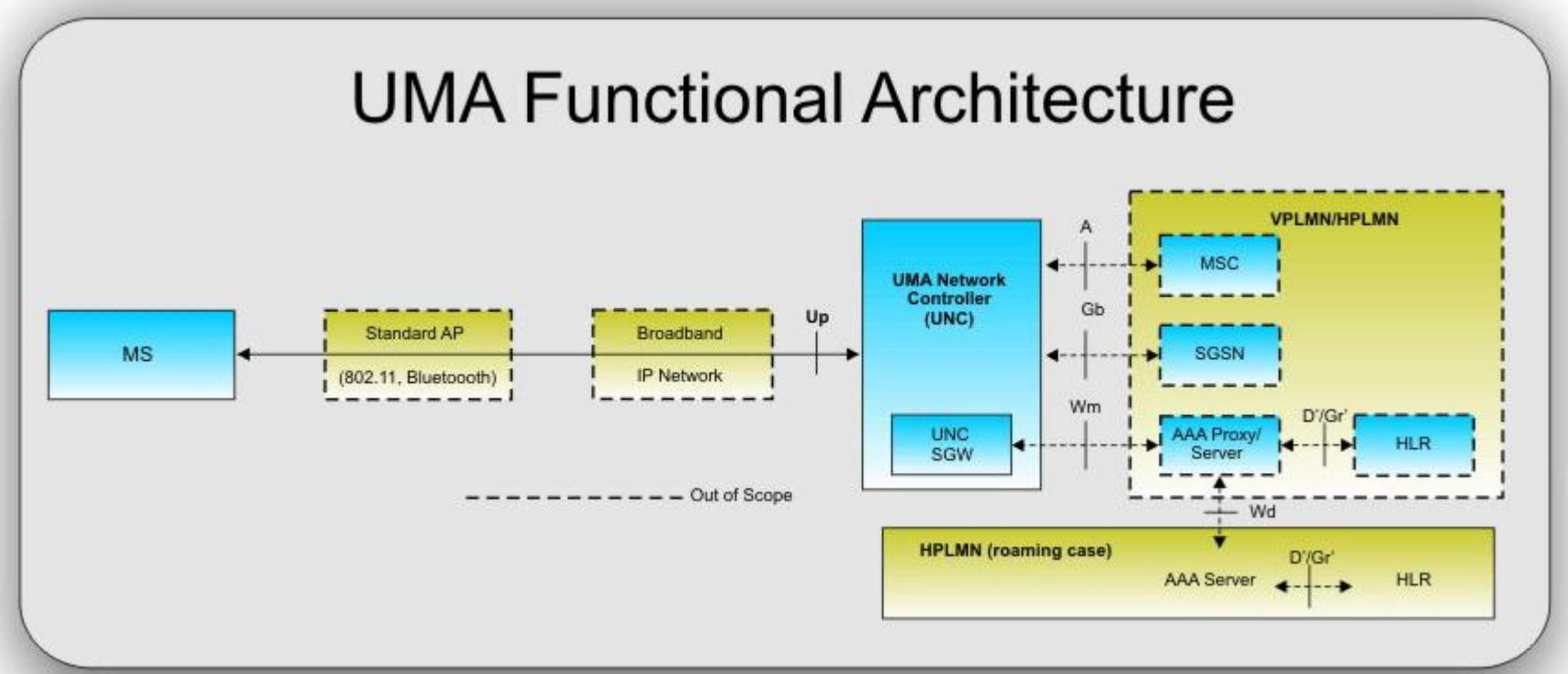
- Premiers tests opérationnels au Danemark (1999)
  - Offre « Duet » de TDC
  - Messagerie unifiée pour GSM / {PSTN | ISDN}
- Première offre commerciale (2005)
  - Offre « BT Fusion » : téléphone bi-mode Bluetooth / GSM
    - Technologie UMA au-dessus de Bluetooth
- Démocratisation en cours en France
  - Après le « Triple-Play », le « Quadruple-Play » ?
  - Technologie GSM / UMA
    - Offre UNiK d'Orange
  - Technologie GSM / Wi-Fi+SIP
    - Offres TWIN de Neuf Cegetel et FreeBox de Free

Architectures
Convergence Fixe-Mobile

Unlicensed Mobile Access

- Extension des services GSM/GPRS
  - Generic Access Network (GAN) par le 3GPP (R6)
  - Spécifiée par un groupe d'opérateurs et constructeurs
    - http://www.umatechnology.org/participants/index.htm
  - Spécifications initiales en septembre 2004
- Intégration de protocoles GSM/GPRS au-dessus d'IP
- Avantages
  - Utilisation d'une bande de fréquence sans licence (Wi-Fi, Bluetooth)
  - Extension de la couverture GSM/GPRS sans coûts d'infrastructure

Unlicensed Mobile Access



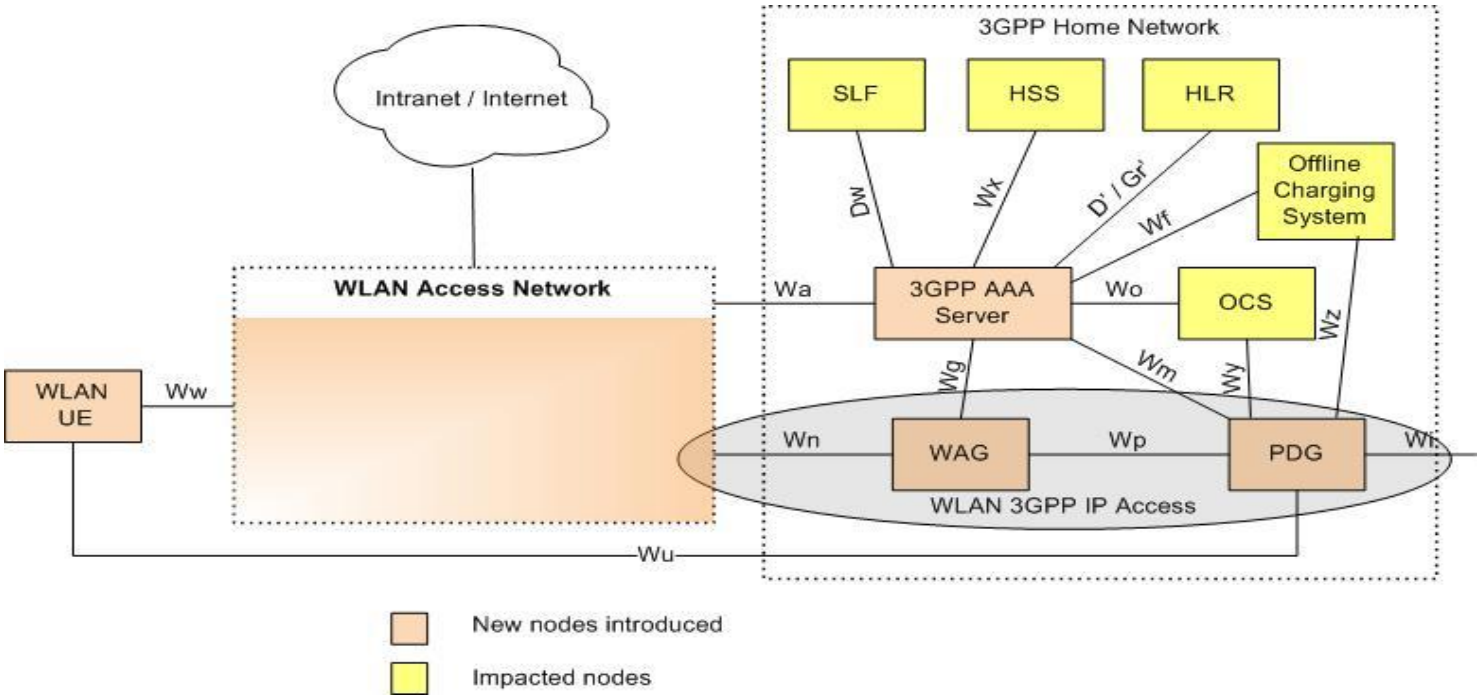
Source : UMA Specifications

Unlicensed Mobile Access

- Internet Key Exchange v2 (IKEv2) : authentification et SA IPsec
  - Authentification UMA Network Controller (UNC) par certificat
  - Authentification utilisateur et réseau par Extensible Authentication Protocol
    - Subscriber Identity Module (EAP-SIM)
    - Authentication and Key Agreement (EAP-AKA)
- IPsec entre le terminal et l'UNC
- Couche de sécurité indépendante de la couche accès réseau

I-WLAN (3GPP R6)

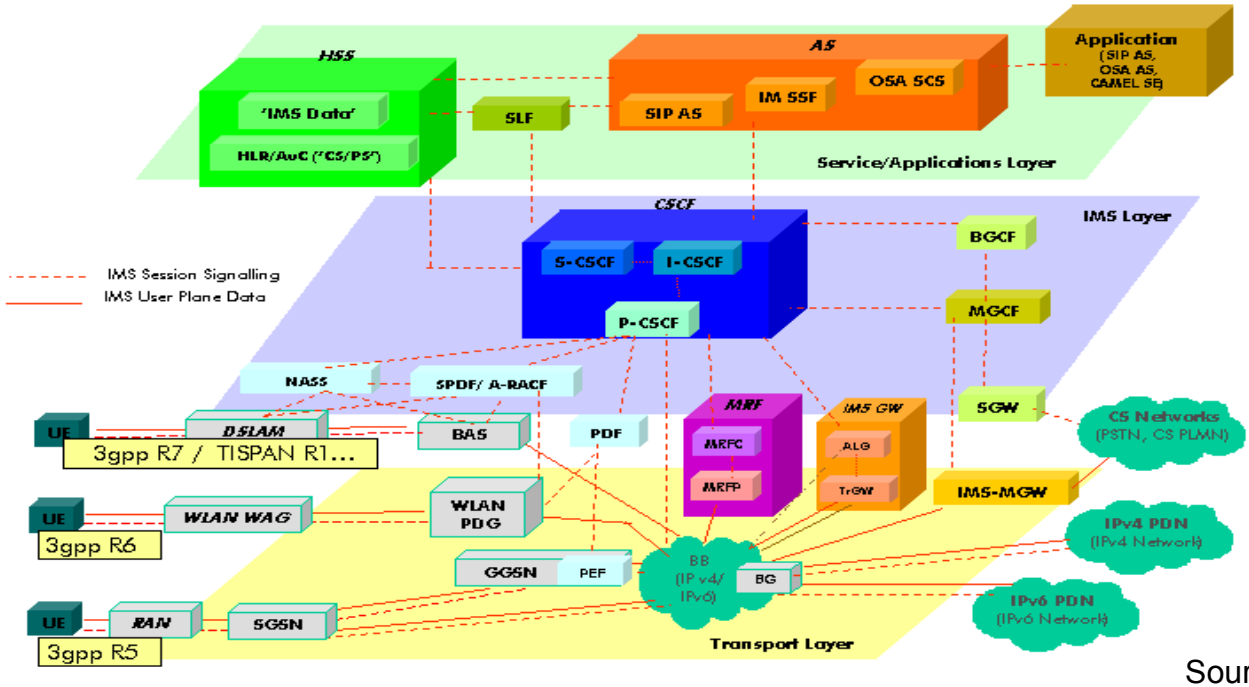
- Accès reposant sur EAP-SIM et/ou EAP-AKA



Source : 3GPP

IMS (3GPP R5)

- Repose sur la sécurité des couches d'accès
- Signalisation basée sur Session Initiation Protocol (SIP)



Source : 3GPP

Sécurité des architectures Convergence Fixe-Mobile

Principe de précaution

- Amélioration de la sécurité des architectures FMC
  - Suivi de standardisation
  - Ingénierie d'architecture réseau
  - Audits de sécurité
  - Développement de nouveaux outils de tests d'implémentations
    - Sur de nouvelles technologies, les outils existants sont inefficaces

Clé de voûte de la sécurité : l'accès

- Points communs à de nombreuses technologies FMC
  - IKEv2
  - EAP et méthodes EAP-SIM / EAP-AKA
  - IPsec
- Accessibles pour tout utilisateur non authentifié
- Risque fort : faille d'implémentation
  - Déni de service
  - Exécution de code arbitraire à distance
- Peu de travaux publiés

Recherche de vulnérabilités

- Reverse engineering
  - Nécessite des compétences pointues et beaucoup de temps
  - Certains environnements sont contraignants (embarqué, pas de symboles...)
- Audit de code source
  - Nécessite d'avoir le code source
  - Peut-être aussi très complexe
- Injecter des données et étudier le comportement de l'application
  - Fonctionne aussi bien en boite noire qu'en boite blanche
  - Focalisé sur les entrées contrôlées par l'attaquant

Recherche de vulnérabilités

- Découverte ET correction
  - Processus d'amélioration !
- Ne pas oublier les intérêts autour des vulnérabilités
  - Vulnérabilité découverte par une personne externe
    - Communication avec l'éditeur de logiciel pour correction et publication
    - Revente de la vulnérabilité à une société tierce pour communication avec l'éditeur de logiciel (intermédiaire)
    - Revente de la vulnérabilité à des tiers pour exploitation
    - La garder pour soi
    - ...
- D'où l'intérêt de faire de la recherche en vulnérabilités
  - Trouver les failles avant que des tiers n'y aient accès !

Fuzzing

- Fuzzing : terme difficilement traduisible !
  - Fuzz testing or fuzzing is a software testing technique that provides random data ("fuzz") to the inputs of a program. If the program fails (for example, by crashing, or by failing built-in code assertions), the defects can be noted. *Source : Wikipedia.org*
  - Fuzz testing or Fuzzing is a Black Box software testing technique, which basically consists in finding implementation bugs using malformed/semi-malformed data injection in an automated fashion. *Source : OWASP*
- Recherche d'erreurs d'implémentation logicielle par injection de données invalides
- Existe officiellement depuis 1989 (Barton Miller)

Fuzzing

- Le fuzzing a une approche meilleur rapport qualité / prix
- Le fuzzing n'a pas de problèmes de faux positifs
- Le fuzzing a (généralement) tendance à découvrir des erreurs d'implémentation simples (quoique...)
- Le fuzzing doit être (généralement) « intelligent » pour chercher aux endroits les plus pertinents
  - Pour une efficacité accrue il faut connaître l'implémentation à tester
- Le fuzzing n'est pas une assurance qualité !
  - N'assure pas l'absence d'erreurs d'implémentation

Recherche de vulnérabilités dans les implémentations IKEv2 et EAP

État de l'art des vulnérabilités sur les implémentations IKEv2 et EAP

- IKEv2
  - CVE-2008-4551 : StrongSWAN
- EAP
  - CVE-2007-5651 : Authenticator (Cisco IOS) (*)
  - CVE-2008-2441 : AAA (Cisco Secure ACS) (*)
  - CVE-2008-5563 : Authenticator (Aruba Mobility Controller)
- Méthodes EAP
  - CVE-2004-1459 : LEAP (Cisco Secure ACS)
  - CVE-2006-1354 : EAP-MSCHAPv2 (FreeRADIUS)
  - CVE-2007-2028 : EAP-TTLS (FreeRADIUS)

(*) découvertes lors de nos recherches

Hypothèses initiales

- Implémentations propriétaires et environnements propriétaires
  - Boite noire : tests de vérification de bon fonctionnement par stimulus réseau
- Protocoles réseaux avec des mécanismes cryptographiques
  - Fuzzing aléatoire non pertinent : approche par modélisation de protocole
- Protocoles avec différents états
  - Atteindre les différentes parties de l'implémentation testée
- Risques critiques côté réseau
  - Recherche de vulnérabilité côté réseau (i.e. pas côté client)

Fuzzing IKEv2

```
Initiator                                   Responder
-----------                                 -----------
 HDR, SAi1, KEi, Ni      -->

                         <--        HDR, SAr1, KEr, Nr

 HDR, SK {IDi, [CERTREQ,]
         [IDr,] AUTH, SAi2,
          TSi, TSr}      -->

                         <--        HDR, SK {IDr, [CERT,] AUTH,
                                             EAP }
HDR, SK {EAP}            -->
                         <--        HDR, SK {EAP (success)}

HDR, SK {AUTH}           -->
                         <--        HDR, SK {AUTH, SAr2, TSi, TSr }
```

Fuzzing IKEv2

- Génération des tests par modélisation de protocole
  - Basé sur Sulley Fuzzing Framework
- Fuzzing avec heuristiques
  - Bytes, words, strings...
- Montée des états
  - IKE_SA_INIT
  - IKE_AUTH

Fuzzing IKEv2

- Étapes de la conception du fuzzer
  - Étude du protocole IKEv2
  - (Optionnel) Étude des implémentations IKEv2
  - Modélisation du protocole IKEv2
  - Modélisation du changement des états IKEv2
  - Choix du test de vérification de bon fonctionnement
  - Tests sur quelques implémentations
  - Améliorations à réaliser en fonction des différentes implémentations testées

Fuzzing IKEv2

- Démonstration !

Fuzzing IKEv2

- Implémentations testées
  - Racoon2 20090327c
  - StrongSWAN 4.3.0
  - OpenIKEv2 0.5
  - Six implémentations propriétaires

- Implémentations vulnérables (un ou plusieurs bugs)
  - Fuzzing IKE_SA_INIT 3 sur 9 (~ 30 %)
    - StrongSWAN, OpenIKEv2 et une propriétaire
  - Fuzzing IKE_AUTH 4 sur 7 (~ 60 %)
    - StrongSWAN, OpenIKEv2 et deux propriétaires

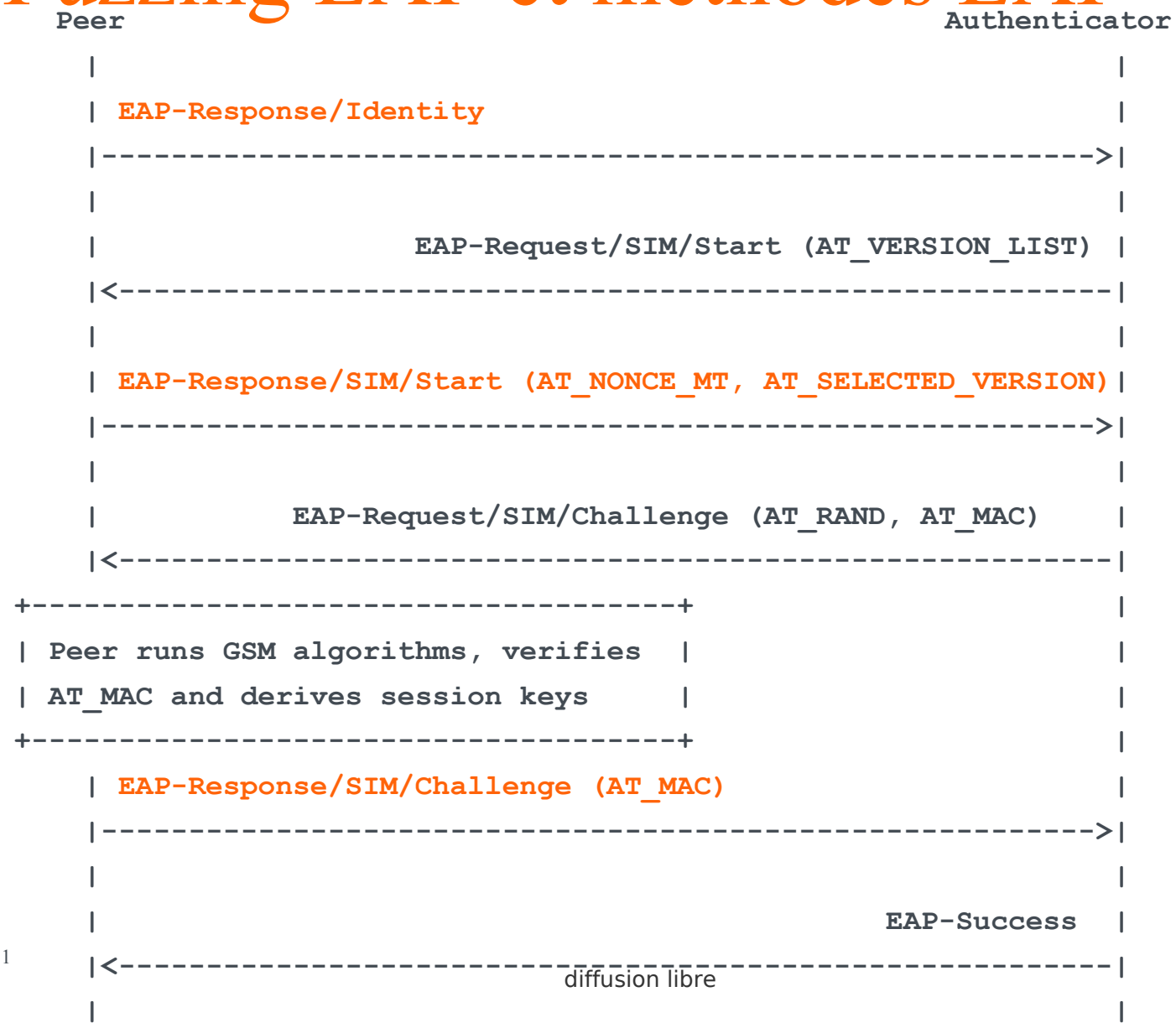
Fuzzing IKEv2

- Exploitabilité des failles découvertes ?
- L'exploitabilité est un mélange de théorique et de pratique
  - Conditions techniques du déclenchement de la faille
  - Environnement (architecture matérielle, système d'exploitation...)
  - Aspects pratiques (boite noire, pas de debug...)
- StrongSWAN 4.3.0
  - Deux failles découvertes et reportées (corrigées dans la 4.3.1)

Fuzzing EAP et méthodes EAP

- Extensible Authentication Protocol (RFC 5247)
  - Transport de méthodes d'authentification
  - Utilise les secrets dérivés par les « méthodes » d'authentification
- Méthodes EAP-SIM (RFC 4186) et EAP-AKA (RFC 4187)
  - Authentification mutuelle
  - Algorithmes GSM (carte SIM) ou AKA (carte USIM)

Fuzzing EAP et méthodes EAP



Fuzzing EAP et méthodes EAP

- Génération des tests par modélisation de protocole
  - Basé sur Sulley Fuzzing Framework
- Fuzzing avec heuristiques
  - Bytes, words, strings...
- Volonté d'une architecture générique pour le fuzzing EAP
  - Fuzzer l'implémentation EAP dans le serveur RADIUS
  - La méthode de transport peut être multiple
    - 802.1X, IKEv2, WiMAX...
- Agir en tant que client RADIUS et supplicant EAP

Fuzzing EAP et méthodes EAP

- Implémentations testées
  - FreeRADIUS avec EAP-SIM
  - Une implémentation propriétaire avec EAP-SIM
- Pas de découverte d'erreur d'implémentation sur les implémentations EAP-SIM
- Une vulnérabilité découverte sur une implémentation EAP
  - CVE-2008-2441 (Cisco Secure ACS)

Retour d'expérience

Difficultés rencontrées

- Modèles intrinsèquement limités et complexes à élaborer
- Détection par stimulus réseau intrinsèquement limitée
- Seuls certains bugs sont détectables en boite noire
- En boite noire l'analyse des bugs reste très approximative
- Certains bugs dépendent d'une séquence de paquets
- Génération automatique d'exploit compliquée si états à monter

Dans notre cas, à propos du fuzzing...

- Le fuzzing n'est pas susceptible aux faux positifs
- Le fuzzing ne s'attarde qu'à des entrées contrôlables
- Toujours intéressant sur des protocoles récents et peu étudiés
- Vulnérabilités (aussi) trouvables par « hasard »
  - Fuzzers de parsers qui trouvent des vulnérabilités d'implémentation de machine à état !

So what?

Conclusions

- Les technologies FMC reposent sur des briques robustes
- L'ingénierie réseau doit être teintée de sécurité
- Les déploiements doivent être audités
- Les implémentations doivent être auditées et / ou fuzzées
- Nos fuzzers ont permis de découvrir quelques vulnérabilités
  - Malgré les hypothèses initiales
- Le fuzzing doit s'intégrer dans une démarche « software testing »

Remerciements

- Gabriel Campana pour ses travaux sur le sujet

Merci !

Annexes

Fixed Mobile Convergence (FMC)

- Next Generation Network (NGN)
  - A Next Generation Network (NGN) is a packet-based network able to provide services including Telecommunication Services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users. *Source : International Telecommunication Union*

- Quels que soient les supports réseaux
  - Fixe, mobile et sans-fil

- Interconnexions avec le réseau téléphonique standard
  - Par l'intermédiaire de passerelles

Fixed Mobile Convergence (FMC)

- IP Multimedia Subsystem (IMS)
  - Architecture fonctionnelle pour unifier les modes mobile et Internet
  - Intégré dans la 3GPP Release 5
  - Utilisation autant que possible des protocoles IETF
    - SIP

- Le tournant des telcos vers le tout-IP est bien entamé
  - Reste à bien le négocier...

Autres technologies...

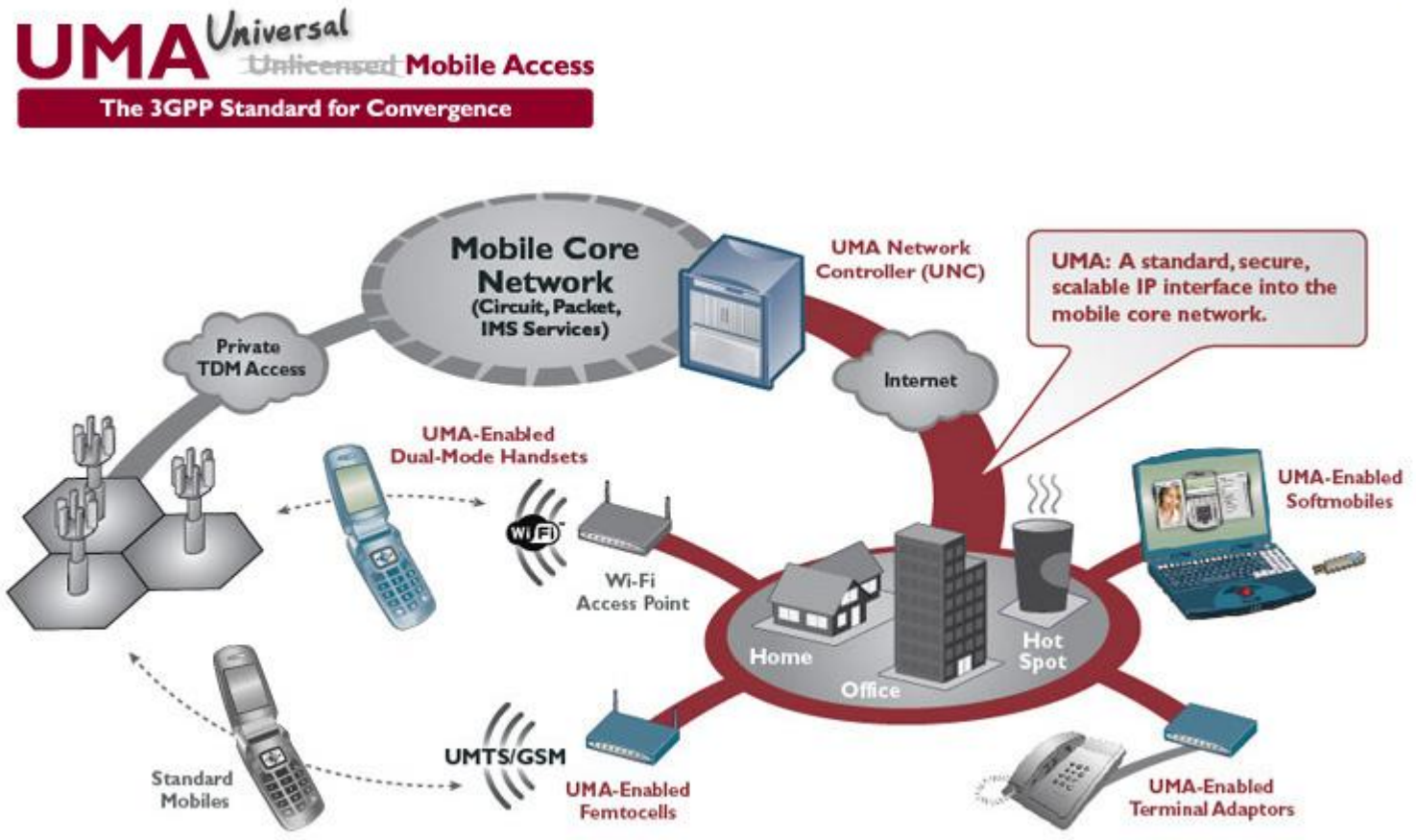
- Skype Phone
  - Première version publique (bêta) en 2003
  - Appels entre usagers Skype gratuitement
  - Appels vers lignes téléphoniques fixes et cellulaires pour un coût

- GPhone / Android
  - The Open Handset Alliance, a group of more than 30 technology and mobile companies, is developing Android: the first complete, open, and free mobile platform. *Source : Google*

Fixed Mobile Convergence (FMC)

- De nombreuses contraintes techniques
  - Besoin de technologies Wi-Fi à basse consommation
    - « Always-On » pour la téléphonie
  - Nécessité de réaliser le « handover » inter-technologies
    - GSM / Wi-Fi+SIP et GSM / UMA
  - Nécessité d'une qualité voix au moins équivalente au GSM

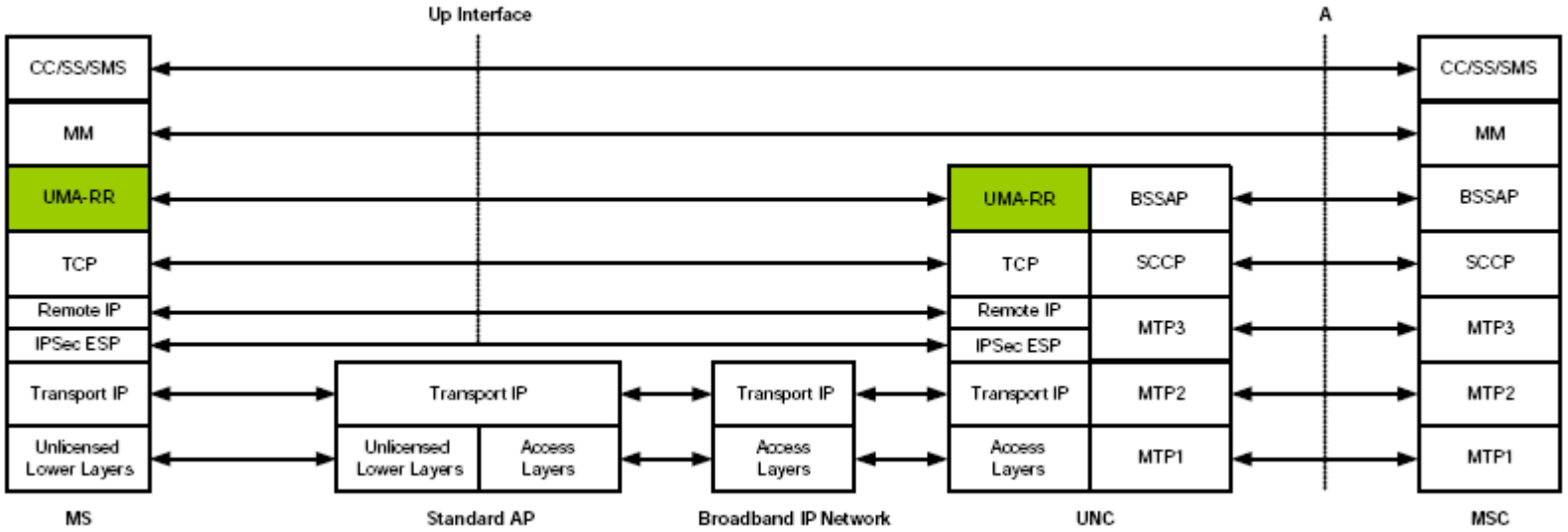
Unlicensed Mobile Access



Source : UMA Forum

Unlicensed Mobile Access

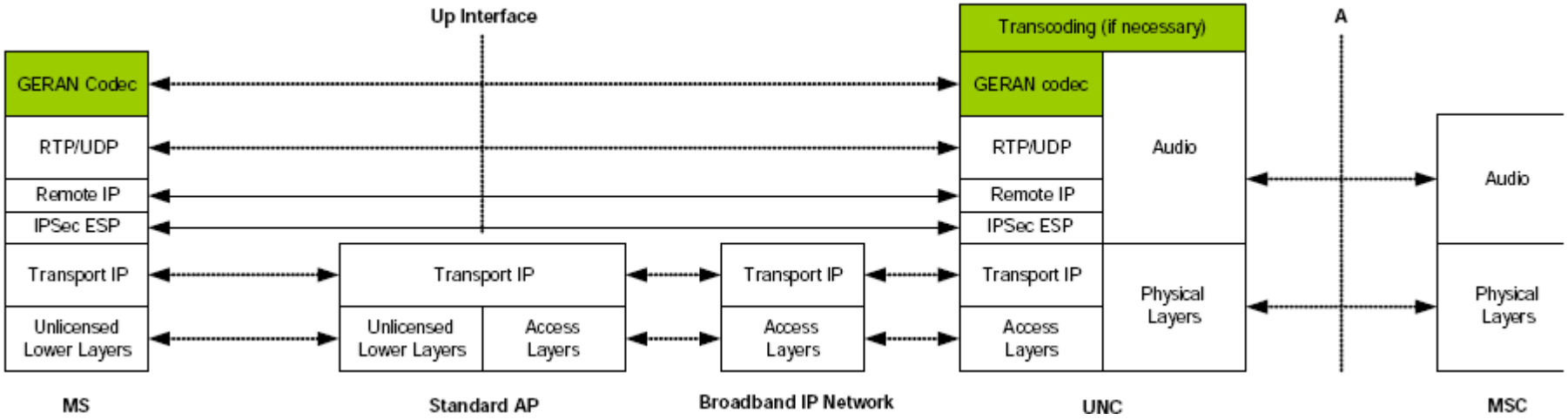
- Up CS Domain Signaling Protocol Architecture



Source : UMA Specifications

Unlicensed Mobile Access

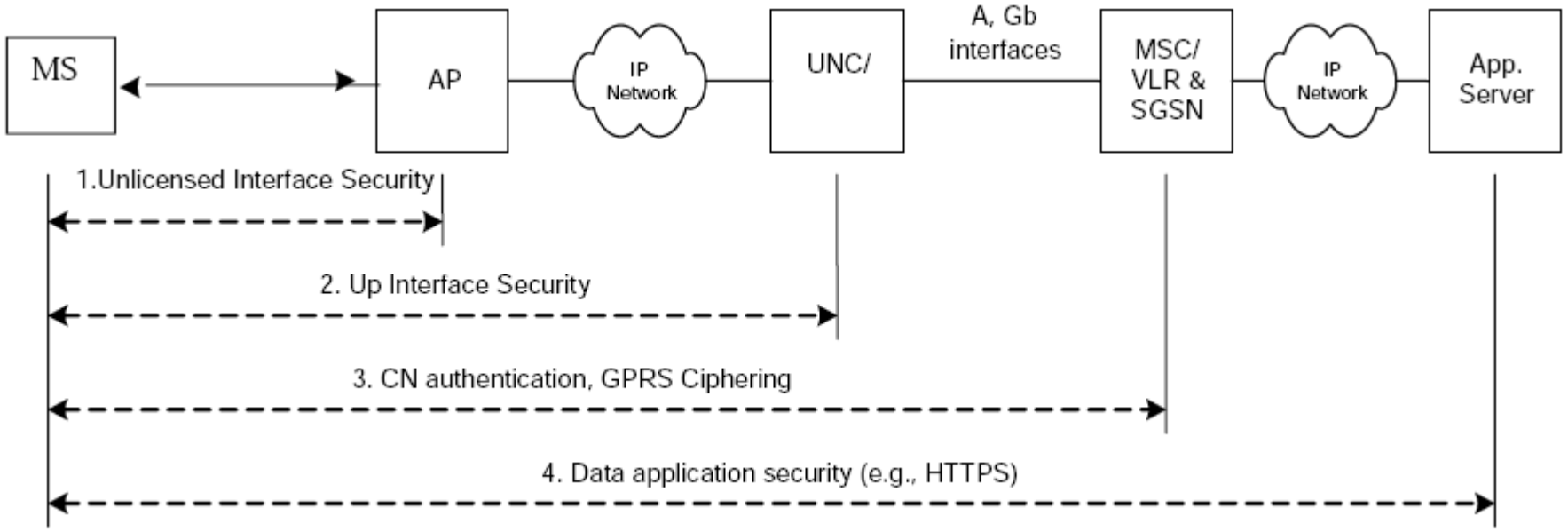
- Up CS Domain Voice Bearer Protocol Architecture



Source : UMA Specifications

Unlicensed Mobile Access

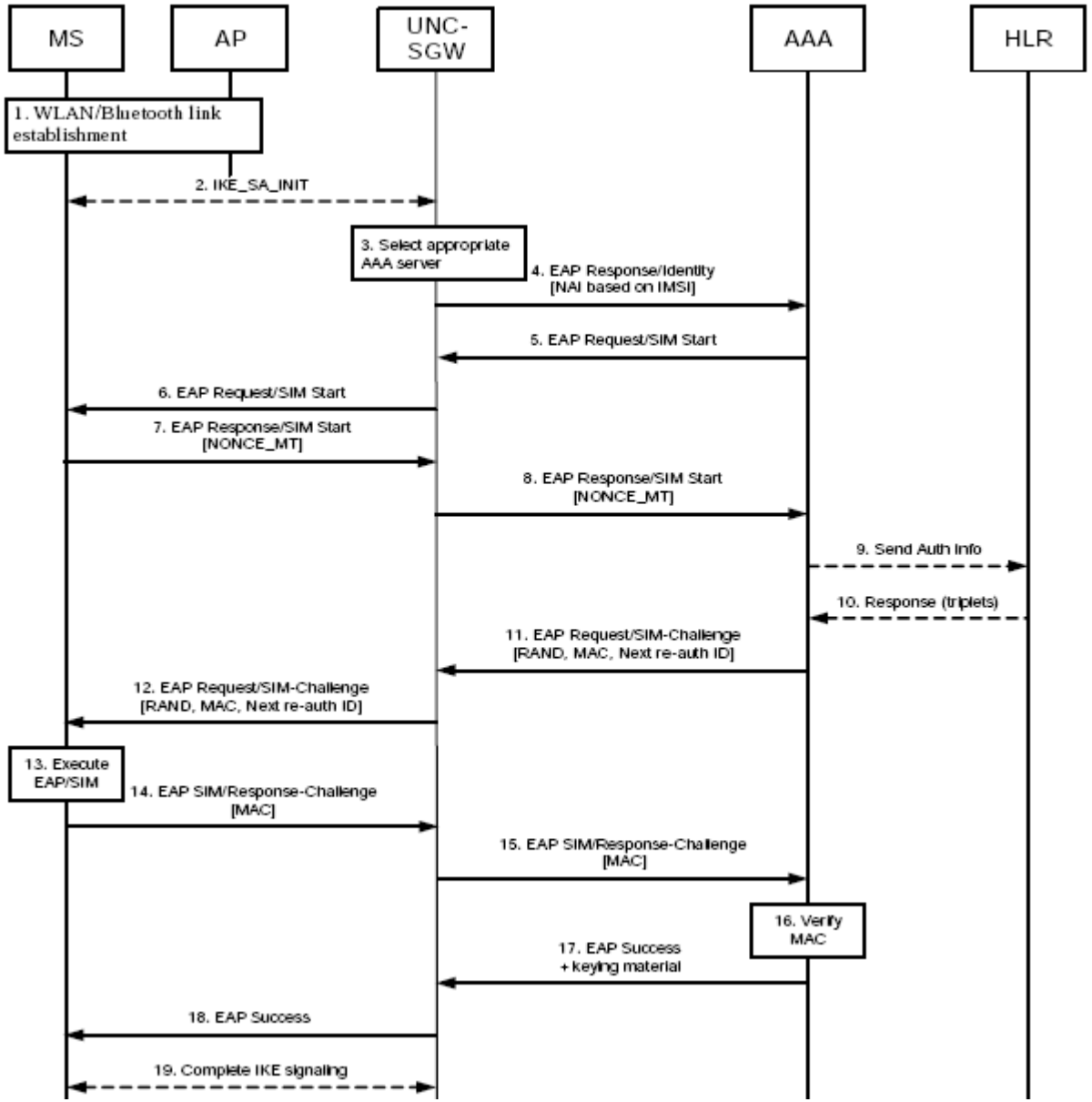
- Couches de sécurité



Source : UMA Specifications

UMA

- Authentification



Source : UMA Specifications

Unlicensed Mobile Access

- La sécurité est assurée à plusieurs niveaux
- Sécurité de la couche réseau (e.g. Wi-Fi avec WPA/WPA2)
  - Optionnelle
- Authentification robuste grâce à IKEv2 avec EAP
  - Authentification de l'UNC par certificat
  - Authentification de l'utilisateur et du réseau par EAP-SIM/AKA
- Confidentialité et intégrité des communications
  - Grâce à IPsec et des profils de confidentialité robustes (AES et 3DES)
  - Attention au mode « NULL encryption »

La sécurité à quel prix ?

- Transporter la voix et assurer sa sécurité impose des
  - Contraintes de temps réel
  - Contraintes de pertes de paquets et de routage IP
  - Contraintes de ressenti utilisateur (délais d'établissement, gigue...)
  - Contraintes d'interception légale
  - Contraintes de législation sur la cryptographie selon les pays
  - Contraintes de législation sur la disponibilité des appels d'urgence
  - Contraintes de législation sur la localisation des appels d'urgence

- Dans ce contexte, sécuriser la voix sur IP n'est pas trivial !

Failles logicielles

- Catégories de failles connues dans l'état de l'art
- Suffirait-il d'appliquer des règles et de s'y tenir ?
  - Oui : code développé par des connaisseurs, code revu par des experts externes, tests de robustesse fonctionnelle et d'injection de données invalides...
    - DJBDNS, OpenBSD (même si parfois...), Postfix...
  - Mais nécessite du temps et des compétences i.e. ça coûte cher !
- Les problèmes classiques resurgissent toujours
  - Les processus de gestion des vulnérabilités diffèrent
    - Contacts avec le constructeur, rapidité des corrections, disclosure...