WiMAX:
Security Analysis and Experience Return

Laurent BUTTI – France Télécom / Orange Division R&D

Network Security Senior Expert

firstname dot lastname at orange-ftgroup dot com

whoami

- Network security expert working for a major Telco.
- Wi-Fi security centric! Lot of Wi-Fi focused talks ;-)
  - Wi-Fi intrusion detection
  - Wi-Fi fuzzing
  - …

Goals of This Talk

- Understand the security mechanisms designed in IEEE 802.16 based standards
- Make the people aware of some weaknesses
- Make the people remember that any wireless technology must be carefully evaluated
- This not an analysis of the end-to-end IP architecture as designed in the NWG of the WiMAX Forum

Agenda

- Introduction (WiMAX, WiMAX Forum…)
- IEEE 802.16 standards overview
- IEEE 802.16 standards security analysis
- Feedbacks and recommendations
- Conclusions

Introduction

Quantitative Analysis ;-)

- IEEE 802.11-1999 standard:
  - 528 pages
- IEEE 802.11i-2004 standard (amendment):
  - 190 pages
- IEEE 802.16-2004 standard:
  - 895 pages
- IEEE 802.16e-2005 standard (amendment and corrigendum):
  - 864 pages

WiMAX (1/2)

- Worldwide Interoperability for Microwave Access

- « Broadband Wireless Access » Technology
  - Wireless MAN « Metropolitan Area Network »
    - Called « last mile » technology
  - Can be used
    - Indoor or outdoor
    - Fixed, nomadic or mobile

- Institute of Electrical and Electronics Engineers Standards
  - *Group 802:* IEEE Standard for Local and Metropolitan Area Networks
  - *Part 16:* Air Interface for Fixed Broadband Wireless Access Systems
  - PHY and MAC layers specifications

WiMAX (2/2)

- WiMAX is a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL.

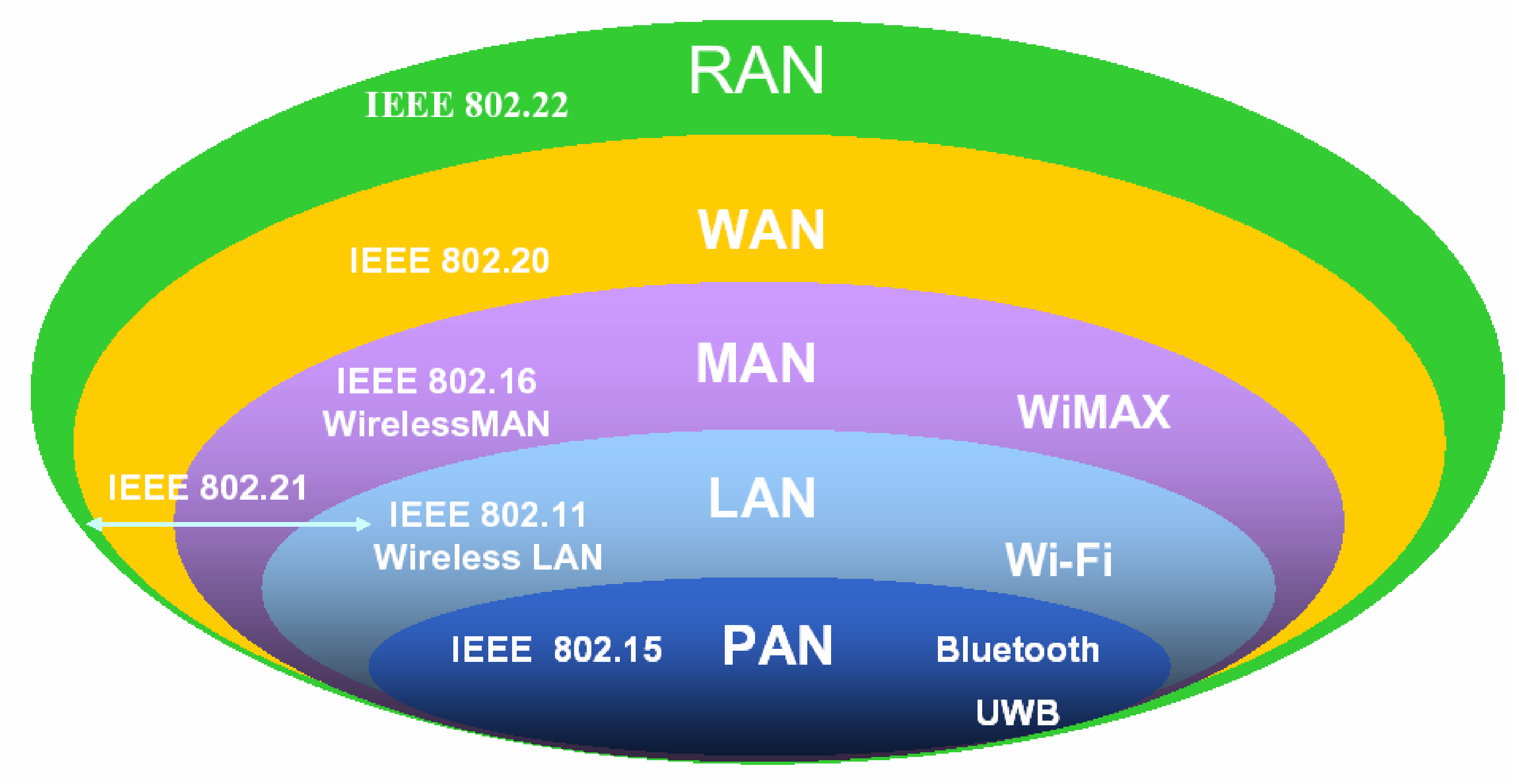
- WiMAX will provide fixed, nomadic, portable and, eventually, mobile wireless broadband connectivity without the need for direct line-of-sight with a base station. In a typical cell radius deployment of three to ten kilometers, WiMAX Forum Certified™ systems can be expected to deliver capacity of up to 40 Mbps per channel, for fixed and portable access applications.

- Mobile network deployments are expected to provide up to 15 Mbps of capacity within a typical cell radius deployment of up to three kilometers.

- It is expected that WiMAX technology will be incorporated in notebook computers and PDAs by 2007, allowing for urban areas and cities to become “metro zones” for portable outdoor broadband wireless access.

Source : WiMAX Forum

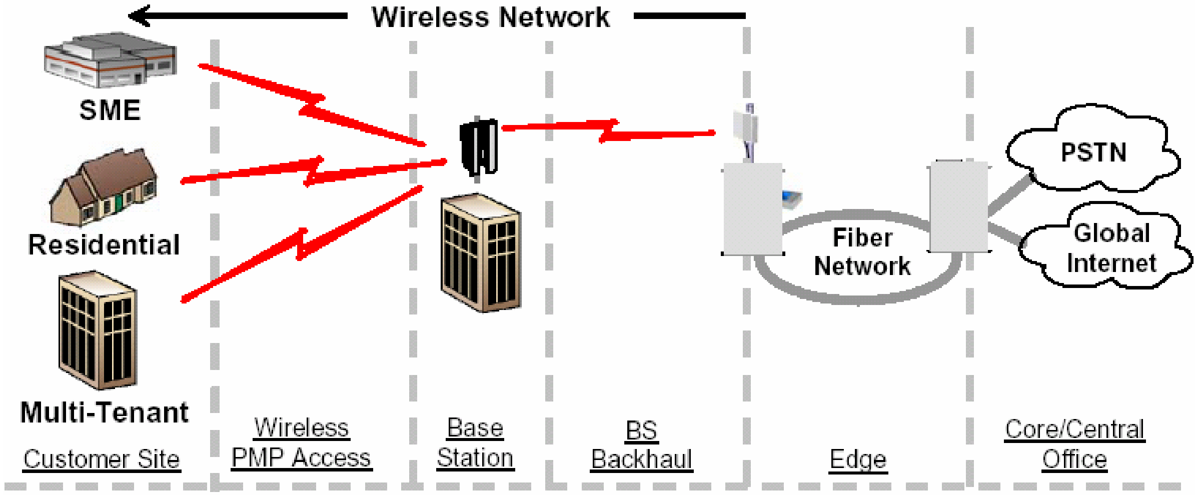
IEEE 802.xx Positioning



Source : WiMAX Forum

Deployment Candidates

- Main interests are in
  - Wireless backhauling
  - Access to non wired areas (rural zones)
  - Broadband access both for residential and enterprises
- Whenever wireless access is a better choice (cost…)
  - Comparing to wired and existing wireless technologies (Wi-Fi, 3G)



Source : WiMAX Forum

Any Forecast?

- Data rates and ranges are promising

- Potential uses seems promising
  - Short-term fixed broadband access
  - Medium-term for nomadic uses
  - Long-term for mobile uses

- Hard to forecast as success factors are numerous…
  - Most key success factors are “business” and “buzz” related
  - So it is important to stay aware
    - Just remember the Wi-Fi technology

WiMAX Forum

- WiMAX Forum ?
  - is an industry-led, non-profit corporation formed to promote and certify the compatibility and interoperability of Broadband Wireless Access (BWA) products using the IEEE 802.16 and ETSI HiperMAN wireless MAN specifications
  - Founded in April, 2002, by Intel and Alvarion
  - The WiMAX Forum® has more than 420 members comprising the majority of operators, component and equipment companies in the communications ecosystem

- Actions
  - Define an end-to-end IP architecture
  - Define a set of WiMAX profiles
  - Provide a certification process

WiMAX Profiles

- What is the difference between IEEE 802.16 and WiMAX?
  - Create a single interoperable standard from the IEEE 802.16 and ETSI HiperMAN standards
  - Decided to focus first on profiles for the 256 OFDM PHY mode of the 802.16-2004 standard
- Which profiles/spectrum bands does the WiMAX Forum address?
  - The WiMAX Forum has begun the process of certifying initial fixed and stationary equipment in the 3.5 and 5.8 GHz bands
  - For mobile applications, initial profiles have been developed for 2.3, 2.5, and 3.5 GHz

Source : WiMAX Forum

Roles

IEEE WirelessMAN® 802.16

- Standardisation
- Radio link
- Evolution

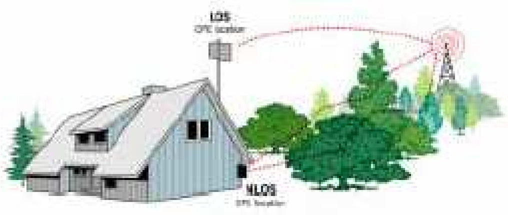
WiMAX FORUM

- Consortium
- Network Technology
- Profiles
- Interoperability
- Marketing/Lobbying

IEEE 802.16 Standards Overview

IEEE 802.16 Amendments (1/2)

- Flexible standard compatible with several bands (licensed or not)
  - IEEE 802.16-2001: 10-66 GHz (December, 2001)
  - IEEE 802.16a: 2-11 GHz (April, 2003)
  - IEEE 802.16c: conformance criteria (January, 2003)
- Major ratification
  - IEEE 802.16d (merged a and c standards) is ratified under IEEE 802.16-2004
  - “Mesh Networks” are also included
- Frequencies impose constraints to deployments
  - Line of Sight (LOS)
  - Non Line of Sight (NLOS)
  - 10-66 GHz implies LOS
    - Strong constraints…



IEEE 802.16 Amendments (2/2)

- Mobility was added thanks to IEEE 802.16e-2005
  - Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands
  - IEEE 802.16-2004 amendment
  - Mobility at ~120-150 km/h
  - WiMAX Forum defines an end-to-end IP network architecture
  - Final approval
    - Draft 12 was approved on December, 2005
    - IEEE 802.16e-2005 is published and available

Expected Rates and Ranges

Standards	IEEE 802.16-2001	IEEE 802.16a	IEEE 802.16e
Band	10 – 66 GHz	< 11 GHz	< 11 GHz
Rate (theorical*)	32 – 134 Mbits	Max. 75 Mbits	Max. 15 Mbits
Mobility	Fixed	Fixed, Portable	Mobility
Cell radius (theorical*)	2 – 5 kms	7 – 10 kms	2 – 5 kms

- * depends on
  - Frequency and modulation
  - LOS or NLOS (and physical environment)

Some Acronyms

- Base Station (BS)
  - Equipment that offers connectivity to 1 or several clients (SS or MS)
- Subscriber Station (SS) or Mobile Station (MS)
  - Equipment that connects to base stations (BS)
- Authorization Key (AK)
  - Key used for trust relationship after a successful authentication
- Traffic Encryption Key (TEK)
  - Key used for data encryption
- Key Encryption Key (KEK)
  - Key used for TEK encryption

IEEE 802.16 Security Analysis

- IEEE 802.16 standards are composed of
  - IEEE 802.16-2004 regarding « fixed » architectures
  - IEEE 802.16e-2005 regarding « mobile » architectures

- Security mechanisms defined in these two standards are quite different
  - Two (different) security analysis

IEEE 802.16-2004 Security Analysis

IEEE 802.16-2004 Security Overview

- IEEE 802.16-2004 Privacy Sublayer
  - Privacy Key Management for authentication and key exchange
  - Encapsulation Protocol for data communication confidentiality and integrity

- Must provide
  - Peer authentication
  - Key hierarchy for deriving encryption and integrity keys
  - Data protocol encryption and integrity

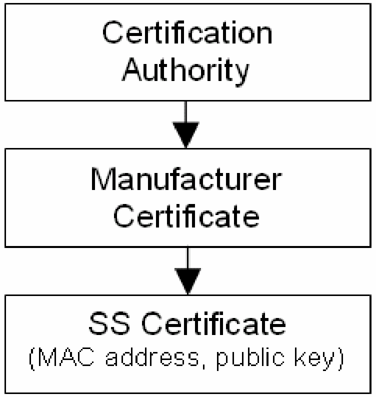
Privacy Key Management (PKM)

- A SS uses the PKM protocol to
  - obtain authorization and traffic protection keying material from the BS
  - support periodic reauthorization and key refresh
  - thanks to digital certificates and encryption algorithms

- The PKM protocol is built around the concept of security associations (SA)
  - A SA is a set of cryptographic methods and associated key materials that a BS and one more of its client SS share in order to support secure communications across the 802.16 network

SS's Certificates Specification

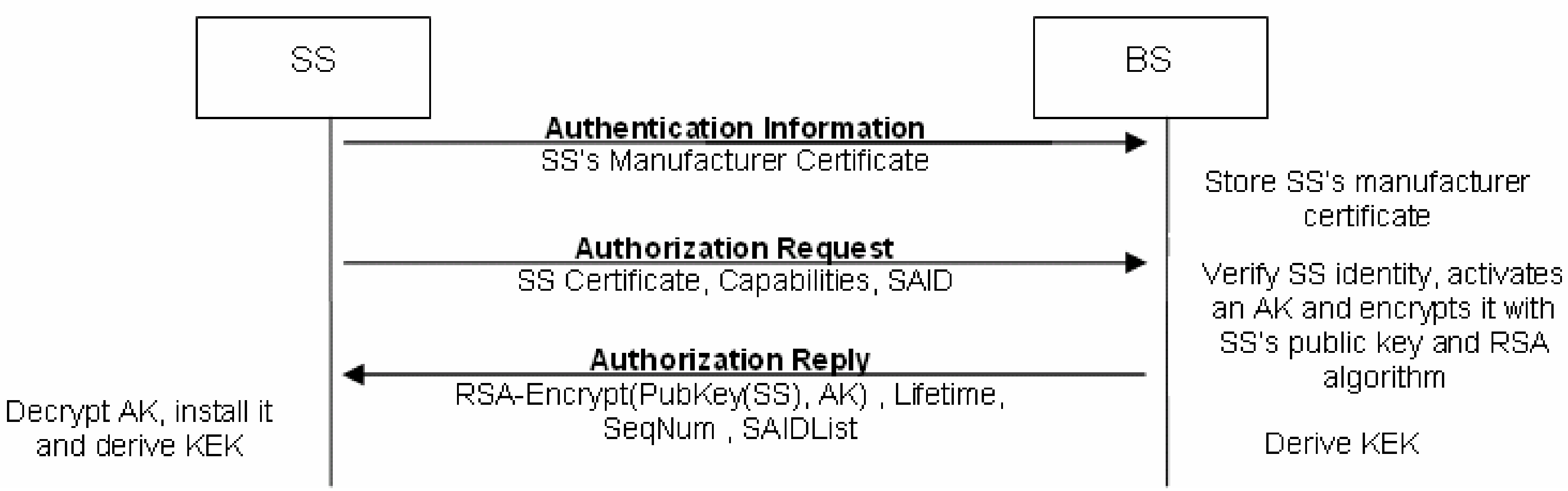
- Defined in section 7.6 ("Certificate profile") of IEEE 802.16-2004
  - Standard defines very precisely the fields of a certificate
    - CommonName = <SS's MAC address>



- SS's certificates shall not be renewable
  - Maximum lifetime of 10 years
- But specifications lacks on how to manage this PKI
  - Factory installed or generated and signed at first installation?
  - Revocation?
- Thus, should be very vendor-dependent…

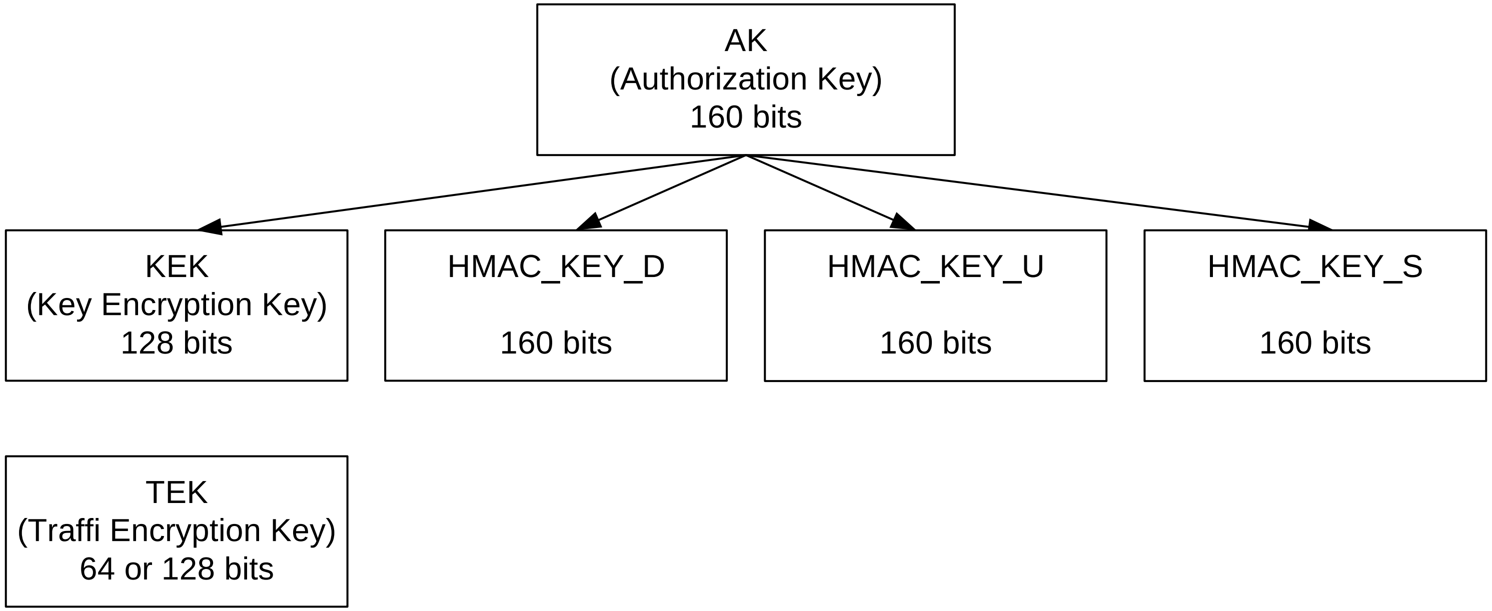
Privacy Key Management (PKM)

- First step: SS authorization and Authorization Key generation
  - Authentication Information message specified as "Informative"
  - AK is "randomly" chosen by the BS


SS
BS
Authentication Information
SS's Manufacturer Certificate
Store SS's manufacturer certificate
Authorization Request
SS Certificate, Capabilities, SAID
Verify SS identity, activates an AK and encrypts it with SS's public key and RSA algorithm
Authorization Reply
RSA-Encrypt(PubKey(SS), AK) , Lifetime, SeqNum , SAIDList
Decrypt AK, install it and derive KEK
Derive KEK

Privacy Key Management (PKM)

- Second step: Deriving keying material from AK
  - KEK and HMAC keys (for the integrity of PKM exchanges)
  - TEK is “randomly” chosen by the BS



AK
(Authorization Key)
160 bits

KEK
(Key Encryption Key)
128 bits

HMAC_KEY_D

160 bits

HMAC_KEY_U

160 bits

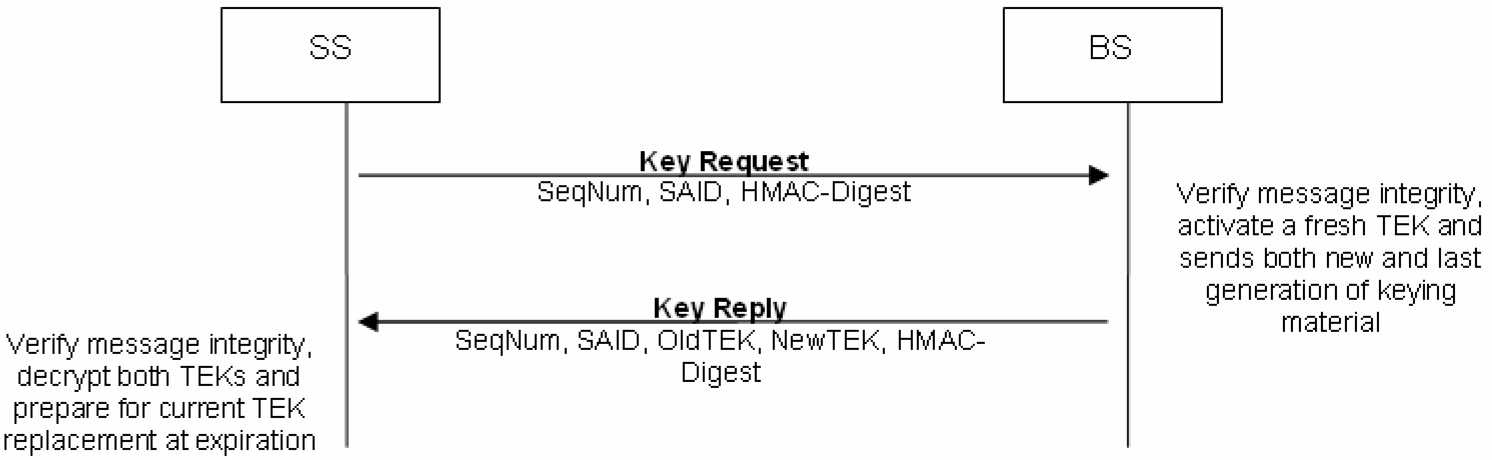
HMAC_KEY_S

160 bits

TEK
(Traffi Encryption Key)
64 or 128 bits

Privacy Key Management (PKM)

- Third step: TEK transport to the SS



SS

BS

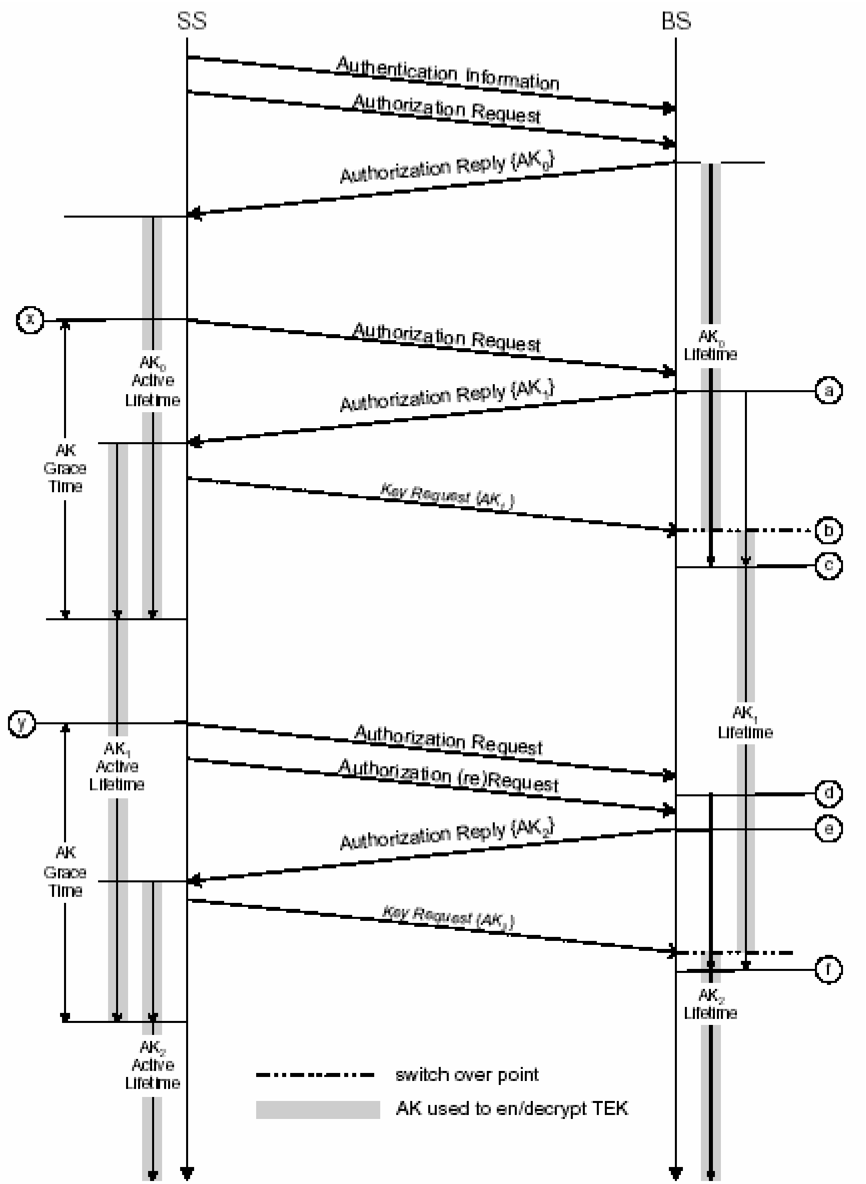
Key Request
SeqNum, SAID, HMAC-Digest

Verify message integrity, activate a fresh TEK and sends both new and last generation of keying material

Key Reply
SeqNum, SAID, OldTEK, NewTEK, HMAC-Digest

Verify message integrity, decrypt both TEKs and prepare for current TEK replacement at expiration

Privacy Key Management (PKM)



Encryption Sublayer

- Two data encryption methods are supported:
  - DES in CBC mode
  - AES in CCM mode

- DES should not be used

- Some vendors may provide proprietary encryption protocols

IEEE 802.16-2004 Weaknesses

- No mutual authentication
  - No network authentication, rogue BS attacks are possible
- Certificates management is out of scope of the specification
  - Certificate provisioning, storage, renewal, revocation, configuration?
- DES is considered insecure
  - Eavesdropping is possible thanks to acceptable financial means
- No integrity protection on management frames
  - Potential denial of service attacks
- Encryption keys are randomly chosen by the BS
  - No nonce from the SS, potentially weak pseudo random number generator on the BS

Deploying IEEE 802.16-2004

- Today IEEE 802.16-2004 security is hard to compromise only because tools are expensive (rogue BS, sniffers…)
  - Remember the very beginning of Wi-Fi?

- Should be considered only in non highly sensitive networks
  - Have further security mechanisms at upper layers

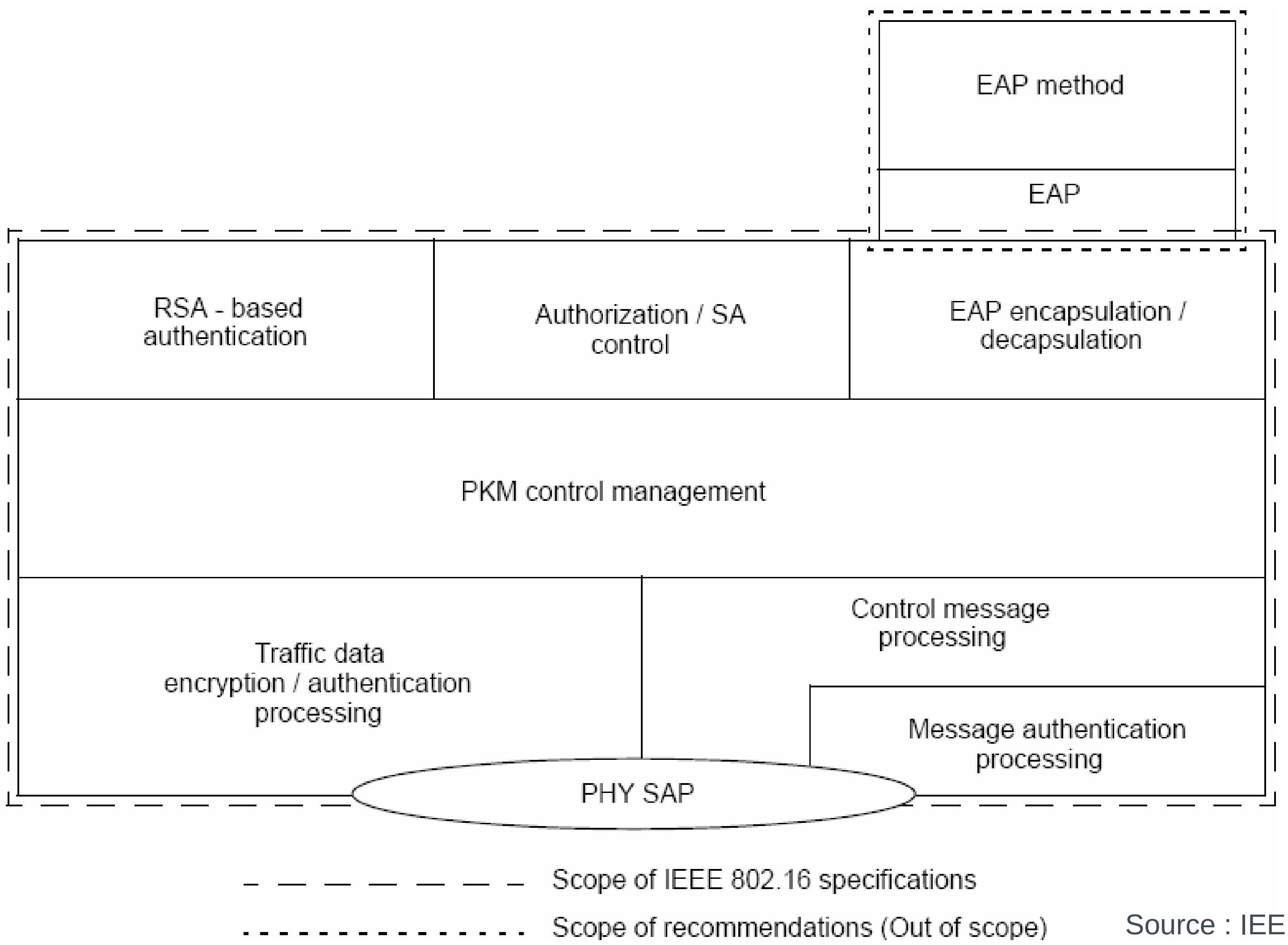
IEEE 802.16e-2005 Security Analysis

IEEE 802.16e-2005 Security Overview

- Same “generic” concept as IEEE 802.16-2004 Privacy Sublayer
  - Privacy Key Management for authentication and key exchange
    - PKMv1 for backward-compatibility (still unilateral authentication)
    - PKMv2 for enhanced security
  - Encapsulation Protocol for data communication confidentiality and integrity
    - New crypto-protocols available

- Must provide
  - Peer authentication
  - Key hierarchy for deriving encryption and integrity keys
  - Data protocol encryption and integrity

IEEE 802.16e-2005 Security Overview


EAP method
EAP
RSA - based authentication
Authorization / SA control
EAP encapsulation / decapsulation
PKM control management
Traffic data encryption / authentication processing
Control message processing
Message authentication processing
PHY SAP
Scope of IEEE 802.16 specifications
Scope of recommendations (Out of scope)

Source : IEEE 802.16e-2005

Privacy Key Management v2 (PKMv2)

- PKMv2 supports several schemes:
  - RSA-based authorization
  - EAP-based authorization
  - RSA followed by EAP-based authorization
  - EAP followed by EAP-based authorization
- All schemes are mutual authentication mandatory
- Negotiation occurs to elect the adequate authentication method
  - SS Basic Capability Request and Response
- Goal is to derive an AK
  - But not randomly chosen by the BS…

Privacy Key Management v2 (PKMv2)

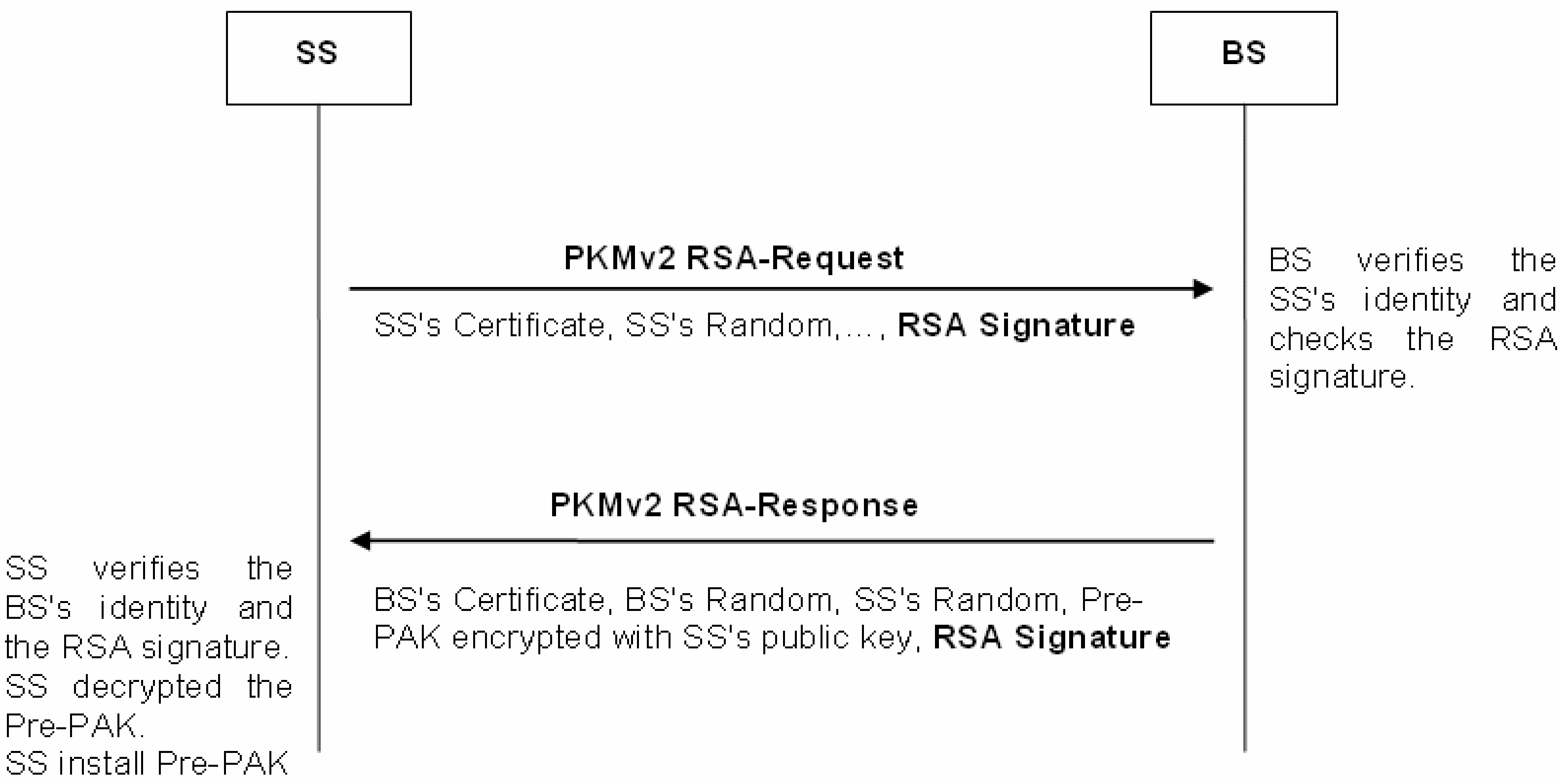
- First step: SS authorization

- Will depend on which authentication scheme
  - RSA-based:
    - EIK | PAK = Dot16KDF (pre-PAK, SS MAC address | BSID | "EIK + PAK", 320)
    - PAK : Primary Authentication Key
  - EAP-based:
    - PMK = truncate (MSK, 160)
    - MSK : Master Session Key
    - PMK : Pairwise Master Key

- pre-PAK is derived from an RSA-based authorization
- MSK is derived from an EAP-based authentication

Privacy Key Management v2 (PKMv2)

- RSA-based authorization



SS's Certificate, SS's Random,…, **RSA Signature**

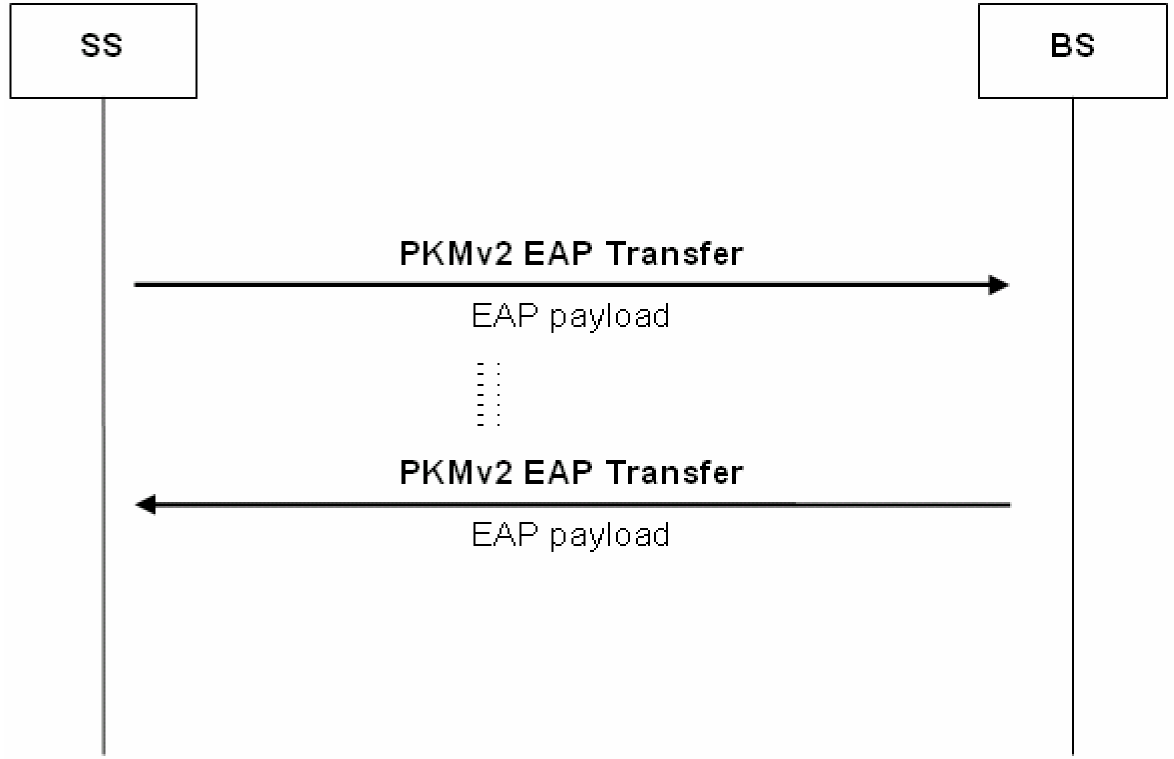
BS verifies the SS's identity and checks the RSA signature.

BS's Certificate, BS's Random, SS's Random, Pre-PAK encrypted with SS's public key, **RSA Signature**

SS verifies the BS's identity and the RSA signature. SS decrypted the Pre-PAK. SS install Pre-PAK

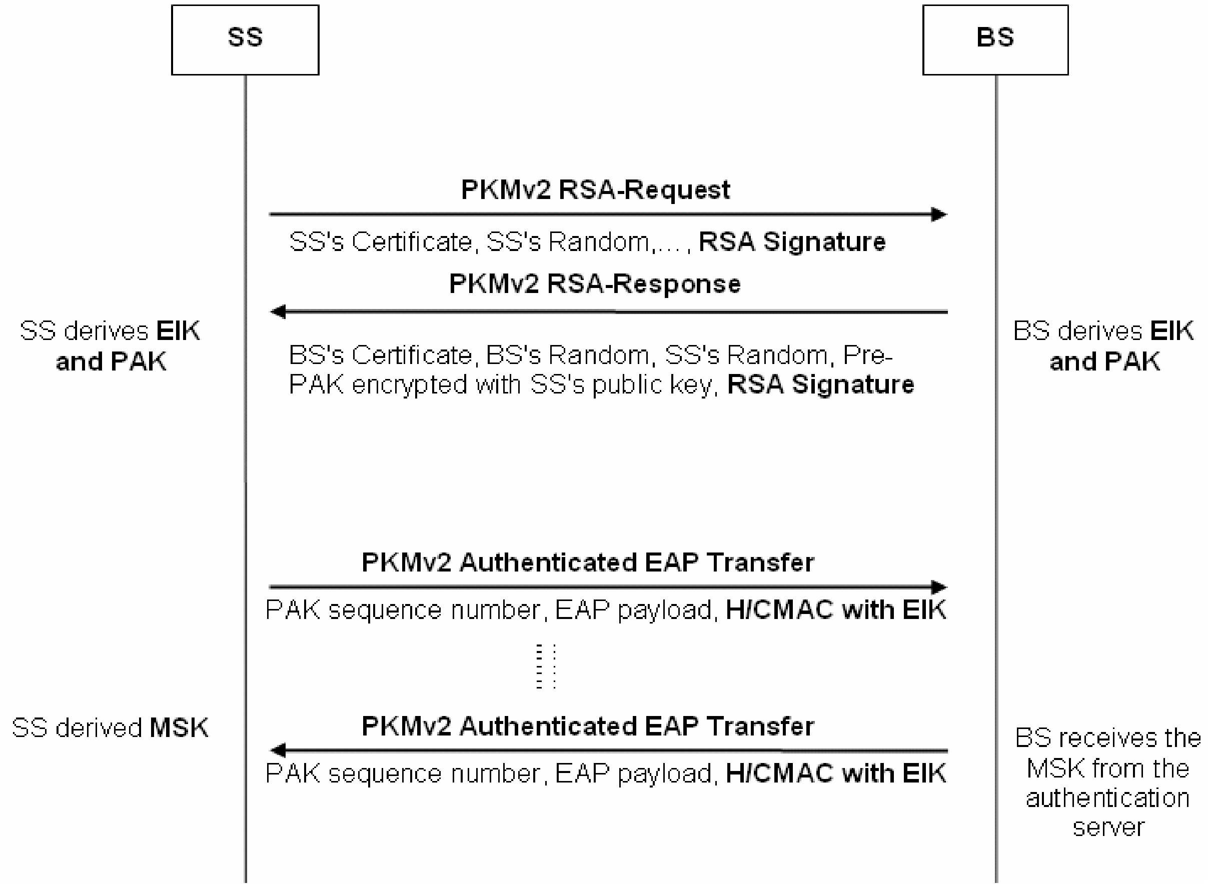
Privacy Key Management v2 (PKMv2)

- EAP-based authorization



Privacy Key Management v2 (PKMv2)

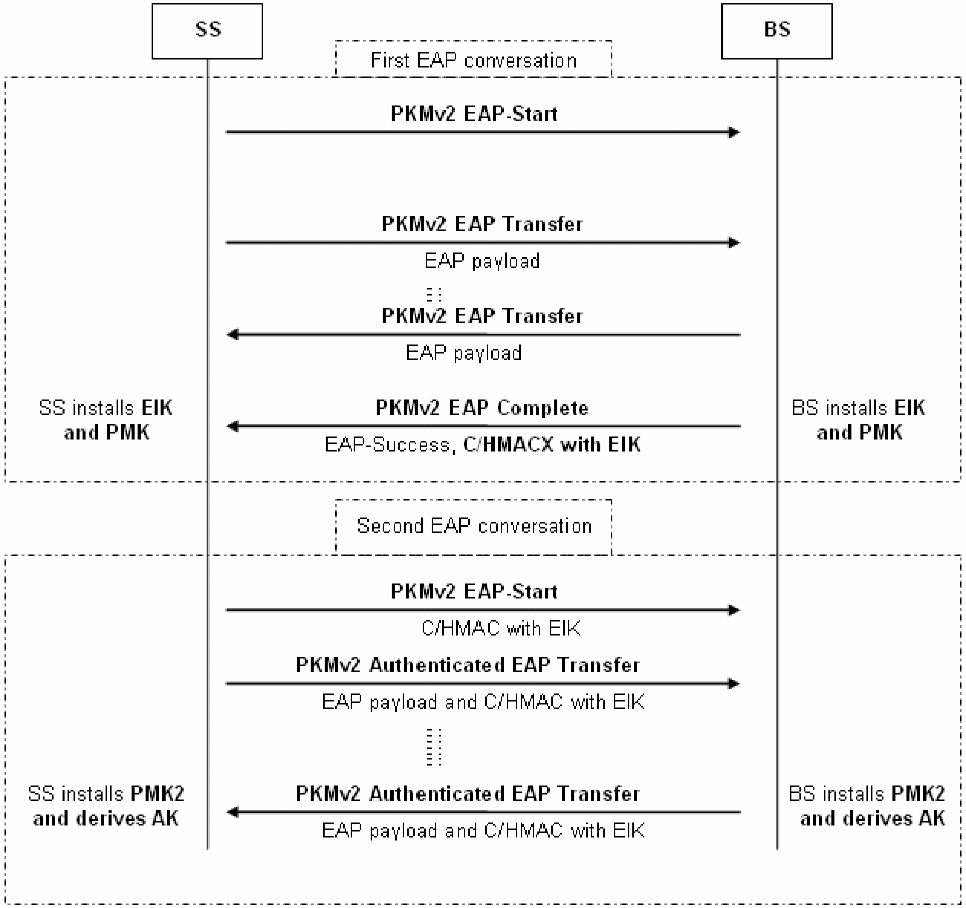
- RSA+EAP authorization



SS
BS
PKMv2 RSA-Request
SS's Certificate, SS's Random,..., **RSA Signature**
PKMv2 RSA-Response
SS derives **EIK and PAK**
BS's Certificate, BS's Random, SS's Random, Pre-PAK encrypted with SS's public key, **RSA Signature**
BS derives **EIK and PAK**
PKMv2 Authenticated EAP Transfer
PAK sequence number, EAP payload, **H/CMAC with EIK**
SS derived **MSK**
PKMv2 Authenticated EAP Transfer
PAK sequence number, EAP payload, **H/CMAC with EIK**
BS receives the MSK from the authentication server

Privacy Key Management v2 (PKMv2)

- EAP+EAP authorization


SS
BS
First EAP conversation
PKMv2 EAP-Start
PKMv2 EAP Transfer
EAP payload
PKMv2 EAP Transfer
EAP payload
SS installs EIK and PMK
PKMv2 EAP Complete
EAP-Success, C/HMACX with EIK
BS installs EIK and PMK
Second EAP conversation
PKMv2 EAP-Start
C/HMAC with EIK
PKMv2 Authenticated EAP Transfer
EAP payload and C/HMAC with EIK
SS installs PMK2 and derives AK
PKMv2 Authenticated EAP Transfer
EAP payload and C/HMAC with EIK
BS installs PMK2 and derives AK

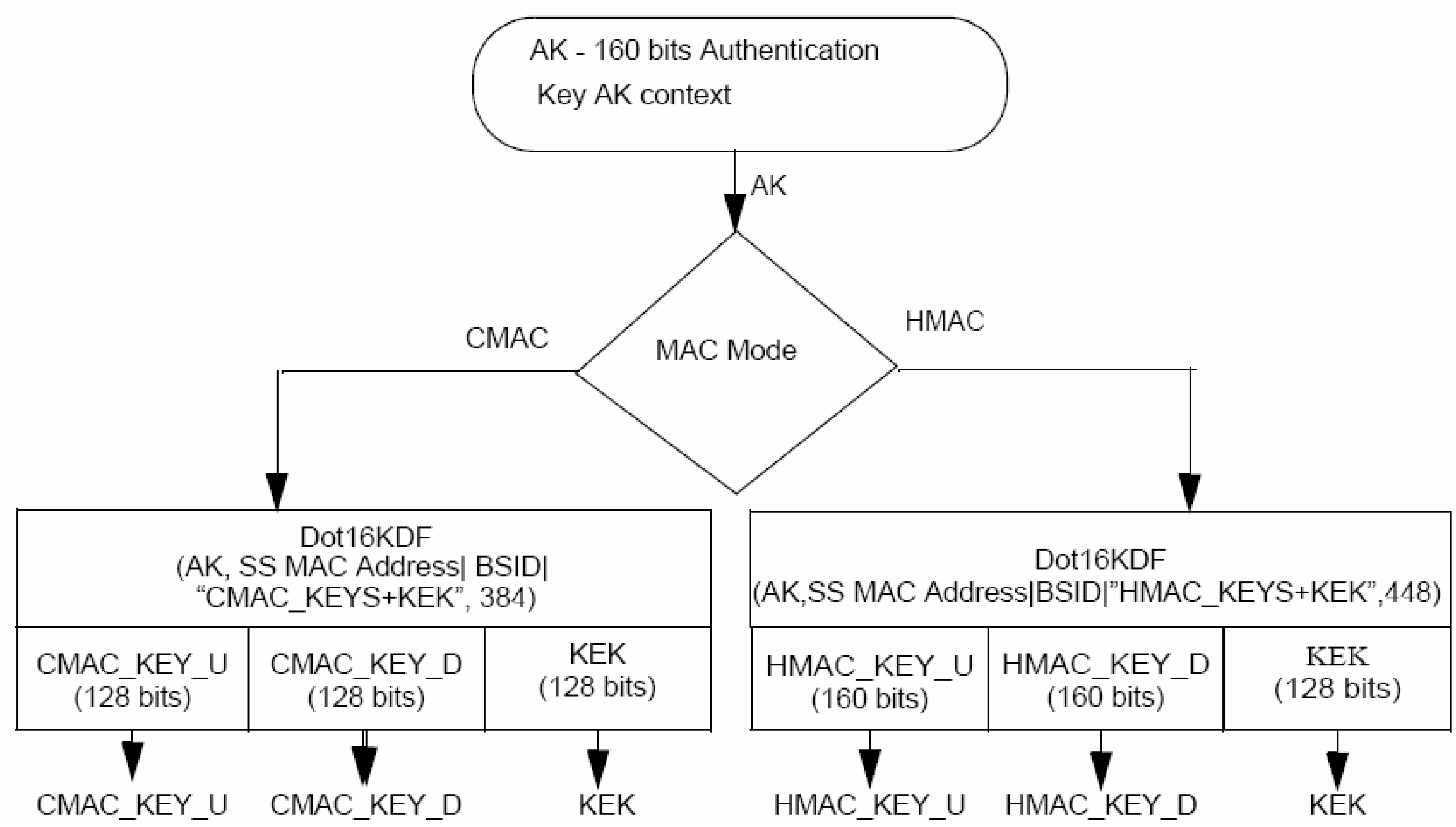
Privacy Key Management v2 (PKMv2)

- Authentication Key derivation depends on authentication scheme

- If RSA-based authorization then:
  - **AK** = Dot16KDF (**PAK**, SS MAC address | BSID | PAK | "AK",**160**)
- If EAP-based authorization then:
  - **AK** = Dot16KDF (**PMK**, SS MAC address | BSID | "AK", **160**)
- If RSA-based and EAP-based authorization then:
  - **AK** = Dot16KDF (**PAK xor PMK**, SS MAC address | BSID | PAK | "AK",**160**)
- If EAP-in-EAP then:
  - **AK** = Dot16KDF (**PMK xor PMK2**, SS MAC address | BSID | "AK", **160**)

Privacy Key Management v2 (PKMv2)

- Second step: Deriving keying material from AK



Privacy Key Management v2 (PKMv2)

- Third step: TEK transport to the SS
  - Three-way handshake
  - TEK is still “randomly” chosen by the BS

Encryption Sublayer

- Two new encryption mechanisms
  - AES in CBC mode
  - AES in CTR mode

- A revision of the AES in CCM mode:
  - Recommendation to use a window size for PN values preventing replay attacks

IEEE 802.16e-2005 Security Analysis

- Authentication mechanisms improvements
  - Improved flexibility thanks to Extensible Authentication Protocol (EAP)
    - Really buzzed since IEEE 802.11i
  - Mutual authentication thanks to PKMv2
    - SS and BS with certificates and RSA
    - SS and BS with EAP
  - Add an (optional) user authentication
    - Thanks to EAP (after previous authentication)

- Confidentiality and integrity
  - (Most) management frames are signed providing integrity protection
  - Robust AES-based encryption protocol for data communications

IEEE 802.16e-2005 Weaknesses

- Some EAP packets are still not protected
  - DoS on authentication is still possible, but it is on the EAP scope
- TEK are randomly chosen by the BS
  - Entropy issues?
- Certificate management is still unclear (when RSA-based)
  - Certificate provisioning?
  - Certificate and private key storing?

Security Analysis Summary

Security Analysis Summary

Weakness	Issue	IEEE 802.16-2004	IEEE 802.16e
No Mutual Authentication	Rogue BS	High risk	Corrected
Management Frames Unprotected	DoS	High risk	Corrected
Anti Replay Not Implemented	Traffic injection and DoS	Implementation dependent	Mostly corrected
Keys Generated by the BS	Key entropy	Implementation dependent	Partially corrected (TEK still chosen by BS)
Certificate Management Unspecified	Potential inconsistencies	Implementation dependent	Implementation dependent
Insecure DES Encryption	Eavesdropping	Potential risk	Backward compatibility

Security Analysis Summary

- IEEE 802.16-2004 suffers from several weaknesses
  - No mutual authentication
  - DES encryption is insecure
  - Management frames are not protected
  - TEK is randomly chosen by the BS

- IEEE 802.16e-2005 is a major step in terms of security
  - Almost all the weaknesses were corrected
  - Authentication may rely on EAP (high level of flexibility)
  - Very few attacks valid for IEEE 802.16-2004 are still possible

Deployments

Auditing Current Deployments

- IEEE 802.16 sniffers are expensive and proprietary
- No information regarding chipset, firmware and driver flexibility
  - Will it be as great as Wi-Fi?
    - Access point mode, monitor mode, arbitrary frame injection
- Till a flexible chipset and an Open Source driver will be available!
- Thus current efforts are aimed at classic stuff
  - Network segmentation
  - Equipment's security

Equipment’s Security

- Reverse engineer a firmware and find implementation (or design) flaws

- Thus retrieving the firmware may be interesting
  - Thanks to the update process
  - Thanks to a JTAG

- This is classic stuff for embedded devices especially when located in unsafe areas (i.e. where physical security cannot be properly enforced)

Product Availability?

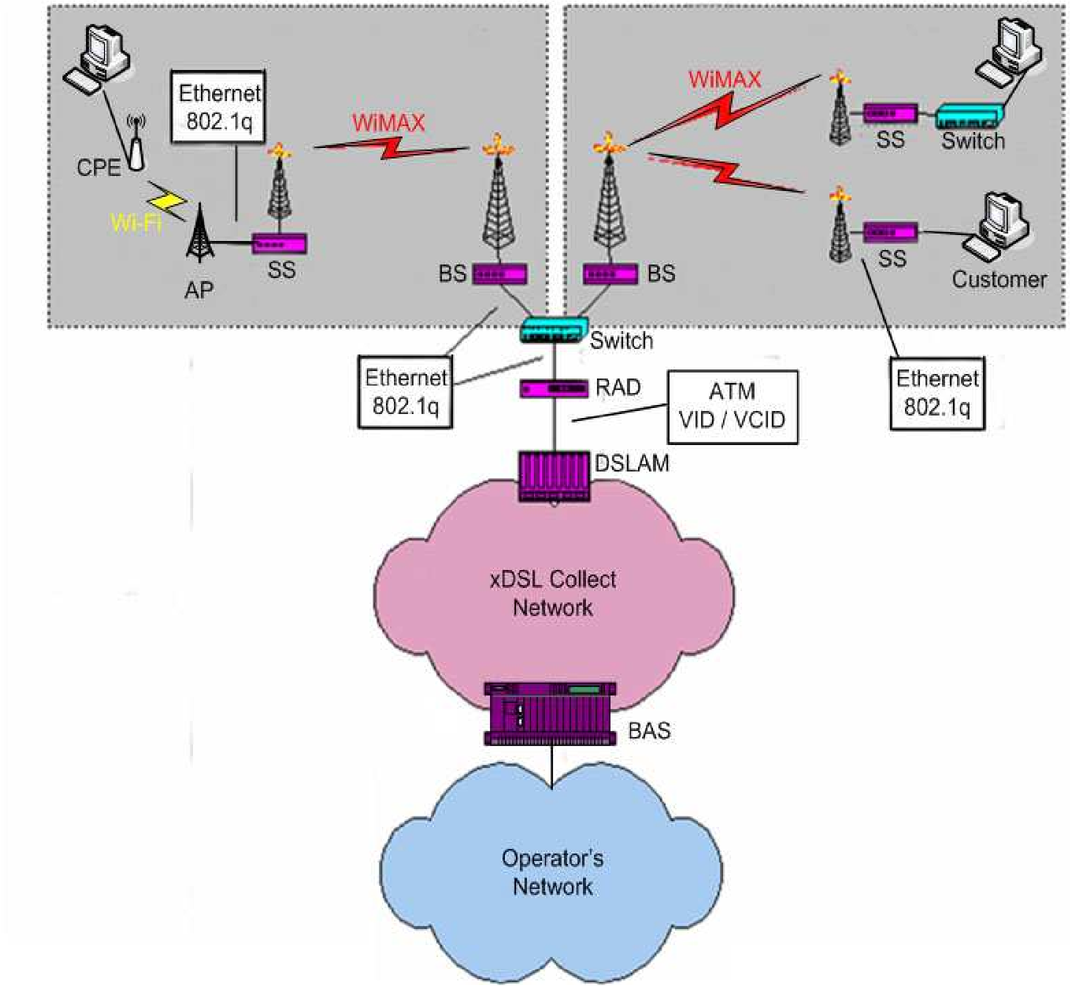
- "Fixed WiMAX" certified products are available
  - Lots of Base Station and Subscriber Station are WiMAX certified
    - Aperto Networks, Redline Communications, Sequans, WaveSat Wireless…
  - First wave of certification occurred on January, 24th, 2006
  - Intel Pro/Wireless 5116 (a.k.a. Rosendale) chipset is available
  - Refer to http://www.wimaxforum.org/kshowcase/view and appendix 2
- "Mobile WiMAX" certified products are expected mid-2007
- Experimental deployments (2005/2006) were based on pre-WiMAX products

Pre-WiMAX Experimental Deployments

- France Telecom deployed 4 pre-WiMAX architectures in France
  - Frequencies were attributed for experimentation by the ARCEP*, and were given back in September, 2005
  - Locations: Amilly, La Salvetat, Léhon and Issy-Les-Moulineaux
- WiMAX was used as a wireless backhaul
  - Wi-Fi extensions were used for point to multi-point access
- Network architectures were hardened
  - Equipments hardening
  - VLAN logical segmentation
  - Security audit
    - VLAN hopping tests

* ARCEP : French's Telecommunications Regulatory Authority

Pre-WiMAX Experimental Deployments



Pre-WiMAX Experimental Deployments

- Short-term applications are mainly focused on broadband access both for residential and enterprise

- Experimental deployments shown that
  - IEEE 802.16-2004 is reliable from a network point of view
  - Deployment costs are lower than satellite for low crowded zones
  - But security at link layer cannot be assessed due to lack of tools… ☹

- Frequency licensing by the ARCEP
  - Licensing on 3.4-3.6 GHz band for wireless backhauling requires an authorization process

Implementations

IEEE 802.16 Fuzzing?

- Fuzzing is a software testing technique aiming at discovering implementation bugs
  - Usually adequate for black-box testing
  - Much more fault injection than conformance tests

- I am a big fan of fuzzing!
  - Found numerous flaws in some wireless drivers
    - Reliable madwifi exploit (not destroying the Wi-Fi stack ☺)
  - One of the best price / earning ratio

IEEE 802.16 Fuzzing?

- Both IEEE 802.16-2004 and IEEE 802.16e-2005 standards are complex
- BS and SS not susceptible to be developed in a high level language ;-)
  - C/C++ will be mandatory!
- Complexity ⇨ More Code ⇨ Implementation Bugs ⇨ Possible exploitable implementation bugs

IEEE 802.16 Fuzzing?

- Taking a look at IEEE 802.16 standards
  - There are numerous signaling frames (management)
    - Much more than in IEEE 802.11
  - Most of them use the TLV encodings
    - So error-prone!

- Vendors generally perform conformance, features and performance tests but not usually regarding fault injection
  - Does the buzz around fuzzing will change this?

Is Wireless a Nightmare For Security?

New Technologies: New Threats (1/2)

- Any technology is susceptible to new attacks

- When deploying a new radio technology, security is critical
  - Any vulnerability may be reachable by the « air »!

- Any complex technology is susceptible to implementation bugs
  - Implementing fuzzing tests is mandatory
  - See Month of Kernel Bugs on wireless drivers vulnerabilities!

New Technologies: New Threats (2/2)

- If “Mobile WiMAX” becomes deployed, it will hit laptops!
  - PCMCIA / USB / mini-PCI interfaces
  - Another radio technology besides IrDA, BlueTooth, Wi-Fi and 3G
    - Next one: Wireless USB?

- Classic stuff on interface hardening
  - Firewalling
  - VPN tunneling for remote access

- Battle for laptop’s security was already lost whenever you open doors… but with wireless it’s even worse!

Conclusions

Conclusions (1/2)

- IEEE 802.16-2004 suffers from several weaknesses
  - No mutual authentication
  - DES encryption insecure and TEK randomly chosen
  - Management frames not protected
  - Certificate management unclear
- Deploying IEEE 802.16-2004 must take these risks into account
  - Non highly sensitive networks
  - Upper layers encryption
- IEEE 802.16e-2005 is a major step in terms of security
  - Almost all the weaknesses were corrected
  - Authentication may rely on EAP (high level of flexibility)
  - Very few attacks valid for IEEE 802.16-2004 are still possible
  - Mobility is a huge enhancement

Conclusions (2/2)

- Deploying any recent wireless technology, care must be taken
  - Deployment experience is a strong advantage
  - Implementation bugs
- Preferably choose “Mobile WiMAX” security features
  - Even if “Fixed WiMAX” may be (in practice) sufficient today
- Choose the right solution by risk assessment
  - But this is not new!

Questions?

Acknowledgements

- Jérôme Razniewski and Roland Duffau