The Phylaws project - An academic + industrial merged view about Physical layer Security

ICC, London, 8 June 2015

François Delaveau

francois.delaveau@thalesgroup.com

Expert Engineer for signal processing and Electronic Warfare
Thales Communications & Security; Gennevilliers, France
Coordinator of the Phylaws project. www.phylaws-ict.org

Supported by PHYLAWS project FP7 ICT Id-317562

Summary

- About the Phylaws Project
- Security lacks of networks' radio interface: the harsh reality
- Advantages and remaining gaps of Physical Layer Security
- About radio protocols for early security pairing

Supported by PHYLAWS project FP7 ICT Id-317562

About the Phylaws project

- **MAIN GOALS:**

  Improve security of wireless links

  Search for key-free solutions based on Physical layer security

  Experiment these solutions in real field

  Search for practical implantations in existing and future public RATs

- **AN ORIGINAL APPROACH:**

  Merge academic and industrial skills about radio-propagation, about radio-communications and about security.

  Shake usual hypothesis with return of practical experience

  Consider any kind of threats at physical layer: meaning passive + various active Eve

  Concentrate on signaling and access phases of RATs, and not only on established data links.

PHYLAWS

PHYsical Layer Wireless Security

Project Coordinator:
Thales Communications and Security
François Delaveau
Tel: +33 (0)1 46 43 31 32
Fax: +33 (0)1 46 13 25 55
Email: francois.delaveau@thalesgroup.com
Project website: www.phylaws-ict.org

+ Five Partners:
Institut Mines-Telecom ParisTech (FR),
Imperial College of Science, Technology and Medicine (UK),
Teknologian tutkimuskeskus VTT (FI),
Celeno Communications Israel Ldt (IS).

Duration 4 years:
November, 2012 – October, 2016

Funding scheme: STREP

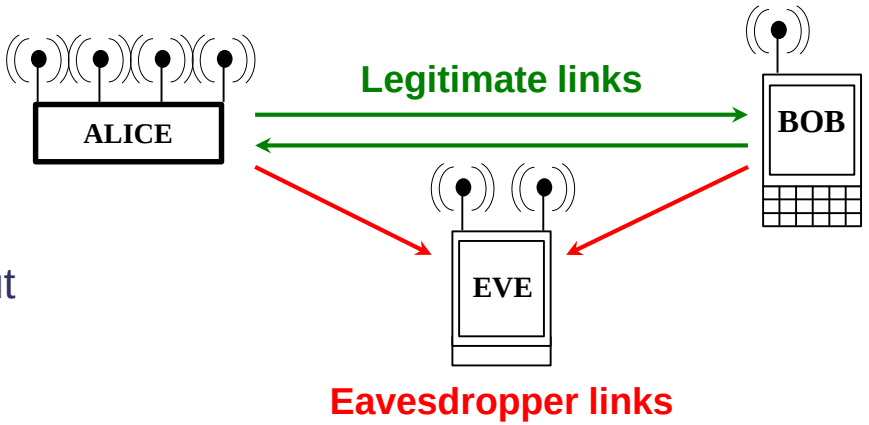
Contract Number: CNECT-ICT-317562

Supported by PHYLAWS project FP7 ICT Id-317562

About terminology and geometry and usual hypothesis in security

Basics

- **LEGITIMATE links are Alice to/from Bob**
- **EAVESDROPPER links are Alice to Eve and Bob to Eve**
- **Usual "Academic" hypothesis are:**
  - complete information of Eve about legitimate RATs/waveforms
  - no Information of Eve about legitimate Keys (e.g. Ki Keys on SIM cards)



- **TRANSEC (Transmission Security) is the waveform protection of the legitimate link face to interception of the transmitted radio signal, to intrusion attempts of the user receiver (and even jamming and direction finding)**
- **NETSEC (Network Transmission Security) is the protection of the signalling of the network of the legitimate link (usual solutions are authentication and integrity control, sometimes ciphering of signalling in military networks)**
- **COMSEC (Communication Security) is the protection of the content of user messages (voice, data). Most of solutions are based on ciphering + integrity control schemes**

Supported by PHYLAWS project FP7 ICT Id-317562

About security lacks of networks' radio interface: the harsh reality

The end of illusions

Usual assumptions of security are no more valid in wireless public networks, whatever the RAT is

- **Eve's knowledge about legitimate key is now usual**

  Using failures of the SS7 and international roaming protocols to get Ki keys

  - Monitoring of Angela Merkel's smartphone during years
  - Security of subscribers is decreased by networks protocol failures and by operators' practices

  SIM card providers may be hacked (to obtain Ki keys)

  - Revelations on hacking of SIM manufacturers by security agencies
  - Subscribers' keys may not be really secret in practice

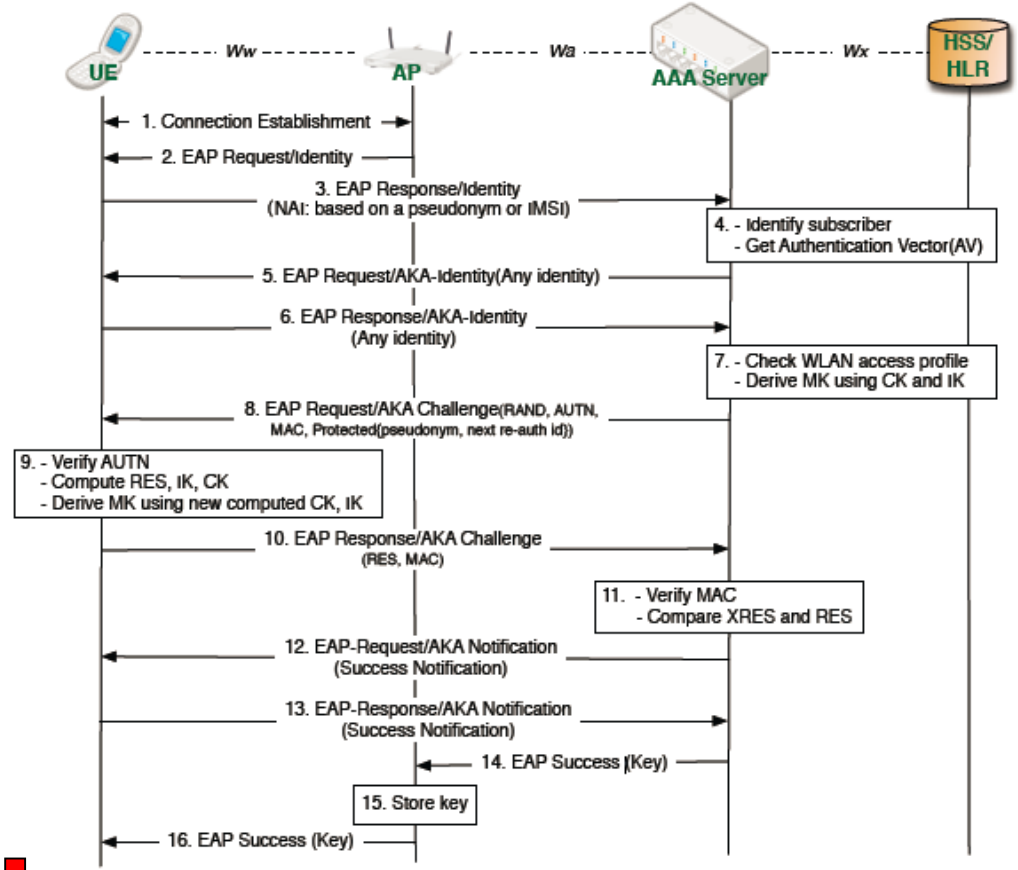
- **Reveals especially that**
  - Subscribers' secret is not efficiently kept within public networks
  - Subscriber authentication, identification and roaming remain weak in 2G/3G/4G etc

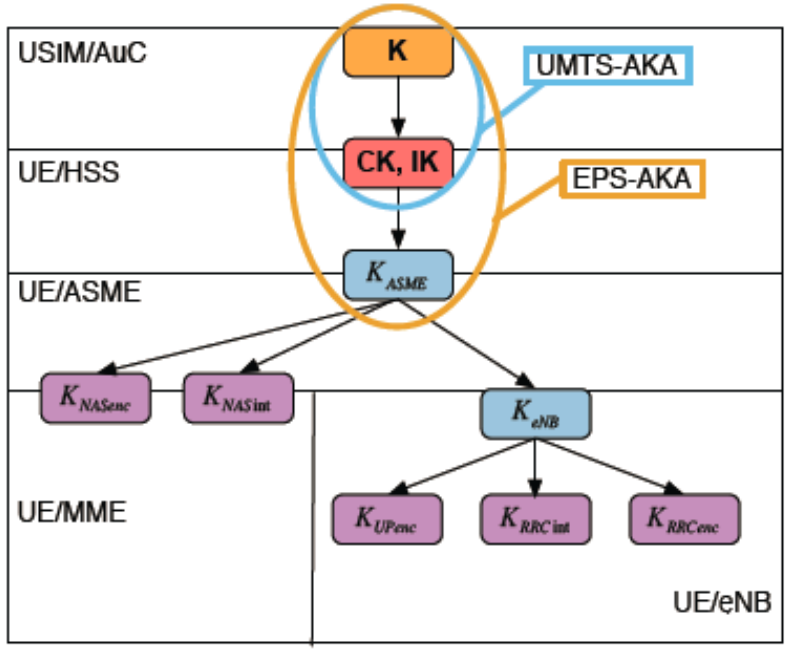
Supported by PHYLAWS project FP7 ICT Id-317562

About security lacks of networks' radio interface: the harsh reality

The end of illusions

Ref: Hyeran Mun, Kyusuk Han and Kwangjo Kim1-4244-2589-1/09/ $20.00 2009 IEEE,
"3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA »





K_{NASenc} : Protection of NAS traffic with particular encryption
K_{NASint} : Protection of NAS traffic with particular integrity
K_{UPenc} : Protection of UP traffic with particular encryption
K_{RRCint} : Protection of RRC traffic with particular integrity
K_{RRCenc} : Protection of RRC traffic with particular encryption

(T/I)MSI AV RAND RES etc. ARE CLEAR TEXT EXCHANGED WITHOUT TRANSEC PROTECTION
ACTIVE EVE CAN JAM, INTERCEPT, SPOOF, REPLAY…

WHEN EVE GET THE KEY K SHE GET ALL…
BY PASSIVE MONITORING ONLY

Supported by PHYLAWS project FP7 ICT Id-317562

About security lacks of networks' radio interface: the harsh reality

Fall of usual assumptions

Usual assumptions of security are no more valid in wireless civilian networks, whatever the RAT is:

- **Keys cannot be pre-distributed nor pre-computed by the legitimate users in wireless public networks**
- **Eve can intercept (and eventually disturb, spoof, replay when active) early negotiation messages between Alice and Bob such as…**
  - Broadcast signaling
  - Channel State Information
  - Geo-located Sensing messages
  - Authentication of Bob and Alice
  - Ciphering key computation

… in order to

- Get information about Alice and Bob
- Impersonate Alice or Bob
- Overcome further protections (Artificial Noise establishment, Ciphering negotiation, etc.)

Supported by PHYLAWS project FP7 ICT Id-317562

What is PHYSEC (Physical Layer Security) ?

- Key-less security technique exploiting propagation randomness to establish secret
- Theory is OK, practical applications in realistic radio-environment are in progress

2 approaches for PHYSEC:

- Secrecy codes: channel codes (FEC) are augmented with secr… …s
  - Require better radio link (SNR) between Alice and B… …ve
  - Approach Shannon capacity for legiti…
  - Mitigate information at "…

Theo… …stablished but explicit design remains an active research domain

See Bloch and Barros,"Physical Layer security" ,Cambridge University Press, 2011

- Secret Key Generation (SKG): keys are computed from prop… …ss
  - Channels between legitimate nodes are recipro… …elsewhere
  - Bits of the secret key are computed f… …urements

Channel quantizatio… …w mismatches between legitimate links
Existi… …ensure few information leakage to third parties

…Hajj et al., "Towards robust key extraction from multipath wireless channels", IEEE Journal of Comm. and Net., vol. 14, no. 4, Aug 2012

Supported by PHYLAWS project FP7 ICT Id-317562

Advantages and remaining gaps of Physical Layer Security (PHYSEC)

Main advantages of PHYSEC

- **PHYSEC should apply well to TDD RATs:** Current WLAN (Wifi), many PCS (DECT), some RATs of LTE, Machine to Machine, future 5G Massive MIMO, etc.

- **PHYSEC avoids the use of ciphering keys, thus is resilient to any attack:**
  - Whatever the knowledge of Eve is about Alice Bob and Operators data bases
  - Whatever Eve's computing capabilities are (even with quantum computing)

- **PHYSEC can be seen as an added security stack:**
  - Especially for transec and netsec,
  - Additionnally for comsec (ex: imput of ciphering modes with propagation random available at equalization output)
  - no replacement nor competition with traditional ciphering

- **PHYSEC schemes can take large benefits of advanced RATs:**
  - MIMO and Artificial Noise
  - Full Duplex,
  - Massive MIMO

- **For TDD RATs, expectation for PHYSEC is software impact only:**
  - low impact at upper layers (MAC, software)

Supported by PHYLAWS project FP7 ICT Id-317562

Remaining gaps of Physical Layer Security (PHYSEC), key items for practical implantation

- **Gaps of numerous existing PHYSEC schemes in TDD RATs**
  - **All PHYSEC schemes need authenticated Channel State Information (CSI)**
    - The channel estimate must be exclusively known by Bob
    - Without exclusivity ➔ no security

    ➔ **how to provide secure CSI for further Physec implantation?**
  - **PHYSEC scheme cannot rely on pre-distributed keys for channel negotiation**
    - No ”industrial” interest in public RATs
    - Eve can also know the key (K)

    ➔ **how to provide a secure CSI without pre-distributed keys ?**
  - **Recent progress concerns Secrecy Coding in more and more realistic scenarios, nevertheless a better SNR/Shannon advantage is still required.**

    ➔ **artificial noise apply only for on-going communications (after CSI)**

    ➔ **how to establish a warranted radio advantage at the access stage ?**

➔ **Need for early and key-free secured security pairing of Alice and Bob which remain resilient to any kind of Eve**

Passive, Man in the Middle (i.e. impersonating Alice and Bob),
Protocol Aware / Intelligent Jammer (i.e. disturbing CSI, AN establishment, etc.)

- **How to implant PHYSEC schemes in FDD RATs by avoiding hardware upgrades of nodes and terminals ?**

Supported by PHYLAWS project FP7 ICT Id-317562

About radio protocols for early security pairing

Towards a key-free radio protocol for authentication and security of nodes and terminals in advanced waveforms

SDR'15 Winncomm, session 1, San Diego, 26 March 2015

Eric Nicollet

François Delaveau, Renaud Molière, Christiane Kameni Ngassa, Claude Lemenager

Thales Communications & Security; Gennevilliers, France

Taghrid Mazloum, Alain Sibille

Telecom ParisTech; Paris, France

Contacts: francois.delaveau@thalesgroup.com

Supported by PHYLAWS project FP7 ICT Id-317562

Supported by PHYLAWS project FP7 ICT Id-317562