EUROPEAN COMMISSION
Community Research

SEVENTH FRAMEWORK PROGRAMME

Funded by EC-FP7-ICT-2011-8 GN 317562
www.phylaws-ict.org

PIMRC'2016 - Workshop W8
Deployment perspectives of Physical Layer Security into wireless public RATs
2016 September 4 – Morning 9h00 – 12h50

CONCLUSION

François Delaveau, (Thales Communications)
Francois.delaveau@thalesgroup.com

Summary

Coming back to PHY layer threats and security challenges

PHYsical Layer SECurity - How ?

=> Implantation perspectives into wireless standards

Maturity check of the Physec technologies

=> Technology – Application

Synthesis of standardization perspectives

Conclusion - Way ahead

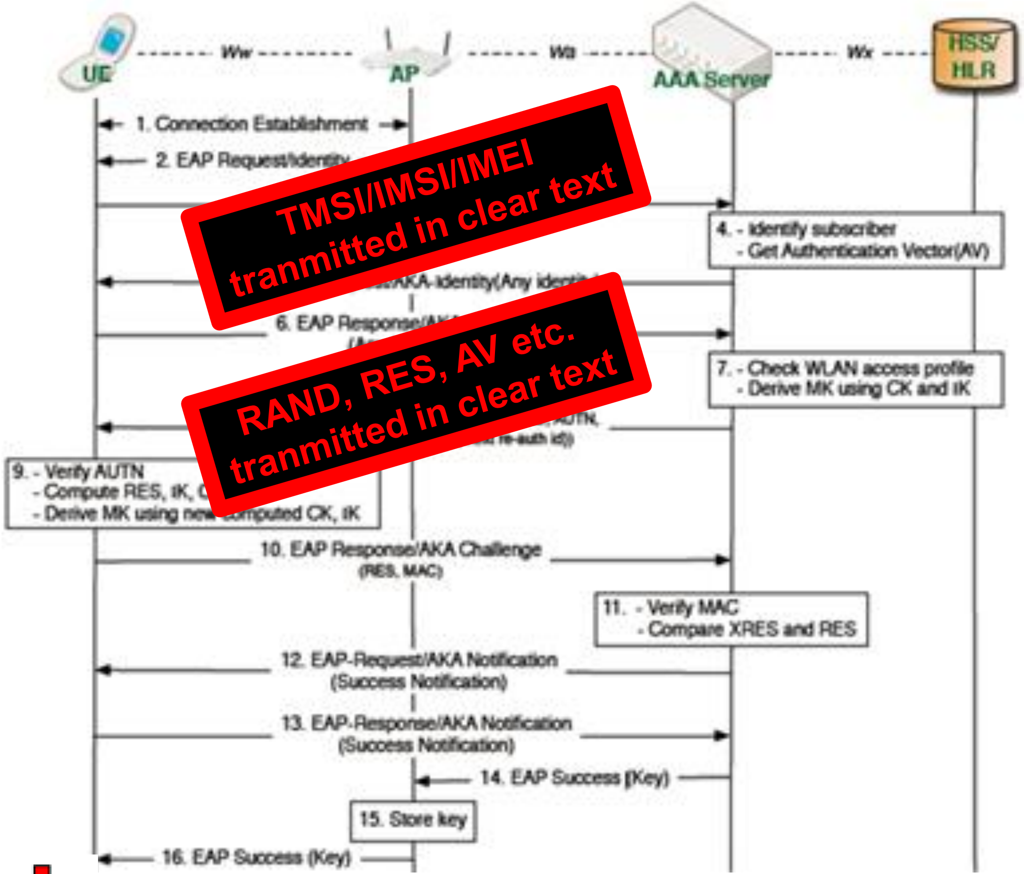
PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Coming back to PHY layer threats and security challenges

Threats and security challenges – examples of radiocells

Figure source

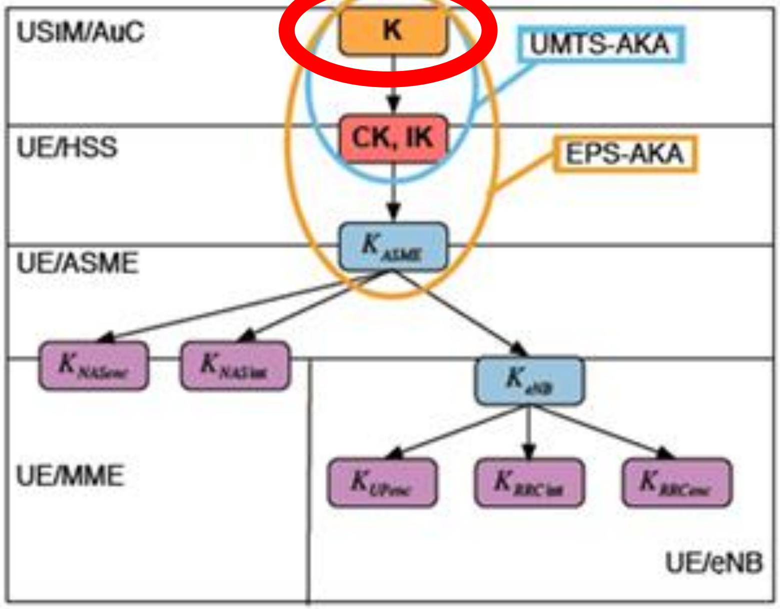
Ref: Hyeran Mun, Kyusuk Han and Kwangjo Kim1-4244-2589-1/09/ $20.00 2009 IEEE,
"3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA »



TMSI/IMSI/IMEI tranmitted in clear text

RAND, RES, AV etc. tranmitted in clear text

Can be hacked or disclosed – see ref.



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 EXCHANGED IN CLEAR TEXT WITHOUT TRANSEC PROTECTION
→ PASSIVE EVE CAN DECODE
→ ACTIVE EVE CAN JAM, SPOOF, REPLAY…
→ MITM EVE CAN IMPERSONATE

WHEN EVE GETS THE KEY K/Ki
SHE BREAKS ALL PROTECTIONS
… BY PASSIVE MEANS ONLY

PIMRC W8 – 2016 September 04 – Welcome - Introduction

PHYLAWS project funded by EC-FP7-ICT-

PHYsical Layer SECurity - How ?

Implantation perspectives into wireless standards

Core ideas for physec-based protection of the PHY layer :

1/ Re-use Channel estimates of the first synchronization and equalization procedures for Channel State Information (CSI)

2/ Input PHYSEC schemes with this CSI :

- ❑ Artificial Noise and Beam Forming
- ❑ Secret Key Generation
- ❑ Secrecy Coding

3/ Protect the early transitted messages in the existing/future RATS

- ❑ Identification request and Ack. messages ((T/I)MSI MAC address)
- ❑ Authentication request and ack. messages
- ❑ Cipher establishment and response messages

=> Thus, Eve has - no more decoding capability of authentication parameters
- no more decoding capability of subscriber/terminal IDs

4/ Add PHY layer protections at on going communication

- ❑ Input of cipher header with SKG
- ❑ Protection of MAC header, IP address, with SKG or SC
- ❑ Integrity control, etc.

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

How PHYsical Layer SECurity - How ?

Implantation perspectives into wireless standards

Improved ideas for physec-based protection of the PHY layer :

Prior to step 1 of the preceding slide

01/ Establish securely paired channels between Alice and Bob

❑ Downlink and Uplink Tag signals (TSs)
❑ Interrogation and Acknowledgement Sequences (IASs)

02/ Negotiate the channel and establish CSI by using TSs and IASs

❑ Channel State information is here Authenticated
❑ Channel State information has more accuracy
❑ TS can support protected Alice-Bob exchanges
⇒ Better security during the SKG processing, longer keys
⇒ Better security during AN-BF and SC establishment

During to step 1, 2, 3, 4 of the preceding slide

Invert the order of Authentication and Identification (in radiocell ntws)

❑ Pre-identication: only UE's HLR has to be transmitted
❑ Authenticate then: needs only HLR Id (and not (T/I)MSI)
❑ Only after Authentication, transmit UE's and Subscriber's IDs.
❑ Therefore, protected Authentication implies protected IMSI transmission

Use of on-going TS and IAS in parrallel to transmission of classical msgs

❑ Integrity control of classical messages, etc.
❑ Use as a low data rate protected control channel

PIMRC W8 – 2016 September 04 – Welcome - Introduction

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

How PHYsical Layer SECurity - How ?

Implantation perspectives into wireless standards

Original Figure source: Y. Zou, J. Zhu, X. Wang, and L. Hanzo, « Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends », Proceedings of the IEEE, **Vol. 104, No. 9, September 2016.**

Short term

I'- PhysecEnhanced
I- ~~Existing~~ EPS-AKA at PHY layer

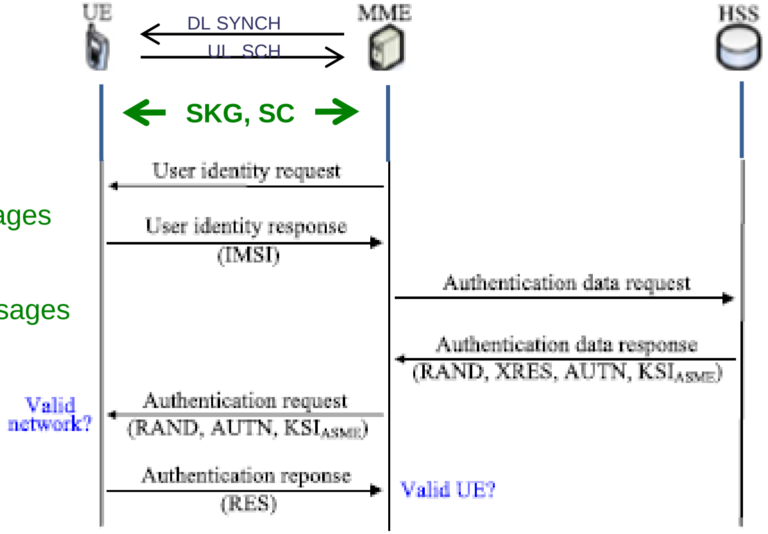
A/ SynchroCH AccessCH, CSI. No protection

A'/ Establishment of physec protections (SKG, AN-BF, SC)

B/ Identification procedure - ~~Clear text messages~~«Physeced » messages

C/ Authentication procedure - ~~Clear text messages~~«Physeced » messages

... then ciphering establishment etc.



Mid term

II- Physec + modified EPS-AKA at PHY layer

01/ Dual sense Tag Signal Tx/Rx under beacon channels
Secure pairing of UE and MME with Interrog. Ack. Sequences

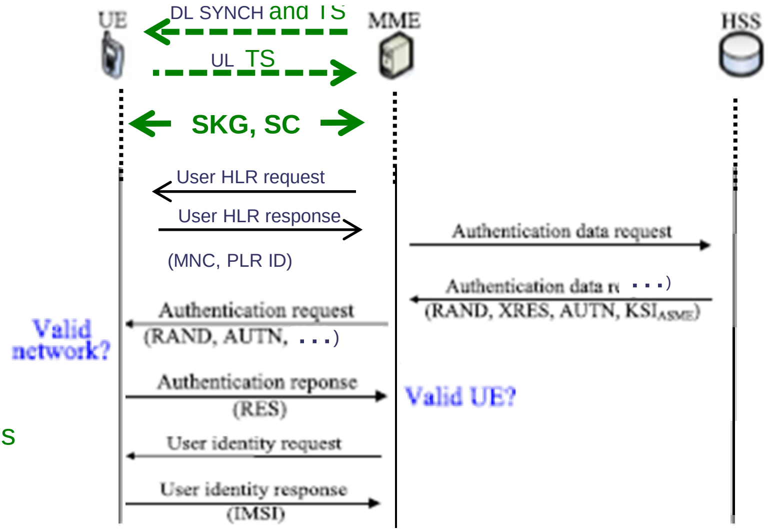
02/ Channel State Information

1/ Establishment of physec protections (SKG, AN-BF, SC)

11/ Pre-identification procedure – with «Physeced » messages

2/ Authentication procedure – with «Physeced » messages

3/ Completed Identification procedure with «Physeced » messages
... then ciphering establishment etc.



PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Maturity check of the Physec technologies

Technology - Application

PHYSEC scheme	Technological Status	Requirement	Secrecy efficiency	Application to public Rats
SKG **-** **Secret Key Gene-ration**	**Mature for TDD RATs** **=> SW add-on only** To be studied for FDD RATs	Authenticated radio channels measur^{Ts} that are shared by Alice and Bob	**NIST & Intel RNG's tests** Directly efficient in mobile environT Improvements exist for fixed geometry Works better with CSI.	IoT and M2M, Automatic Factory 3/4G Radiocells WLANs 5G
SC **-** **Secrecy Coding**	**Schemes now exist** for realistic radio envirT **Apply to TDD+FDD**	Controlled Radio (SINR) advantage. (Artificial Noise & Beam Forming)	Controlled with SNR embedded measur^{T} **Ultimate protection**	MISO and MIMO 3/4G radiocells & WLANs & 5G. IoT + M2M Auto. Factory
SP **-** **Secure Pairing**	**TSs and IASs** **in progress** **Related technos:** ➔ IFF ➔ FuD.	None	Expected high. To be proven experimentally	Signaling and access. RSSI and CSI UIM/identity Auth. IoT + M2M 3&4G - 5G

Synthesis of standardization perspectives

	Technical readiness for standardization	Associated Technology	3GPP Cellular IoT,…	IEEE 802.11ac, …	ITU IoT, 5G,…
SKG - Secret Key Gene-ration	**Ready for standardization of IoT** **Ready year 2016 for FDD RAT standards.** **Ready before year 2020 for FDD RAT standards.**	None	Open a **Study item** at **SA3** Propose **evolution of the PHY layer at RAN**	**Contrib. to PRSG** (Privacy Recommendation Study Group) **and WNG WGs** (Wireless Next Generation) **under RFC 6973** (Privacy Cons. for Internet Prot.)	IoT: Propose a **Contribution to WP5A** under Res. ITU-R 66 (RA-15) IMT 2020 and 5G: .Open a **new question at WP 5D** **.Contribution to WP5D** under Res. COM6/15 (WRC-15)
SC - Secrecy Coding	**Ready year 2016 for TDD and FDD RAT standards**	. Artificial Noise & Beam Forming . Possible TSs and IASs (see below)	Same as above	Same as above	Same as above
SP - Secure Pairing	**TSs and IASs Ready before year 2020 for TDD and FDD RAT standards**	.DSSS .Identification Friend of Foe. . Full Duplex and Self Interf. Mitig.	Same as Above	Same as above	Same as above

PIMRC W8 – 2016 September 04 – Welcome - Introduction

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562

Conclusion - Way ahead

1/ Secret Key Generation is mature

Efficient pre-industrial implantions have been tested OH ➔ **ready for any TDD standards**

One remaining Challenge is the implementation for FDD RATs

2/ Artifical Noise and Beam-Forming are mature

➔ **Standardization into 802.11 and Wi-Fi Alliance**

➔ **ready now for proposals into LTE releases, IoT & Cellular IoT, 5G, etc.**

2b/ Secrecy Coding feasibility proof is achieved !!

« First » SC schemes for realistic radio communications are proposed and tested

➔ **ready in 2016 for proposals into LTE releases, IoT & Cellular IoT, 5G, Wifi)**

3/ Key-free secure pairing of Alice and Bob seems achievable:

Resilient to any kind of threats (Passive, Intelligent Active, Man in the Middle…)
=> Radio protocol close to FuDu RATs with Self Interference Mitigation
=> Practical implementations tested year 2016.

4/ Ready for security upgrade proposals of the PHY layer into WLANs, radiocells, Near Tranmissions and other standards!

Thank you for your presence and your attention

Good PIMRC’2016 Congress !

PHYLAWS project funded by EC-FP7-ICT-2011-8 GN 317562