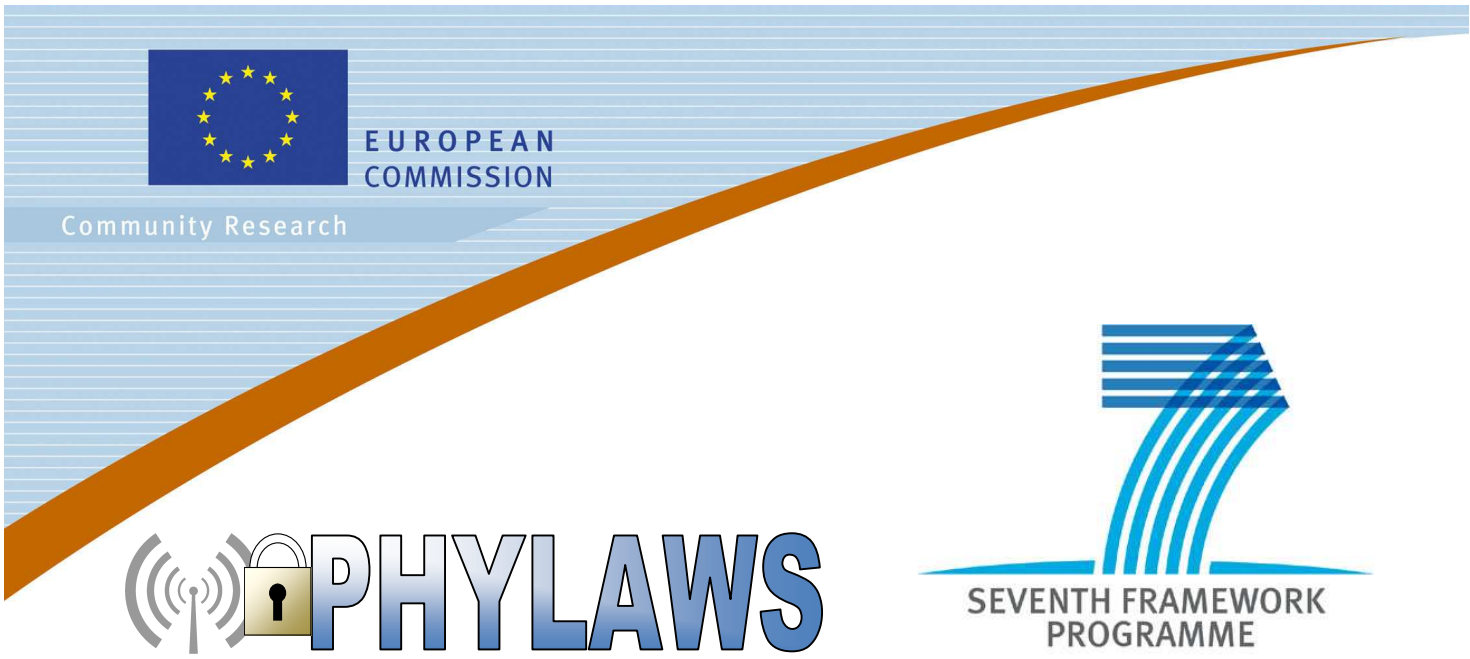

Project PHYLAWS (Id 317562)
PHYsical LAyer Wireless Security

One page description

FP7 Collaborative Projects, Networks of Excellence, Coordination and Support Actions in Collaborative Projects, Research for the benefit of Specific Groups (in particular SMEs)

version 1 - 10 / 10 / 2012

Synthetic Recall of the PHYMAWS project

A/ Problems relevant to future networks that will be solved by the project: The domination of Wireless Communications (as an universal way to access information for nearly every human around the world) **now presents a major risk to society**, because of widely recognized security leaks in the current wireless radio access technologies. **Basically, all of the security today relies on bit level cryptographic techniques** and associated protocols at various levels of the data processing stack, **but these solutions have drawbacks, that are currently major retarders to the progress of the digital society.**

- **Standardized protections within public wireless networks are not secure enough**, and many of their weaknesses are well known.
- The economical importance of protections within public networks highly increases.
- Enhanced cryptographic protections exist, but they occur high constraints and additional costs for the users of public networks

B/ Project solution compared to alternate solutions: In the recent years therefore, **new approaches have been investigated in order to exploit security opportunities offered by the handling signals operating at the physical layer level**. These works have been based on a fundamental analysis of the notion of security **in the context of information theory**: the existing and potential leaks have been seriously addressed and possible ways to avoid them have been investigated too (see references). **On the other side, R&D laboratories and industrial dealing with secured radio-communications have specific experience and practical means in order to design and build secured communications devices.**

The PHYLAWS project will elaborate on this knowledge basis in order to develop focused and synthetic ways to enhance the security of radio-communications in an affordable, flexible and efficient manner, and will propose relevant metrics for evaluation of security enhancements.

C/ Business, industrial or other opportunities for the project solution: simple to implement, easy to develop and validate, requiring no or low hardware modification of existing or future communications devices, the targeted concepts and techniques will also consume less resources, let that be in terms of energy (especially at the terminal level) and in terms of data consumption overhead (i.e. acting on the overall net spectral efficiency). The project outputs will thus **benefit to a wide variety of existing and future standards for a large set of communication services, from citizen to professional needs (GSM, 3GPP, WiFi, LTE…).** Ultimately, PHYLAWS will **facilitate the penetration of wireless technologies in the personal and professional sphere, by guaranteeing a more efficient and safe access to the digital world through the future internet**. Thus PHYLAWS will strongly impact the lives of citizens and will very much contribute to trustworthy ICT in the following years.

D/ Key performance indicators set to measure the project success: These objectives will be reached thanks to **a suitably sized consortium combining complementary skills (academics, R&D center, SME, communication manufacturer), helped by recommendations and advices of an international Advisory Board**, constituted of very high level personalities from governmental and standardization bodies, and academia (this Board will be one of the cornerstones of the project, based on the recognition that excellent technical developments and demonstrations will not be enough to ensure their wide spreading). **This complementary consortium will ensure either advanced researches** (information theory fundamentals, design of optimal codes and modulation schemes) **innovative industrial development** (design of PHYSEC solutions for existing radio networks, design of advanced secured RATs, experiments and simulation of proposed solutions) **and impact towards wireless operators, regulators and users of radio-communication services** in order to assess validation of the commercial goals and to validate of the society use relevance. Assuming well defined objectives, PHYLAWS will apply relevant qualitative and quantitative metrics (recurrent reporting and meetings, pro-active dissemination and standardization efforts, experimental proof of developed concepts, large number of publications in major journals and of participations to congresses) in order verify their achievement in a reliable manner.

Annex - Basic definitions of security concepts

TRANSEC (transmission Security): Transec is relevant to the protection of the wave form face to interception/direction Finding of the transmitted radio signal, to jamming of the user receiver, and to intrusion attempts into the radio-communication access protocol. Transec applies mainly at the radio interface.

NETSEC (Network Transmission Security): Netsec is relevant to the protection of the signalling of the network. Netsec applies mainly either at the radio interface and at the medium access protocol layer, with request to upper protocol layers. Netsec techniques involve mainly transmitter authentification protocols, integrity control and ciphering of signalling data.

COMSEC (Communication Security): Comsec is relevant to the protection of the content of the user messages (voice, data). Comsec applies either at the radio interface and at upper layer. Comsec techniques involve ciphering, authentification and integrity control of signalling and users data at several protocol layer and interfaces (examples are point to point ciphering of each user data flux, ciphering of IP packets, ciphering of artery, etc.).

INFOSEC module or CSS module (Information security Module/cryptographic Sub-System): The Infosec/CSS module manages the generation of pseudo-random data that are used for TRANSEC NETSEC or COMSEC protection

PHYSEC (Physical Layer Security) : generic term that will be used in the project do design all kind of protection technique that is based on the use of the physical layer sensing and/or measurement. Trustworthy[1] is defined as: secure, reliable and resilient to attacks and operational failures; guaranteeing quality of service; protecting user data; ensuring privacy and providing usable and trusted tools to support the user in his security management.