PHYsical LAyer Wireless Security

**PHYLAWS**

**PHYsical LAyer Wireless Security**

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

**Partners:** Institut Mines-Telecom Paris Tech (FR), Imperial College of Science, Technology and Medicine (UK), Teknologian Tutkimuskeskus VTT (FI), Celeno Communications Israel Ltd (IS).

**Duration:** November, 2012 – October, 2015
**Funding scheme:** STREP
**Total Cost:** € 4,070,872
**EC Contribution:** € 2,810,186
**Contract Number:** CNECT-ICT-317562

**Main Objectives**

The domination of Wireless Communications (as 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, the security today relies on bit-level cryptographic techniques and associated protocols at various levels of the data processing stack. These solutions have drawbacks, which 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; even if enhanced ciphering and authentication protocols exist, they occur high constraints and additional costs for the users of public networks; etc.

New security approaches are issued from information theory fundamentals and focus on the secrecy capacity of the propagation channel. PHYLAWS will investigate them for handsets and communications nodes that operate at the radio interface. On the other side, R&D laboratories and industrials dealing with secured radio-networks have specific experience and practical means in order to design secure-improved terminal architectures, wave forms and radio access protocols, and to build relevant embedded modules. PHYLAWS elaborates on these wide knowledge bases in order to enhance the privacy of wireless public radio networks in an affordable, flexible, efficient and measurable manner. The project outputs will benefit to a wide variety of existing and future standards and to a large set of services, from citizen to professional needs (GSM, 3GPP, WiFi, LTE…). PHYLAWS is thus expected to sustain academic research and industrial development, to strongly impact standardization, to facilitate the penetration of wireless technologies in the personal and professional sphere, and to deeply contribute to trustworthy ICT in the following years.

**PHYLAWS intends to** design, prove efficiency and demonstrate realistic implantations of new privacy concepts for wireless networks that exploit radio-propagation phenomena.
Technical Approach

The following technical topics are addressed:

. Study privacy threats for wireless public networks. Establish state of the art and requirements relevant to privacy enhancements of the radio-interface of wireless public networks

. Merge physical layer security concepts (secrecy coding, cooperative jamming, etc.) that are issued from information theory fundamentals, with industrial practices relevant to transmission security (transec), to network security (netsec), and to communication security (comsec).

. Imagine innovative security solutions operating at the physical layer, design trustworthy wave forms and radio access protocols that should take benefit of these concepts, define relevant security metrics.

. Experiment and demonstrate feasibility and efficiency of these new concepts for local loop applications: WiFi.

. Simulate and proof feasibility and efficiency of these new concepts for radio-cells: LTE.

Key Issues

Assuming these well-defined objectives, PHYLAWS will apply relevant qualitative and quantitative metrics in order verify their achievement in a reliable manner: recurrent reporting and meetings, pro-active dissemination and standardization efforts, experimental and simulation proof of developed concepts, large number of publications in major journals and of participations to congresses.

In addition, the project will be helped by recommendations and advice of an international Advisory Board, constituted of very high level personalities from governmental bodies, 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.

Project organisation

Finally, PHYLAWS is organised in five technical work packages completed with a management work package (that includes reporting, dissemination tasks, standardization efforts, relationship with the Advisory Board), such as described in the following figure:

Expected Impact

The complementary skills of partners are expected to ensure both innovation and impact towards industrial applications, to assess validation of the commercial goals and of the society use relevance (economical, legal etc.).

The project impact will largely benefit from an academic + industrial merged vision, from realistic feasibility proof and from the Advisory Board councils. Our purpose is to penetrate existing and future standards at first, and then to ensure support from the major stakeholders.

Security notions

Transmission security is relevant to the protection of the transmitted radio signal face to interception, to jamming, and to intrusion attempts into the radio access protocol at the physical layer.

Network security is relevant to the protection of the signalling of the network. It involves authentication protocols, integrity control and ciphering of signalling data.

Communication security is relevant to the protection of the content of the user messages (voice, data, SMS…). It usually involves ciphering and integrity control at several layers of the protocol stack (IP packets, artery…).

Physical layer security is a generic expression that is used for all kind of protection based on the use of the radio-interface characteristics.