EUROPEAN COMMISSION

Community Research

SEVENTH FRAMEWORK PROGRAMME

ICT Call 8

PHYLAWS
PHYsical LAyer Wireless Security
Brief synthesis of the project

Concertation Meeting
Brussels, 10 October 2012

Negotiation Meeting Brussels, 23-May 2012

BRIEF SYNTHESIS OF THE PROJECT IN FIVE SLIDES

Problems relevant to future networks that will be solved by the project

⇒ Slide p 3 on the needs of the PHYLAWS project

Project solution compared to alternate solutions:

=> Slide p.4 on the Main objectives of the project.

=> Slide p.5 on the main technical objectives

Business, industrial or other opportunities for the project solution

=> Slide p.6 on the expected concrete results

Key performance indicators set to measure the project success:

=> Slide p.7 on the measurable success criteria

Annexes

Pbs relevant to future networks that will be solved - Need of the PHYLAWS project

Wireless communications have become dominant to access information for citizen, for economical actors, for administrations, etc.

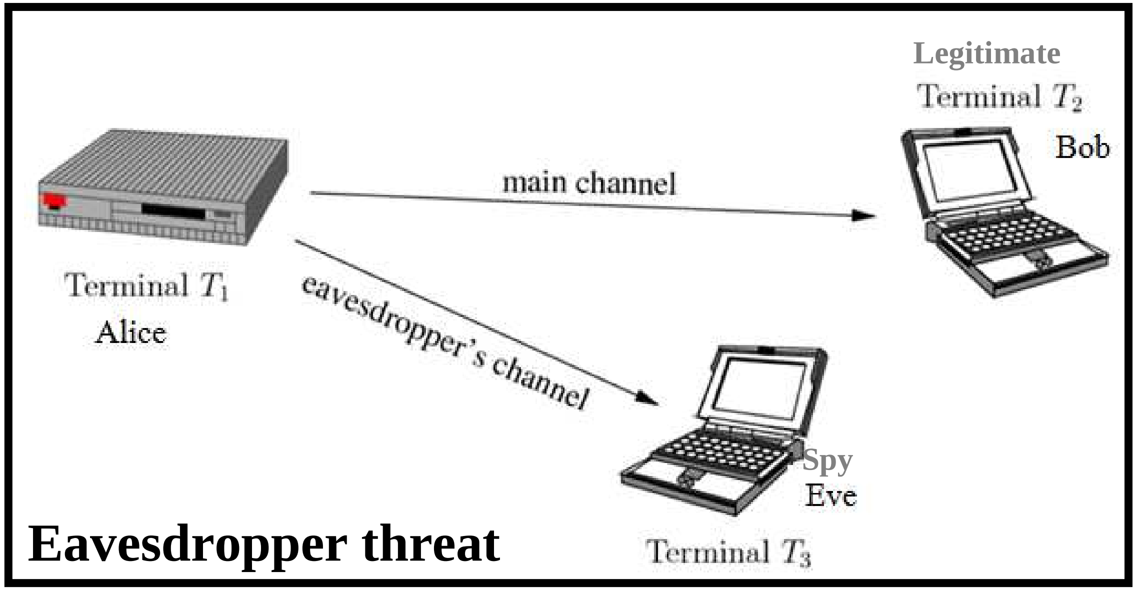
Protection leaks and non-suffisant security technologies of the current civilian wireless networks also **induce major risks to society**

Dedicated Authentification procedures and crypto. techniques exist but

- They reduce spectrum efficiency, increase computations latencies and complexity
- They induce added costs
- They are often not sufficiently secure, especially for worldwide public wireless systems.

PHYLAWS is needed to counter these difficulties in order to sustain the progress of the digital society and wide band internet for

- Future networks
- Trustworthy ICT



Eavesdropper threat

Negotiation Meeting Brussels, 23-May 2012

PHYLAWS FP7 ICT call 8 - Id 317562

Project solution compared to alternate solutions - Main objectives of the project

Enhance the security of wireless communications in an affordable, flexible and efficient manner : apply fundamentals of security and information theory in order to upgrade and design suitable radio architectures, wave forms and protocol stacks

Elaborate, study and demonstrate of TRANSEC and NETSEC upgrades :

- add PHYSEC concepts to existing authentification and cyphering procedures
- exploit the characteristics of the wireless radio channel, especially when dispersive
- enhance wave forms and radio access protocol of digital radio networks.
- search for easily developed and easily validated algorithms,
- consume less resources : less energy of the terminal level, reduced data consumption overhead (i.e. upgrade the spectral efficiency).
- reduce security management costs in wireless networks.

Facilitate the penetration of wireless technologies in the personal and professional sphere, guarantee a more efficient and safe access to the digital world through the future internet. Target a wide set of existing and future uses.

Disseminate PHYSEC solutions, propose upgrades to existing and influence new standards.

Project solution compared to alternate solutions - Main technical objectives

Review theorical and practical constraints of eavesdroppers:

Remain reasonable: no angelic but no paranoia. Physical constraints apply to Eve too.
Distinguish legal/administrative interceptions and radio non legal/pirates/hackers threats.

Target a wide set of existing and future wireless networks:

Focus on worldwide spread local loop : WiFi - experimental proof of concepts.
Focus on worldwide 4G radiocells : LTE - proofs of concepts based on simulation.
Study/demonstrate feasibility to existing 2G/3G radiocells, to PMR, to peripheral Wireless.
Short Range communication (Bluetooth, Zigbee, etc.).
Derive new secure communications services:

. wireless broadband internet,
. wireless e-commerce, wireless bank operations,
. machine to machine,
. inter-device communication
. 3G/4G network management (with sensing and network local downloading, etc.).

Upgrade existing and imagine new security concepts with PHYSEC:

- Secrecy coding
- Enhanced Cooperative Jamming
- Combination of PHYSEC and self synchronizing cyphering schemes.
- Combine SIMO and MIMO RAT with secrecy coding, with transec/netsec protections,
- Study capabilities of Double Talk modems transposed to earth communications.
- Study capabilities of IFF wave forms and protocols.

Business, industrial or other opp. for the project solution - Expected concrete results

Add of physical dependant random at the transmitted signal and combine PHYSEC capabilities with other security procedures.

=> Upgrade existing security and propose new concepts

=> Establish new wireless security metrics,

=> Proof feasibility of the proposed PHYSEC upgrade/concepts

=> Demonstrate performances

- Experimental proof for secure upgraded WiFi
- Simulation proof for LTE-based cellular systems

Upgrade the security of wireless networks and reduce its cost. Identify the relevant services / economical / industrial applications

=> Evaluate the added economical value

=>Evaluate the citizen benefit

=> Search/propose for industrial application

Disseminated the most promising PHYSEC outputs, maximize their impact, take into account legal and administrative implications.

=> publications and patents

=> propose standardization : upgrade of existing, influence new standards

=> take into account legal/policies implications of security ugrades

Key performance indicators - Measurable success criteria

QUAL: qualitative objectives and QUANT: quantitative objectives, will be achieved and measured by :

- contents of reports
- content of demonstrations
- content of simulations
- patent actions
- dissemination actions
- standardization actions

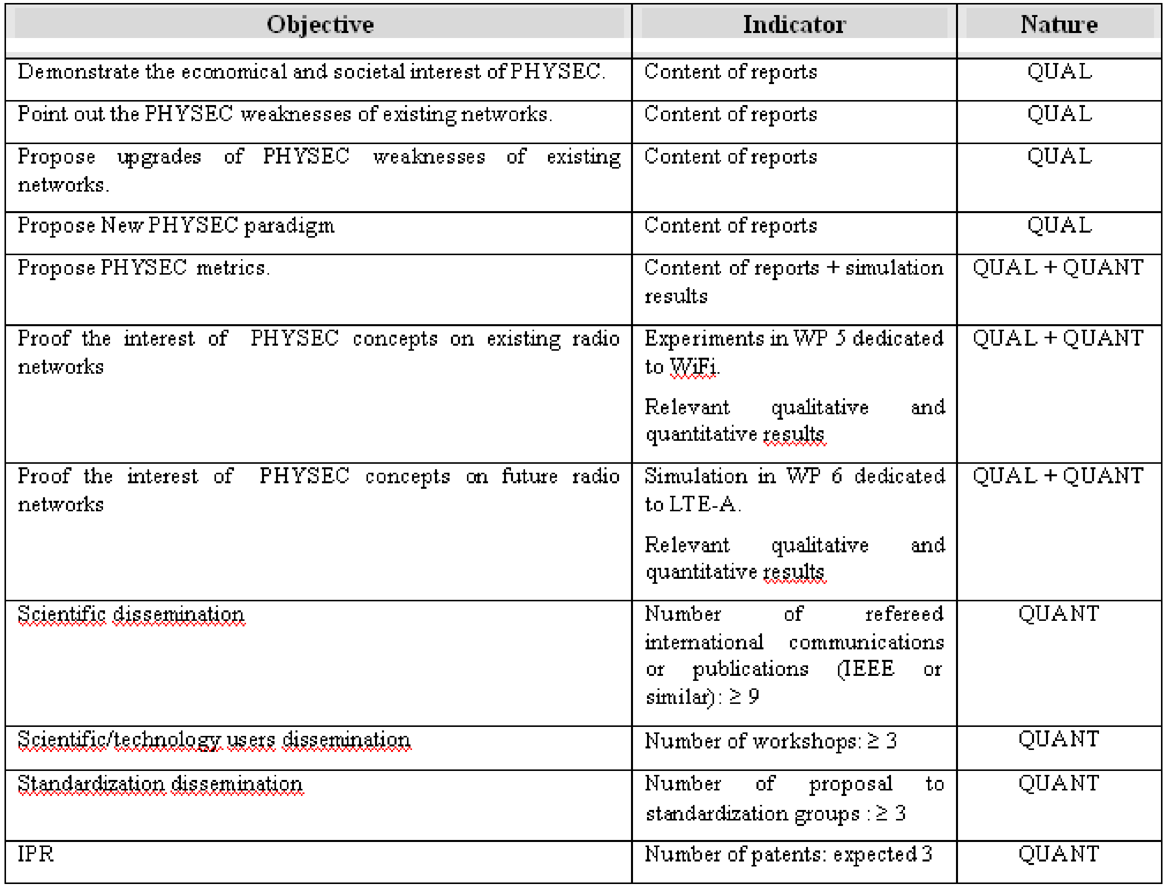
=> 17 to 20 publications

- **papers,**
- **conferences**

=> Extended dissemination

- **about 40 reports**
- **most of reports are PU**

Recall of PHYLAWS objectives and of metrics to verify their achievement



Objective	Indicator	Nature
Demonstrate the economical and societal interest of PHYSEC.	Content of reports	QUAL
Point out the PHYSEC weaknesses of existing networks.	Content of reports	QUAL
Propose upgrades of PHYSEC weaknesses of existing networks.	Content of reports	QUAL
Propose New PHYSEC paradigm	Content of reports	QUAL
Propose PHYSEC metrics.	Content of reports + simulation results	QUAL + QUANT
Proof the interest of PHYSEC concepts on existing radio networks	Experiments in WP 5 dedicated to WiFi. Relevant qualitative and quantitative results	QUAL + QUANT
Proof the interest of PHYSEC concepts on future radio networks	Simulation in WP 6 dedicated to LTE-A. Relevant qualitative and quantitative results	QUAL + QUANT
Scientific dissemination	Number of refereed international communications or publications (IEEE or similar): ≥ 9	QUANT
Scientific/technology users dissemination	Number of workshops: ≥ 3	QUANT
Standardization dissemination	Number of proposal to standardization groups : ≥ 3	QUANT
IPR	Number of patents: expected 3	QUANT

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.

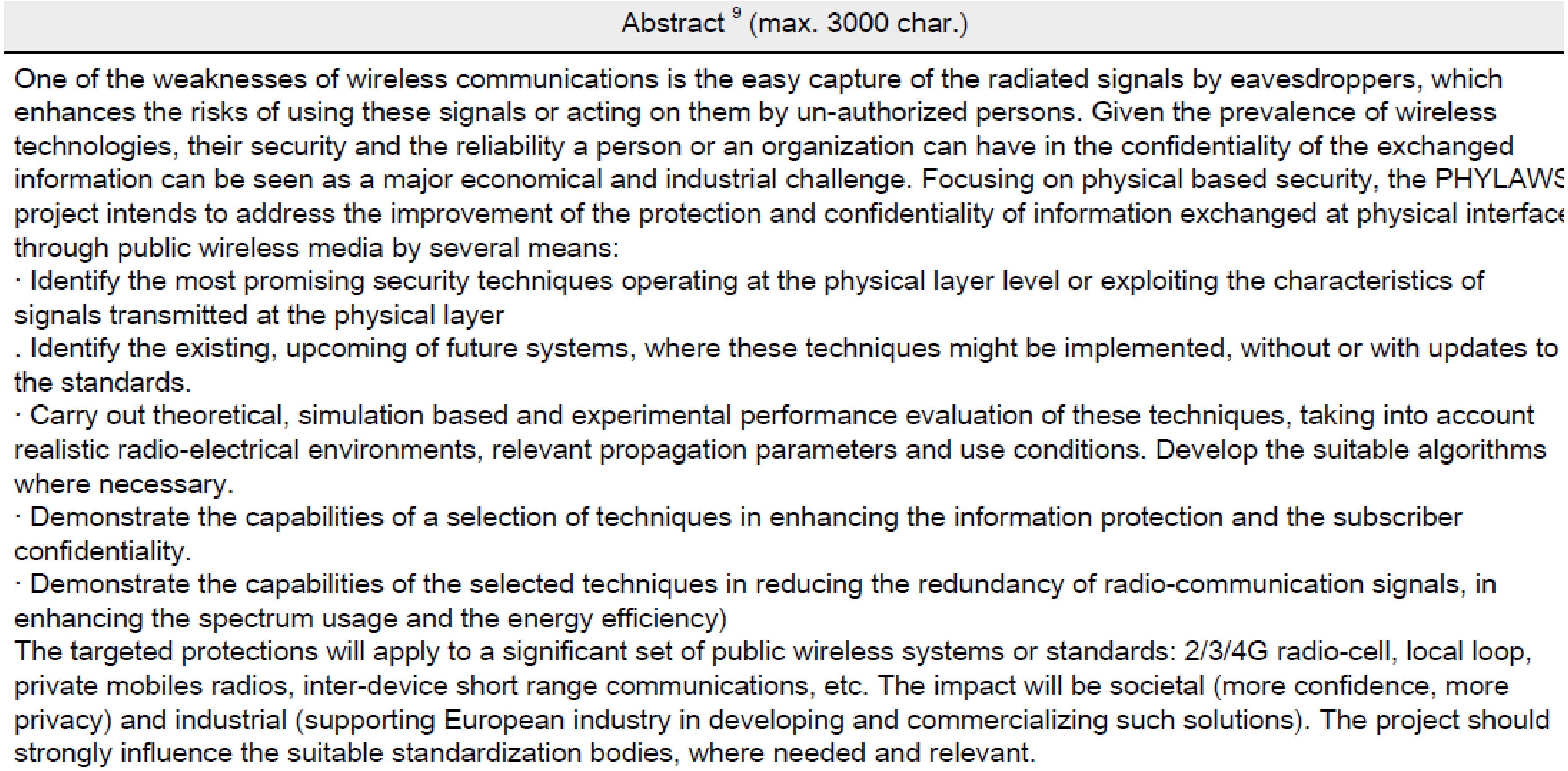
NETSEC (Network Transmission Security): Netsec is relevant to the protection of the signalling of the network. Netsec applies mainly either at the radio interface and at the medium access protocol layer, with request to upper protocol layers. Netsec techniques involve mainly transmitter authentification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

RECALL – ABSTRACT OF PHYLAWS



Abstract [9] (max. 3000 char.)

One of the weaknesses of wireless communications is the easy capture of the radiated signals by eavesdroppers, which enhances the risks of using these signals or acting on them by un-authorized persons. Given the prevalence of wireless technologies, their security and the reliability a person or an organization can have in the confidentiality of the exchanged information can be seen as a major economical and industrial challenge. Focusing on physical based security, the PHYLAWS project intends to address the improvement of the protection and confidentiality of information exchanged at physical interface through public wireless media by several means:

· Identify the most promising security techniques operating at the physical layer level or exploiting the characteristics of signals transmitted at the physical layer

. Identify the existing, upcoming of future systems, where these techniques might be implemented, without or with updates to the standards.

· Carry out theoretical, simulation based and experimental performance evaluation of these techniques, taking into account realistic radio-electrical environments, relevant propagation parameters and use conditions. Develop the suitable algorithms where necessary.

· Demonstrate the capabilities of a selection of techniques in enhancing the information protection and the subscriber confidentiality.

· Demonstrate the capabilities of the selected techniques in reducing the redundancy of radio-communication signals, in enhancing the spectrum usage and the energy efficiency)

The targeted protections will apply to a significant set of public wireless systems or standards: 2/3/4G radio-cell, local loop, private mobiles radios, inter-device short range communications, etc. The impact will be societal (more confidence, more privacy) and industrial (supporting European industry in developing and commercializing such solutions). The project should strongly influence the suitable standardization bodies, where needed and relevant.