

Preface

In recent years, communication and data security is becoming of paramount importance, and some significant academic and industrial research efforts are being directed in this area.

Besides classical approaches to security, new paradigms are taking root, with immense potential in a number of scenarios. Among them, physical layer security is one of the most fascinating, though partly unexplored research areas. The first impulse to this approach has been given in the seventies with Wyner's study on the wiretap channel, and since then this field knew an exponential growth. The chance to exploit the random and unique character of the transmission channel to achieve security and authentication is very attractive, and may pave the way to new and more user-oriented security solutions.

However, physical layer security is still not sufficiently mature to provide practical solutions to be included in current communication systems and standards, therefore some effort is still needed in this direction. On the other hand, classical solutions rely on computational security techniques, like cryptography, and work at the data-link layer, assuming perfect transmission at the physical layer. This is a known limit of classical security techniques, especially when they are used over the wireless channel, which always represents a great security challenge, due to its intrinsic broadcast nature. In several occasions, the use of classical security solutions over the wireless channel has resulted in overlooked security threats and vulnerabilities, thus demonstrating the need for a more comprehensive security design, starting at the physical layer. Despite this, the integration of physical and data-link layer security techniques is still in initial stages. Other channels, as the powerline communication channel, pose similar problems as the wireless transmissions, as well as many privacy concerns for the applications usually running on this medium.

The *enhancing communication security by cross-layer physical and data-link techniques* (ESCAPADE) research project supported by the Italian Ministry of Education aims at providing a contribution in the direction to fill the gap, by studying innovative and practical physical and data-link layer security techniques,

as well as their integration. The Workshop on Communications Security (WCS 2014) was organized in the framework of the project to foster discussion among researchers working in both these fields, with the aim to address important open problems in the relevant areas and exchange new ideas concerning the links between them.

This book originates from the workshop, and collects extended versions of the works presented on that occasion, together with some relevant invited contributions, addressing some of the most important problems in the two fields of physical and data-link layer security techniques. We believe that this can provide a useful collection of reference material to those interested in these areas, thus fostering the adoption of mixed physical and data-link layer security solutions.

The first part of the book is devoted to physical layer security, with an invited tutorial on advances in this area, starting from a general view and then focusing on some specific scenarios and practical techniques. Among them, we find the use of fading channels and practical codes to achieve security, which are two important solutions in this area, addressed in detail in the next two chapters. Then, two important variants of the basic physical layer security setting are considered, that is, transmission over broadcast channels with confidential messages and extraction of secret keys from the wireless channel. The implementation of these techniques in practical scenarios is then addressed by two chapters on key extraction in ultra wideband transmissions and power line communication networks. The security features of two special settings are then studied. In fact, the next two chapters focus on security in compressed sensing—where the aim is to reduce the sampled size of signals—and fuzzy vaults—which aim at providing secure authentication based on biometric features. The latter chapter opens the second part of the book, which is devoted to computational security techniques, with contributions concerning cryptosystems, like the Naccache-Stern and AES schemes, and their cryptanalysis. The last two chapters of the book provide an insight into the implementation of security and authentication techniques in practice, which is an important target to achieve by any newly introduced security solution.

The editors wish to gratefully acknowledge Franco Chiaraluce and Nicola Laurenti for their precious help throughout the ESCAPADE project, and Nicola Maturò and Giacomo Ricciutelli for their tireless support concerning the organization of WCS 2014.

We also want to thank Matthieu Bloch, Arsenia Chorti, David Elkouss, Frederic Gabry, Ingmar Land, Ayoub Otmani, Edoardo Persichetti, Francesco Renna, Davide Schipani, and Aydin Sezgin for having reviewed the chapters and helped to improve the book quality.

Ancona, Paris
June 2015

Marco Baldi
Stefano Tomasin



<http://www.springer.com/978-3-319-23608-7>

Physical and Data-Link Security Techniques for Future
Communication Systems

Baldi, M.; Tomasin, S. (Eds.)

2016, X, 212 p., Hardcover

ISBN: 978-3-319-23608-7