

Title: Security and Cooperation in Wireless Networks
Duration: Half Day (3 hours)
Speaker: Prof. Levente Buttyán

Affiliation:

Laboratory of Cryptography and System Security (CrySyS)
Department of Telecommunications
Budapest University of Technology and Economics

Rational: the overall objective of the tutorial:

We have entered the era of wireless networks: by now, the number of wireless phones has superseded the one of wired ones; wireless LANs are routinely used by millions of nomadic users; wireless devices have become commonplace in private houses, factories, and hospitals; and technologists promise us a world of ubiquitous computing, in which myriads of tiny, untethered sensors and actuators will communicate with each other, promptly taking care of our various needs and wishes.

In addition to this pervasiveness, we are witnessing a change of paradigm: initially, wireless networks (such as cellular networks) used to interconnect devices of no or limited programmability, in a highly centralized fashion. Nowadays, high tier end systems are full-fledged personal computers, taking an increasingly active role in the networking mechanisms: in the extreme case of multi-hop ad hoc networks, the end systems *are* the network.

Unfortunately, this evolution is creating new vulnerabilities; even existing wireless networks (and especially wireless LANs) exhibit a number of security weaknesses, some of which have been painstakingly fixed *a posteriori*. It is now clear to everyone that the security solutions devised for wired networks cannot be used as such to protect the wireless ones.

The purpose of this tutorial is to contribute avoiding that ubiquitous computing becomes a ubiquitous nightmare. We believe that the protection of wireless networks now requires more attention, and a more systematic approach. In addition to the usual security concerns, we need to address *selfish* behavior. Indeed, each wireless communication makes use of a fraction of the spectrum, which has been and will remain a scarce resource; in addition, most wireless devices are battery-powered, and for them energy is scarce as well. This is the reason why we mention "cooperation" in the title of this tutorial.

Outline: a brief structure of the tutorial:

1. New wireless networks and new challenges (30')

In this first part we explain what is changing in wireless networks. Their organization is moving from centralized to self-organized, meaning that security must be redesigned accordingly. The programmability of the end user device opens the door to much more sophisticated attacks, and greedy behavior becomes a serious threat. The emergence of wireless communications between embedded systems (e.g., wireless sensors, or cars) means that communication does not necessarily involve people anymore. Multi-hopping requires secure routing and cooperative packet forwarding. Miniaturization means limited computing power and battery constraints, hence limited resources to carry out sophisticated operations for security. Finally, the pervasiveness of technology raises major privacy concerns. This evolution raises a number of new challenges that we describe, and which motivate Parts 2 and 3 of this tutorial. In this introductory part, we also present a few examples, which we also use in Parts 2 and 3, such as wireless sensor

networks, vehicular networks, and RFID systems. We also stress the crucial role that trust is going to play in this field.

2. Thwarting malicious behavior

In this part of the tutorial, we focus our attention on mechanisms to thwart malicious attacks. More specifically, we concentrate on fundamental security issues in wireless networks, such as naming and addressing, key establishment, and secure routing. We introduce the background, present basic concepts, and illustrate them with examples taken from concrete proposals published in the literature.

2.0 Brief introduction to cryptography and security techniques (20')

2.1 Naming and addressing (20')

2.2 Key establishment (20')

2.3 Secure routing (30')

3. Thwarting selfish behavior

In this last part, we focus on the danger of greedy behavior of the users or the operators. We provide the appropriate theoretical background to model this problem, and we illustrate this topic by two examples: selfishness in packet forwarding and operators competing for serving users in a shared spectrum.

3.0 Brief introduction to game theory (20')

3.1 Selfishness in packet forwarding (20')

3.2 Operators in shared spectrum (20')

Intended audience:

The potential audience includes researchers in wireless networks from academia and corporate research centers. In order to fully benefit of this tutorial, a participant should have some background in wireless networking and at least a basic knowledge of security principles.

Biography of the speaker:

Levente Buttyán was born in 1970 in Salgótarján, Hungary. He received the M.Sc. degree in Computer Science from the Budapest University of Technology and Economics (BME) in 1995, and earned the Ph.D. degree from the Swiss Federal Institute of Technology -- Lausanne (EPFL) in 2002. From 1997 to 2002, he worked in the group of Prof. Jean-Pierre Hubaux in the Laboratory of Computer Communications and Applications at EPFL. In 2003, he joined the Department of Telecommunications at BME as Assistant Professor; he was promoted to Associate Professor in 2006.

At BME, he played an instrumental role in setting up a special education program on Security of Information and Communication Systems in 2003. Within the context of this program, he teaches two courses: Network Security Protocols, and Foundations of Secure Electronic Commerce.

Within the Department of Telecommunications, he works in the Laboratory of Cryptography and Systems Security (CrySys) where he supervises PhD students and leads various national and international research projects (see <http://www.crysys.hu/research.html> for more details). His research interests are in the design and analysis of security protocols for wired and wireless networks, including wireless sensor networks, vehicular networks, and delay tolerant networks.

He is an editor of the Hungarian journal Híradástechnika (Communication techniques), and was a guest editor of the IEEE Journal on Selected Areas in Communications, Special Issue on Non-cooperative Behavior in Networking. He has served on the Program Committee of various conferences and workshops. He is member of the Steering Committee of the European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS). (see <http://www.hit.bme.hu/~buttyan/cv.html> for more details)

He has co-authored around 60 scientific publications (see <http://www.hit.bme.hu/~buttyan/publications.html> for more details).

He is a member of the ACM. He has held visiting positions at EPFL.

Currently, he is completing the manuscript of a book together with Prof. Jean-Pierre Hubaux from EPFL. The title of the book is the same as the title of the proposed tutorial, and the tutorial will be based on the contents of this book. The book will be published by Cambridge University Press in 2007. More information (including the full manuscript in pdf format) can be found at the web site of the book at <http://secowinet.epfl.ch/>

Levente Buttyan has been teaching undergraduate courses at the Budapest University of Technology and Economics on Network Security, Secure Electronic Commerce, and Cryptography for 4 years. Part of these courses are based on the material of the proposed tutorial. He also gave a 4 hour tutorial on Internet Security for a private company.