Mobile and Wireless Networks Security

MWNS 2009. May 15th 2009, Aachen Germany

MWNS 2009

General co-Chairs

Chaouchi, Hakima,
Telecom SudParis, France

Maknavicius, Maryline,
Telecom SudParis, France

Technical Program Committee Chair

Carle, Georg,
University of Tübingen, Germany

Technical Program Committee

Alonistioti, Nancy,
University of Pireus, Greece
Benslimane, Abderrahim,
University of Avignon, France
Bader, Faouzi,
CTTC, Spain
Badra, Mohamad,
CRNS LIMOS Laboratory, France
Beylot, André-Luc,
ENSEEIHT, France
Carle, Georg,
University of Tübingen, Germany
Chaouchi, Hakima,
Telecom SudParis, France
Cho, David,
Nanyang Tech. University, Singapore
Combes, Jean Michel,
Orange Labs, France
Friderikos, Vasilis,
King's College of London, UK
Ganchev, Ivan,
University of Limerick, Ireland
Hecker, Arthur,
ENST, France
Heen, Olivier,
INRIA, France
Jose, Araujo,
Alcatel Lucent, France
Maknavicius, Maryline,
Telecom SudParis, France
Moustafa, Hasnaa,
Orange Labs, France
Naït-Abdesselam, Farid,
University of Lille, France
Nogeira, Jose Marcos,
UFMG, Brazil
O'Droma, Mairtin,
University of Limerick, Ireland
Pujolle, Guy,
University of Paris VI, France
Roux, Kobus,
Meraka Institute, South Africa
Schoo, Peter,
DoCoMo Euro-Labs, Germany
Veysset, Franck,
Orange Labs, France

Workshop Scope

Network security being for many years addressed in wired networks, it becomes more and more challenging in mobile and wireless networks since those environments are widely open and accessible.

In this context, mobile and wireless terminals and communication are more vulnerable than wired terminals and networks to different attacks such as denial of service, man in the middle, hijacking, spoofing, etc. In addition, they have less resources which is a real problem in security solution design. This poses new challenges in a sense that we need to design secure and robust solution and light enough to be supported by those wireless and mobile terminals and communications.

Different wireless and mobile technologies are available today such as RFID, Wifi, Wimax, 3G, etc. promising the deployment of a variety of services for mobile users. However, security needs to be robust enough in order for the user to trust the services offered on top of those technologies. Other technologies such as ad hoc or sensor networks are also very interesting for new type of services, but they also need to prove that security level is high enough to support user services.

After a successful MWNS 2008 workshop held in Singapore, this year the workshop will be held on the last day on the IFIP Networking 2009 on May 15th. This international workshop on mobile and wireless network security is seeking original research work. It addresses and is not limited to these topics:

- *Security in wireless PAN, LAN, MAN, RAN*
- *Security in Mobile networks (2G, 3G, 4G, …)*
- *Security in IP Mobility networks*
- *Security in ad hoc networks*
- *Security in Mobile P2P*
- *Security in sensor/RFID networks*
- *Fault tolerance and Self-healing*
- *Security policies and models*
- *Security of wireless and mobile terminals (smart cards, biometry, …)*
- *Privacy, anonymity, and tracking*
- *Identity management*
- *AAA — Authentication, Authorisation , Accounting*

MWNS 2009
Co-located with
Networking 2009

May 15, 2009,
Aachen, Germany

Important Dates

- **Paper Submission**
  December 15th, 2008
- **Acceptance Notification**
  January 31st, 2009
- **Camera Ready Due**
  February 23rd, 2009
- **Workshop**
  May 15, 2009