IFIP NETWORKING 2006

SecPri_MobiWi 2006:
Workshop on
Security and Privacy in Mobile and Wireless Networking

May 19, 2006, Coimbra, Portugal

Aims and Scope

Mobile and Wireless communication networks offer organizations and users several benefits, such as portability, mobility and flexibility, while increasing everyday business productivity, and reducing installation cost. *Wireless Local Area Networks*, for instance, have been used in various environments, such as business, home, conference centers, airports and many more, allowing users to move from place to place, avoiding cabling restrictions and without being disconnected from the network. *Ad Hoc Networks* are collections of wireless computers communicating among themselves over possibly multihop paths, without the help of any infrastructure such as base stations or access points; these networks allow data synchronization with network systems and application sharing between devices. *Mobile Ad Hoc Networks* are autonomous collection of mobile entities that communicate over relatively bandwidth constrained wireless links, establishing survivable, efficient, dynamic communication for emergency operations. *Wireless Ad Hoc Sensor Networks* consist of a number of sensors spread across a geographical area, offering certain capabilities and enhancements in operational efficiency in civilian applications, as well as assisting in international effort to increase alertness to potential threats.

However, although Mobile and Wireless Networking environments eliminate many of the problems associated with traditional wired networks, the new security and privacy risks introduced by such environments need to be reduced by exploiting appropriate security measures and safeguards, ensuring an acceptable level of overall residual hazard.

The objectives of the *SecPri_MobiWi 2006* Workshop are to bring together researchers from research communities in Mobile and Wireless Networking, Security and Privacy, with the goal of fostering interaction.

List of topics

We welcome the submission of papers from the full spectrum of issues related with *Security and Privacy in Mobile and Wireless Networking.* Papers may focus on protocols, architectures, methods, technologies, applications, practical experiences, simulation results and analysis, theory and validation on topics include, but not limited to:

• Cryptographic Protocols for Mobile and Wireless Networks

• Key Management in Mobile and Wireless Computing

• Reasoning about Security and Privacy

• Privacy and Anonymity in Mobile and Wireless Computing

- Public Key Infrastructure in Mobile and Wireless Environments
- Economics of Security and Privacy in Wireless and Mobile environments
- Security Architectures and Protocols in Wireless LANs
- Security Architectures and Protocols in B3G/4G Mobile Networks
- Security and Privacy features into Mobile and Wearable devices
- Location Privacy
- Ad hoc Networks Security
- Sensor Networks Security
- Wireless Ad Hoc Networks Security
- Role of Sensors to Enable Security
- Security and Privacy in Pervasive Computing
- Trust Establishment, Negotiation, and Management
- Secure PHY/MAC/routing protocols
- Security under Resource Constraints (bandwidth, memory, energy, and computation constraints)

SecPri_MobiWi 2006 Workshop Program co-Chairs

Stefanos Gritzalis, University of the Aegean, Greece (sgritz@aegean.gr)

Angelos Rouskas, University of the Aegean, Greece (arouskas@aegean.gr)

Charalabos Skianis, University of the Aegean, Greece (cskianis@aegean.gr)

Paper Submission

The *SecPri_MobiWi 2006* workshop welcomes original papers from academic, government, and industry contributors dealing with the above or related issues. Papers, which describe ongoing research or provide an excellent surveying work, are welcome too. All submissions will be subjected to a thorough review by at least three reviewers. Submitted papers should be up to 6.000 words in English, including tables, figures, bibliography and well-marked appendices. The paper must start with a title, paper's authors names and affiliations, a short abstract of about 150 words, a list of 3-5 keywords, as well as the corresponding author's email and postal address, following the template indicated by Springer LNCS Series http://www.springer.de/comp/lncs/authors.html. Following the IFIP NETWORKING 2006 procedures, papers must be submitted electronically using the following link: http://www.webchairing.com/wsec/submission/. Problems related with paper submission should be reported to networking2006@dei.uc.pt. At least one author of each accepted paper is required to register at the IFIP Networking 2006 Conference and present the paper at the Workshop.

Proceedings

Accepted papers will be published in the *SecPri_MobiWi 2006* Proceedings under an ISBN reference and will be distributed to the workshop attendees. The best papers of the *SecPri_MobiWi 2006* will also be considered publication for a limited Book and/or special issue Journal edition.

Important Dates

Submission of papers: March 5, 2006

Notification of acceptance/rejection: March 20, 2006

Camera-ready version of papers: April 1, 2006

SecPri_MobiWi 2006 Workshop date: May 19, 2006