Synopsis

We are witnessing a phenomenal growth in wireless communications and untethered computing technology. In fact, wireless communications have triggered a paradigm shift that is expected to have a significant impact on applications ranging from military, to scientific, to industrial, to healthcare, to domestic, establishing ubiquitous wireless networks that will pervade society redefining the way in which we live and work.

However, wireless networks are only as good as the information they produce. Due to the fact that individual nodes in the network communicate by radio, wireless networks are inherently vulnerable to security attacks. In this respect, perhaps the most important concern is information security. Indeed, if an adversary can thwart the work of the wireless network by perturbing the information produced, stopping production, or pilfering information, then the perceived usefulness of these networks will be drastically curtailed.

Given the importance of securing wireless networks, it is not surprising that the past few years have seen a flurry of activity in the area with dozens of papers published in the open literature. As a consequence, important advances have been made and a consensus is emerging in the research community: while securing wireless networks is a daunting task, effective solutions are close at hand. Unfortunately, in spite of these advances, many people still do not know exactly what the weaknesses of wireless networks are. As a result, most have accepted the prevailing wisdom that wireless networks are inherently insecure and nothing can be done about it. Can wireless networks be deployed securely today? What exactly are the security holes in the current standard, and how do they work? Where is wireless security headed in the future?

The main goal of this NATO-sponsored workshop is to bring together leading researchers and practitioners in an attempt to identify the fundamental challenges and future prospects. Technical papers describing original, previously unpublished research, not currently under review, are solicited. We are especially interested in the theory, practice, and evaluation of security solutions in wireless communications. Topics of interest include but not limited to:

- Secure architectures, protocols and tools
- Vulnerabilities, attacks and countermeasures
- Anonymity in wireless networks
- Self-awareness and context-awareness
- Resilient virtual infrastructures
- Adaptive security support
- Formal representation and verification
- Privacy-aware services
- Testbeds, simulation and visualization
- Prototypes and hands-on experience with secure wireless systems

For more information please visit our website: http://iwiswn.usv.ro

Universitatea Ștefan cel Mare Suceava

"Stefan cel Mare" University
Suceava, Romania

NATO Advanced Research Workshop

Information Security in Wireless Networks

September 4-8, 2006
Suceava, ROMANIA

Universitatea
Ștefan cel Mare
Suceava

Organizing Committee

- Professor Stephan Olariu, Old Dominion University, Norfolk, VA, USA, co-director
- Assoc. Professor Doru E. Tiliute, "Stefan cel Mare" University, Suceava, Romania, co-director
- Professor Azzedine Boukerche, University of Ottawa, Canada, member
- Professor Ferucio Laurentiu Tiplea, "Al. I. Cuza" University, Iasi, Romania, member
- Professor Alan Bertossi, University of Bologna, Italy, member
- Professor Aurel Serb, Romanian Naval Academy, Constanta, Romania, member
- Professor Mohamed Eltoweissy, Virginia Tech, USA, member
- Professor Adrian Graur, "Stefan cel Mare" University, Suceava, Romania, member
- Professor Jingyuan Zhang, University of Alabama, USA, member
- Professor Aurel Burciu, "Stefan cel Mare" University, Suceava, Romania, member
- Professor Ivan Stojmenović, University of Ottawa, Canada, member
- Professor Ioan Bogdan, Technical University of Iasi, Romania, member

Schedule

Letter of intent due:	May 31, 2006
Manuscript due:	July 15, 2006
Acceptance Notification:	August 15, 2006
Final Manuscript Due:	October 15, 2006
Publication:	December 2006

Submission Guidelines

Prospective authors are encouraged to submit an electronic version (Postscript or PDF) of their manuscript by e-mail to:

nato-arw@cs.odu.edu

Submissions must be of at most 10 pages plus, optionally, a clearly marked appendix to be read at the discretion of the organizing committee. Simultaneous submission to other conferences or workshops with published proceedings is specifically disallowed.

The proceedings of the workshop will be published as a book in the **NATO Security Through Science** series.

Universitatea "Ştefan cel Mare" Suceava, Str. Universităţii nr. 13, 720 229 Suceava, România, Tel: +40 230 520 081, Fax: +40 230 520 080
Web: www.usv.ro