

The Internet has become essential for the exchange of information. Many user groups from different backgrounds and with different objectives depend on it to perform their daily tasks. Various activities are carried out via the Internet: between companies (B2B), between businesses and consumers (B2C), or between individuals who create their own virtual communities. Moreover, many companies are interconnecting their IT systems, including SCADA (Supervisory Control And Data Acquisition) systems, directly or indirectly to the Internet.

At the same time, the use of the Internet is facing increasing risks regarding privacy and security, in particular due to vulnerabilities induced by the increasing complexity of Internet-related applications. Therefore, new security mechanisms and techniques should be deployed to achieve an assurance level acceptable for critical domains such as transportation, health, defence, banking, critical infrastructures, etc.

Attackers nowadays do not lack motivation and they are more and more experienced. The existence of vulnerabilities encourages different kinds of attackers to exploit them and gain access to personal computers or penetrate into IT systems belonging to companies or administrations. The attackers can be inquisitive students, groups of pirates, criminal organizations, terrorists, or intelligence agents specialized in electronic war. To make matters worse, the attacking tools are more and more easily available and accessible for anybody.

In this context, dependability, security and privacy become a priority that should be addressed by all actors in research, industry, services and governments.

SCOPE

The topics addressed by CRISIS range from the analysis of risks, attacks and vulnerabilities to system survivability, passing through security policies and models, security mechanisms and privacy enhancing technologies. The authors are invited to submit research results as well as practical experiment or deployment reports. Industrial papers about applications or case studies are also welcomed in different domains (e.g., telemedicine, e-government, e-learning, e-commerce, critical infrastructures, etc.). The list of topics includes but is not limited to:

- *Analysis and management of risk, attacks and vulnerabilities*
- *Security and dependability of operating systems and network components*
- *Web services and middleware security*
- *Dependability and fault tolerance of Internet applications*
- *Security and safety of critical infrastructures*
- *Security and privacy of peer-to-peer system, wireless networks, VPN and embedded systems*
- *Security of new generation networks, security of Voice-over-IP and multimedia*
- *Security of database systems, security of e-commerce and electronic voting systems*
- *Authentication, authorization and audit*
- *Privacy protection and anonymization*
- *Traceability and forensics*
- *Security models and security policies*
- *Formal methods, verification and certification*
- *Key management Infrastructure (PKI) and trust management*
- *Biometrics, watermarking, cryptography and security protocols*
- *Access controls and security mechanisms*
- *Use of smartcards and personal devices for Internet applications*
- *Firewalls and intrusion detection systems*
- *Viruses, worms and malicious codes*
- *Attack data acquisition (honeypots) and network monitoring*
- *Metrology, security evaluation, and security management*

- *Organizational, ethical and legal issues*

SUBMISSIONS

Papers must be written in English or French, and must be submitted electronically in PDF format. Maximum paper length will be **8 printed pages** for *full papers* or **4 pages** for *short papers*, including figures in IEEE 2-column style.

The cover page should include paper title, author's full names, affiliations and complete addresses (telephone, fax, email), abstract, and a list of keywords.

Paper submissions must be received by March 31, 2007, via the CRiSIS 2007 website.

IMPORTANT DATES

- Paper submission deadline: **March 31, 2007**
- Notification of acceptance: **May 1, 2007**
- Camera ready due: **May 15, 2007**

GENERAL CHAIR

Yves Deswarte

PC CHAIR

Anas Abou El Kalam

PROGRAM COMMITTEE (will include)

Anas	Abou El Kalam	ENSI de Bourges, France
Rachida	Ajhoun	ENSIAS, Morocco
Mahmoud	Boufaïda	University of Constantine, Algeria
Michel	Cukier	University of Maryland, USA
Frédéric	Cuppens	ENST de Bretagne, France
Marc	Dacier	Eurecom, France
Sabrina	De Capitani	Università di Milano, Italy
Hervé	Debar	France Télécom R&D, France
Mourad	Debbabi	Concordia Institute of Information Systems, Canada
Yuri	Demchenko	Universiteit van Amsterdam, Netherlands
Geert	Deconinck	Katholieke Universiteit Leuven, Belgium
Yves	Deswarte	LAAS – CNRS, France
Rachida	Dssouli	Concordia, University, Canada
Aziz	El Fazziki	Université de Marrakech (FSSM), Morocco
Jean-Guy	Fontaine	Istituto Italiano di Tecnologia, Italy
Dieter	Gollmann	Technische Universität Hamburg, Germany
Frédéric	Kratz	LVR – ENSI de Bourges, France
Catherine	Meadows	Naval Research Laboratory, USA

Jean-Jacques	Quisquater	Université de Louvain, Belgium
Michael	Rusinowitch	LORIA – INRIA, France
Hesham	Soultan	IBM, Egypt
Gilles	Trouessin	Oppida, France
Paulo	Verissimo	Universidade de Lisboa, Portugal