

Appel à communications

Call for papers



6, 7, 8 novembre

November 6, 7, 8

Rennes, France

**Cryptographie :
nouveaux usages, nouveaux défis**

**Cryptography:
new stakes, new challenges**

<http://www.rennes.supelec.fr/CESAR>

Le Centre d'Electronique de l'Armement (Ministère de la Défense) organise chaque année depuis 1997 des journées SSI réunissant autour d'un sujet donné des acteurs gouvernementaux, industriels et académiques de la sécurité des systèmes d'information.

L'objectif visé par ces journées thématiques est double, scientifique mais surtout didactique, en proposant à la communauté SSI, c'est à dire à une audience qui va des chercheurs aux praticiens et aux décideurs, un tour d'horizon sur un sujet particulier du domaine de la sécurité des systèmes d'information. Ce sujet pourra être abordé sous l'angle théorique ou pratique, matériel ou logiciel, mais toujours avec une optique pédagogique afin d'en faciliter la compréhension. C'est en effet cette vision didactique qui permettra aux utilisateurs de terrain la prise de connaissance des avancées théoriques ou techniques susceptibles de répondre à leurs besoins, mais qui fournira aussi dans ces échanges les éléments des problèmes réels utiles aux travaux des chercheurs et des développeurs.

The Ministry of Defense have been organizing infosec thematic workshops every year since 1997. These conferences bring together information system security specialists coming from government, industry or university.

The goal of CESAR meeting is scientific, and also didactic. It aims at presenting a survey of a specific issue of information system security. The audience pictures the whole ISS community, including fundamental researchers as well as practicing specialists and managers. The subject will be presented from a theoretical as from a practical point of view, while keeping a pedagogic angle in order to facilitate understanding. Indeed, this peculiar point of view will allow practicing specialists to get aware of theoretical and technical breakthroughs able to help them to solve their difficulties . But on the other hand, researchers and developers will have the opportunity to become acquainted with some potentially interesting real-life problems.

L'édition 2007 des journées SSI (CESAR2007) aura lieu du 6 au 8 novembre, à Rennes.

Le thème retenu cette année, la cryptographie, est à comprendre au sens large : en effet ce retour sur un thème déjà traité lors des journées SSI de 1999 est davantage motivé par le foisonnement actuel de ses applications (protocoles sécurisés, réseaux sans fil, voix sur IP, e-commerce, e-administration, gestion des droits numériques, sécurisation des systèmes d'exploitation, etc...) et les problèmes qu'elles soulèvent, que par l'importance des évolutions techniques du domaine, encore que certaines soient fort intéressantes.

Les exposés concerneront donc bien sûr la conception cryptographique (génération d'aléa, algorithmes et protocoles, infrastructures de gestion de clés), mais aussi l'implémentation matérielle et logicielle (standards, exemples d'applications -protocoles, composants, produits de chiffrement-, nouvelles problématiques), l'évaluation (organismes, critères, attaques), et la législation (besoins des états, écoute, impact technologique), en mettant autant que possible l'accent sur les problématiques émergentes.

Les propositions de communication sur cette thématique devront être en Français ou en Anglais, avec un résumé dans chacune de ces langues. Elles devront parvenir à l'adresse électronique cesar@rennes.supelec.fr sous forme de pièce jointe au format pdf, ou à défaut postscript, doc, rtf, ou open office. Devront y figurer le titre de la communication et sa catégorie (didactique, générale, spécialisée), les nom et prénom du ou des auteurs et leur affiliation, l'adresse de courrier électronique de l'un des auteurs, les deux résumés (15 lignes environ) et une liste de mots clés. La proposition pourra prendre la forme d'un plan détaillé de la présentation ou d'un texte qui ne devra pas dépasser 8 pages.

Les critères de sélection des communications seront principalement l'effort pédagogique et la clarté de l'exposé, ainsi que le lien avec les

CESAR conference will take place in Rennes on November, 6th, 7th and 8th, 2007.

This year's topic is cryptography, to be understood in a broad sense. The theme has already been dealt with in the 1999 conference, but the surge of new cryptography applications (secured protocols, wireless networks, voice over IP, e-business, e-administration, digital rights management, security of operating systems, ...) and the related problems, justify this choice more than technical evolutions of the field (some of them being nevertheless quite interesting...).

The talks will deal with cryptographic design (random generation, algorithms and protocols, key management infrastructure), as well as hardware and software implementation (standards, examples of applications, protocols, components and devices, equipments), evaluation issues (technical centers, criteria, attacks), and legislation (governments' needs, eavesdropping, technological impacts). They will point out emerging issues as far as possible.

Submissions should be written in French or English with an abstract in both languages. They will be electronically sent as an attached file to a mail to cesar@rennes.supelec.fr. They should be in PDF format, although PostScript, doc, RTF and OpenOffice formats will be allowed. They should begin with a title, the category (tutorial, general article or a specialized one), author(s)' name(s), affiliation(s) and mail(s), the two abstracts (roughly 15 lines), and a list of keywords. The proposition may be a detailed outline of the presentation or a text that should not exceed 8 pages.

Selection criteria of the submissions will mainly be the pedagogic effort, the clarity of the paper, and the relation with the topics of the

thèmes de la conférence. Les exposés techniques spécialisés seront considérés dans la mesure où ils présentent un état de l'art d'un domaine (survey) et non un résultat scientifique particulier.

Les articles retenus, rédigés en français ou en anglais, seront publiés dans les actes du colloque.

Dates importantes

Date limite de soumission : 15 juin 2007
Notification aux auteurs : 30 juillet 2007
Soumission des présentations finales : 5 octobre 2007
Déroulement des journées : 6-7-8 novembre 2007

conference. Technical talks will be considered provided that they present a survey of a given area instead of a particular scientific result.

Accepted submissions will be published in the proceedings of the conference

Important dates

Submission deadline: June, 15th, 2007
Notification to authors: July, 30th, 2007
Final presentation: October, 5th, 2007
Conference: November, 6th, 7th and 8th, 2007

Comité de pilotage

- Pascal Chour (Services du Premier Ministre, SGDN/DCSSI)
- Yves Correc (Ministère de la Défense, DGA/CELAR), président
- Olivier Heen (Thomson)
- Ludovic Mé (Supélec)

Steering committee

Comité de programme

- Hervé Chabanne (Sagem Défense Sécurité)
- Florent Chabaud (Services du Premier Ministre, SGDN/DCSSI), président
- Yves Correc (Ministère de la Défense, DGA/CELAR), secrétaire
- Henri Gilbert (France Télécom R&D)
- Louis Granboulan (EADS)
- Marc Joye (Thomson)
- François Larbey (Thalès)
- David Lubicz (Ministère de la Défense, DGA/CELAR)
- David Pointcheval (Ecole Normale Supérieure)
- Guillaume Poupard (Ministère de la Défense)
- Nicolas Sendrier (INRIA)
- Frédéric Valette (Ministère de la Défense, DGA/CELAR)

Program committee