

# C&ESAR 2008

Rennes, France

## *Trusting Trusted Computing?*

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

### Dates importantes

Date limite de soumission : 1<sup>er</sup> juin 2008  
 Notification aux auteurs : 30 juillet 2008  
 Article définitif : 5 octobre 2008  
 Conférence : 2-3-4 décembre 2008

### A propos de C&ESAR 2008

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 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.

### Trusting Trusted Computing?

Le thème traité cette année est l'informatique de confiance, considérée du point de vue matériel autant que logiciel, du point de vue du fournisseur comme de l'utilisateur. On tentera de mieux cerner la définition de la confiance et ses liens parfois mal compris avec la sécurité, ainsi que les diverses techniques susceptibles d'apporter la dite confiance, des modèles à leur implémentation logicielle ou matérielle, des simples mécanismes aux architectures.

Ce thème a été, dans une déclinaison restreinte au multi-niveau, celui de la première édition de cette conférence en juin 1997. Mais les progrès rapides de la technologie, avec leurs aspects éventuellement polémiques (TCPA Palladium, DRM, ...), l'ont remis à l'ordre du jour.

Les problématiques abordées dans les exposés pourront couvrir entre autres les plates-formes de confiance et les technologies sous-jacentes (cryptographie, composants, preuve, évaluation), les systèmes d'exploitation, les architectures multiniveaux, les cartes à puce, la labellisation, la gestion des droits numériques, la certification des applications... tant du côté du besoin que des solutions, ou des attaques.

### Key Dates

Submission deadline: June the 1<sup>st</sup> 2008  
 Notification to authors: July the 30<sup>th</sup> 2008  
 Camera ready version: October 5<sup>th</sup> 2008  
 Conference: December 2-3-4 2008

### About C&ESAR 2008

*The Ministry of Defense has been organizing infosec thematic workshops every year since 1997. These conferences bring together information system security specialists coming from the governmental, industrial and academic world.*

*The goal of C&ESAR meeting is scientific, but 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.*

### Trusting Trusted Computing?

*This year's topic is Trusted Computing seen from several points of view: software/hardware, provider/user, needs/solutions. First of all, we shall try to come to a better understanding of the relations between trust and security, as far as computing is concerned.*

*Then we shall consider various trust enabling techniques, from abstract models to software implementation, from isolated mechanisms to whole architectures.*

*A part of the present thema was the topic of the first edition of the conference, in 1997 (multi-level security).. A decade of fast technological evolution has brought back this topic to the front of the scene, with even some polemic aspects (former TCPA Palladium, DRM, ...).*

*The talks will deal with trusted platforms and the underlying technologies (cryptography, chips, proof, evaluation), operating systems, multilevel architectures, smartcards, labelling techniques, digital rights management, software modules certification, ... Needs can be described as well as solutions or attacks.*

## Processus de soumission

Première étape : Les propositions de communication (5 à 10 pages) parviendront au comité de programme avant le 1<sup>er</sup> juin 2008, via le site web de CE&SAR. Le format recommandé est pdf. Figureront 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, un résumé (15 lignes environ) et une liste de mots clés. Les auteurs seront prévenus de l'acceptation ou du rejet le 30 juillet 2008.

Seconde étape : Les auteurs fourniront pour le 5 octobre 2008 une version définitive de la communication, de 8 à 20 pages, via le site web de CE&SAR. Le délai tient compte des contraintes liées à l'impression des actes de la conférence et ne pourra pas être négocié. Ces versions définitives tiendront compte des remarques des relecteurs. Elles seront fournies en LaTeX préférentiellement (à défaut en Word), en respectant dans les deux cas le format LNCS :

<http://www.springer.com/computer/lncs?SGWID=0-164-7-72376-0>

Les communications seront rédigées en français ou en anglais. Les critères de sélection seront principalement l'effort pédagogique et la clarté, ainsi que le lien avec les thèmes de la conférence. Les exposés techniques spécialisés seront considérés dans la mesure où ils présentent un état de l'art d'un domaine et non un résultat scientifique particulier.

Les communications acceptés seront publiés dans les actes du colloque. Les meilleures communications, désignées par le comité de programme, pourront faire l'objet d'une publication, en anglais obligatoirement, dans le journal *Annals of Telecommunication*.

## Submission Process

*First stage: June 1<sup>st</sup> 2008, 5 to 10 pages communication proposal will be sent to the program committee through the CE&SAR web site. The recommended format is pdf. Accompanying information must include: title, category (tutorial, general, expert), author's identification and affiliation, contact (email) with the main author, 15 lines abstract and relevant key-words. On July the 30th 2008, authors will be notified of acceptance or rejection.*

*Second stage: Authors will provide committee through the CE&SAR web site, before October the 5<sup>th</sup> 2008 their final version (8 to 20 pages) including eventual corrections issued from the reviewing process.*

*NB: This deadline is tied to the printing of the proceedings, and therefore cannot be changed. Articles will preferably be typeset using LaTeX. Word files will nevertheless also be accepted. Note that, in both cases, the LNCS format must be used:*

<http://www.springer.com/computer/lncs?SGWID=0-164-7-72376-0>

*Language for the communications is either French or English. The main selection criteria will be pedagogy and readability, as well as suitability for the conference topic. Technical communications can be accepted, with special attention to the quality of the survey part.*

*Accepted communications will be published in the proceedings. The best communications, as rated by the program committee, may be published in the journal "Annals of Telecommunication".*

## Comité de pilotage / Steering Committee

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

## Comité de programme / Program Committee

José Araujo	(Alcatel-Lucent)
Christophe Bidan	(Supélec)
Ciaran Bryce	(INRIA/IRISA)
Christophe Clavier	(Gemalto)
Guy Cogniat	(Lab-STICC/Université Bretagne Sud)
Yves Correc	(Ministère de la Défense, DGA/CELAR), secrétaire
Olivier Courtay	(Thomson)
Loïc Dufлот	(Services du Premier Ministre, SGDN/DCSSI)
Emmanuel Gureghian	(Bertin Technologies)
Olivier Heen	(INRIA/IRISA)
Ronan Keryell	(ENSTB)
David Naccache	(Univ. Paris 2 et ENS)
Ludovic Mé	(Supélec), président
Alain Merle	(CEA/LETI)
David Pointcheval	(ENS)
Emmanuel Prouff	(Oberthur)
Patrick Radja	(EADS)
Frédéric Valette	(Ministère de la Défense, DGA/CELAR)