



Chip-to-Cloud Security Forum

Smart Trusted Technologies & Services for the Networked Society

September 19-20, 2012 – Nice, French Riviera

(previously e-Smart & Smart Mobility conferences of Smart Event)

CALL FOR PAPERS 2012

Deadline for abstract submission is **March 30, 2012 (extended)**

BACKGROUND & SCOPE

The *Chip-to-Cloud Security Forum* is the continuation of *Smart Event*, combining together *Smart Mobility*, *e-Smart* and partly *World e-ID* conferences into a wide-ranging single event dedicated to the Future Networked Society security.

For 12 years, *Smart Event* has addressed Academic and Industry key advances in Smart Security. Starting from purely embedded and smart cards security, then adding mobile and biometrics applications, *Smart Event* has gradually enlarged its scope to cover a larger "digital security domain" including trusted applications in telecoms, Internet, banking, e-gov., etc. Along with the continuously increasing performance of the nano-, micro- technologies and the cheaper and faster modern communication networks, every physical resource now form part of massive infrastructures supporting on-line services such as M2M, Mobile Internet, Mobile Payments, Cloud Computing Applications & Services, Social Networks... This shift from off-line secure personal devices (mostly embedded secure microcontrollers and smart cards) based transactions to mobile and on-line trusted services is reflected by the new title *Chip-to-Cloud Security Forum*.

Taking a step forward, those connected services announce a near future best described by the Internet of Things (IoT) design paradigm: a smart environment where devices, sensors, actuators, mobile phones, etc. are able to interact with each other and cooperate through the Internet. This perspective raises new security, trust and privacy challenges at unseen levels, impacting the digital world in all its components, from the "things" to users' everyday life, from the physical space to the society. The *Chip-to-Cloud Security Forum* will also address these IoT's broad security challenges arising from our Networked Society.

OBJECTIVES

The Forum offers a high level international conference for researchers from Academia, Industry experts and engineers, Industry decision-makers, practitioners from standardization bodies and government professionals to share their vision, to figure out strategies for the future, to point out business opportunities and seek collaboration prospects, to present state-of-the-art research and discuss the most recent advances in embedded, mobile and cloud security at both hardware and software levels with regards to the dynamics of these technologies towards the Internet of Things challenges.

The Chip-to-Cloud Forum Program Committee is looking for technical papers describing original ideas groundbreaking results, new techniques, new methodologies, proposing new research directions, highlighting standardization and regulatory issues for resolving open problems spanning from all aspects of current and future IoT systems security and trust ability.

Reinforcing the interactions between academic research and Industry:

In order to reinforce the interactions between academic research and Industry, the Chip-to-Cloud Security Forum Program Committee is also looking for Industry specific papers preferably focusing on:

- academic research challenges resulting from the industry context,
- the design, implementation, deployment and use cases of realistic systems that have been built and deployed,
- the engineering challenges faced by the Industry in a commercial context and versus business opportunities, success stories and/or failures.

LIST OF TOPICS

The submissions may address one or more of the topics mentioned below or others that authors believe to be of great interest to the audience.

SECURE EMBEDDED SYSTEMS TECHNOLOGIES	TRUSTED MOBILE COMMUNICATIONS & TRANSACTIONS	TOWARDS THE INTERNET OF THINGS
<ul style="list-style-type: none"> - Secure embedded systems design: <ul style="list-style-type: none"> - Advanced architectures - Secure HW/SW co-specification - Formal verification - HW/SW co-validation - System validation - Run-time & design time reconfigurable secure platforms & processors - Multiple constraints driven embedded systems design & optimization - Secure hardware technologies - Secure software architectures & engineering - Secure embedded software & OS - Advances in ubiquitous and domain specific cryptography, PUFs, etc. - Strong authentication technologies (HW& SW) for Cloud Computing, Services Security and other Enterprise and personal usages. - Advances in embedded Java & Java Card - NFC and contactless technologies security - (Mobile) Trusted Computing architectures - Packaging issues & innovations 	<ul style="list-style-type: none"> - Advances in Secure Element technologies: USIM/UICC, embedded SIM, SD card - TEE in mobile devices - Smart card web server - Trusted Services Management technologies - Smartphone's security: device, OS and secure mobile apps development - Contactless/wireless /mobile systems security risks analysis - Advances in NFC and contactless technology - Electronic Identity security: <ul style="list-style-type: none"> - Biometrics advances & applications - e-ID domain specific cryptography - e-ID based secure applications - Privacy protection - Mobile Internet, Mobile and cloud computing - Trusted mobile services - Use cases and deployments of m-payment, transportation, media & content applications - Smart mobility research projects such as impaired and handicapped people, location-aware apps, smart cities, etc. - Innovative business models between MNOs/ Service Providers/Banks/Other Stakeholders 	<ul style="list-style-type: none"> - Cloud Computing Security, Security as a Service (SaaS) - M2M Deployment & Security - M2M applications to: <ul style="list-style-type: none"> - Transportation, automotive, - Smart grids/meter, - SCADA system, - Smart physical infrastructure, - Energy efficiency, - Environmental monitoring, medical devices, telematics and robotics... - LTE and mobile broadband security issues - Mobility in enterprise security management - Cyber Physical Systems and Cyber Physical Society security issues - Wireless Sensor Networks (WSNs) and Advanced Wireless Sensors - Wireless Personal Area Networks technologies (UWB, 6LoWPan, etc.) - Wireless Body Area Networks
<p>HORIZONTAL CONTRIBUTIONS:</p> <ul style="list-style-type: none"> - Standardization issues & progresses for increasing trust and interoperability - Security, privacy and content protection: standardization issues & progresses, security evaluations methodologies (attacks & countermeasures, best practices, etc.), certifications criteria and schemes - Products and systems security evaluation and certification standards - Transnational collaborative R&D frameworks, initiatives and programs - Transnational regulatory issues & progresses to make the internet and services infrastructures more trustable and secure. 		

CALL FOR KEYNOTES CONTRIBUTIONS: The Future Networked Society

Beyond the scope of Internet of Things and Cyber-Physical Systems, which globally include H2H, H2M, M2H, & M2M Communications Systems and Services, the Future Networked Society (or Cyber-Physical Society) concerns not only the cyber space and the physical space but also the humans, knowledge, society and culture. In this session we solicit innovative keynotes contributions and "wild & crazy ideas" on topics such as, but not limited to:

- Complex real world social networks analysis methods, applications, privacy and security issues
- Smart Planet and new resources management models and low carbon economy
- Cyber-Physical-Socio Intelligence and services
- Self Organized networks for organizing versatile resources
- Systems based on semantics, knowledge and grid/cloud/P2P for e-health, e-business, e-science, e-learning, e-city, and e-culture
- Major initiatives to make the Internet and services infrastructure more stable and predictable, more scalable and secure
- Future and Emerging Technologies development initiatives on Ambient Security & Dependability
- Internet neutrality
- Disrupting business models for the Future Internet, who among MNOs, Device Makers, Applications - Service Providers will be leading?

HOW TO SUBMIT?

Prospective authors **must submit a short abstract using the [submission template](#)** (Word document).

1. Short, explicit and appealing title.
2. Name, function, address, phone, e-mail, and affiliation of all the author(s) of the presentation together with a short description of the author(s)' expertise.
3. The name of the actual speaker (only 1 person is allowed to present).
4. 3 to 4 bullet points (1 line max. each).
5. Length of the abstract: between 300-500 words (one A4 page).

Submissions not conforming to these formatting instructions risk rejection regardless of their technical merit.

All submissions must be original ones, not previously published elsewhere, publicly presented or submitted in parallel to any other event. **They should be informative and impartial. The Program Committee will review all submissions and will reject any commercially-oriented ones.**

Submission Procedure

Authors are invited to submit their proposals electronically to lperron@strategiestm.com

If authors do not receive acknowledgment within 72 hours, they are kindly invited to contact directly Lenick Perron – Strategies Telecoms & Multimedia - Phone + 33 1 48 59 99 32

➔ **Deadline for abstract submission is ~~MARCH 23, 2012~~ extended to **MARCH 30, 2012****

Decisions and Presentation

Notification of acceptance or rejection will be sent to authors on April 30, 2012

Authors of accepted papers commit themselves to present their paper at the conference. In case of personal impediment, the speaking person shall arrange a substitute speaker.

Speaker's registration

The speaker's registration rate is €485 before vat (60% discount on the regular rate) giving access to any session of the conference, coffee-breaks & lunch, proceedings.

Co-authors also benefit from preferential attendance rates. Speakers' travel and accommodation expenses are not covered by the organizers.

Proceedings of the conference will be available at the opening of the event. Clear instructions about the proceedings will be sent to the authors of accepted papers.

The organizers commit themselves not to disseminate the presentations before the conferences.

Other important dates

- ▶ Official Program Appearance: May 25, 2012
- ▶ Complete presentation for the proceedings: August 31, 2012

COMPLEMENTARY CALLS:

Chip-to-Cloud Security Forum will propose **demos & posters sessions** for exchange of ideas and presentation of on-going research, development or projects relative to the topics listed above.

- Call for Demos:

The Program Committee welcomes demos proposals providing sufficient information to evaluate their quality and importance. Accepted demos will be held during the conference breaks in a dedicated area. Each demos session will be scheduled two times during the event.

The Demo presenters will need to register at a specific fee of 785€ before vat including one delegate pass and covering the logistics part handled by the organizers (plasma screen, table and chairs, power supply, Internet connexion...).

Submit your demo proposals to lperron@strategiestm.com

Deadline for abstract submission is March 23, 2012. Notification of acceptance: April 30, 2012

If authors do not receive acknowledgment within 72 hours, they are kindly invited to contact directly Lenick Perron – Strategies Telecoms & Multimedia - Phone: + 33 1 48 59 99 32

- Call for Posters:

The Program Committee welcomes posters proposals providing sufficient information to evaluate their quality and importance.

Presenters will need to register for the conference as speakers. There is no waiver of conference fees. Poster presentations will not be interactive except during lunch time and after the presentations are over for the day.

Submit your posters to lperron@strategiestm.com

Deadline for abstract submission is March 23, 2012. Notification of acceptance: April 30, 2012

If authors do not receive acknowledgment within 72 hours, they are kindly invited to contact directly Lenick Perron
– Strategies Telecoms & Multimedia - Phone: + 33 1 48 59 99 32

PROGRAM COMMITTEE

PC Chairman: Jean-Paul Thomasson, Security Expert, Strategies Telecoms & Multimedia
Housseem Assadi, Head of R&D Department "Security & Trusted Transactions", Orange
Vincent Barnaud, Electronic Payment & Transactions, France Telecom Orange
Gil Bernabeu, Technical Director, GlobalPlatform
Marc Bertin, Chief Technology & Strategy Officer, Oberthur Technologies
Alain Boudou, Product and System Security Working Group Convenor, Eurosmart; Security Certification Manager, Gemalto
Dr. Joerg Borchert, President and Chairman, Trusted Computing Group; VP Chip Card and Security, Infineon Technologies Americas
Fevzi Çakmak, Director of Business Development, Irdeto
Sergio Cozzolino, ICT Mobile Solutions VP, Telecom Italia; Chair SC Group GSMA
Augustin Farrugia, Head of DRM Technologies, Apple
Pr Erol Gelenbe, Denis Gabor Chair, Imperial College London
Christian Goire, President, Java Card Forum
Dr. Slawomir Grzonkowi, Leader of Security, Privacy and Trust Unit, Digital Enterprise Research Institute (DERI), National University of Ireland (NUI), Galway, Ireland
Nader Henein, Security Advisory, BlackBerry Security Group, Research in Motion UK
Dr. Detlef Houdeau, Senior Director of Business Development, Identification Market, Infineon / Silicon Trust
Francois Lecomte, Managing Director Forum-SMSC; NFC World Congress Program Committee Chair
Holger Lenz, Director Business Development, Cinterion Wireless Modules
Dr.Thierry Lestable, Technology & Innovation Manager, Sagemcom
Pr Carlo Maria Medaglia, RFID Lab CATTID, University of Rome "La Sapienza"
Dr. Gisela Meister, Head of Technologie Consulting R&D, Standardisation Manager C-TO, Giesecke & Devrient
Marc Muller, Head of Common Technologies, Gemalto
José M. Hernández-Muñoz, SmartSantander EU Project Coordinator, Telefonica I+D
Pr David Naccache, ENS Paris, CIM PACA
Pr. Pierre Paradinas, Embedded Systems Chair, CNAM/CEDRIC Paris
Pr. Bart Preneel, Director, COSIC KU Leuven
Helmut Scherzer, Senior Technology Manager CTO Office, Giesecke & Devrient
Clotilde Servajean, Communication Working Group Convenor, Eurosmart
Pr. Georg Sigl, Deputy Director, Fraunhofer Institute for Secure Information Technology, Munich; Chair of Security in Information Technology, Technical University of Munich
Laurent Sourgen, Board Member, Eurosmart / STMicroelectronics
Jörg Suchy, Senior Manager Strategic Marketing Chip Card and MCU EMEA, Samsung
Janne Uusilehto, Chair Mobile Group, TCG, Head Product Security, Nokia
François Vacherand, Head of Architecture & Security, CEA LETI Minatec
Philippe Vallée, EVP Telecommunication Business Unit, Gemalto
Dr. Eric Vétyillard, Java Card Principal Product Manager, Oracle