chist-era

CHIST-ERA Conference 2015

Participate in CHIST-ERA Call 2015 Definition

The CHIST-ERA ERA-NET is a consortium of funding organisations in Europe and beyond with programmes supporting ICST. The consortium is itself supported by the European Union's Future & Emerging Technologies scheme (FET). CHIST-ERA promotes multidisciplinary and transnational ICT research with the potential to lead to significant breakthroughs. The funding organisations jointly support research projects selected in the framework of CHIST-ERA, in order to reinforce European capabilities in selected topics.

The Call 2015, to be published in October, addresses two new and hot topics:

Security and Privacy in Internet of Things (SPIoT)

Terahertz Band for Next-Generation Mobile Communication Systems (TENXSYS)

The CHIST-ERA Conference 2015 in Lisbon, June 16-18, brings together scientists working in these research areas and CHIST-ERA representatives to refine the topics contour and scope of the Call 2015. The topic keywords illustrate the topics, but will be refined. All attendees will participate in plenary and facilitated break-out sessions to identify and formulate the promising scientific and technological challenges at the frontier of research. High level keynote talks by internationally renowned scientists and poster presentations will further contribute to the discussions. This event represents a unique opportunity for the scientific community to directly participate in scoping the call topics content and exchanging their views on the future of the domain with their peers. Many successful CHIST-ERA research proposals have been initiated at CHIST-ERA conferences. Note that the SPIoT session of June 16 is organised jointly with the IoT Week Lisbon 2015 event. The conference and the IoT Week are co-located at the Lisbon Congress Centre.

June 16-18, 2015
Lisbon, Portugal

Information: http://conference2015.chistera.eu

Topics of the Call 2015

Security and Privacy in Internet of Things

The current IoT vision is grounded in the belief that the steady advances in microelectronics, communications and information technology witnessed in recent years will continue into the foreseeable future. However, technical flaws and threats of intrusions might significantly lower the benefits of the new developments. Traditional protection techniques are insufficient to guarantee users' security and privacy within the future unlimited interconnection. There is a widely acknowledged need to guarantee both technically and regulatory the neutrality of the future internet. Moreover, all aspects of security and privacy of the user data must be under the control of their original owner by means of as simple and efficient technical solutions as possible.

Keywords: Internet of things, Smart objects, Mobile and ubiquitous computing, Big data, User privacy, Security, Information protection, Trustworthiness

Terahertz Band Next-Generation Mobile Communication Systems

Within a decade a 1000-fold increase in wireless communication traffic volume is expected, requiring increased throughput and data rates. Although usage of already allocated spectrum frequencies should be further optimised, the Terahertz (THz) band, which remains largely unexplored and is yet unallocated for frequencies over 275 GHz, offers new possibilities. The development of cutting edge low-cost THz devices has recently started, and new network concepts have the potential to cover the connectivity requirements of 5G systems. However, further research on Terahertz band transceivers, antennas, channel models and networking techniques is needed towards the realization of efficient and practical THz Band communication networks.

Keywords: Future wireless communications, Terahertz communications, Terahertz waves

Conference Programme

Schedule	16/06/2015	17/06/2015	18/06/2015
08:30		Welcome	Welcome
09:00		Brainstorming on call content	Brainstorming on call content
11:30		Coffee break	Coffee break
12:00		Brainstorming on call content	Brainstorming on call content
12:50		Conclusions	Conclusions
13:00		End of SPIoT half day 2	End of TENXSYS half day 2
13:30	Registration for SPIoT	Registration for TENXSYS	
14:00	Welcome address and introduction	Welcome address and introduction	
14:30	Keynote session	Keynote session	
16:00	Coffee break	Coffee break	
16:30	Poster presentation (plenary, 1’ per poster)	Poster presentation (plenary, 1’ per poster)	
17:20	Info session for Call 2015 applicants	Info session for Call 2015 applicants	
17:40	Introduction to brainstorming session of SPIoT half day 2	Introduction to brainstorming session of TENXSYS half day 2	
17:45	Poster networking session	Poster networking session	
19:00	End of SPIoT half day 1	End of TENXSYS half day 1	
20:00	Networking dinner	Networking dinner	

Book of Abstracts

chist-era

Security and Privacy in Internet of Things

1. Keynote Talks

Enrico Del Re, University of Florence

Security and Privacy in IoT – Challenges to Be Won

The Internet of Things can be characterized as “a proposed development of the Internet, in which everyday objects have network connectivity, allowing them to send and receive data.” The IoT vision is grounded in the belief that the steady advances in microelectronics, communications and information technology witnessed in recent years will continue into the foreseeable future.

However, technical flaws and threats of intrusions might significantly lower the benefits of the new developments. Traditional protection techniques are indeed not sufficient any more to guarantee the users’ privacy and security within the future unlimited interconnection.

The outcomes of fundamental and unbiased research projects within this topic will contribute to fill in the gap of the missing foundations, built on a holistic view for all IoT elements at all stages, especially regarding security and privacy.

Major challenges towards this ambitious goal to rebuild security and privacy concepts in IoT from scratch include but are not limited to adaptation in case of malfunction or intrusion, strengthening of weak links in embedded devices to avoid propagation of issues, reliable authentication and transparent data management.

The best solution (as agreed upon at the major scientific international levels including some on-going preliminary activities in FP7 and Horizon2020 projects) is to guarantee (technically and regulatory) the neutrality of the future internet and that all aspects of security and privacy of the user data must be under the control of their owner (citizen) by means of as simple and efficient as possible technical solutions.

The presently available solutions do not meet the requirements and deserve a European coordinate effort, also to contrast contrary economic and industrial interests.

Miranda Mowbray, HP

Internet of Things Research Study by HP

I will present findings from the Internet of Things Research Study done by my colleagues at HP in 2014. The report shows that Things are being currently sold that lack the most basic privacy and security protections. I will describe what these protections should be (from recommendations of the Open Web Application Security Project, owasp.org), and discuss why these are not being implemented, and what we can do about it. One conclusion from the study is that IoT security is not just about security of the device. Things are also vulnerable to weaknesses in network security, application security and mobile security. I will also suggest that there are some aspects to IoT security and privacy that cannot be addressed purely through technology, and need to be considered from a wider business and organizational perspective.

Elena Trichina, Rambus Inc.

Security and Privacy Challenges in Personal Healthcare Systems in the Context of the IoT

The integration of computing devices and healthcare has changed the landscape of modern medicine. Low power system optimizations, ultra-low-power wireless connectivity, and the development of lightweight communication protocols have helped make small-scale sense-actuate systems like Implantable Medical Devices (IMD) and Body Area Networks (BAN) a reality. This, in its turn, gave rise to Personal Healthcare Networks (PHN) that connect IMD and BANs via Internet with healthcare infrastructure.

Through sensors, these systems can collect physiological values (e.g., heart rate, blood pressure, oxygen saturation, temperature, or neural activity) and provide appropriate actuation or treatments (e.g., regulate heart rate or halt tremors). Embedded software and on-board radios enable wireless data transfer (or wireless medical telemetry) for monitoring, configuration and treatment updates without sacrificing patient mobility or requiring surgical procedures to physically access the devices.

However, all these advances in capabilities and flexibility of medical devices and their wide proliferation create severe security and privacy threats. Some of them are known from the Wireless Sensor Networks studies, some are new, related to ultra-low power requirements for many of these devices.

In this talk we review the security and privacy threats, goals and vulnerabilities of Personal Healthcare Systems and address merits and pitfalls of current solutions. The security and privacy challenges of PHS illustrate the complexity of the broader security issues in the emerging IoT.

2. Posters

Alberto Ferrante, University of Lugano

Lightweight Privacy-Preserving Protocols for IoT

Internet of Things, which is based on information sharing and data collection at different levels, opens up exciting new possibilities and applications. However, it also poses potentially unacceptable threats to privacy of individuals. In order to minimize privacy problems and being able to provide the required services, we propose to develop lightweight privacy-preserving protocols and methods. For these protocols, novel and/or targeted implementations of existing standard algorithms will be used as lightweight primitives.

Ali Ahmadinia, Glasgow Caledonian University

Secure Wireless Sensing and Processing in Smart Homes

With ever increasing data communication between various devices and wireless sensors in smart homes, there is an urgent need for secure data communication and processing in such environments, however current security solutions have large overheads in terms of processing time and power consumption. Lightweight and low power hardware security techniques need to be investigated to tackle this issue.

Ana Guimaraes, Trust Systems

IoT and Health Monitoring Privacy Assuring Framework

Ensuring Privacy associated with IoT and Health Monitoring is a challenge that covers multiple layers in the overall private information flow and stock.

Multiple and consistently increasing in number and complexity services and technologies providers are not yet prepared to address these matters and a methodology to assure these privacy requirements is of material interest to all the supply chain levels in this industry, and particularly to the end customer.

Addressing these subjects in a joint European mission is a major contribute to the fundamental values in our Society we propose to pursue.

Atta Badii, University of Reading

Context Aware Security and Privacy Filtering Solutions

High resolution surveillance systems are essential for security. However, these powerful tools have been misused by several CCTV operators. The governments and civil society are attempting to strike a balance between safety and privacy. Privacy filters can be used to help protect part of an image which included Personally Identifiable Information (PII).

This poster presents a novel approach to improve the privacy protection in the CCTV displays. Our method uses context cues to determine the required privacy filtering level for each person in the image. We also present a systematic methodology to handle the context cues. We use a rules engine to generalise and facilitate the customisation of this system that by design should be specialized for operation in a given environment. In addition, we present a case study as a proof-of-concept whereby we have created an environment providing with high levels of privacy protection whilst allowing the required level of surveillance monitoring.

Carles Ferrer, UAB Barcelona

Security System for a Wireless Sensor Network

Security is a major concern today for a wider deployment of WSN and the reliable use of some applications involving private user data. Authentication schemes prevent from impersonation or flooding attacks, for privileges scaling and node’s batteries depletion respectively; while Key Management guarantee data privacy. Such schemes involve high power consumer algorithms, then efficient implementations are needed. Hardware cryptographic implementations execute efficiently, but they can be easily attacked (Side Chanel Attacks). In that sense, countermeasures are being tested on our cryptographic algorithms to avoid this risk.

David F. Nettleton, CSIC

Users Can Trust that Data they Designate as Confidential Remains So

In this project we propose mechanisms that enable individual users to evaluate the tradeoffs in privacy with respect to disclosure:

1. Each individual chooses what information-items about themselves they consider private and which they consider public;
2. We provide warnings about information-items left public that are useful and informative in generating predictive models of the private attributes for the individual user.

The proposal is highly novel from a technical point of view because using the information-gain component of a rule induction algorithm it generates rules which are individualized for each user, rather than the typical general model for all users.

Gurhan Gunduz, Pamukkale University

Popularity-Based Scalable Peer-to-Peer Topology Growth

Peer-to-peer (P2P) networks have gained importance and spread significantly during the last decades resulting in raised research interest in this area. The basic premise of P2P design is higher scalability and many existing largescale applications, such as Twitter and Skype, use a form of P2P design. Although structured P2P designs enable one to guarantee finding of every item (rare or popular), they do not scale beyond a point and support from servers are needed. This breaks the decentralized design of the P2P system and results in a hybrid scheme. Unstructured P2P networks, on the other hand, can scale to much larger nodes but yet cannot give time guarantee for finding a rare item.

Isabel Trancoso, INESC ID

Privacy Preserving Speech Processing

As voice-based services become increasingly popular, awareness is also increasing that these services pose privacy risks. A person's voice is a legally-accepted biometric, and carries information about their identity, gender, nationality, health, emotional state and a variety of other factors, in addition to the actual spoken content. Voice services could potentially infer any of these factors which may be unrelated to the actual service provided, even when such inference is not desired by the speaker.

We discuss "privacy preserving" computational approaches for voice processing that prevent such undesired inferences through cleverly-designed cryptographic and hashing schemes.

Javier Rodríguez Fonollosa, Polytechnic University of Catalonia

Security and Privacy Issues in Vehicular Communications

Security and Privacy issues still demand significant research efforts in Vehicular Networks, one of the most important implementations of the Internet of Things paradigm. A distinctive social benefit of these networks is the set of applications related to active road safety characterized by stringent latency and capacity constraints but also by security and privacy requirements. Current specifications of the standard require enrolment, authentication, authorization and integrity, and the corresponding procedures create substantial communication and computation overhead compromising latency and capacity in the 30 MHz bandwidth ITS-G5A band reserved for these applications. Altogether the multiple conflicting Security and Privacy issues in Vehicular Networks call for a global and dynamic optimization framework.

Joao Magalhaes, Universidade Nova de Lisboa

Secure Wearable Health Sensors Data in Cloud Repositories

Wearable health sensors are becoming a pervasive family of devices that are constantly connected and capturing data. They are the most personal devices that fitting into the broad area of the Internet of Things (IoT). Once this data is produced and stored, technology must be in place to store the encrypted data in the cloud in such a way that the cloud manager cannot read the data. However, the data owner should be able to not only access the data but also perform operations over the encrypted data. This poster discusses the challenges in accessing health data from IoT devices data stored by a third cloud storage.

Loïc Lagadec, ENSTA Bretagne

Reconfigurable Computing for IoT

IoT focuses on interconnecting millions of smart devices. These devices manipulate personal and sensitive data and control physical systems. Hence, any breach in these devices may result in compromising human lives and lowering privacy protection. It is then mandatory that these devices support receiving security updates, on the field, with no manual intervention. Also, they must get enough computing power to support next generation security policies. Besides, some constraints such as low-power cannot be disregarded, as in any embedded system. Reconfigurable computing matches these requirements. It offers a high performance/low power hardware support for implementing complex policies. We discuss adding RC support to IoT devices in order to implement complex solutions such as multi-level proxies supporting virtualization and cryptography.

Mehmet Aktas, Yildiz Technical University

Capturing and Disseminating Provenance Data for NASA Earth Science Data Products

We review the current procedures for capturing and disseminating provenance data for NASA Earth Science Data Products. We identify provenance collection and representation methodologies for the provenance data that is driven by instrumenting the e-Science applications within the NASA-funded Instant Karma project. We illustrate the identified ideas of provenance collection to support Earth science research with the specific example of Sea Ice Data Processing Workflows. We present a model of thinking about provenance instrumentation. We discuss the model by applying it to data processing workflows with the use of Karma provenance collection framework.

Miguel L. Pardal, University of Lisbon

TrakChain Protects Track & Trace Data in the Internet of (Many) Things

RFID technology enables traceability systems that capture detailed data about goods as they move in the supply chain. Securing this data requires evaluating dynamic conditions to authorize business partners that are not known in advance. Furthermore, the system must promote trust and give incentives so that each partner shares its own data.

TrakChain implemented data visibility restriction policies using RDF and SPARQL. These policies can be converted to a standard format, XACML, to reuse existing enforcement infrastructures and tools. The expressiveness of the policies was evaluated against a set of requirements for a pharmaceutical traceability system.

Terahertz Band for Next-Generation Mobile Communication Systems

1. Keynote Talks

Jordi Romeu, Polytechnic University of Catalonia

The Challenging World of Terahertz Radiation

The use of the terahertz band for wireless communications is impaired by some physical limitations. The vision of any application based service must consider these limitations. The high expectations of “tera bit per second” data throughput are shadowed by the limited range imposed by the huge atmospheric attenuation. Nevertheless this limited range can be turned into an opportunity for secure communications, and where very short range high data throughput communications are required. Potential expansion of terahertz wireless communications is hindered by the shortcomings of present technologies, amongst them the inexistence of efficient sources and detectors. Some graphene based devices may overcome these difficulties. Finally there are plenty of issues related to coding, medium access, synchronization that must be considered.

Guillaume Ducournau, University of Lille

THz Communications for Next Generation HD Rate Wireless Links

The talk will give a general overview of THz com systems already reported, based on photonic or electronic devices. Even if THz links are by essence more robust to dusts and fig than IR optics, THz link budgets may first induce only real point to point applications over km range, using active signal tracking and possibly channel effects compensations. THz radio will also rely in the future on key advanced technologies, using cutting edge active devices, electronic or photonics-based. First THz applications may concern back-hauls for next 5 or 6G cell networks, or direct optical to radio-THz bridges. On the later, the huge development of fiber-optic networks, especially on coherent networks let think that optical-to-THz transceivers could play a major role in that systems. Some results of multi 10 Gbit/s links realized using QPSK channeling and photonic devices will be presented.

Martyn Fice, University College London

Photonics-Enabled Sub-THz Wireless Communications

Global IP traffic from wireless and mobile devices is growing exponentially, due to both increased numbers of networked devices and the use of higher-bandwidth applications such as video streaming. It is predicted that huge increases in wireless data rate (perhaps by a factor of 1000) will be required in the next 10 to 20 years. The bandwidth available for current mobile data networks (3G and 4G) and WLAN (Wi-Fi) will not support the expected increased data rates, and new bands in the mm-wave region of the spectrum are already being proposed for 5G networks. Vast bandwidth is available at sub-THz frequencies (>200 GHz), potentially addressing the large data rates that may be required in future generations of mobile networks or for very short range WLANs or machine-to-machine networks.

The combination of greatly increased wireless path loss at sub-THz carrier frequencies, increased data rate, and low source power implies that wireless link lengths will be much shorter than we are used to. Highly directional links will be required and improvements in key components will help, but these are unlikely to be sufficient on their own. New network architectures will also be needed, with wireline connections delivering high-speed data to a plethora of wireless antenna units serving much smaller cells than are used today. Fiber distribution networks and photonic THz generation could leverage the coherent detection and digital signal processing techniques used in the latest generation of optical fiber transmission systems, providing last-hop mobility for the user and a truly converged fiber-wireless network. As this scenario pushes photonics closer to the end user, achieving low cost will be essential. This issue can be addressed by the development of application-specific THz-photonic integrated circuits.

In this presentation, I will review current work on photonics-enabled sub-THz wireless communications, discuss how some of the issues mentioned above can be addressed, and speculate on the timescale for their implementation.

2. Posters

Eugen Dedu, FEMTO-ST

High-Level Protocols for Nanonetworks

Nanonetworks have several characteristics which make them unique from network and transport point of view. For example, receivers are slower than network, and senders have hardware specific limitations on data sending timing. Novel protocols specific to nanonetworks need to be proposed.

Guillaume Ducournau, University of Lille

THz High Data Rate Wireless Communications: Towards 5/6G Backhaul and Fiber to Radio Bridge

The authors will present recent achievements obtained in the field of THz wireless links, up to 32 Gbit/s data rates at 0.4 THz, for back-haul or fiber-to-(high data-rate) radio systems.

Guillermo Carpintero, Carlos III University of Madrid

Photonic-Enabled Coherent Ultra-Wideband Wireless Communications

Photonic integrated circuits (PIC) are finding their way into the development of photonic-enabled coherent wireless communications systems, since they allow for the generation of stable carrier waves in the millimeter wave frequency range (30 GHz to 300 GHz) and above. Several structures are discussed which provide the elements to develop a single chip transmitter using optical heterodyne generation of millimeter wave carrier frequencies.

Yang Hao, Queen Mary University of London

Manipulating THz Waves Radiation and Propagation for Future Generation Communications

The aim of our research is to investigate and establish models of its electromagnetic properties of advanced materials across THz frequencies and to demonstrate proof-of-concept antennas and devices for end-user wireless communications. Recent work will be presented in terms of active THz antennas, metamaterials for directive radiation and graphene for enhanced THz detection and absorption etc.

The Laboratory at QMUL has also established comprehensive measurement facilities for THz antenna systems. These include a Compact Antenna Test Range (CATR) for frequencies up to 200 GHz and a 9-metre far-field anechoic chamber, a THz-TDS system, and NSI planar near-field measurement range.