Challenges and Opportunities [in Digital Security] in H2020

Techdays@Aveiro

Dr. Jorge Pereira,
DG CONNECT

Contents

- **Introduction**
- **Call - Digital Security Focus Area (DS)**
  - Topics & Planning
- **Call – SME Instrument (SMEInst)**
  - Topic & Planning


JP Morgan sees 76 million customer accounts hacked
3 October 2014 | Business
JPMorgan to double cyber security spending to £310 million after hack


Fiat Chrysler recalls 1.4 million cars after Jeep hack
24 July 2015 | Technology

- **Situation:** ICT-driven transformations bring opportunities across many important sectors.
- **Complication**: "Smart", "Connected", "Digital" also introduce vulnerabilities...
- **R&D&I challenge:** Innovative and multidisciplinary actions addressing cyber security, data protection and privacy across individual H2020 pillars and calls.

Call – Digital Security Focus Area – Topics

- **DS-06-2017**: Cryptography;
- **DS-07-2017**: Addressing Advanced Cyber Security Threats and Threat Actors;
- **DS-08-2017**: Privacy, Data Protection, Digital Identities;

DS-06-2017: Cryptography (RIA)

- *In line with technological developments and emerging threats, the improvement of performance and efficiency of cryptographic solutions is a persistent need across ICT.*

- Nine thematic research challenges, including:
  - Ultra-lightweight
  - High speed
  - Implementation
  - Authenticated encrypted tokens
- Increase trust in ICT and online services
- Protect the European Fundamental Rights of Privacy, Data Protection

DS-07-2017: Addressing Advanced Cyber Security Threats and Threat Actors

- Situational Awareness (RIA);
  - Detect and quickly and effectively respond to sophisticated cyber-attacks;
  - Interdisciplinary research to counter threat actors and their methods;
  - Assess and address the impact to fundamental rights, data protection and privacy in particular;
- Simulation Environments, Training (IA);
  - Prepare those tasked with defending high-risk organisations;
  - Realistic environments; Tools for producing both benign and malicious system events;
  - May also address crisis management and decision making processes in relation to obligations stemming from applicable legal frameworks

DS-08-2017: Privacy, Data Protection, Digital Identities (IA)

- Privacy-enhancing Technologies (PET)
- General Data Protection Regulation in practice
- Secure digital identities
- Support for Fundamental Rights in Digital Society.
- Increased Trust and Confidence in the Digital Single Market
- Increase in the use of privacy-by-design principles in ICT systems and services

Call - DS – 2017 - Planning

Two separate opening dates - deadlines for submission		
Topic(s)	DS-06-2017	DS-07-2017 DS-08-2017
Opening	08 Dec 2016	01 Mar 2017
Deadline	25 Apr 2017	24 Aug 2017

Topic	Instr.	Funding (M)
DS-06-2017	RIA	18.50
DS-07-2017	RIA	10.0
	IA	8.0
DS-08-2017	IA	18.0

Call – SMEInstr – Topic & Planning

- **SMEInst-13-2016-2017**: Engaging SMEs in security research and development.
- **Topic:** "[…] cover any aspect of the Specific Programme for "secure societies - protecting freedom and security of Europe and its citizens" (Horizon 2020 Framework programme and Specific programme):"
  - 7.1. *Fighting crime, illegal trafficking and terrorism, …*
  - …
  - **7.4. *Improving cyber security***
  - 7.5. *Increasing Europe's resilience to crises and disasters*
  - **7.6. *Ensuring privacy and freedom, including in the Internet, and enhancing the societal legal and ethical understanding of all areas of security, risk and management***
  - …
- **Funding:** Approximately 19M in 2017
- **Logistics** and more information on SME Instrument: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/sme-instrument

Call - CIP – Topic & Planning

- CIP-01-2016-2017: Prevention, detection, response and mitigation of the **combination of physical and cyber threats** to the critical infrastructure of Europe.

Opening date - deadline for submission in 2017	
Opening	01 Mar 2017
Deadline	24 Aug 2017

Topic	Instr.	Funding (M)	
CIP-01-2016-2017	IA	20.0	➢ At least 2 operators of the chosen type of critical infrastructure operating in 2 countries must be beneficiaries (possibly, but not necessarily: coordinator) of the grant agreement and should be directly involved in the carrying out of the tasks foreseen in the grant. ➢ The participation of industry able to provide security solutions is required.

References

Draft work programmes 2016-17
http://europa.eu/!Dh67Gk

National Contact Points (NCPs)
http://europa.eu/!up97Wv

CNECT-H4@ec.europa.eu
@EU_TrustSec

European Commission

Where else to find cybersecurity and privacy R&D&I in H2020?

Everywhere!

change of mindset

4th EU-Brazil Coordinated Call

Opening: 08 Nov 2016
Deadline: 14 Mar 2017

4th Coordinated Call EU-Brazil

EUB-01-2017: Cloud Computing 2.5M€

Specific Challenge: Cloud computing is now an established global paradigm for the delivery of IT services in all sectors of the digital economy. However, further enhancements are still required in critical aspects of cloud computing, including **enhanced security and privacy**; trustworthy clouds; resource pooling; data management and traceability; virtualization; and hybrid systems. Support towards intercontinental experimentation on cloud infrastructures and services are necessary as well, especially in the context of EU-Brazil cooperation.

4th Coordinated Call EU-Brazil

EUB-02-2017: IoT Pilots

Specific Challenge: In order to make use of the rich potential of the Internet of Things (IoT) in real-world scenarios, technologies and tools developed so far need to be demonstrated in controlled environments with the ultimate goal of validation. Given the specific nature of this Call, widely replicable pilots are targeted in view of solving specific societal challenges, in the context of EU-Brazil cooperation.

Pilots aim at validating IoT approaches to specific socio-economic challenges in real-life settings. Pilots' objectives include user acceptability, technology assessment and optimisation, business model validation, approaches to sustainability and replicability. They should be implemented through close cooperation between users and suppliers with the active involvement of relevant stakeholders on the demand side.

4th Coordinated Call EU-Brazil

EUB-03-2017: 5G Networks

Specific Challenge: 5G is expected not only to boost the services already provided by 4G (LTE-Advanced-PRO), but also to enable several new services and applications in multiple environments, as identified notably by ITU, NGMN, 3GPP SA group and 5G PPP. 5G standardisation started in 2016 and is expected to extend until 2020 for a full specification. Within this time frame, there is still significant work to carry out to make sure that the multiple technologies contemplated for 5G will meet the full range of service requirements. Early validation with the widest possible footprint of candidate technologies for 5G is hence needed to support global consensus based on "derisked" technologies.

Contact

Call Coordinator
Jorge Pereira, DG CONNECT E1
Jorge.Pereira@ec.europa.eu

http://5g-ppp.eu

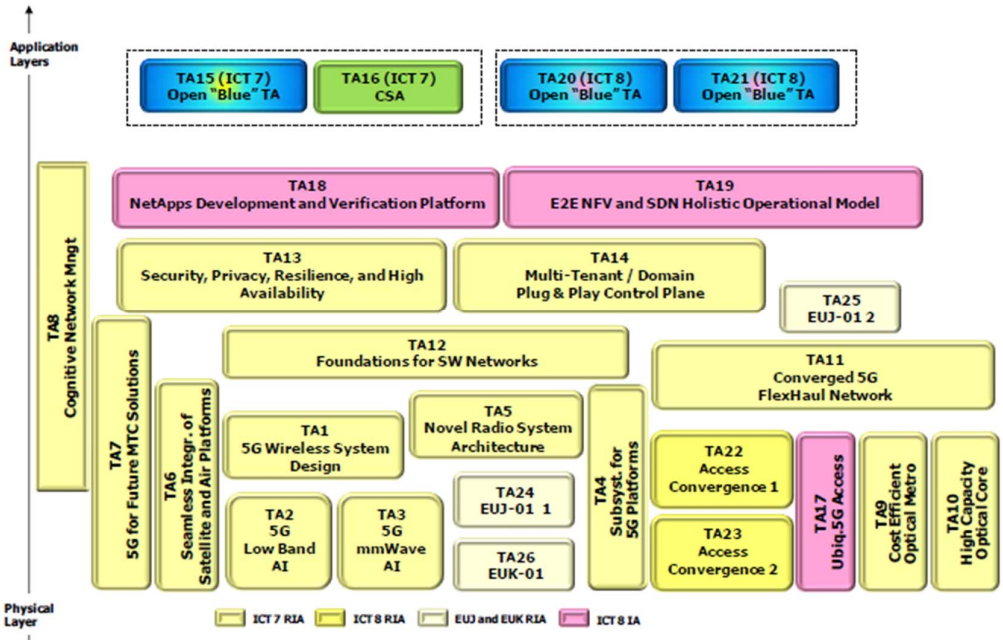
5G PPP Phase 2

Opening: 10 May 2016
Deadline: 08 Nov 2016

5G PPP Phase 2

- ICT-07-2017: 5G PPP Research and Validation of critical technologies and systems: 101+3 M€
  - RIA Strand 1: Wireless Access and Radio Network Architectures/Technologies.
  - RIA Strand 2: High Capacity Elastic – Optical Networks.
  - RIA Strand 3: Software Networks.
  - CSA.
- ICT-08-2017: 5G PPP Convergent Technologies: 41+5 M€
  - IA Strand 1: Ubiquitous 5G Access Leveraging Optical Technologies.
  - IA Strand 2: Flexible Network Applications.
  - RIA: Cooperation in Access Convergence.

5G PPP Phase 2 pre-structuring model



TA13: Security, Privacy, Resilience, and High Availability

Rationale

Security, privacy, resiliency, and high availability are mandatory for 5G success and adoption both in general, and specifically by verticals (Automotive, Industry, Smart Energy, Smart Health, Smart City, Smart Transport, ...). Existing methods of assuring these aspects fall short of delivering the required levels of reliability, thus require further research and innovation for enabling 5G deployments.

Objective

- A resilient & secure dynamically configurable, adaptive and highly available virtualised/sliced infrastructure supporting end-to-end 5G services as well as critical vertical services
- Secure (and privacy-preserving) and reliable solutions for setting up services across multiple domains

Scope

Research & Innovation actions related to 5G requirements towards high guarantees of resilience and security of infrastructure & virtualised/sliced infrastructures:

- Designing and implementing high availability of 5G services and solutions to deal with extreme reliability requirements under unprecedented system complexity, involving heterogeneous networks, services and devices. This includes reliability of: SDN control, architecture and deployment of network functions, and software updates
- End-to-end security of 5G services and solutions in virtualised and softwarised deployments that include multi-domain services and service-chains deployed over on-demand infrastructure. This includes security across all software lifecycle, security in the control plane, adaptation of security mechanisms to different verticals, and evolution of relevant regulation and liabilities aspects
- Integrate security risks into availability considerations by extending reliability models by cyber attacks as causes for failure
- QoS/QoE control in the presence of transport encryption: Means for QoS/QoE control of encrypted communication
- Supporting 5G MTC with specific protocols and critical requirements, dynamic, scalable and self-adaptable monitoring mechanisms supporting integrated and predictive monitoring of 5G IoT stack implementation

Expected Impact

- Technologies and methodologies for resilient, secure and highly available end-to-end deployments of Software Networks
- A resilient execution and usage framework on top of dynamically composed infrastructures
- Standard functions, interfaces, and reference implementations
- Contribution to EU booth at MWC 2019 with demo / testbed showcasing the set of 5G PPP Phase 2 projects results

Contact (Security, Open Hardware)

Jorge Pereira, DG CONNECT E1
Jorge.Pereira@ec.europa.eu