SPARTA

PLACE, DATE: FRANCE, 26/02/2019

SPARTA — Re-imagining the way cybersecurity research, innovation, and training are performed in the European Union

Cybersecurity is an urgent and major societal challenge. Highly correlated with the digitalization of our societies, cyberthreats have an increasing impact on our lives. It is therefore essential to ensure digital security and strategic autonomy of the EU by strengthening leading cybersecurity capacities. This challenge will require the coordination of Europe's best competences, towards common research and innovation goals.

SPARTA is a novel Cybersecurity Competence Network, supported by the EU's H2020 program, with the objective to develop and implement top-tier research and innovation collaborative actions. Strongly guided by concrete challenges forming an ambitious Cybersecurity Research & Innovation Roadmap, SPARTA will setup unique collaboration means, leading the way in building transformative capabilities and forming a world-leading Cybersecurity Competence Network across the EU. From basic human needs (health) to economic activities (energy, finance, and transport) to technologies (ICT and industry) to sovereignty (eGovernment, public administration), four research and innovation programs will push the boundaries to deliver advanced solutions to cover emerging challenges.

The SPARTA consortium, led by CEA, assembles a balanced set of 44 actors from 14 EU Member States, including ANSSI, Institut Mines-Télécom, Inria, Thales, and YesWeHack for France, at the intersection of scientific excellence, technological innovation, and societal sciences in cybersecurity. Together, along with SPARTA Associates, they aim at re-imagining the way cybersecurity research, innovation, and training are performed in Europe across domains and expertise, from foundations to applications, in academia and industry.

In sharing experiences and excellence, challenges and capabilities, SPARTA makes decisive contributions to European strategic autonomy.

* *
*

CEA *will coordinate SPARTA and drive its strategic direction to maximize its impact for the community. It will be responsible for all aspects of the interface between SPARTA and the European Commission, and will create and maintain communication channels with national cybersecurity authorities. By leveraging its experience in collaborative networks, it will ensure the governance follows best practices and guarantee its performance and effectiveness through continuous improvement.*

ANSSI *will mainly contribute to the elaboration of the R&D Roadmap of this novel Cybersecurity Competence Network, as well as contribute to the impact study of the technical programs on the certification capacities and to the elaboration of the training program. SPARTA has the capacity to support ANSSI's missions at the European level, especially regarding the coordination of national and European R&D efforts in Europe, in the perspective of the establishment of the future European Cybersecurity Research and Competence Centre, keeping the European strategic autonomy as the overall objective in view.*

Institut Mines-Télécom will manage the CAPE program (Continuous Assessment in Polymorphous Environments). This program aims at developing methods and tools for assessing the properties of modern devices and services, with a focus on dynamic environments and security/safety co-design. Institut Mines-Télécom is also involved in the HAII-T Program, through its long-standing activities in hardware security and industrial control systems security. As an academic institution, Institut Mines-Télécom is also strongly involved in training and awareness, leading the task on professional education. From these contributions, Institut Mines-Télécom will also address the governance issue, and will participate at the strategic level in the relevant bodies of SPARTA.

Inria will be involved in Sparta on both a technical and strategic level. This notably includes the HAII-T (High-Assurance Intelligent Infrastructure Toolkit) program, where the Inria teams Celtique, Cidre, Eva, Infine, Inde, Grace, and Privatics contribute with their expertise in secure systems software, formally verified cryptography, security of the Internet of Things, intrusion detection, and security analysis and certification of software. Moreover, its high security laboratories (LHS) in both Rennes and Nancy join forces with other European platforms to facilitate access for research and industry to high quality experimentation facilities. Finally, Inria leads three tasks in the definition of the SPARTA roadmap, which will establish a Cybersecurity Research and Innovation Roadmap for the European cybersecurity ecosystem at large.

Thales, one of the consortium's original founders, will share with the consortium its 40 years of expertise, focusing on two objectives: the technical analysis of cyberattacks and the development of AI-based secure systems. To help companies and organizations appreciate the IT threat and better protect themselves, Thales aims at developing European capabilities in cyber threat intelligence and at facilitating the safe sharing and usage of this knowledge. Thales will also bring its long-standing experience in the development of secure systems based on a trusted and explainable AI. By bringing together its cyber expertise and its knowledge of hackers' modus operandi, Thales will also be able to simulate new AI-based attacks to learn how to react and protect the ecosystem.

YesWeHack will strengthen the cooperation between the stakeholders by including diverse key players: ethical hackers, IT researchers, students, and the scientific community. To this end, YesWeHack will organize workshops in cities across Europe, along with the SPARTA Associates, to bring together cybersecurity experts from different horizons.

* * *

About CEA
CEA is a public multidisciplinary research organization whose research fields range from nuclear industry to bio-sciences, fundamental physics, and information and communication technologies. CEA represents 16,110 employees, B€4.4 budget, 1,689 patents registered or active, 1,300 contracts signed with industry, 178 new companies created since 1972 in high technologies sectors, and 9 research centers located in France.
More information: http://www.cea.fr/english

About ANSSI
ANSSI is the national authority in the area of cyberdefence and network and information security. To fulfil its missions, ANSSI deploys a broad range of regulatory and operational activities, from issuing regulations and verifying their application, to monitoring, alert and rapid response – particularly on government networks.
More information: http://www.ssi.gouv.fr/en/

About Institut Mines-Télécom
Institut Mines-Télécom is a public institution dedicated to higher education and research for innovation in the fields of engineering and digital technology. Always tuned in to the economic world, it combines high academic and scientific legitimacy with close business relations and a unique positioning in 3 major transformations of the 21st century: Digital Affairs, Energy and Ecology, and Industry. Its training and research for innovation are conducted in the Mines and Télécom Graduate Schools under the supervision of the Minister for Industry and Electronic

Communications, in one subsidiary and in institutions that are associate partners or under contract. Institut Mines-Télécom is a founding member of the Industry of the Future Alliance. It has two Carnot labels for the quality of its research partnerships. Every year, around one hundred startup companies leave its incubators.
More information: http://www.imt.fr/en/

About Inria
Inria, the French national research institute for the digital sciences, promotes scientific excellence and technology transfer to maximise its impact. It employs 2,400 people. Its 200 agile project teams, generally with academic partners, involve more than 3,000 scientists in meeting the challenges of computer science and mathematics, often at the interface of other disciplines. Inria works with many companies and has assisted in the creation of over 160 startups. It strives to meet the challenges of the digital transformation of science, society and the economy.
More information: http://www.inria.fr/en

About Thales
In a constantly changing and increasingly connected world, Thales stands by those with great ambitions: to put digital technology at the service of a better and more secure world. Our 5000 specialists in critical information technology and cybersecurity design a unique range of exceptional technological solutions that meet the most demanding requirements of our customers - governments, administrations, large companies, vital operators. More than 50 countries and 130 large companies handling critical business processes and sensitive data rely on Thales, the European leader in cybersecurity and the world leader in data protection, to ensure their digital transformation. With 66,000 employees in 56 countries, Thales generated sales of €15.9 billion in 2018.
More information: http://www.thalesgroup.com/en

About YesWeHack
Created in 2013, YesWeHack is the 1st European Bug Bounty platform, connecting organizations with a global community of cybersecurity researchers (7000+) to continuously detect and report their vulnerabilities. YesWeHack makes security an enabler of your digital transformation by providing an agile, cost effective and proactive solution.
More information: http://www.yeswehack.com/en/

<p style="text-align:center">★   ★
★</p>

Press contacts

CEA
Élisabeth Lefèvre-Rémy
elisabeth.lefevre-remy@cea.fr
+33 1 69 08 24 26

ANSSI
Margaux Vincent
margaux.vincent@ssi.gouv.fr
+33 1 71 75 84 04

Institut Mines-Télécom
Jérôme Vauselle
jerome.vauselle@imt.fr
+33 1 45 81 75 05
Hervé Debar
hervé.debar@imt.fr
+33 1 60 76 45 83

Inria
Laurence Goussu
laurence.goussu@inria.fr
+33 1 39 63 57 29

Thales
Constance Arnoux
constance.arnoux@thalesgroup.com
+33 1 57 77 91 58

YesWeHack
Nicolas Diaz
n.diaz@yeswehack.com
+33 6 11 29 96 76
Marine Magnant
m.magnant@yeswehack.com
+33 6 02 16 93 20