

THIS IS SPARTA

Thibaud Antignac^a, Géraud Canet^b, and Florent Kirchner^a

^aSoftware Reliability and Security Lab | ^bEuropean Partnerships
CEA, List
`first.last@cea.fr`

European scientists hold pioneering positions in cybersecurity research fields such as cryptography [5, 4], formal methods [2], or secure hardware components [6]. Yet this excellence on focused domains does not translate into larger-scale, system-level solutions and services: too often, small scattered teams fall short of critical mass capacities, despite demonstrating world-class talent and results. In a competitive international environment, and with cyberspace becoming a geopolitical asset [1], such a limited capacity-building can constitute a weakness of Europe’s strategic autonomy [3].

In response, the SPARTA pilot project proposes to establish a *network of competence centers*, with a governance aiming to encourage collaborations between research teams, across geographies, disciplines, and organizations – spanning through academic, industrial, institutional, and grassroots cybersecurity. Two major artifacts will serve as pivotal elements for this governance: an ambitious and continuously-evolving *research and innovation roadmap*, and a set of *joint platforms and infrastructure*.

The SPARTA network will demonstrate its operation over the course of four *Programs* focused on strategic challenges for digital societies:

T-SHARK will explore innovative work in full-spectrum situational awareness, with the goal of enabling the supervision of complex systems over heterogeneous time scales;

CAPE will investigate new avenues for continuous assessment in polymorphous environments, creating new evaluation tools and techniques for handling tomorrow’s dynamic and elastic digital systems;

HAI-T will aim to create a toolkit for high-assurance intelligent infrastructure, incorporating pivotal components for secure and resilient intelligent infrastructures;

SAFAIR will devise secure and fair AI systems for citizen, delving into innovative approaches to make systems using AI more reliable and resilient.

These Programs are supported, in turn, by activities on ethical, legal, and social aspects of research with a particular attention to privacy and data protection; on exploitation and intellectual property rights; and on potential interactions with existing and new certification practices.

Project	SPARTA
Lead / Part.	CEA / 44 partners / 50+ associates
Topology	AT, BE, CZ, DE, EE, EL, ES, FR, IT, LT, LU, LV, PL, PT
Instrument	H2020-SU-ICT-03-2018
Timeline	T_0 : 01/02/2019, 36 months
TRL	3-6

To ensure the proper dissemination of SPARTA results with all relevant stakeholders, all partners will engage with their respective communities. SPARTA results will also be shared with SPARTA Associates and the general public through *bi-annual days* and monthly workshops throughout the network.

Through innovative governance, ambitious demonstration cases, and active community engagement, SPARTA aims at re-thinking the way cybersecurity research is performed in Europe across domains and expertise, from foundations to applications, contributing *inter alia* to achieve the objective of European strategic autonomy.

References

- [1] Cybersecurity: Paris call of 12 november 2018 for trust and security in cyberspace.
- [2] Gérard Berry. Prouver les programmes : pourquoi, quand, comment ? Cours au Collège de France, 2015.
- [3] Jean-Claude Juncker. State of the union 2018: The hour of European sovereignty.
- [4] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *J. Cryptology*, 13(3):361–396, 2000.
- [5] Bart Preneel, René Govaerts, and Joos Vandewalle. Hash functions based on block ciphers: a synthetic approach. In Douglas R. Stinson, editor, *Advances in Cryptology — CRYPTO' 93*, pages 368–378, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.
- [6] Marc Renaudin, G. Fraidy Bouesse, Ph. Proust, J. P. Tual, Laurent Sourgen, and Fabien Germain. High security smartcards. In *DATE*, pages 228–233. IEEE Computer Society, 2004.