COMPUTER AND CONTROL ENGINEERING

DAUIN - Secure and trusted network channels

Funded By	Dipartimento DAUIN
Supervisor	LIOY ANTONIO - antonio.lioy@polito.it
Contact	
Context of the research activity	Modern ICT applications are highly distributed and networked. Given the intrinsic insecurity of the networks, inter-node communications must face several security problems: protection of the data being transmitted, authentication of the peer, and trust in the application executed by the peer. The research objective is the design and test of secure and trusted network channels ,to be used in both lightweight and standard computing systems (e.g. IoT as well as cloud).
Objectives	Modern ICT applications are highly distributed (e.g. cloud, edge, IoT, and personal devices) and heavily rely on network communications. However, networks are inherently insecure and this generates various threats. In this scenario, when an application on a node communicates with another one on a different node, several security problems arise, such as protection of the data being transmitted, authentication of the peer, trust in the application executed by the peer, and proof of transit The gross objective of this research is the design and test of secure and trusted network channels to be used in both lightweight and standard computing systems (e.g. IoT as well ad cloud). The specific objectives of the research activity are: 1. Identify, design, and implement appropriate software elements to support the creation of secure and trusted network channels. 2. Extend existing open-source systems (e.g. Linux and Keystone could be suitable targets) to support the designed secure and trusted network channels. 3. Implement a system with the hardware and software components needed to demonstrate the feasibility and performance of the designed secure and trusted network channels. The first year will be spent studying the existing paradigms for secure network channels (TLS, IPsec, …) and trusted execution (Intel TXT and SGX, the Trusted Computing platform, and the ARM TrustZone). The PhD student will also analyse modern security paradigms applied to software infrastructures. During this year, the student should also follow most of the mandatory courses for the PhD and submit at least one conference paper.

	During the second year, the PhD student will design a custom approach for secure channels in a trusted execution environment, enriched with hardware root-of-trust. The application domain should be oriented to modern infrastructures, for personal/edge/fog devices that support lightweight virtualisation technologies. At the end of the second year, the student should have started preparing a journal publication on the topic and submit at least another conference paper. Finally, the third year will be devoted to the Implementation and evaluation of the proposed solution, compared with the existing ones. At the end of this final year, a publication in a high-impact journal shall be achieved. Possible target publications: IEEE Security and Privacy, Springer International Journal of Information Security, Elsevier Computers and Security, Future Generation Computer Systems. This research is part of the H2020 project SPIRS (Secure Platform for ICT systems Rooted at the Silicon manufacturing process). https://www.spirs-project.eu/ and of the HE project iTrust6G (that will start on January 2024).

Skills and competencies for the development of the activity	Cybersecurity (mandatory) Network security (mandatory) Trusted computing (preferred) Hardware design and related firmware (preferred)