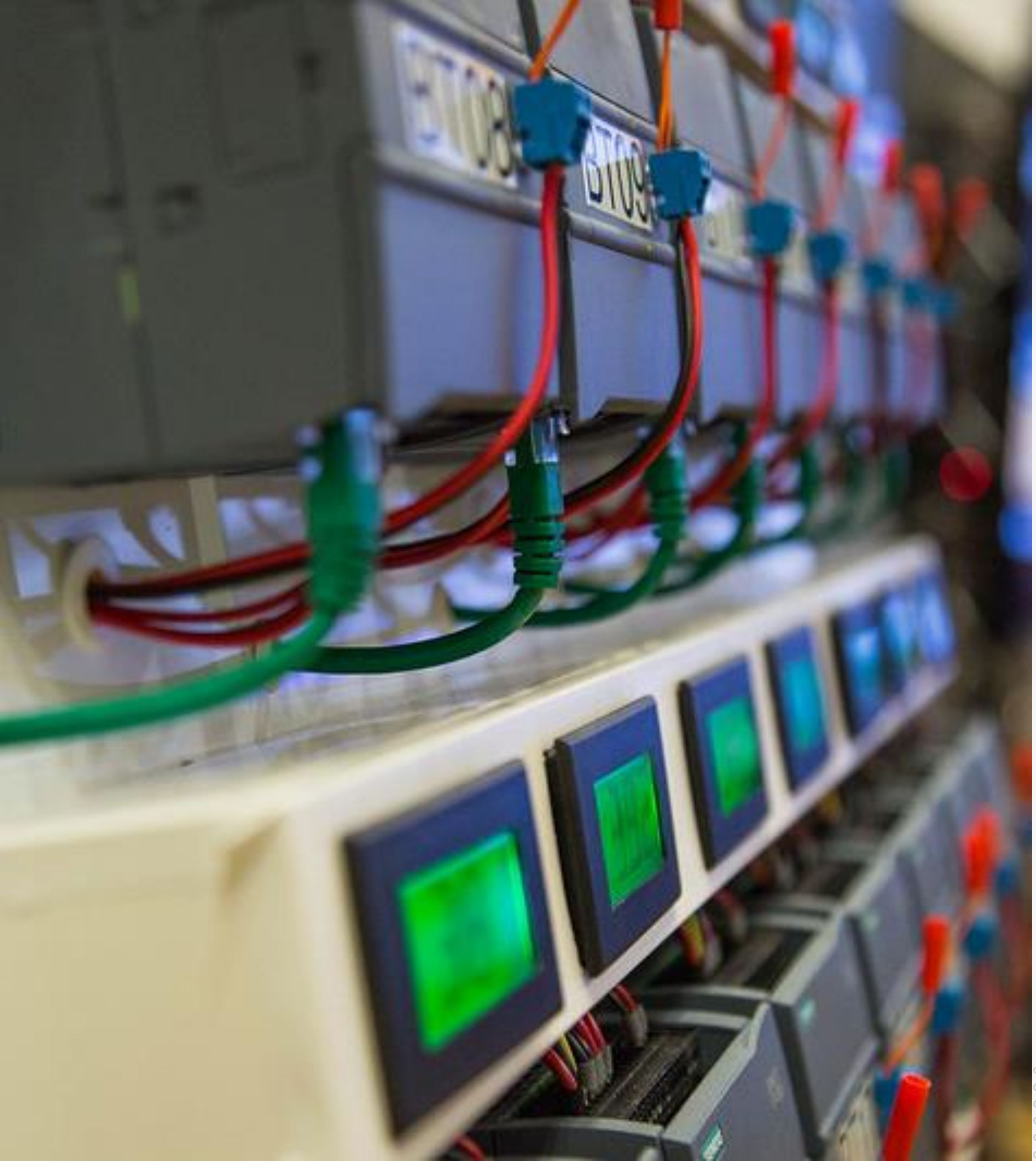
REGIONE PIEMONTE
CSI your digital partner
Politecnico di Torino
links
INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA
top-ix
CYBERSECURITY 4.0
Il futuro della sicurezza informatica è ora

Sicurezza delle Infrastrutture Critiche e IoT

Edoardo Calia - CTO

EVENTO ONLINE IN DIRETTA DALLA SALA TRASPARENZA DELLA REGIONE PIEMONTE

GIOVEDI 3 MARZO 2022



IoT systems Architecture

- Digital transformation of critical infrastructures starts from installing advanced, distributed information systems which actually represent one of the most relevant examples of large IoT architectures
- The installed system must be secure, reliable and resilient to events potentially undermining its 24/7 operation

IoT, Critical Infrastructures and Cybersecurity

- Monitoring and controlling an infrastructure requires the deployment of a large number of sensors and actuators, together with information systems installed at different levels: cloud, *fog*, edge, up to the periphery hosting the embedded systems for sensing and controlling
- All these systems and devices are potential targets for a cyber-attack. Obtaining resiliency and cybersecurity for such a system requires a bottom-up approach:
    - Secure design and configuration of each of the devices and systems, as well as of the network infrastructures
    - Plan for robustness and resiliency of the cybersecurity subsystem itself, on top of robustness and resiliency of the services and functionalities of the operational system

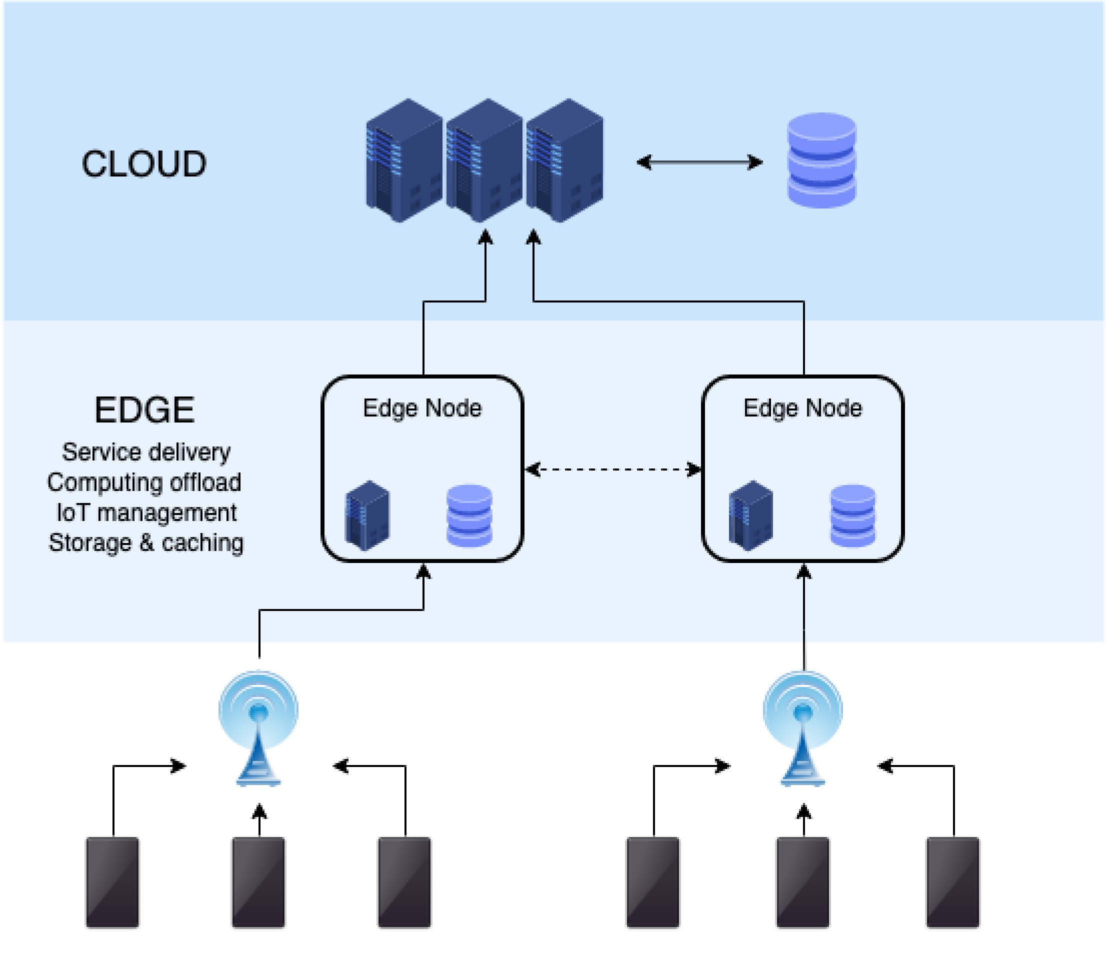


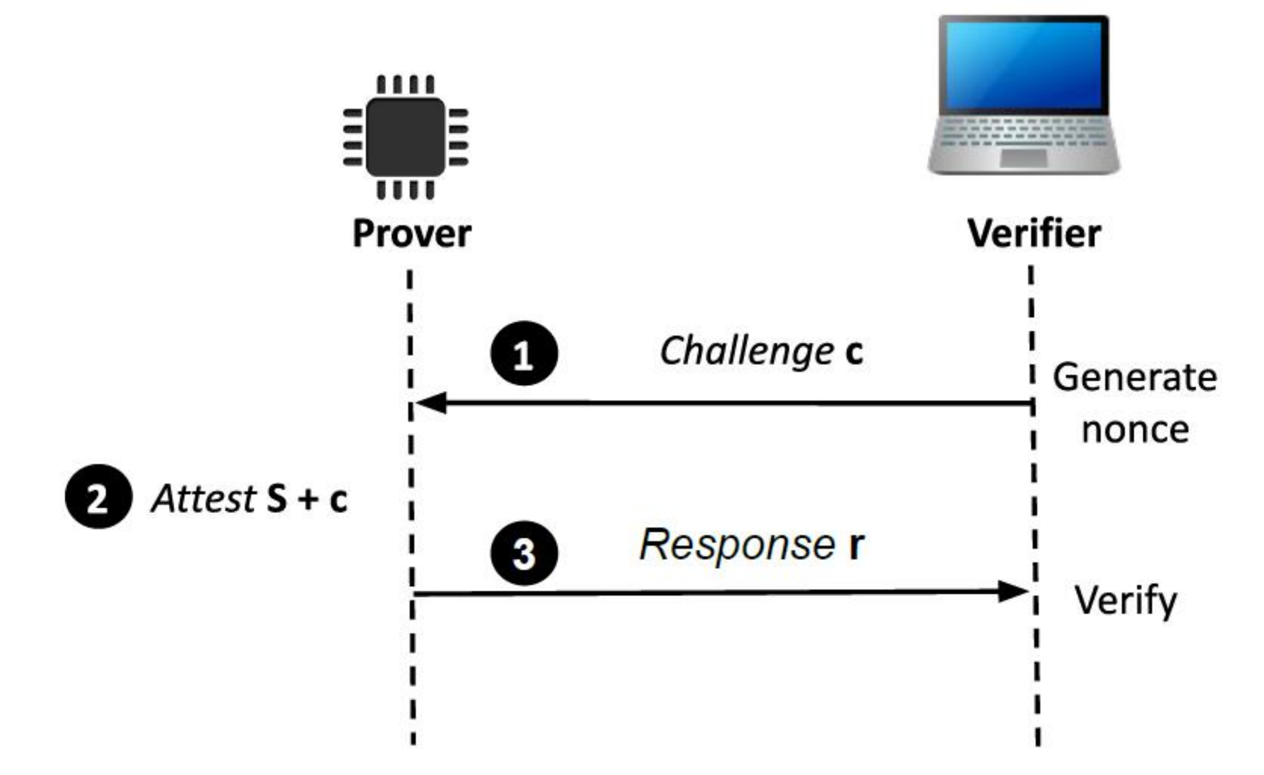
Image by NoMore201 - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=82034067

Cybersecurity at the periphery

- Cybersecurity is mainly based on cryptography principles and algorithms, which are known as being computing-intensive
- Embedded systems used as sensors and actuators have limited computing power and resources
- A solution for that is embedded trusted computing: bringing the principles of trusted computing to embedded systems
    - A cryptographic chip installed on the board of the devices carries out all the heavy work, checking for the integrity of each piece of software executed on the device: the system completes its bootstrap only if no changes to the software are detected
    - Once correctly started, the device presents itself to a remote attestator node, which does additional checks on the identity of the device and its authorization to be part of the overall IoT architecture

Resiliency in the cybersecurity subsystem

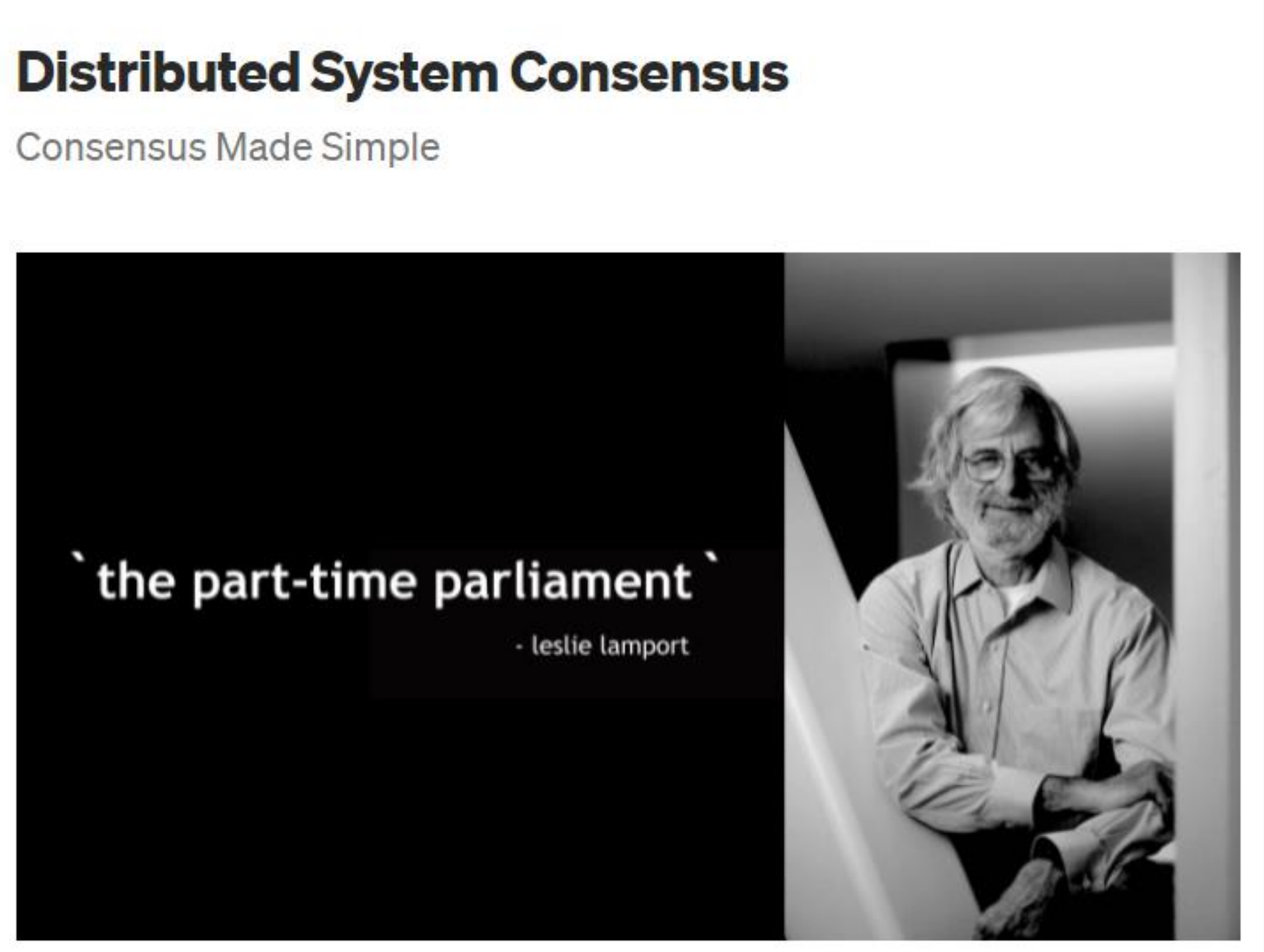
- Remote attestation is a critical task in the secure IoT system described so far
- The remote attestator is a potential bottleneck and a critical point of attack
- In order to introduce resiliency in the system, remote attestation capabilities could be distributed (replicated) among different nodes in different locations (for geographically distributed infrastructures)
- Replicating data and services is a simple (conceptually!) but very effective way to protect the system against failure, but also against attacks: the digital infrastructure evolves into a redundant, decentralised system
- Principles studied for 50+ years and widely validated are still supporting security and resilience of complex information systems



Remote Attestation Challenge-Response protocol

Ankergård, S.F.J.J.; Dushku, E.; Dragoni, N. "State-of-the-Art Software-Based Remote Attestation: Opportunities and Open Issues for Internet of Things" Sensors **2021**, 21, 1598. https://doi.org/10.3390/s21051598

Consensus in Distributed Systems



Distributed System Consensus

Consensus Made Simple

- When several independent systems are required to maintain copies of the same evolving set of information (i.e. a ledger of transactions), a mechanism is needed to make sure that all of them agree about the «next» event to register, without using a coordinator (which would become a single point of failure)
- Consensus protocols are one of the most complex and fascinating features of distributed systems and databases
- In a network run and maintained by a consensus protocol, attacking and changing the information requires normally doing so on a large number of nodes (the «50% + 1 attack»), making the attack almost impossible

Computing Continuum and resiliency to attacks

- The architecture resulting from the installation of «intelligent» systems at different layers (cloud, edge, periphery) offers the opportunity to implement what is commonly known as the «computing continuum» paradigm
- Computing continuum is becoming the reference architecture in a world where data processing is required (possibly with different performance) at different locations in the network
- Some computation must be done *fast* and *close* to the places where data is collected. Sophisticated processing services that can tolerate some delay can be carried out centrally, in the *cloud,* by High Performance Computing (HPC) systems

Orchestration of resources in a Computing Continuum system

- Computing continuum will get even more popularity when mobile connected device start being deployed (starting from vehicles): such systems will need to connect to the closest computing node

- Managing resources in a computing continuum architecture may also include the capability to «move» or «dispatch» software modules to different nodes, based on opportunistic principles (availability of resources, failure of one or more nodes, mobility of end users)

Summing up

- Critical Infrastructures must become smarter, and this requires the deployment of smart devices in a geographically distributed architecture
- The starting points must be smart and safe: all computing systems, from cloud to embedded systems and other IoT devices, must be *secure by design*
- Once all components are safe, they can start collaborating
- Features typical of distributed and resilient system achitectures can be applied also to the cybersecurity subsystem, making the fundamental services (identity check, access credentials management etc) available in a reliable, robust and attack-resilient way

CYBERSECURITY 4.0

Il futuro della sicurezza informatica è ora

Thanks

for your attention!

Edoardo Calia

edoardo.calia@linksfoundation.com

@edocalia

FONDAZIONE LINKS
Via Pier Carlo Boggio 61 | 10138 Torino
P. +39 011 22 76 150
LINKSFOUNDATION.COM