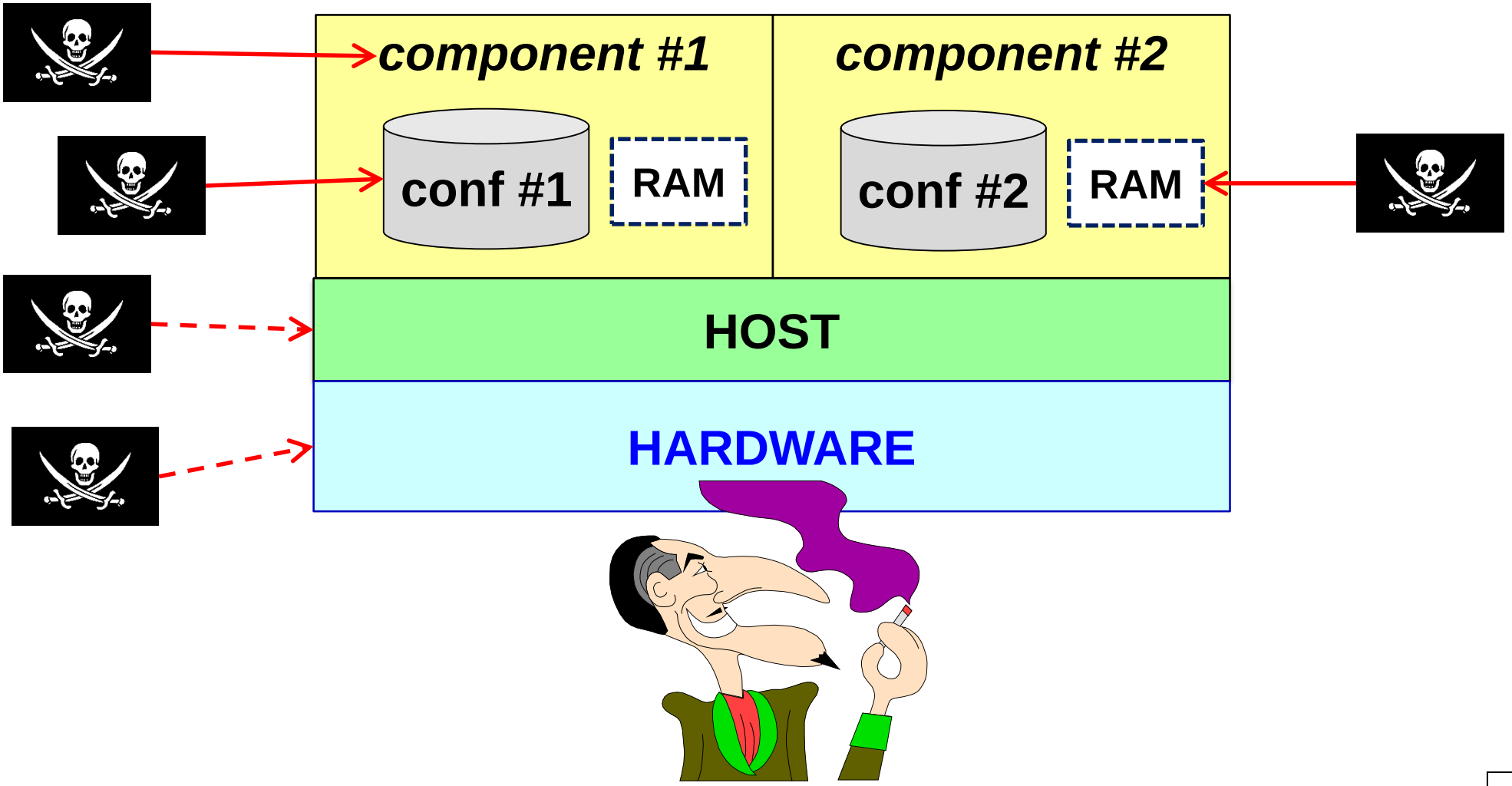
Trust and integrity in SDN environments

Antonio Lioy
< antonio.lioy@polito.it >
Politecnico di Torino

SDN security workshop
at the CODE-2018 event

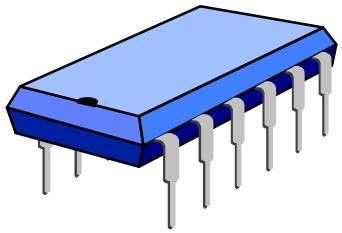
Munich (Germany)
July 11th, 2018

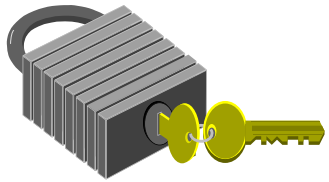
Trust (and integrity)



Hardware root of trust

- **useful to have a stronger foundation (can still be attacked by physical access, unless made tamper-proof)**
- **important to create a TEE (Trusted Execution Environment)**
  - chain of trust (from firmware up to applications)
- **we use the TPM (Trusted Platform Module)**
  - special registries (PCRs) accumulate the measures of executed components
    - BIOS, boot, OS loader, …
    - state = set of specific PCR values
  - QUOTE operation to report PCR values (w/ challenge and digital signature)

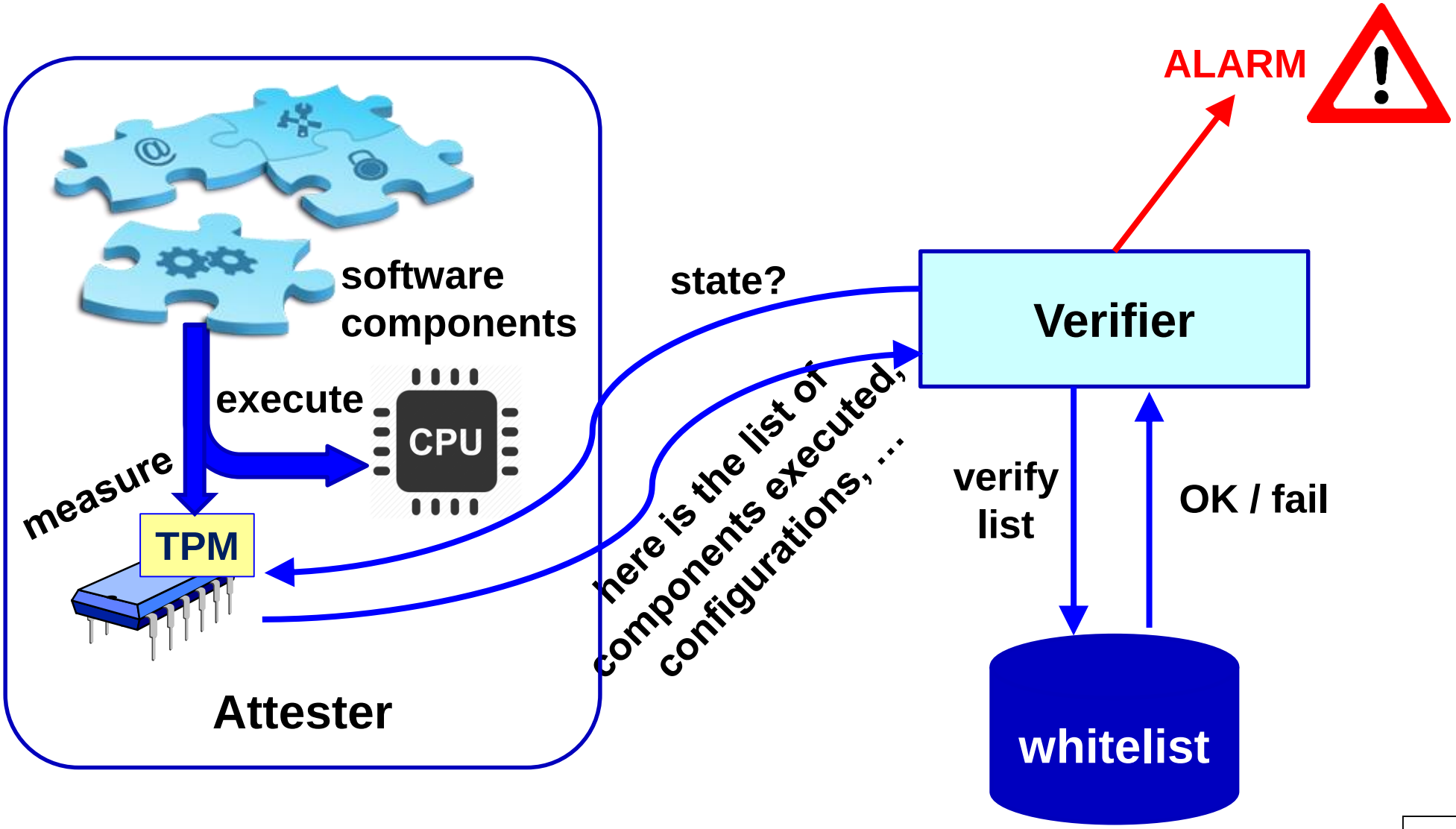




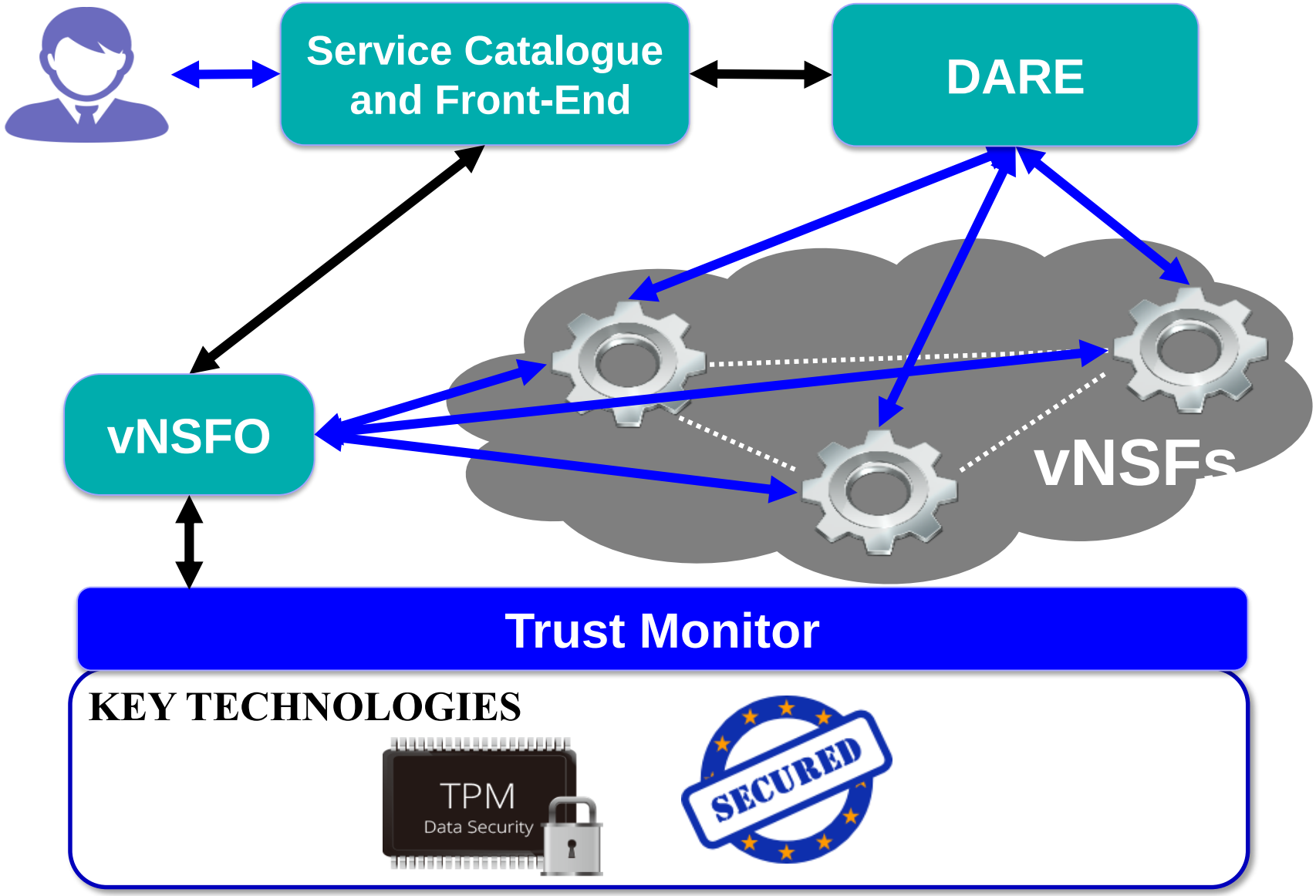
Which is your trust perimeter?

- **load time**
  - measure **components** when loaded for execution
    - what is "executable"?
- **run time (components that change their behaviour while running)**
  - measure **configuration files** (when loaded or re-loaded)
    - beware of caching!
  - measure **in-memory configuration** (e.g. filtering or forwarding rules modified by CLI or network protocol)
    - needs appropriate firmware/host (L.Jacquin et al.)

Remote attestation



The SHIELD Trust Monitor



Audit and forensic analysis

- **network behaviour cannot be given for granted any more**
- **increasingly important as more intelligence / computation is moved into the network**
- **especially important for multitenant infrastructure**
- **open questions:**
  - network state at time T?
  - network path+processing for user U at time T?

THANK YOU !

Project SHIELD (www.shield-h2020.eu)

Project SECURED (www.secured-fp7.eu)