SecureCloud – Secure Big Data Processing in Untrusted Clouds

Florian Kelbert *, Franz Gregor †, Rafael Pires ‡, Stefan Köpse ‡, Marcelo Pasin ‡, Aurélien Havet ‡, Valerio Schiavoni ‡, Pascal Felber ‡, Christof Fetzer †, Peter Pietzuch *

* Imperial College London, United Kingdom, {fkelbert, prp}@imperial.ac.uk
† TU Dresden, Germany, {firstname.lastname}@tu-dresden.de
‡ University of Neuchâtel, Switzerland, {firstname.lastname}@unine.ch

Context

- Confidentiality, integrity and availability in the cloud
- Critical infrastructures (financial, health care, smart grids)
- Small trusted computing base (trusted execution environment)
- Commodity hardware

- Objectives:
  - Improve the state-of-the-art in cloud dependability
  - Seamlessly integrate into standard cloud stacks
  - Validate through use cases in the domain of critical infrastructures (smart grids)

Intel SGX

- Secure containers for QoS-aware applications
- Dependable micro-services for the cloud
- Secure distributed big data applications

Layered architecture

SecureCloud approach

- Secure docker containers (SCONE)
- SCBR and performance overhead (page faults)

Conclusions

- SecureCloud designs and develops technologies for future cloud environments
- Enhanced dependability to host critical infrastructure applications in the cloud
- Initial SGX-based prototypes demonstrate SecureCloud’s promising approach

The road ahead:

- Management and orchestration services
- Effective partitioning of applications
- Efficient memory usage
- Infrastructure and micro-services development
- Components validation and integration

H2020 EU-Brazil joint call. Grant agreement #690111 2016-2018