11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Tamper Resistant Secure Digital Silo for Log Storage in Critical Infrastructures

Khan Ferdous Wahid[a], Helmut Kaufmann[a], and Kevin Jones[b]

[a] *Airbus Group Innovations, Munich, Germany*
[b] *Airbus Group Innovations, Newport, UK*

AIRBUS
GROUP

Why another secure storage system?

- Clouds are not yet ready for the CIs due to various security challenges*
  - Unavailability, Cross-Border Policies, Metadata spoofing, Insecure API etc.
- SW based solutions lack memory protection
  - Potential disclosure of the keys to attackers
- HW based solutions have limitations
  - Share keys or do calculation without memory protection
  - Functional limitations of HW
- Most of them do not address Truncation attack.

* Younis, Y.A., Merabti, M., Kifayat, K.: Secure Cloud Computing for Critical. Infrastructure: A Survey.

Our goal

- Build a practical tamper resistant log storage system

Where the system has-

- no shared secret with user or OS
- memory protected operations
- separation of secrets for local storage
- remote integrity verification capability
- detection of system power cycles
- COTS hardware reliance

To provide-

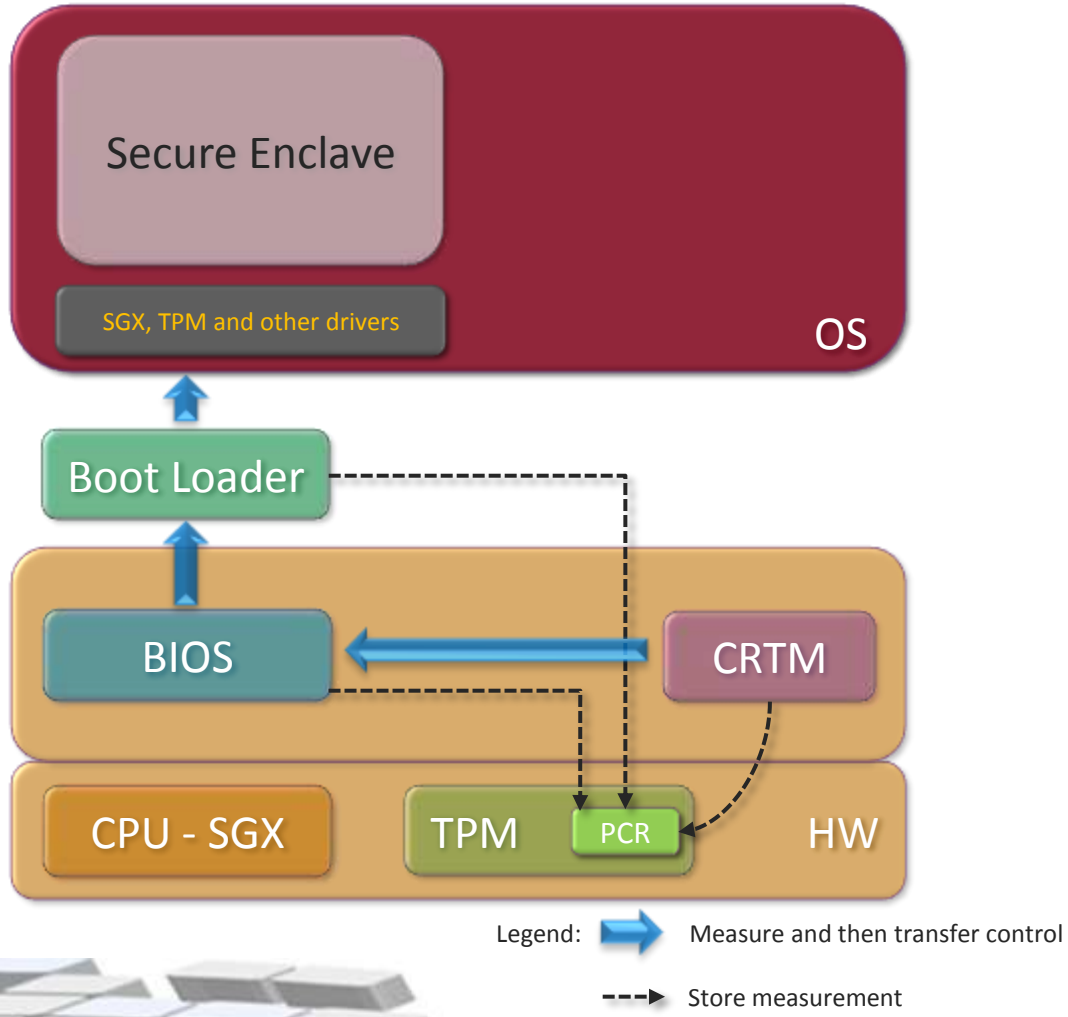
- integrity
- unforgeability
- availability
- authenticity
- remote verification
- fail-safe
- accountability
- safety
- correctness
- seamlessness

Our Solution

Based on:

- TPM: Trusted Platform Module to initialize the system in good state
- Intel SGX: completely memory protected cryptographic operations with muti-core support
- eCryptfs: first layer of security to prevent non-root attackers
- SBD: second and tamper-proof layer of security to prevent even privileged attackers

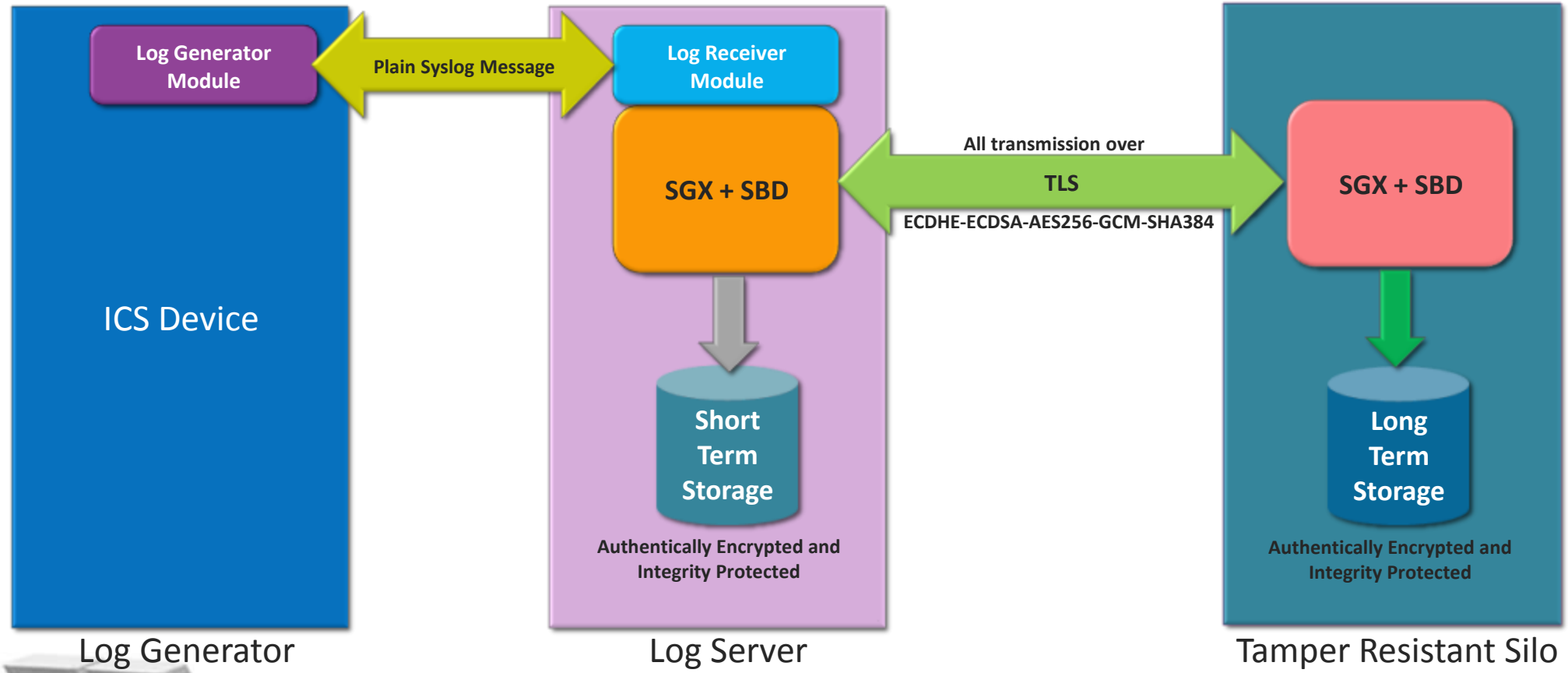
Our Solution



- The integrity measurement architecture (IMA), available in Linux, can measure the system initialization steps, but unable to detect TOCTOU class of attacks
- Execution inside SGX supported Secure Enclave, after the trusted initialization of OS and drivers, prevents such attacks and guarantees run-time integrity

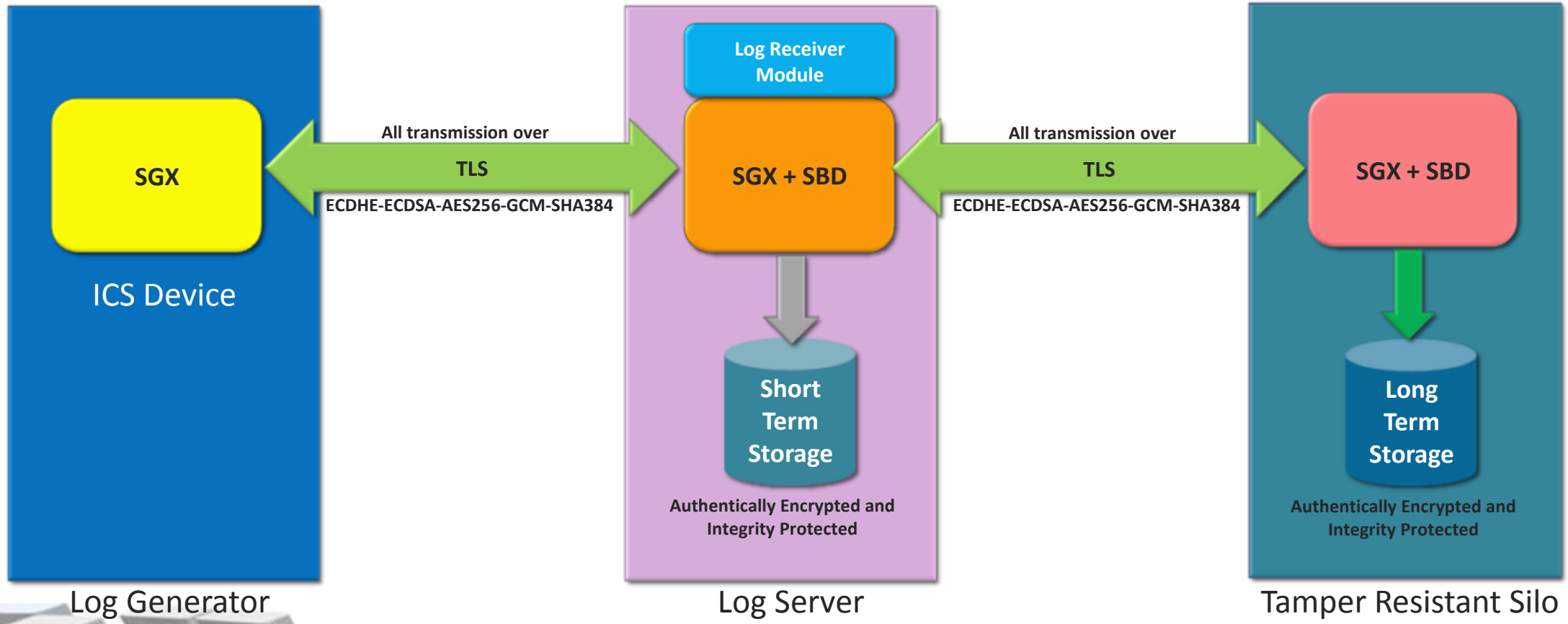
Our Solution

Proprietary Log generator:



Our Solution

Customized Log generator:



Is our goal fulfilled or not?

- Build a practical tamper resistant log storage system

Where the system has-

- no shared secret with user or OS
- memory protected operations
- separation of secrets for local storage
- remote integrity verification capability
- detection of system power cycles
- COTS hardware reliance

To provide-

- integrity
- unforgeability
- availability
- authenticity
- remote verification
- fail-safe
- accountability
- safety
- correctness
- seamlessness

Acknowledgement

This work is funded by the European FP7 security project - European COntrol System Security Incident Analysis Network, ECOSSIAN (607577).

Thank you.