Secure Embedded Systems

Michael Vai, David J. Whelihan, Benjamin R. Nahill, Daniil M. Utin, Sean R. O'Melia, and Roger I. Khazan

Presented by: Huachuan Wang

Introduction

Cyber security

Security coprocessor

Cryptography

2020 NEW Smart Digital Satellite TV Receiver DVB-T2+DVB-S2 FTA 108(Tuner MPEG4 EU/US Plug

$20.00 Wish - Yanwen59

2020 NEW Smart Digital **Satellite TV** Receiver **DVB**-T2+**DVB**-**S2** FTA 1080P Decoder Tuner M

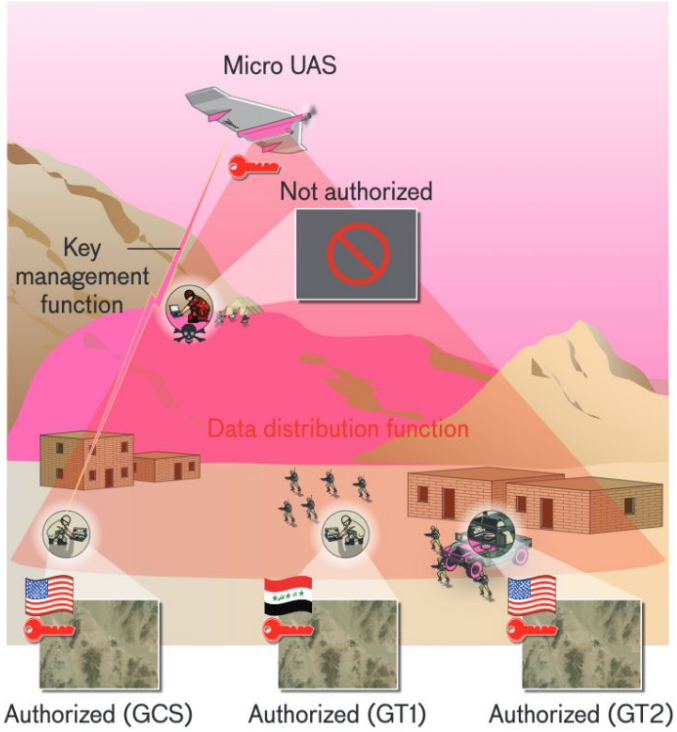


FIGURE 2. In this example of an unmanned aircraft system (UAS) application in its execution phase, the intelligence collected by the UAS needs to be shared by coalition partners yet protected from adversaries. Cryptography is the key technology enabling this operation.

Cybersecurity

Computer security, cybersecurity or information technology security is the protection of computer systems and networks from the theft of or damage to their **hardware, software,** or electronic **data**, as well as from the disruption or misdirection of the **services** they provide. (Wikipedia)

Security goals: Confidentiality, integrity, availability (CIA Triad) and usability

Security system design process->

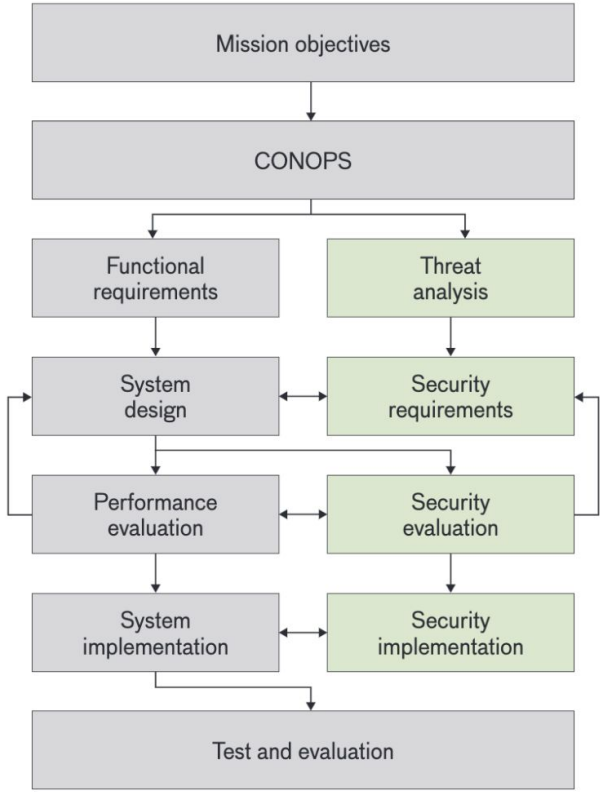


FIGURE 1. In an ideal secure embedded system design process, functionality (gray) and security (green) are co-designed, yet they are appropriately decoupled during testing so that security does not interfere with functionality.

Security Difficulties

- Limited protection
- Defense is often based on unverifiable and incomplete assumptions
- Defense is asymmetric
- SWaP or usability requirements, very little tolerance on overhead incurred by security
- Incompatibility of individual secure solutions

UAS example,

- high probability of equipment loss
- Many attack surfaces
- Question:Which attack surface the weakest? Self-destruct means fragility?

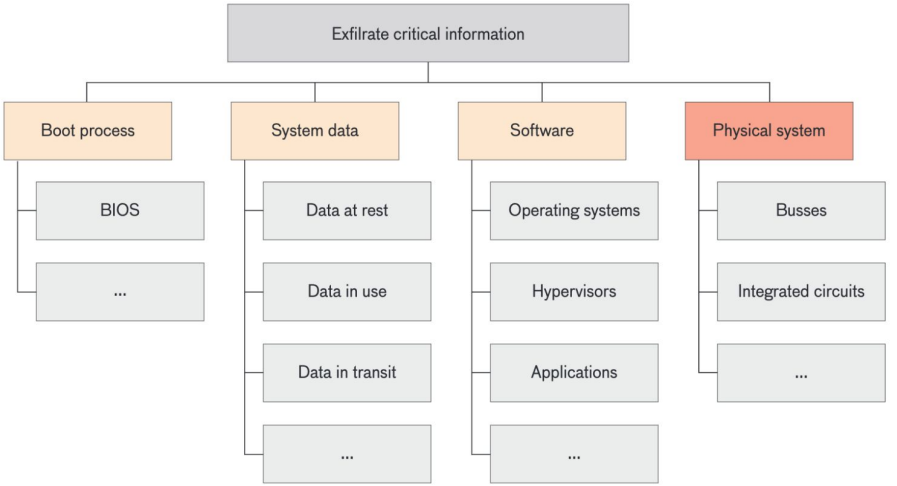


FIGURE 4. Example unmanned aircraft system (UAS) attack targets illustrate the vulnerabilities and sources of a threat scenario with three attack surfaces (boot process, system data, and software) and one physical attack surface (physical system).

Security Building Blocks

- Trusted Platform Module (TPM):

Allow the chip to perform platform and hardware device authentication.

- Security coprocessor (S-COP) : RISC-V?

Security coprocessor uses cryptography to securely boot the CPU into a known configuration

– Separation, attestation, and data encryption.

- Physical unclonable function (PUF):

Provides a root of trust for cryptographic uses

- Field-programmable gate array (FPGA)

encrypt and authenticate configuration bitstreams, zeroization to protect critical information.

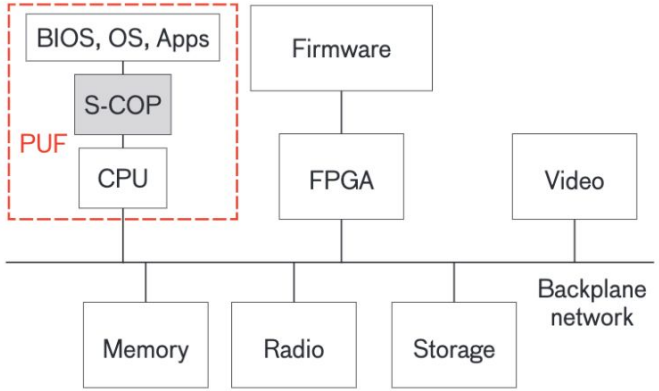


FIGURE 6. A security coprocessor (S-COP) is used along with a physical unclonable function (PUF) to secure a commercial off-the-shelf central processing unit (CPU).

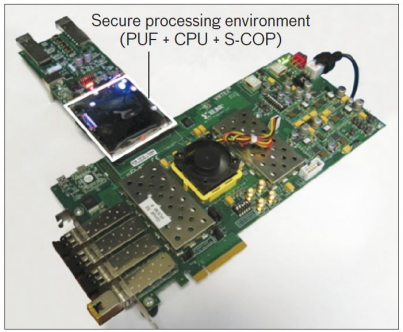
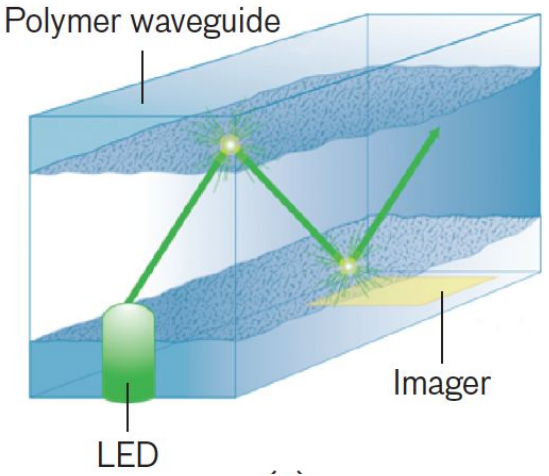


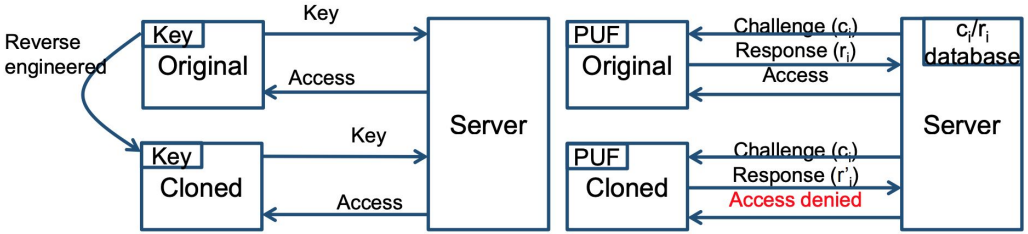
FIGURE 8. A secure processing environment integrates a central processing unit (CPU), a security coprocessor (S-COP), and a physical unclonable function (PUF).

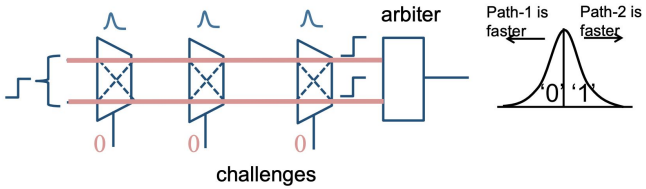
Cryptography

Cryptography is the foundation of the system's overall security. Physical unclonable function(PUF), unique digital identification for key derivation.

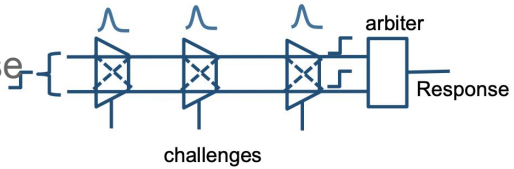
- Unique key generated per instance
- Implementable on a fully assembled printed circuit board



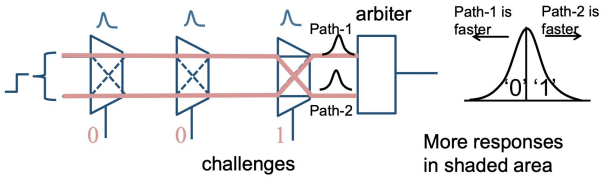




Fuzzy extractor: tolerance for noise



Process variation results in unique die-to-die response



https://past.date-conference.com/date16/system/files/private/date16/tutorials/DATE16-Tutorial-M09-Handouts.pdf

S-COP–based secure architecture

- Authenticate the BIOS, OS, and applications.
- Protect data

Security metrics:

Trustworthiness, Protection, Usability.

Evaluate a system four phases during operation:

Startup, Execution, Shutdown, Off

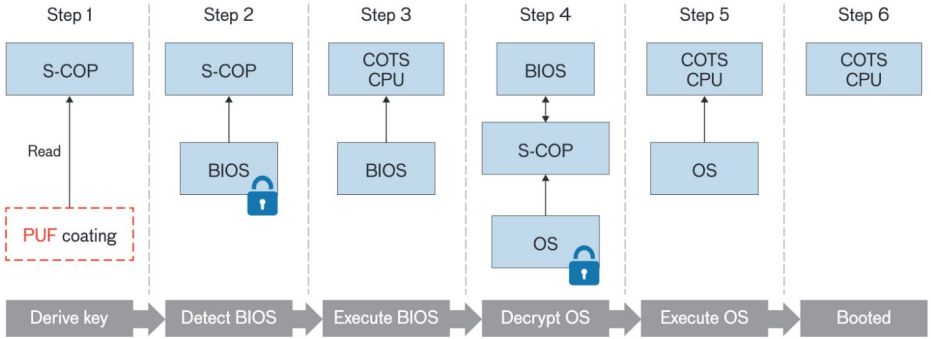


FIGURE 9. During the secure boot process, the central processing unit (CPU) is halted until the security coprocessor (S-COP) successfully verifies system integrity. Data that are protected by encryption are indicated by lock symbols.

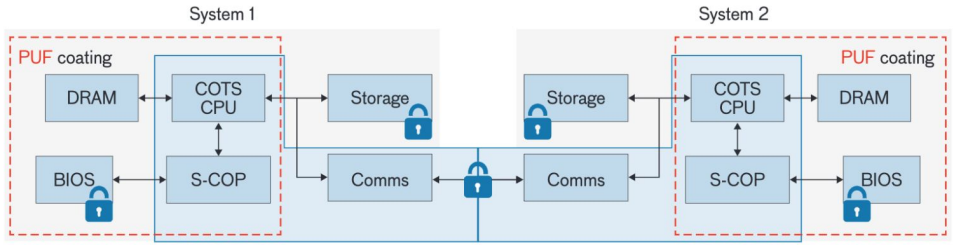


FIGURE 10. The security coprocessor (S-COP) enables data-at-rest and data-in-transit protection. Data that are protected by encryption are indicated by lock symbols.

Lincoln Open Cryptographic Key Management Architecture (LOCKMA) Software Library

LOCKMA

Automated and seamless key management protocol

- API abstraction for key management and crypto
- Minimize errors from implementation

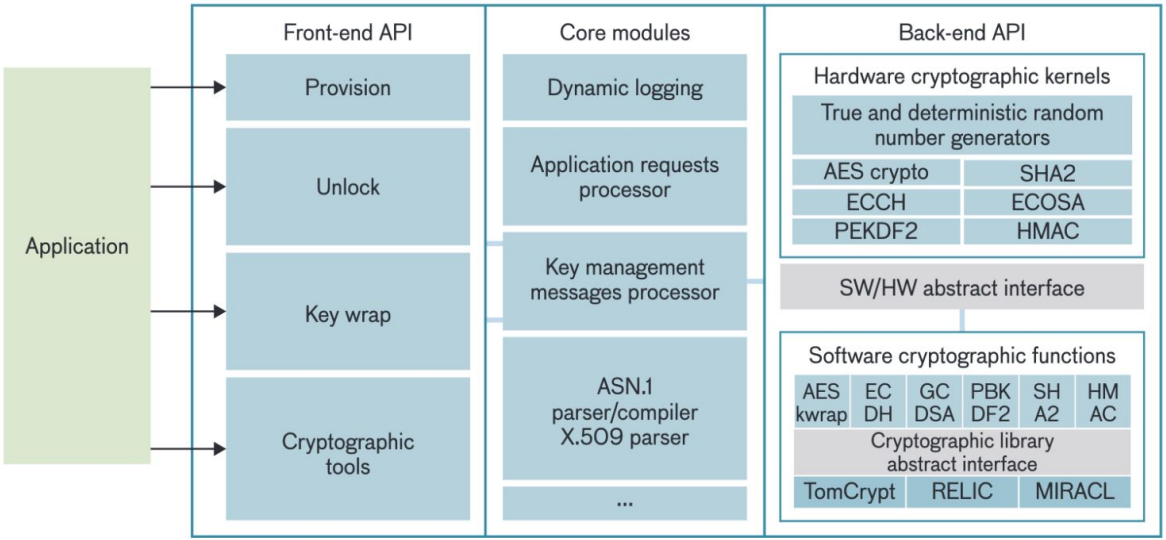


FIGURE 5. The LOCKMA software provides a front-end application programming interface (API) for high-level security functions that application developers can use directly. Complicated cryptographic algorithms are captured as core modules, which are hidden from application developers. The back-end API supports the use of low-level cryptographic kernels implemented in either hardware or software.

LOCKMA security framework

LOCKMA security manager (LSM) checks subsystem credentials against a config file to ensure that the configuration is authorized

 # Principals
A, B, C, D, ...

 # Constraints
A or B
A and D
...

Digital signature

 # Channels
Channel 1:
Pub: A
Sub: D, E
...

FIGURE 12. A security config file, an example of which is shown at left, is used to enforce payload authorization and secure communication channels.

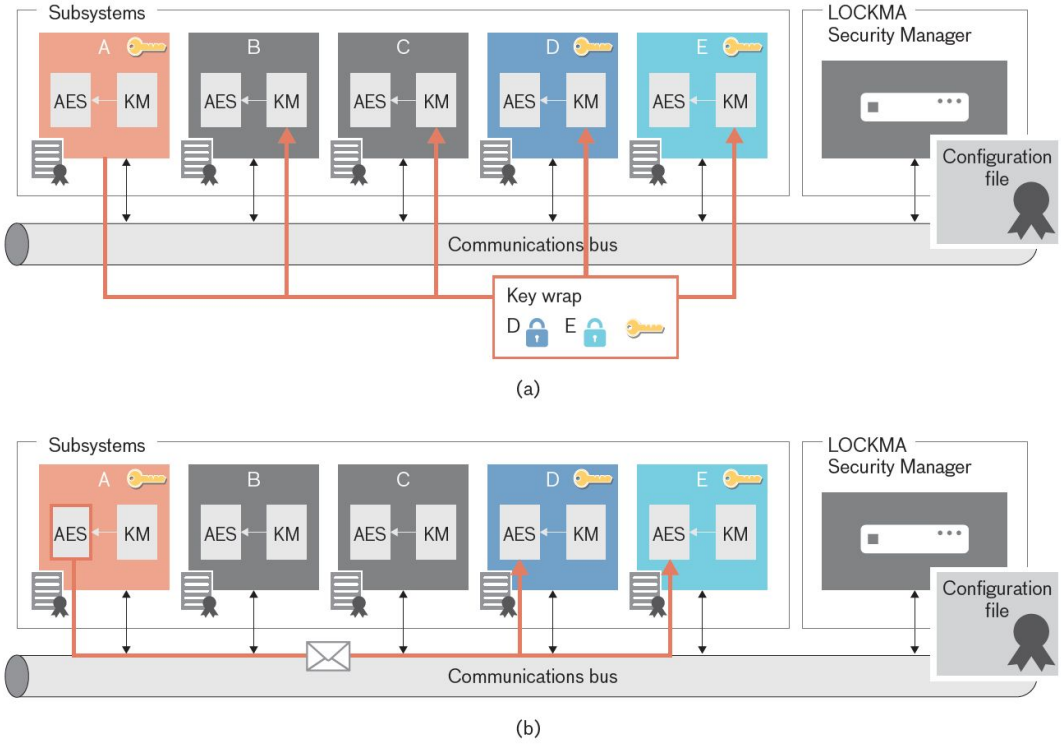


FIGURE 13. In a LOCKMA security framework, a publisher (e.g., subsystem A) sends a key wrap only accessible by intended subscribers (e.g., subsystems D and E) to retrieve a session key (a). The publisher and subscribers are then able to carry out encrypted communication (b). Each subsystem contains an Advanced Encryption Standard (AES) and a key management (KM) function.

Fail safe mechanisms?

- Hover
- Return to base
- Land
- Self-destruct

Questions

@bushidocodes Sean McBride Comprehension

1. Open and extensible ISAs (RISC-V) will benefit the development of coprocessors?
2. Self-destruct and reliability? Self-destruct means fragility?
3. The ability of resilience with limited power?

@reesealanj Reese Jones Critical

1. Does cryptography enable system availability from a security standpoint?

@searri Rick Sear Comprehension

1. Separation kernels is another name for microkernels?
2. PUF's cost, "fuzzy extraction" technique?

@s-hanna15 Sam Hanna Comprehension

1. The availability of the techniques?
2. The purpose of the decoupling of S-COP and CPU?

@zacharied Zach Day Critical

1. System software to be rewritten to utilize LOCKMA?
2. Is the PUF "fuzzy extraction" reliable?

Questions

@rachellkm Rachell Kim Comprehension

1. If S-COP is compromised will UAS still have the cryptographic operation?

@grahamschock Graham Schock Critical

1. What is the least secure part of a computer process?

@ericwendt Eric Wendt Critical

1. Memory storage is a necessary for UVS?
2. The remote control attack of UVS?

@anguyen0204 Andrew Nguyen Comprehension

1. "fuzzy extraction" in PUF?

@tuhinadasgupta Tuhina Dasgupta Comprehension

1. What are the applications of LOCKMA?

Critique

GPS related attacks are not addressed, no solution?