Anti-Tamper in Open Architecture Systems

Michael Vai, Kyle Ingols, Josh Kramer, Ford Ennis, Michael Geis, Ted Lyszczarz, Rob Cunningham

HPEC 2011

20 September 2011

1951–2011
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

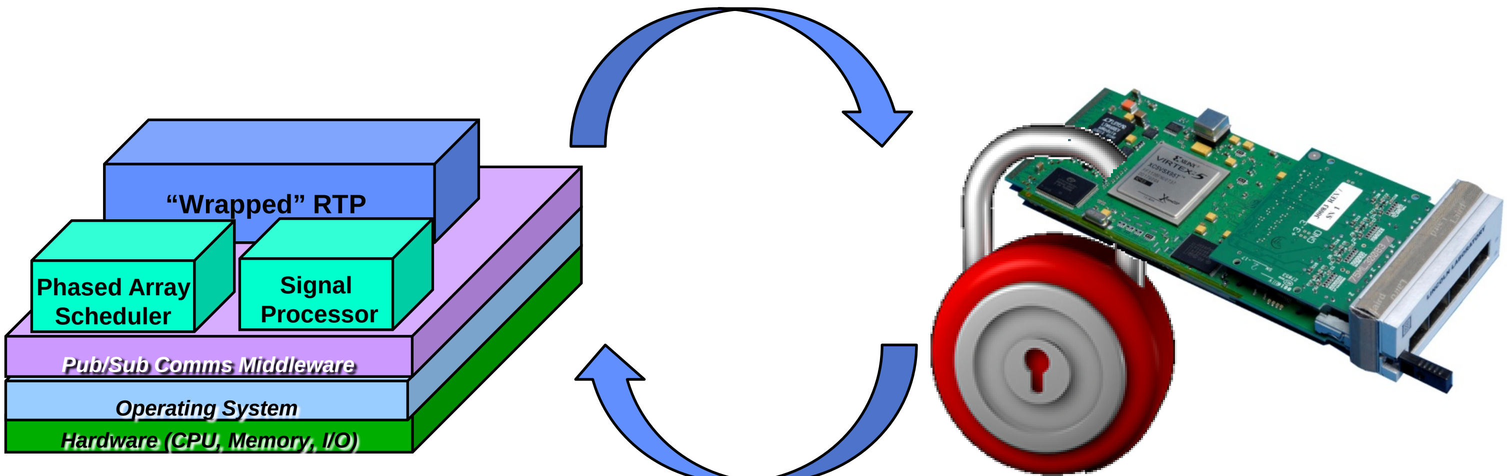
This work is sponsored by the Department of the Air Force under Air Force Contract FA8721-05-C-0002.
Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

Overview

- **Talk Objectives**
- **Background**
  - **Anti Tamper (AT)**
  - **Open Architecture System**
- **Open Architecture vs. AT**
- **Crucial Open AT Technologies**
- **Summary**

Talk Objectives

- **Discuss two key challenges in combining anti-tamper and open architecture systems**
  - **How can Anti-Tamper (AT) requirements be integrated into open-architecture systems and still maintain benefits of openness?**
  - **How can open-architectures be applied to AT itself to improve the state-of-the-art, foster competitive technology insertion, and promote re-use?**



Open-Architecture System **Anti Tamper**

Overview

- **Talk Objectives**
- **Background**
  - **Anti Tamper (AT)**
  - **Open Architecture System**
- **Open Architecture vs. AT**
- **Crucial Open AT Technologies**
- **Summary**

Anti-Tamper (AT)

Hainan Island incident

The damaged EP-3 on the ground on Hainan Island

eReader? Android Tablet?

- **Why do adversaries tamper systems?**
  - **Countermeasure development**
  - **Unauthorized technology transfer**
  - **Unauthorized modification to increase capabilities**
- **Anti-Tamper:**
  - **Technologies aimed at deterring and/or delaying unauthorized exploitation of critical information and technologies**
  - **Schemes range from simple "lock-it-up" to "deter-detect-react"**

http://en.wikipedia.org/wiki/Hainan_Island_incident
http://www.npr.org/2011/03/27/134897271/cheaper-than-a-tablet-rooting-your-e-reader

Attacks

For HPEC, a large percentage of CT/CPI is in software/firmware!

Adversary objective: Access/tamper protected code and data

Remote Attack

- Gained remote "login" to the system
  - Malware
  - Lost credentials
  - Trusted relationships
- Timing attack to discover secret keys

Local Attack

- Gained physical access
  - Captured or FMS
- Testbench characterization
- Side-channel attacks
  - Timing
  - Power, radiation
  - Acoustic

Intrusive Attack

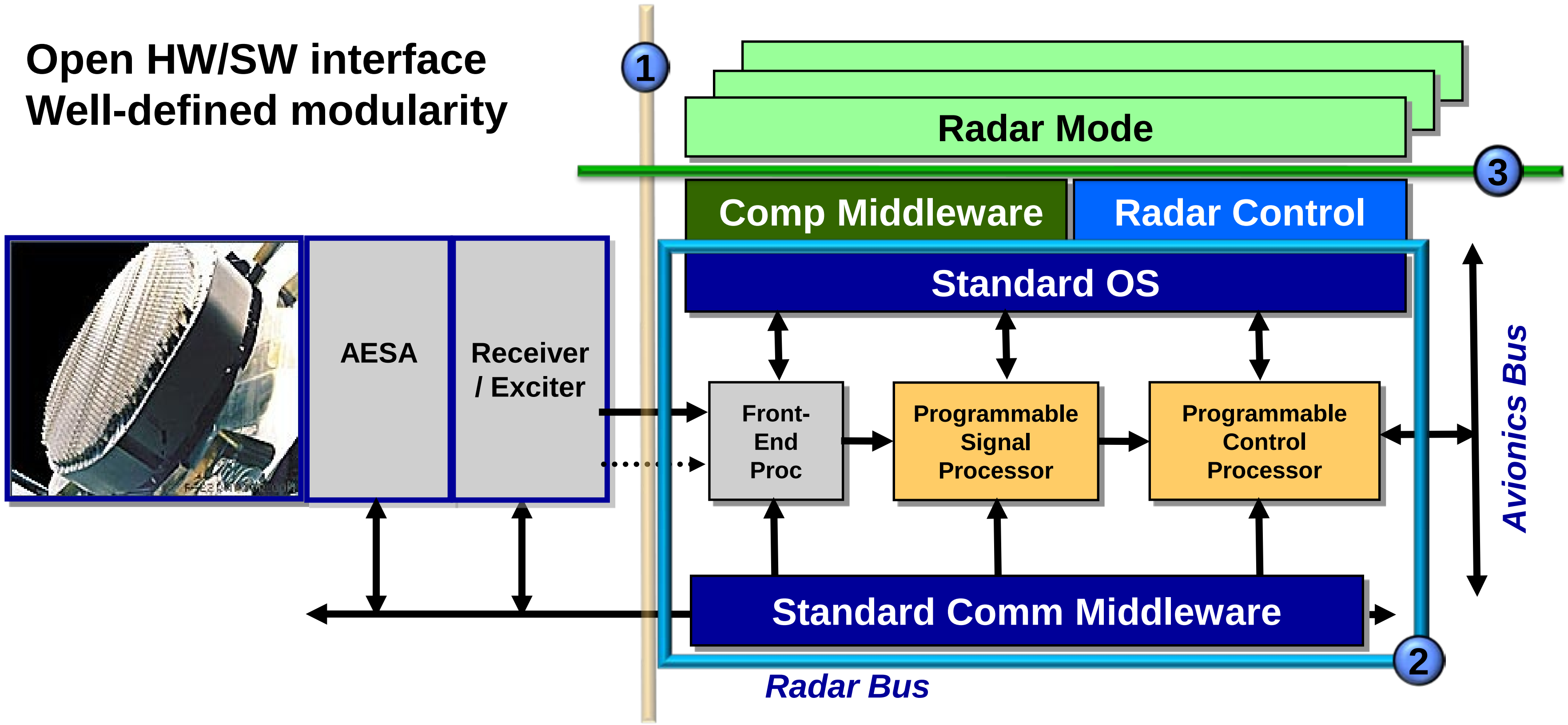
- Gained access to inside of the system
  - Signal probing
  - Fault analysis
  - Foreign HW/SW insertion
  - Explore memories and disks

Destructive Attack

- Gained chip level access
  - Depackaging, drilling, shaving, etc.
- Reverse engineering
  - ASICs, FPGAs

Open Architecture Systems

- Open HW/SW interface
- Well-defined modularity



Benefits:

1. Permit procurement of subsystems from independent sources
2. Enable computing hardware refresh without major software rewrite
3. Facilitate algorithm insertion ("modes") by 3rd parties.

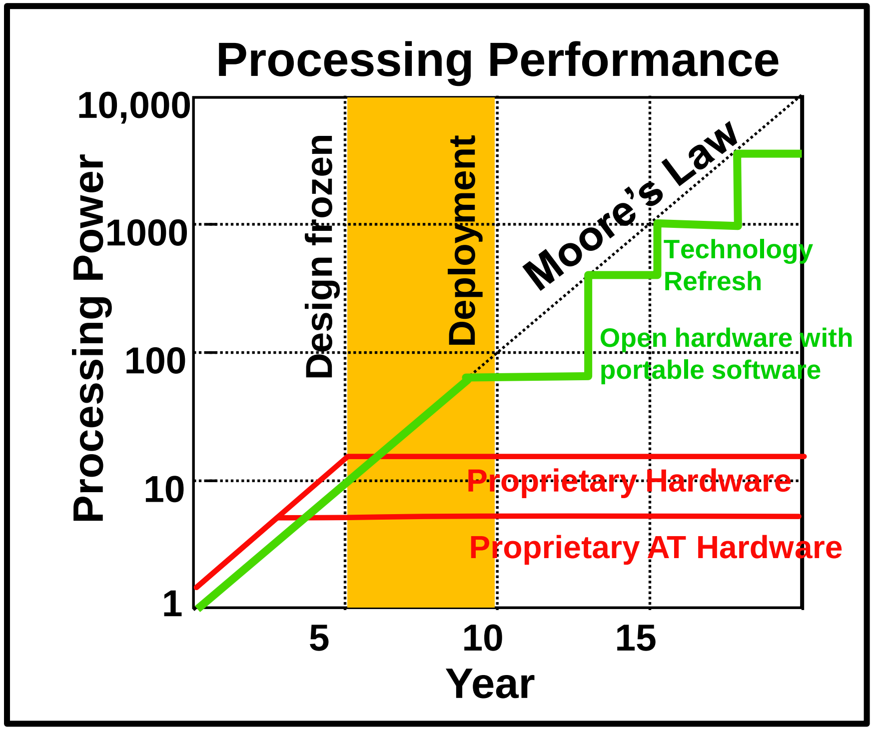
Overview

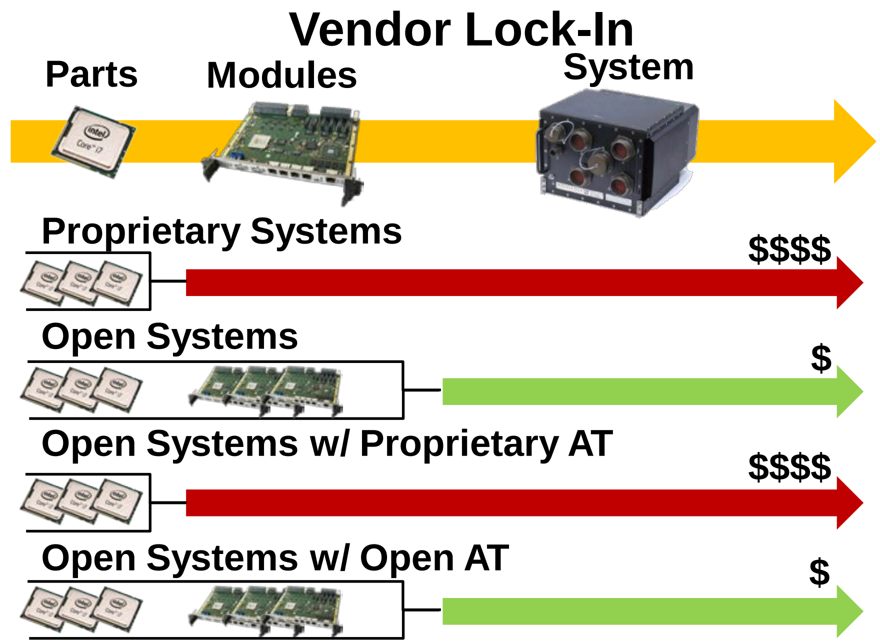
- **Talk Objectives**
- **Background**
  - **Anti Tamper (AT)**
  - **Open Architecture System**
- **Open Architecture vs. AT**
- **Crucial Open AT Technologies**
- **Summary**

Open Architecture vs. Anti Tamper

Open Architecture Desirable Features	AT Desirable Features	
Open standard interface: Predictable behavior	Deny unauthorized access and obfuscate responses	
Modularity: Self-contained, well-defined functional units	Prevent isolation and attack of individual units	
Refresh: Adoption of 3rd party hardware and software	Prohibit insertion of unauthorized hardware and software	
Extensibility & scalability: Enable new capabilities	Avoid non-essential points of entry for exploration	
Maintainability: Easy to diagnose and repair	Disallow poking and changes	

AT Implications on Open Systems





- AT requirement can force open systems back to being closed and proprietary
- Solution: Apply open AT technology decoupled from the system
  - Maintain competition and technology refresh
  - Reduce acquisition cost and time

Open AT Technologies

Open System Desirable Features	AT Desirable Features	Open AT Technologies
Open standard interface: Predictable behavior	Deny unauthorized access and obfuscate responses	Personalizable standard AT approaches
Modularity: Self-contained, well-defined functional units	Prevent isolation and attack of individual units	Units only operate in authenticated systems
Refresh: Adoption of 3rd party hardware and software	Prohibit insertion of unauthorized hardware and software	Authenticated hardware and software
Extensibility & scalability: Enable new capabilities	Avoid non-essential points of entry for exploration	Encryption of signals and data
Maintainability: Easy to diagnose and repair	Disallow poking and changes	Personalizable protective packaging and sensing

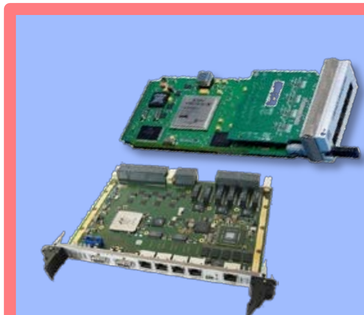
Vision of Open AT Technologies
Protect Lowest Replaceable Units and CPI

Open

Processing Components

Open

Lowest Replaceable Units (LRUs)



Protected

Personalized LRUs (Unique IDs)

Protected

Embedded CPI (Critical Program Information)

Openness: LRUs manufactured in compliance with published standards

- Decouples AT technology from processing components/units
- Develops personalizable LRUs
- Reuses LRUs in multiple systems

Tech. Competition and Refresh

AT: only operate with authenticated hardware, software, and firmware

- Protects at-rest and in-motion critical information with cryptography
- Authenticates software/firmware in verified LRUs

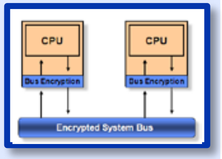
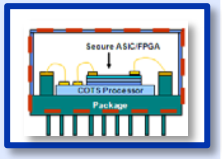
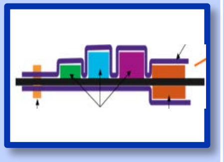
Confidence in System Operations

1951–2011
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Overview

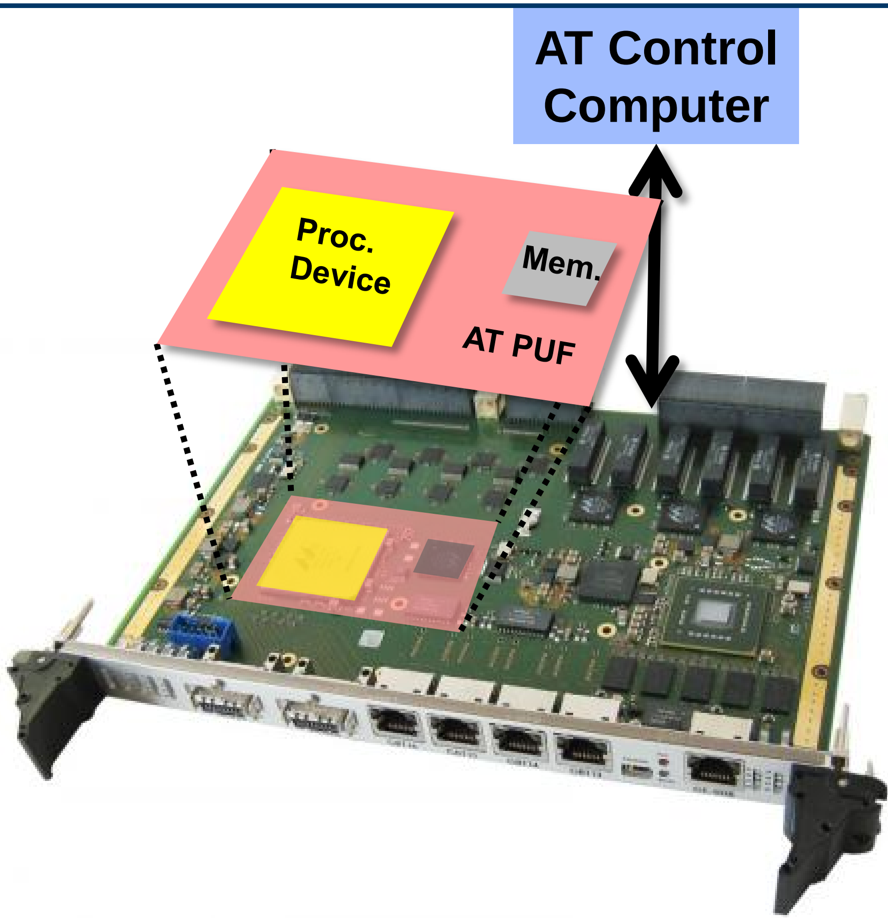
- **Talk Objectives**
- **Background**
  - **Anti Tamper (AT)**
  - **Open Architecture System**
- **Open Architecture vs. AT**
- **Crucial Open AT Technologies**
- **Summary**

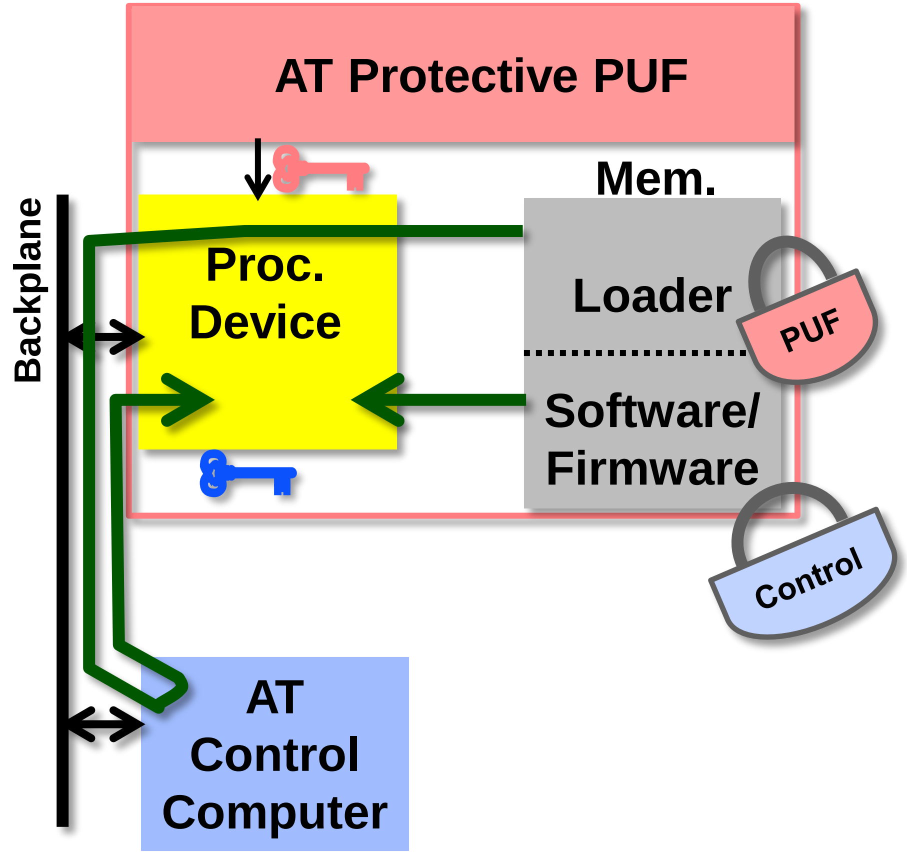
Crucial Open AT Technology Candidates

Technology		AT Functions			Assessment
		Prevent	Detect	React	
Unit Personalization		✓	✓	✓	• Allows HW/SW units to be authenticated • Can leverage standard cryptography schemes • Must standardize protocols and interfaces • Needs red teaming
Signal/Data Encryption		✓			• Protects CPI at rest or in motion • No unencrypted data ever travel in the clear • Can leverage standard encryption algorithms • Must standardize interfaces
Side-Channel Resistance		✓			• Protects secret keys from being extracted • Many protection schemes are proprietary • Need to evaluate their effectiveness • Room for innovation
Packaging & Sensing		✓	✓	✓	• Provides volume protection • Many inexpensive and small-size sensors • Needs effective integration approaches • Issues with standby power
Protective PUF* Coating		✓	✓	✓	• Provides protection and unique personalization • Several commercial products • Needs effective integration approaches

*PUF: Physical Unclonable Function

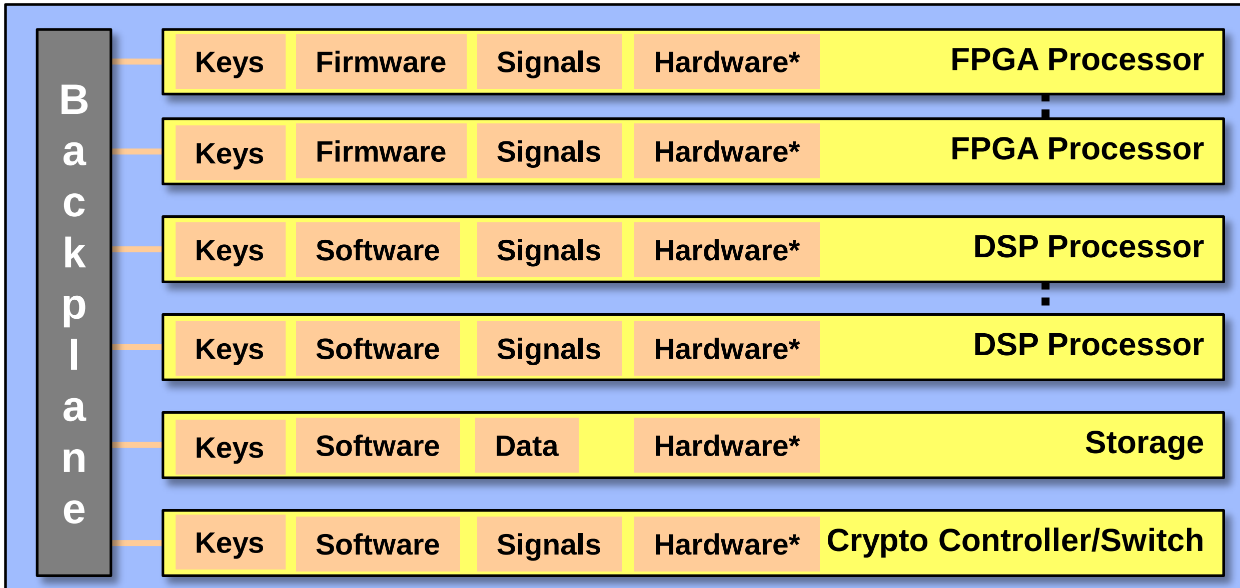
Hardware and Software Authentication





- AT PUF (physical unclonable function) is the "key" of authentication
  - PUF provides a unique ID for hardware personalization
  - AT control computer verifies the authenticity of the HW/SW assembly
- Damaged PUF prevents loading software/firmware

AT Open-Architecture Signal Processor

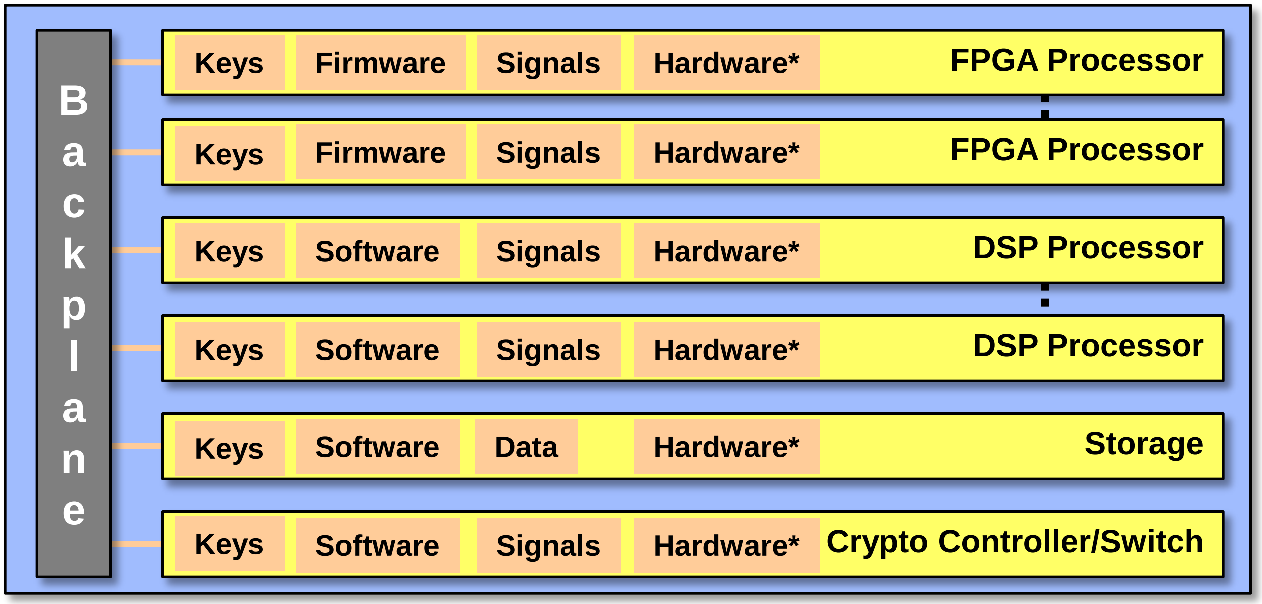


* Hardware substitution

- **Critical Technology (CT) / Critical Program Information (CPI)**
  - **Timing protocol, multi-platform coordination**
  - **Advanced signal processing algorithm**
    - **Spectral analysis and discrimination**
    - **Frequencies, waveforms, etc.**

Essential to protect CT/CPI from being tampered and exploited in all different phases of its life cycle

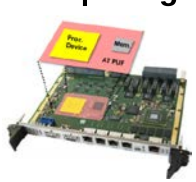
Open AT Capabilities



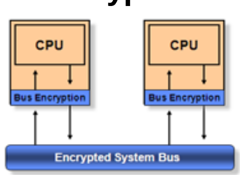
Open AT Capabilities
Prevents unauthorized software and firmware access
Disallows hardware/software/firmware replacement
Defends against reverse engineering
Shields signals from probing
Protects storage from exploration
Guards against secret key extraction
Minimum performance impact
Ready-to-use architecture

* Hardware substitution

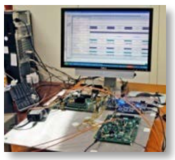
Authenticated Computing



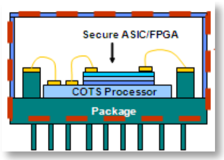
Signal/Data Encryption



Side-Channel Resistance



Packaging & Sensing



PUF Coating

Crucial Open AT Technologies

1951–2011
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Open AT Capabilities

Backplane

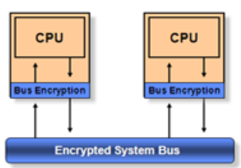
Keys	Firmware	Signals	Hardware*	FPGA Processor
Keys	Firmware	Signals	Hardware*	FPGA Processor
Keys	Software	Signals	Hardware*	DSP Processor
Keys	Software	Signals	Hardware*	DSP Processor
Keys	Software	Data	Hardware*	Storage
Keys	Software	Signals	Hardware*	Crypto Controller/Switch

Open AT Capabilities
Prevents unauthorized software and firmware access
Disallows hardware/software/firmware replacement
Defends against reverse engineering
Shields signals from probing
Protects storage from exploration
Guards against secret key extraction
Minimum performance impact
Ready-to-use architecture

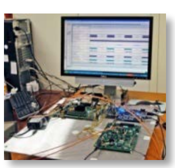
* Hardware substitution

Authenticated Computing

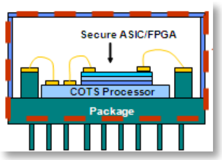
Signal/Data Encryption



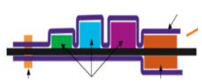
Side-Channel Resistance



Packaging & Sensing



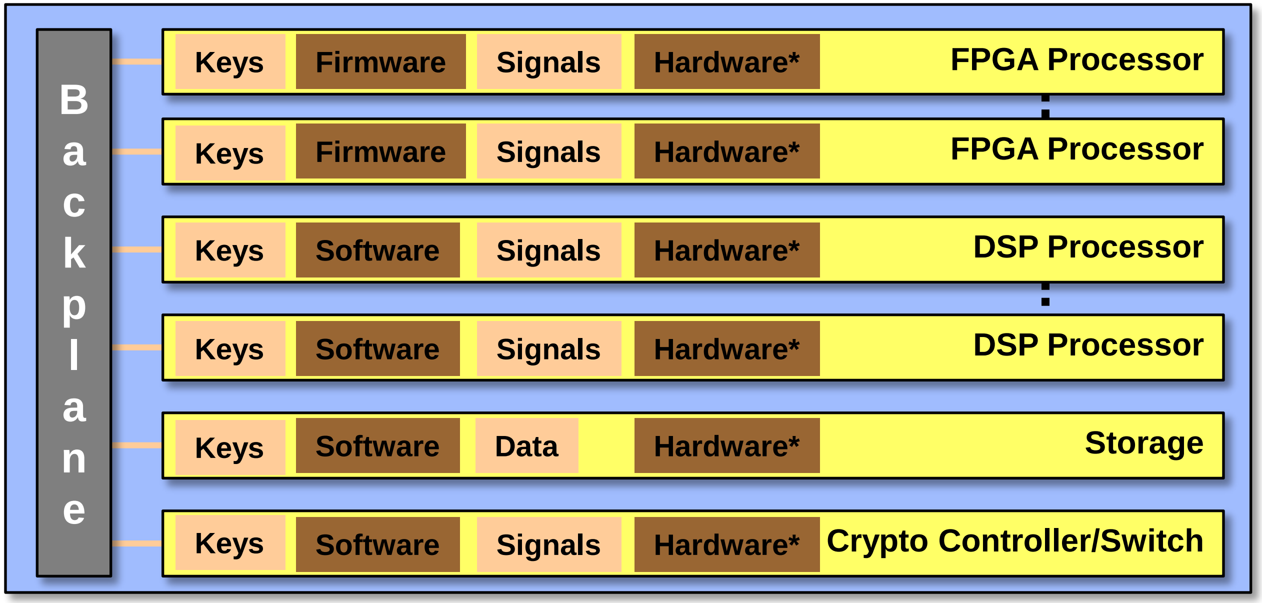
PUF* Coating



Crucial Open AT Technologies

1951–2011
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Open AT Capabilities

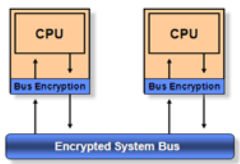


Open AT Capabilities
Prevents unauthorized software and firmware access
Disallows hardware/software/firmware replacement
Defends against reverse engineering
Shields signals from probing
Protects storage from exploration
Guards against secret key extraction
Minimum performance impact
Ready-to-use architecture

* Hardware substitution

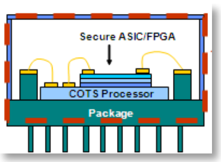
Authenticated Computing

Signal/Data Encryption

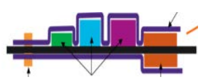


Side-Channel Resistance

Packaging & Sensing



PUF* Coating



Crucial Open AT Technologies

Open AT Capabilities

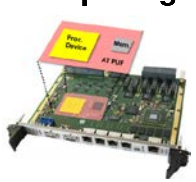
Backplane

Keys	Firmware	Signals	Hardware*	FPGA Processor
Keys	Firmware	Signals	Hardware*	FPGA Processor
Keys	Software	Signals	Hardware*	DSP Processor
Keys	Software	Signals	Hardware*	DSP Processor
Keys	Software	Data	Hardware*	Storage
Keys	Software	Signals	Hardware*	Crypto Controller/Switch

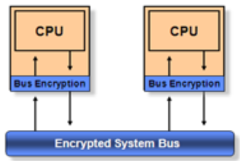
Open AT Capabilities
Prevents unauthorized software and firmware access
Disallows hardware/software/firmware replacement
Defends against reverse engineering
Shields signals from probing
Protects storage from exploration
Guards against secret key extraction
Minimum performance impact
Ready-to-use architecture

* Hardware substitution

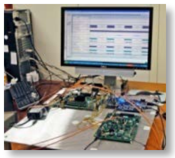
Authenticated Computing



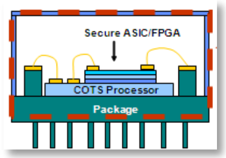
Signal/Data Encryption



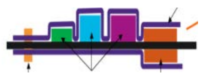
Side-Channel Resistance



Packaging & Sensing



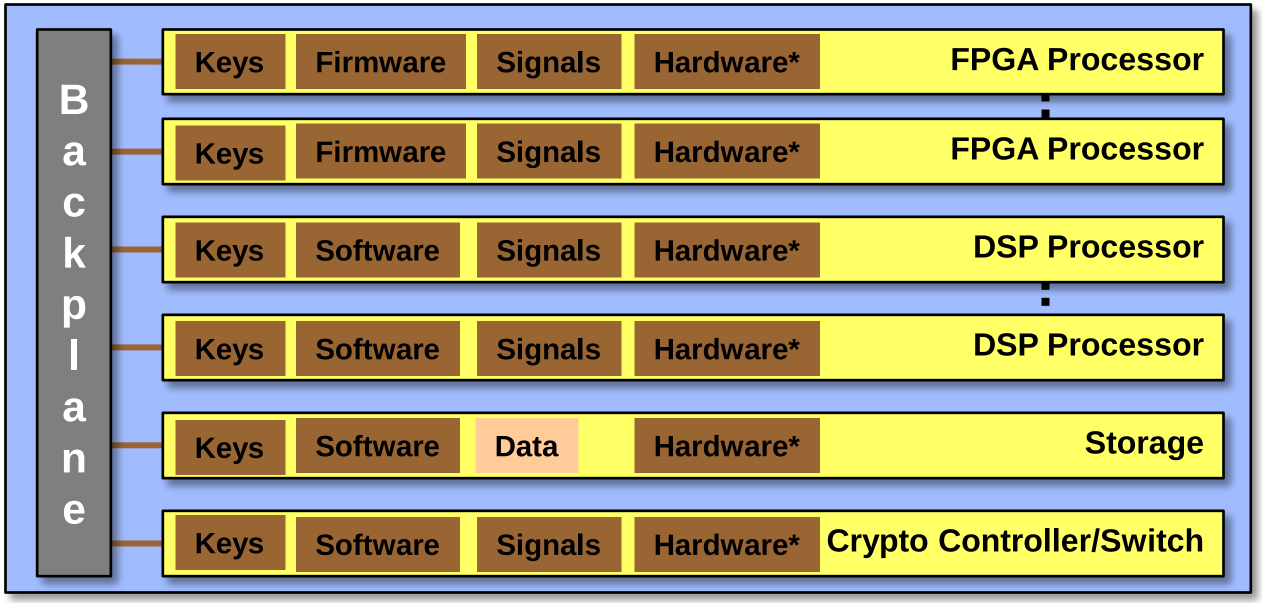
PUF* Coating



Crucial Open AT Technologies

1951–2011
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Open AT Capabilities

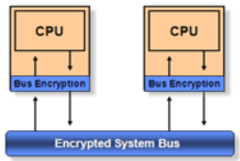


Open AT Capabilities
Prevents unauthorized software and firmware access
Disallows hardware/software/firmware replacement
Defends against reverse engineering
Shields signals from probing
Protects storage from exploration
Guards against secret key extraction
Minimum performance impact
Ready-to-use architecture

* Hardware substitution

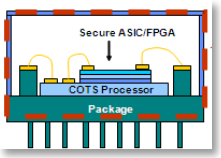
Authenticated Computing

Signal/Data Encryption

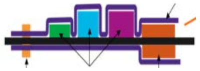


Side-Channel Resistance

Packaging & Sensing

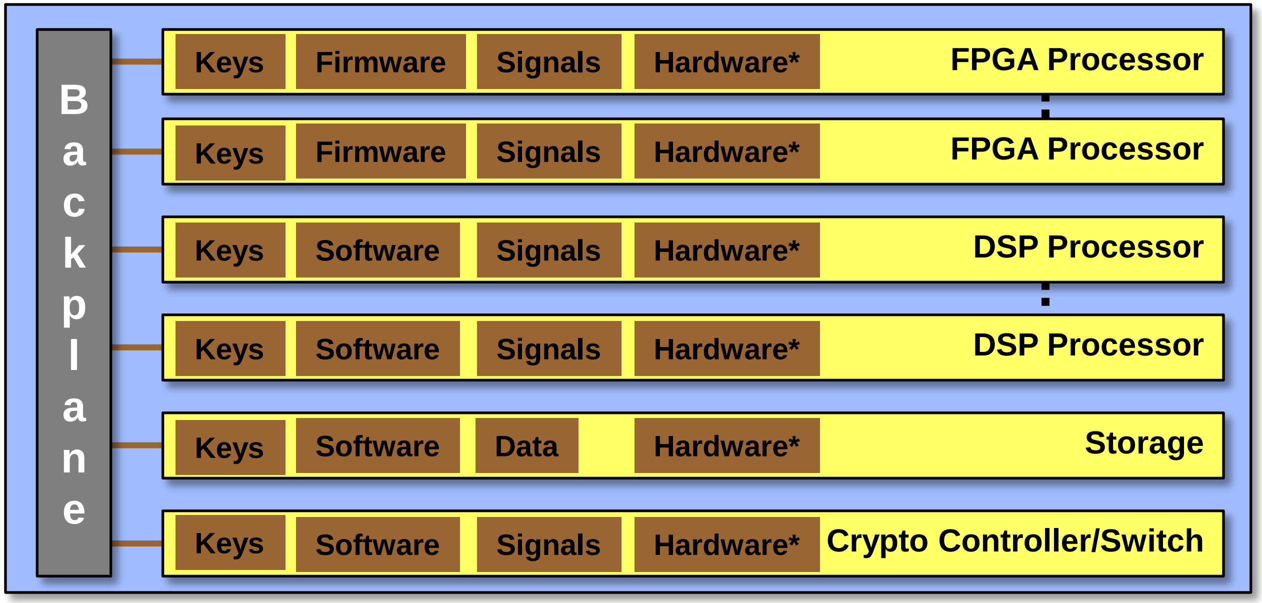


PUF* Coating



Crucial Open AT Technologies

Open AT Capabilities

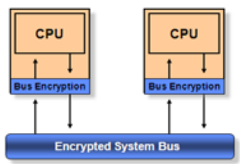


Open AT Capabilities
Prevents unauthorized software and firmware access
Disallows hardware/software/firmware replacement
Defends against reverse engineering
Shields signals from probing
Protects storage from exploration
Guards against secret key extraction
Minimum performance impact
Ready-to-use architecture

* Hardware substitution

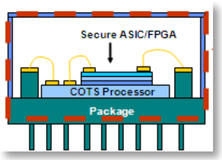
Authenticated Computing

Signal/Data Encryption

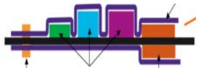


Side-Channel Resistance

Packaging & Sensing



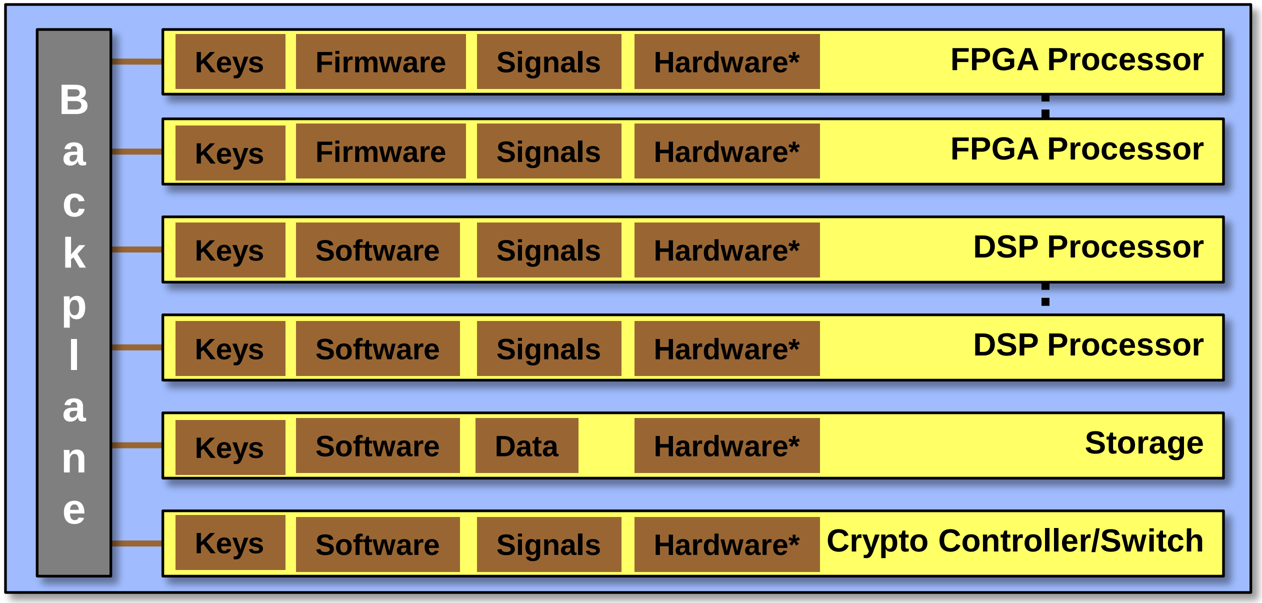
PUF* Coating



Crucial Open AT Technologies

1951–2011
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Open AT Capabilities

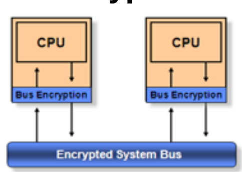


Open AT Capabilities
Prevents unauthorized software and firmware access
Disallows hardware/software/firmware replacement
Defends against reverse engineering
Shields signals from probing
Protects storage from exploration
Guards against secret key extraction
Minimum performance impact
Ready-to-use architecture

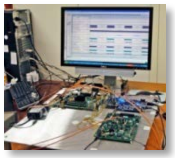
* Hardware substitution

Authenticated Computing

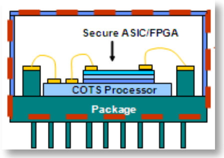
Signal/Data Encryption



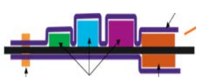
Side-Channel Resistance



Packaging & Sensing



PUF* Coating



Crucial Open AT Technologies

Open AT Capabilities

Backplane

FPGA Processor	Keys	Firmware	Signals	Hardware*
FPGA Processor	Keys	Firmware	Signals	Hardware*
DSP Processor	Keys	Software	Signals	Hardware*
DSP Processor	Keys	Software	Signals	Hardware*
Storage	Keys	Software	Data	Hardware*
Crypto Controller/Switch	Keys	Software	Signals	Hardware*

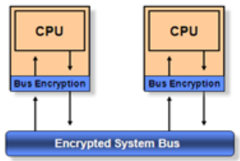
Open AT Capabilities

- Prevents unauthorized software and firmware access
- Disallows hardware/software/firmware replacement
- Defends against reverse engineering
- Shields signals from probing
- Protects storage from exploration
- Guards against secret key extraction
- Minimum performance impact
- Ready-to-use architecture

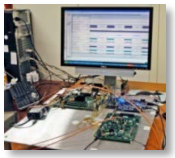
* Hardware substitution

Authenticated Computing

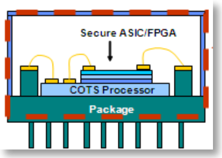
Signal/Data Encryption



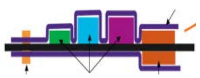
Side-Channel Resistance



Packaging & Sensing

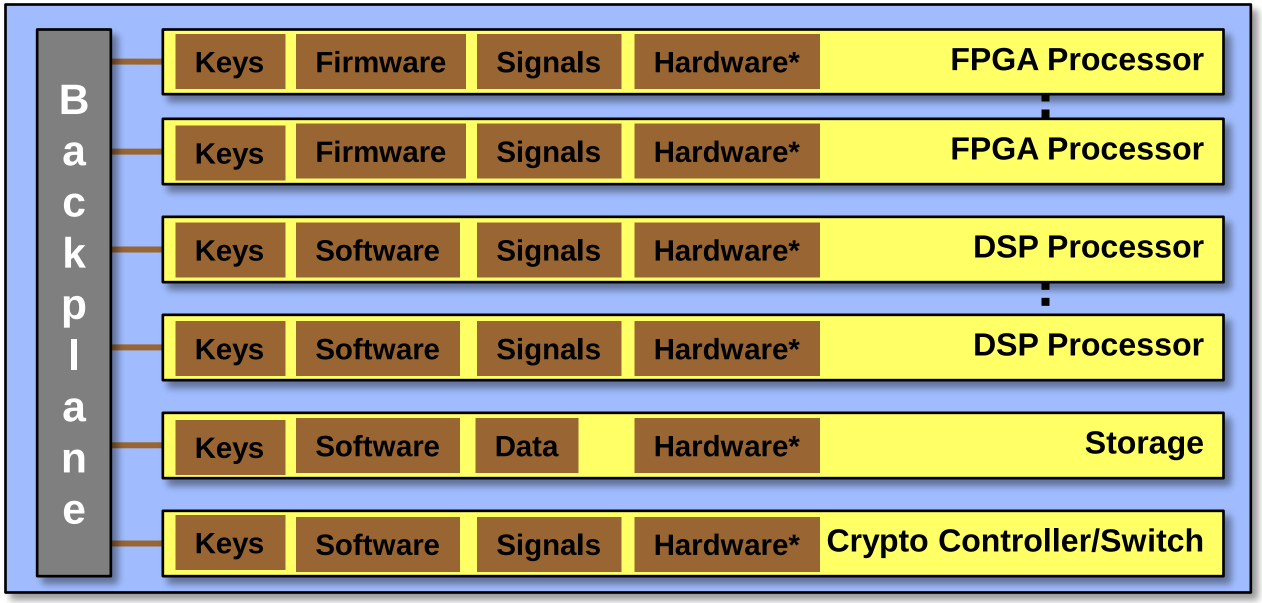


PUF* Coating



Crucial Open AT Technologies

Open AT Capabilities

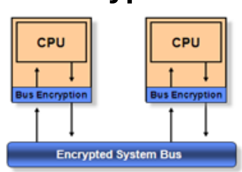


Open AT Capabilities
Prevents unauthorized software and firmware access
Disallows hardware/software/firmware replacement
Defends against reverse engineering
Shields signals from probing
Protects storage from exploration
Guards against secret key extraction
Minimum performance impact
Ready-to-use architecture

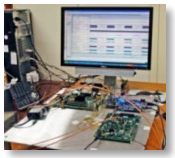
* Hardware substitution

Authenticated Computing

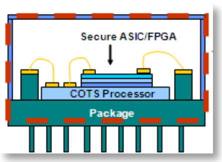
Signal/Data Encryption



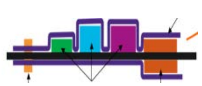
Side-Channel Resistance



Packaging & Sensing



PUF* Coating



Crucial Open AT Technologies

Summary

Anti-Tamper in Open Architecture Systems

- **Two key challenges**
  - How can Anti-Tamper (AT) requirements be integrated into open-architecture systems and still maintain benefits of openness?
  - How can open-architectures be applied to AT itself to improve the state-of-the-art, foster competitive technology insertion, and promote re-use?
- **A few research directions**
  - Assess program-specific needs for AT open systems
  - Research/identify/evaluate crucial AT technologies for open systems
  - Establish AT technology risk reduction roadmap and strategy for AT open systems