Freescale Technology Forum

Design Innovation.

November, 2008

System Security - Protecting Systems from Hacking and Cloning

PZ115

Rudan Bettelheim

Product Manager

freescale™ semiconductor

Agenda

- Introduction – Why Security?
- What Requires Protection
- Cryptography – Protecting Data
- Secure Systems – Preventing Hacking and Cloning
- Q & A

freescale™ semiconductor

Introduction - Why Security?

freescale™ semiconductor

Industrial Market Evolution

Last Decade

- Increasingly sophisticated electronic control systems
- Extensive spread of networking of industrial control systems
- Remote and mobile equipment becomes part of the control network
- Increasing concerns over equipment cloning

Future expectations

- The global industrial market for MPU/MCU/DSP is projected to grow from $2.8B in 2005 to $4.6B in 2011 (source: Semicast)
- Increasing use of Cryptography to protect communications
- Growing need and implementation of Secure Embedded Control Systems, facilitated by an ecosystem of hardware, software, and tools
- Emerging security standards such as EMV/Visa PCI
- A high profile event could lead to a sudden and strong market and regulatory requirement for system protection across many industrial applications
  - **Suppliers that are ready to meet system security requirements are likely to gain significant market advantage and share**

freescale™ semiconductor

Example of Infrastructure Vulnerability

updated 11:06 p.m. EDT, Wed September 26, 2007

Sources: Staged cyber attack reveals vulnerability in power grid

WASHINGTON (CNN) -- Researchers who launched an experimental cyber attack caused a generator to self-destruct, alarming the federal government and electrical industry about what might happen if such an attack were carried out on a larger scale, CNN has learned.

Sources familiar with the experiment said the same attack scenario could be used against huge generators that produce the country's electric power.

Some experts fear bigger, coordinated attacks could cause widespread damage to electric infrastructure that could take months to fix.

CNN has honored a request from the Department of Homeland Security not to divulge certain details about the experiment, dubbed "Aurora," and conducted in March at the Department of Energy's Idaho labIn a previously classified video of the test CNN obtained, the generator shakes and smokes, and then stops.

DHS acknowledged the experiment involved controlled hacking into a replica of a power plant's control system. Sources familiar with the test said researchers changed the operating cycle of the generator, sending it out of control.

Watch the generator shake and start to smoke

The White House was briefed on the experiment, and DHS officials said they have since been working with the electric industry to devise a way to thwart such an attack.

"I can't say it [the vulnerability] has been eliminated. But I can say a lot of risk has been taken off the table," said Robert Jamison, acting undersecretary of DHS's National Protection and Programs Directorate.

Government sources said changes are being made to both computer software and physical hardware to protect power generating equipment. And the Nuclear Regulatory Commission said it is conducting inspections to ensure all nuclear plants have made the fix.

Industry experts also said the experiment shows large electric systems are vulnerable in ways not previously demonstrated.

http://www.youtube.com/watch?v=fJyWngDco3g

freescale semiconductor

Infected Photo Frame

Best Buy confirms it sold virus-infected Insignia photo frames, no recall in the works

Posted Jan 24th 2008 9:46AM by Paul Miller
Filed under: Household

As we noted a week back, Best Buy's house-brand Insignia photo frames are indeed virus-infected, but now it appears Best Buy is doing something about it. Unfortunately, info is still slim at the moment from company lips. Best Buy says it's "connecting with our customers who may have been impacted," and has pulled remaining inventory from the shelves, but there are no plans for a recall of the infected NS-DPF10A, and Best Buy won't specify what specific type of malware we're dealing with. Best Buy seems to think that anti-virus software should have no problem dealing with the old-ish trojan in the frames, and recommends customers plug the frame into a PC and run some current anti-virus software to eradicate the malware. Macs are unaffected, and Apple could be seen on the playground making smarmy remarks about the incident to anyone who'd listen.

freescale semiconductor ™

Transportation System Security

Hardware: 14-Year-Old Turns Tram System Into Personal Train Set

Posted by ScuttleMonkey on Friday January 11, @02:37PM
from the **no-volume-control-on-this-tv** dept.

F-3582 writes

> "By modifying a TV remote a 14-year-old boy from Lodz, Poland, managed to gain control over the junctions of the tracks. According to The Register the boy had 'trespassed in tram depots to gather information needed to build the device. [...] Transport command and control systems are commonly designed by engineers with little exposure or knowledge about security using commodity electronics and a little native wit.' Four trams derailed in the process injuring a number of passengers. The boy is now looking at 'charges at a special juvenile court of endangering public safety.'"

▶ hardhack, transportation, awesomeresumeitem, ratatouille, pwnt *(tagging beta)*

freescale semiconductor

Phlashing

Hardware: New 'Phlashing' Attack Sabotages Hardware

Posted by timothy on Tuesday May 20, @09:29AM
from the **not-so-nice** dept.

yahoi writes

> "A new type of denial-of-service attack, called permanent denial-of-service (PDOS), damages a system so badly that it requires replacement or reinstallation of hardware. A researcher has discovered how to abuse firmware update mechanisms with what he calls 'phlashing' — a type of remote PDOS attack."

▶ hardware, it, security, bricking *(tagging beta)*

Read More... | hardware.slashdot.org 160 comments

freescale™ semiconductor

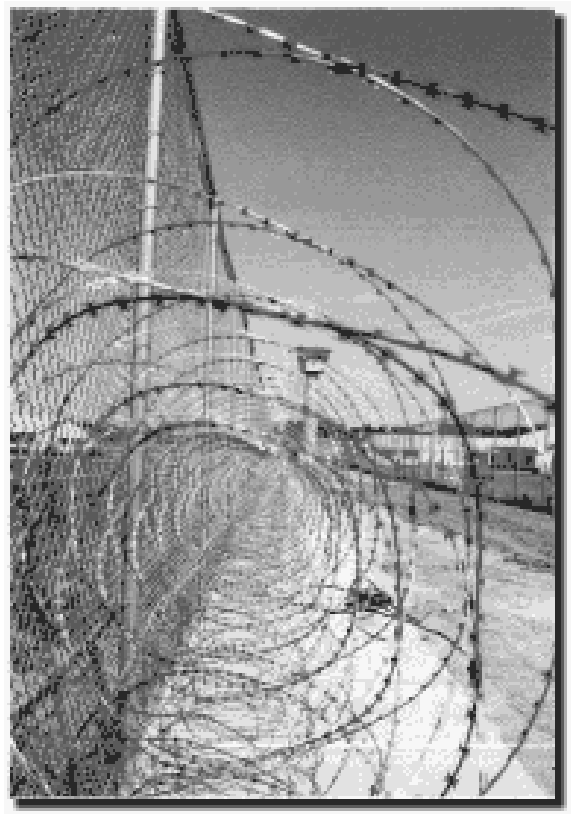
What Requires Protection?

freescale™ semiconductor

How Much Security?

When protecting a system you must consider:

- What are you trying to protect?
- What types of attack do you need to protect against?
- What are the likely attack points, and methods?
- How much security do you require?
  - How much are you willing to pay?
- How will security impact the underlying system?
- How will you upgrade/maintain the system and security over time?



freescale™ semiconductor

Types of Attacks

Electrical

- Over/Under voltage
- Power analysis
- Frequency analysis
- Electrostatic discharge
- Circuit probing

Software

- Spy software insertion
- Flow analysis
- Trojan horse
- Virus

Physical

- Temperature variation (into extremes)
- Temperature analysis
- De-processing
- System theft
- Partial destruction
- Hardware addition/substitution

freescale™ semiconductor

Classic Security Requirements:

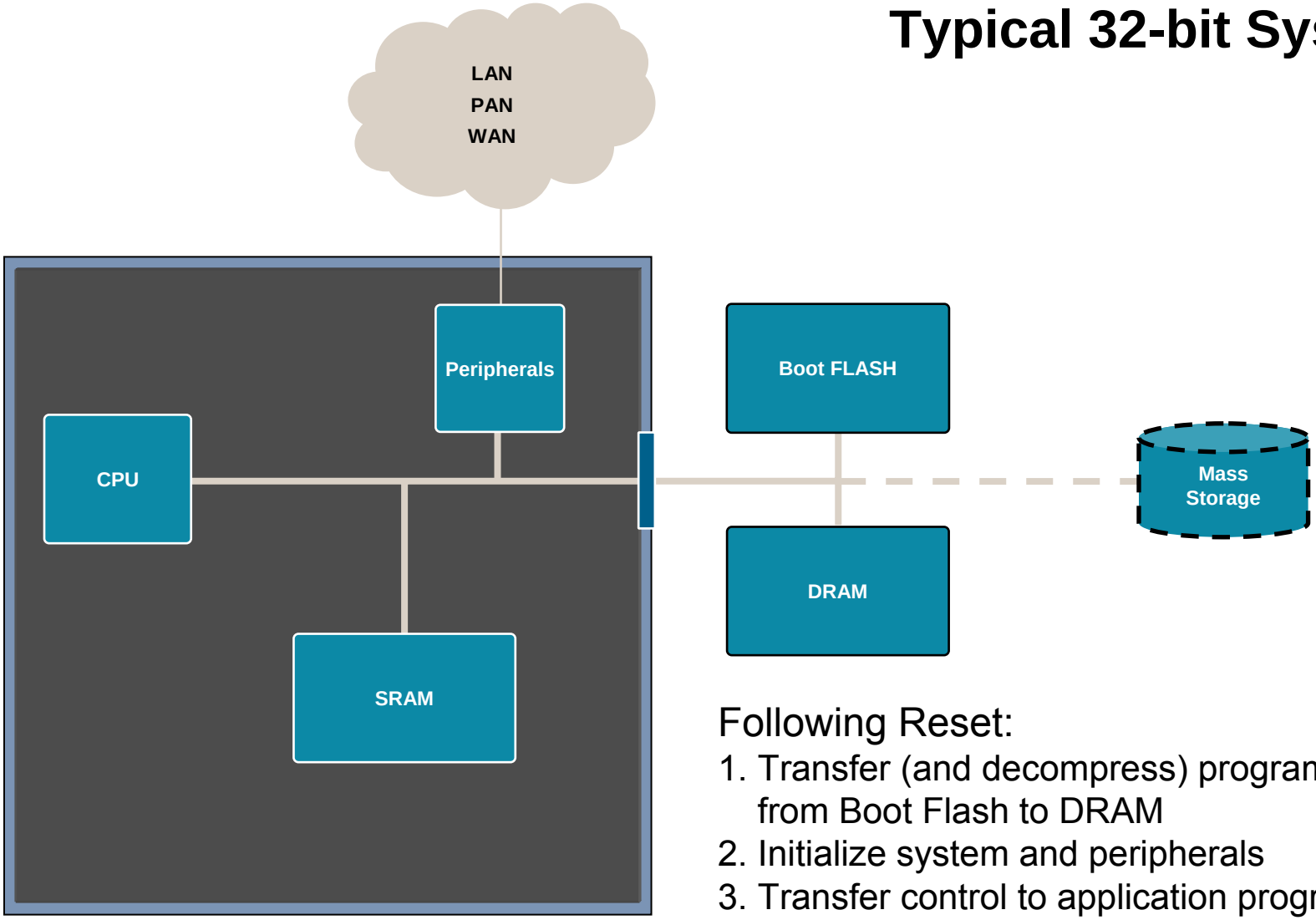
- **Confidentiality** - prevents eavesdropping
- **Authentication** - prevents impersonation
- **Data Integrity** - prevents tampering
- **Non-repudiation** - prevents denial
- **Trusted Processing** - enables trusted platform for authorized access to program and data
- **IP Protection** - prevent software/IP theft

Security System Requirements

Industrial systems may have a wide range of security requirements:

- Secure communications key storage
  - To secure communications in a control system
  - For remote equipment authentication
- Program code authentication
  - To prevent unauthorized code from being executed
  - To prevent use of unlicensed software
- Program code protection
  - To prevent code from being copied and used on clone equipment
  - To prevent code tapering
- Data protection
  - To protect system or user data
- Reduce cost of physical system protection

Typical 32-bit System



Following Reset:

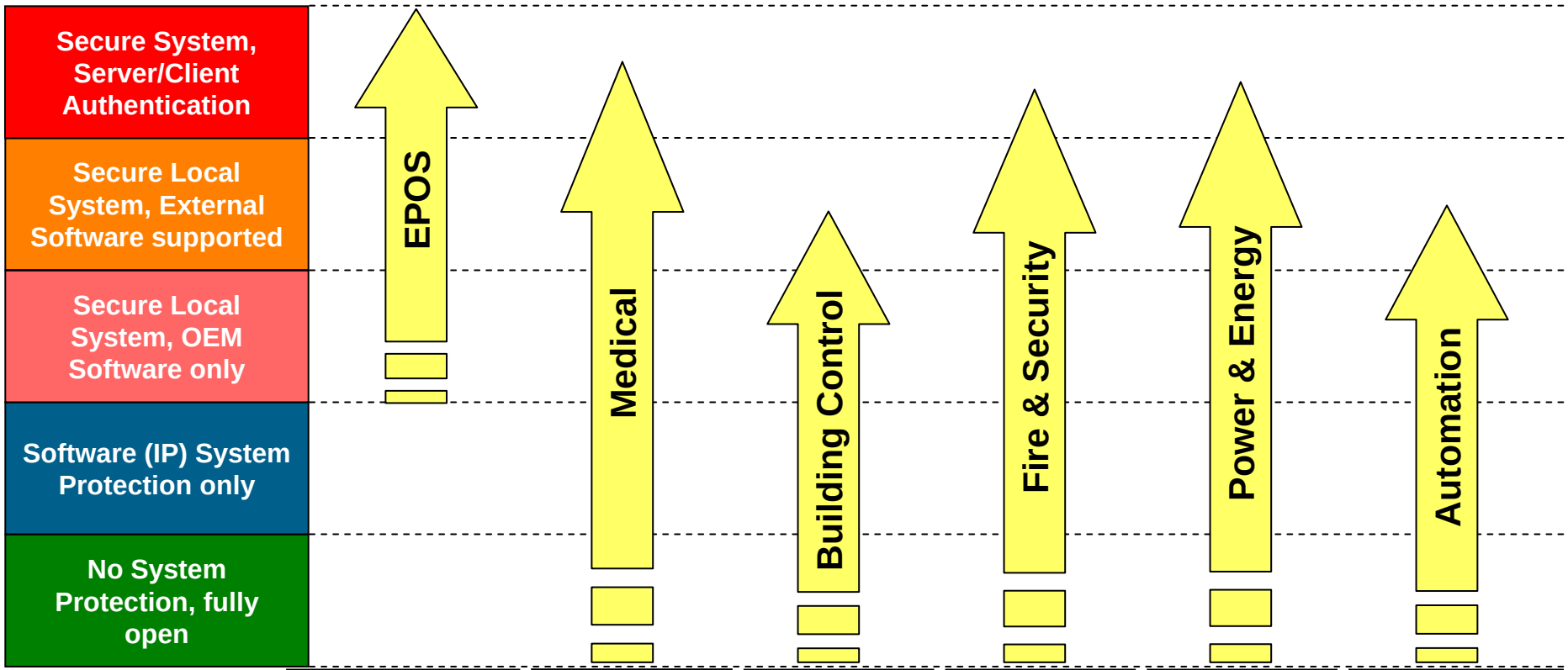
1. Transfer (and decompress) program code from Boot Flash to DRAM
2. Initialize system and peripherals
3. Transfer control to application program

freescale semiconductor

Application Security Levels

Secure System, Server/Client Authentication	Limits access to core system resources to OEM supplied and authorized software and data, and this is periodically authenticated with a secure server. Restricted execution of additional software without authorization is allowed.
Secure Local System, External Software supported	Limits access to core system resources to OEM supplied and authorized software and data, but restricted execution of additional software without authorization is allowed.
Secure Local System, OEM Software only	Ensures that only OEM supplied and authorized software and data can be used on the system, no other software can be executed.
Software (IP) System Protection only	Protection for system software and data IP, prevents software and data from being copied only
No System Protection, fully open	No system protection

Application Security Requirements Trends



Comments:

EPOS	Medical	Building Control	Fire & Security	Power & Energy	Automation
• Currently using mostly "physical" security • Electronic security will reduce system cost • Electronic security is essential to enable next generation features (user specific functions)	• Currently using no security • Will require security for patient privacy protection and to prevent tampering	• Currently using no security • Will require security to prevent tampering	• Currently using no security • Will require security to prevent tampering	• Currently using Security Bit, or no security • Will require security to prevent tampering	• Currently using or no security, or just firewalls • Will require security to prevent tampering for systems not sufficiently protected by firewalls

freescale™ semiconductor

How are Systems Protected Today?

Physical security:

- Secure packaging
- Secure packaging with tamper detect (i.e. pressure monitoring)
- Secure packaging with tamper detect and destruction (i.e. dynamite)
- Obscured part numbers
- Hidden layers
- Protected location

Electronic Security:

- **Security bit, to protect on-chip non-volatile memory (e.g. Flash), on MCUs**
  - Prevent external access to on-chip resources:
    - Locks device into Single Chip mode (disables external parallel bus)
    - Disables Background Debug Mode
    - Disables Test Mode
    - Disables JTAG
    - Disables any (serial) “Bootstrap” functions
  - Memory array bulk erase turns security bit off
- **Secure System (e.g. PISA)**
  - Code signing to prevent software tampering
  - Assurance for stored IP
  - Data stored encrypted in external memory
  - Data decrypted and stored in on-chip private memory at runtime
    - How do you protect software IP?
- **Proprietary (CPU) Design**
- **Silicon Obfuscation (e.g. obscuring metal layer)**
- **On-Chip Encryption Acceleration**
  - How do you protect the key?

freescale™ semiconductor

Cryptography – Protecting Data

freescale™ semiconductor

Cryptography

Symmetric Key Cryptography:

- Same key used to encrypt and decrypt
- Very fast
  - Typically used for bulk of encryption/decryption
- Same key must be at both end points

Asymmetric (Public) Key Cryptography:

- 2 related keys are required (known as a public and a private key)
- 1000 times slower than symmetric key
- Typically used for exchange of symmetric keys and sender authentication
- End points need have had no prior contact

Authentication:

- Necessary to know who you're speaking to
- Certificates used to verify identity

Asymmetrical (Public) Key Cryptography (RSA)

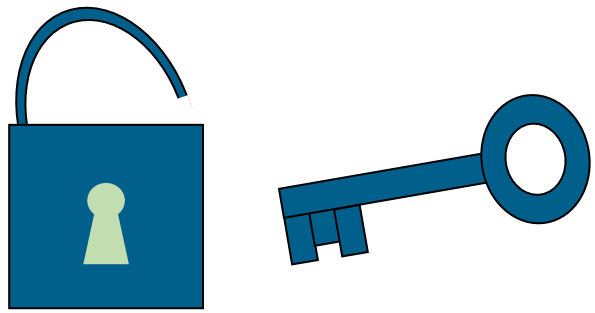
Public key cryptography is based on a pair of keys:

- Public key for encryption (open padlock, anyone can lock)
  - Consists of the modulus (*n*), which is the product of two large prime numbers (*p* and *q*, which are kept secret), and the public exponent (*e*), typically $2^{16} + 1 = 65537$
- Private key for decryption (only the key can unlock the padlock)
  - Consists of the modulus (*n*), and the private exponent (*d*) which is based on the two large prime numbers (*p* and *q*)

For more information refer to:

http://en.wikipedia.org/wiki/RSA

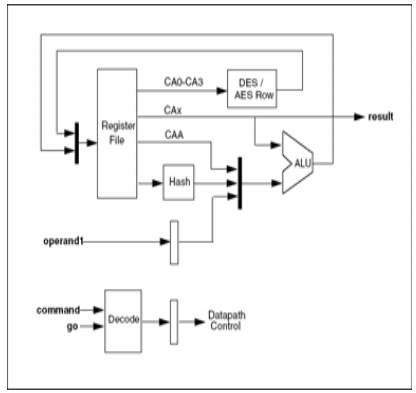
The Code Book, by Simon Singh (Anchor)



RSA - Rivest, Shamir, Adleman

Cryptographic Acceleration Units

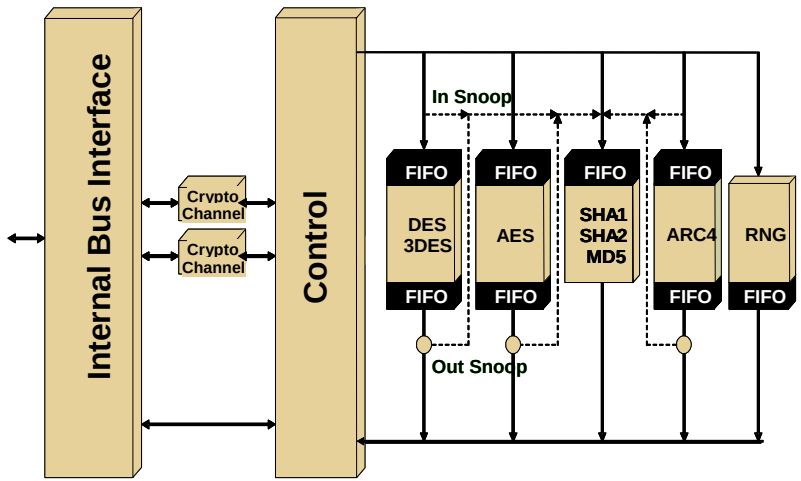
Freescale has a range of crypto modules, from slave units to descriptor driven bus mastering units



CAU Block Diagram

Typical Functionality:

- **Data Encryption Standard Execution Unit (DEU)**
  - DES, 3DES
  - Two key (K1, K2, K1) or three key (K1, K2, K3)
  - ECB and CBC modes
- **Advanced Encryption Standard Unit (AESU)**
  - Key lengths of 128, 192, and 256 bits
  - ECB, CBC, CTR, CCM modes
- **Message Digest Execution Unit (MDEU)**
  - SHA-1 160-bit digest
  - SHA-2 256-bit digest
  - HMAC with all algorithms
  - MD5 128-bit digest
- **ARC Four Execution Unit (AFEU)**
  - Compatible with RC4 algorithm
- **Hardware Random Number Generator (RNG)**
  - FIPS compliant (with appropriate software)



freescale semiconductor

Symmetrical (h)macs and Random Numbers

Cipher/Algorithm	Type	Block Size	Key Size	Common Modes
DES	Symmetric Block Cipher	64 bit	56 bit	CBC
3DES	Symmetric Block Cipher	64 bit	168 bit	CBC
AES	Symmetric Block Cipher	128 bit	128 bit, 192 bit, 256 bit	CBC
ARC-4	Symmetric Block Cipher	8 bit	40 - 128 bit	–
RSA	Asymmetric Stream Cipher	NA	Up to 2048 and 4096	–
MD-5	Hashing Cipher	512 bit	Up to 512 bit	HMAC
SHA-1/SHA-2	Hashing Cipher	512 bit	Up to 512 bit	HMAC

Options for Device and Communications Security

	IPsec	SSL/TLS	SSH
Type of Security	Network	Transport/Session	Application
Typical Usage	Data Path	Management	Management/Control
UDP Security	Yes	No	No
Supports User Authentication	Yes	Yes	Yes
Compatible with NAT & Firewalls	Limited	Yes	Yes
Ease of provisioning	Moderate	Extremely Easy	Extremely Easy

IPsec/IKE - IP Security, provides data confidentiality and node authentication, works at layer 3 and secures everything in the network

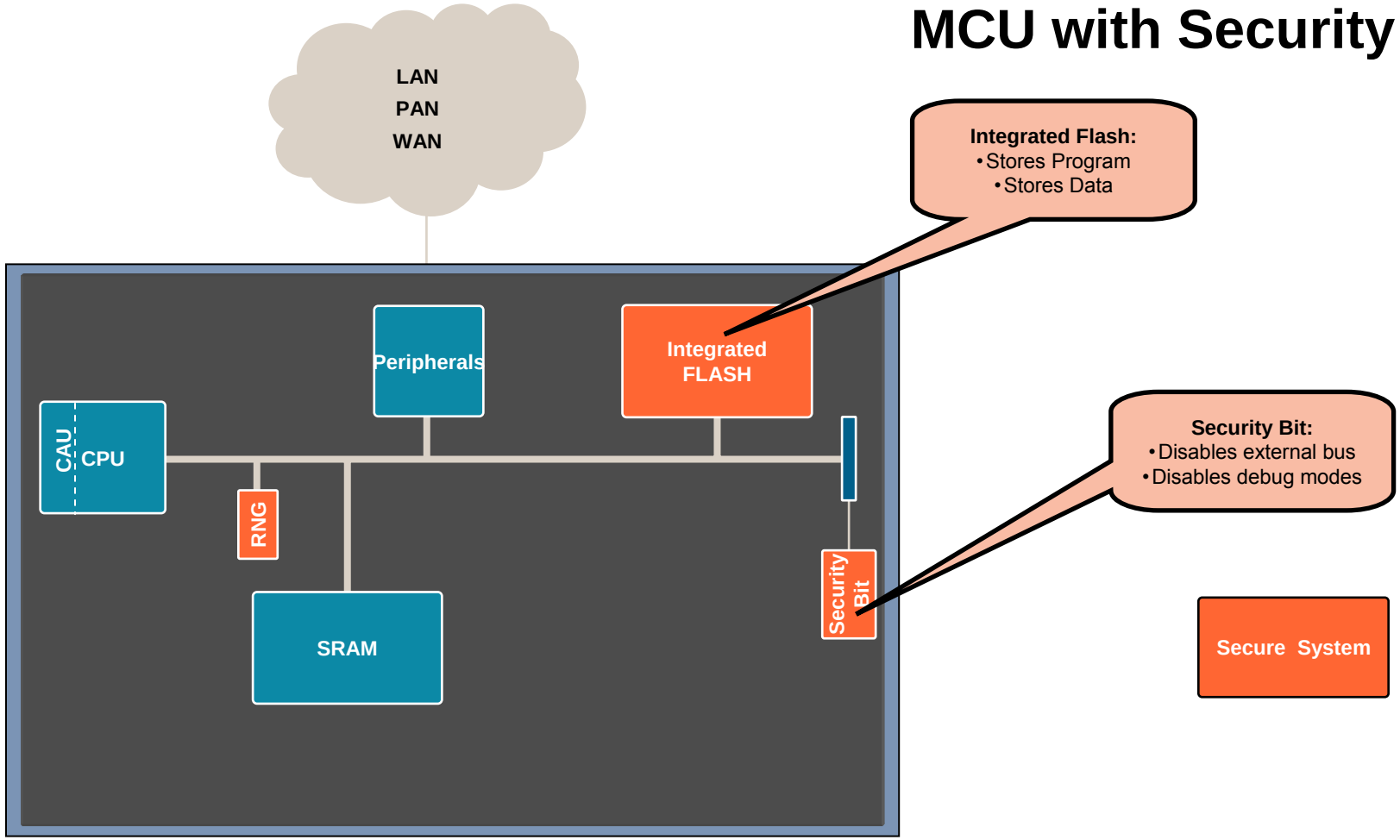
SSL/TLS - Secure Socket Layer/Transport Layer Security, provides communications confidentiality and node authentication across public networks, works at layer 4 and secures applications

SSH - Secure Shell, supports remote log into and control of a system with secure communications

Secure Systems – Preventing Hacking and Cloning

freescale™ semiconductor

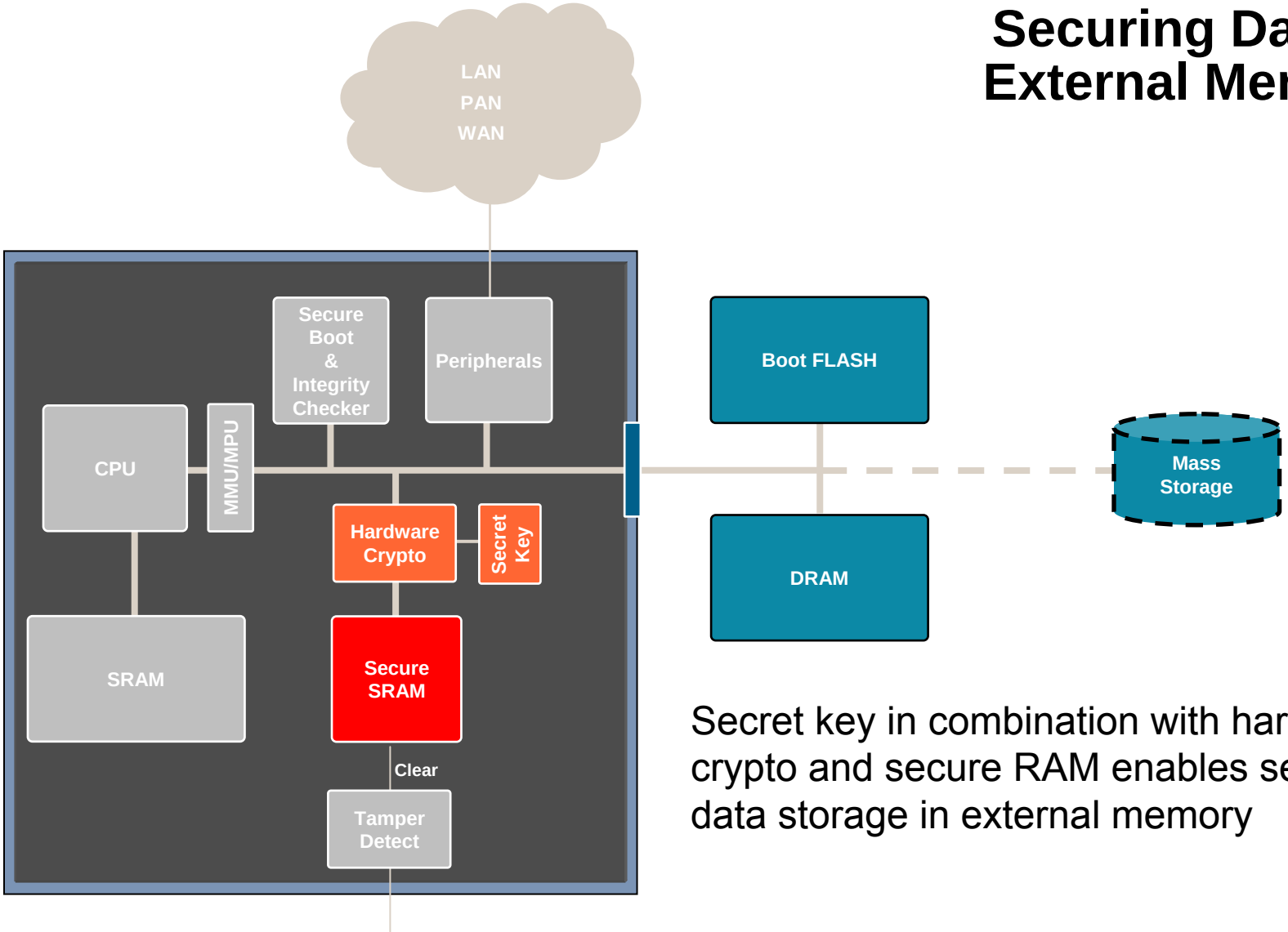
MCU with Security Bit



Security bit is available today on most MCU products, provides good Cloning, and some Hacking Protection. Future developments will improve Hacking protection

freescale semiconductor

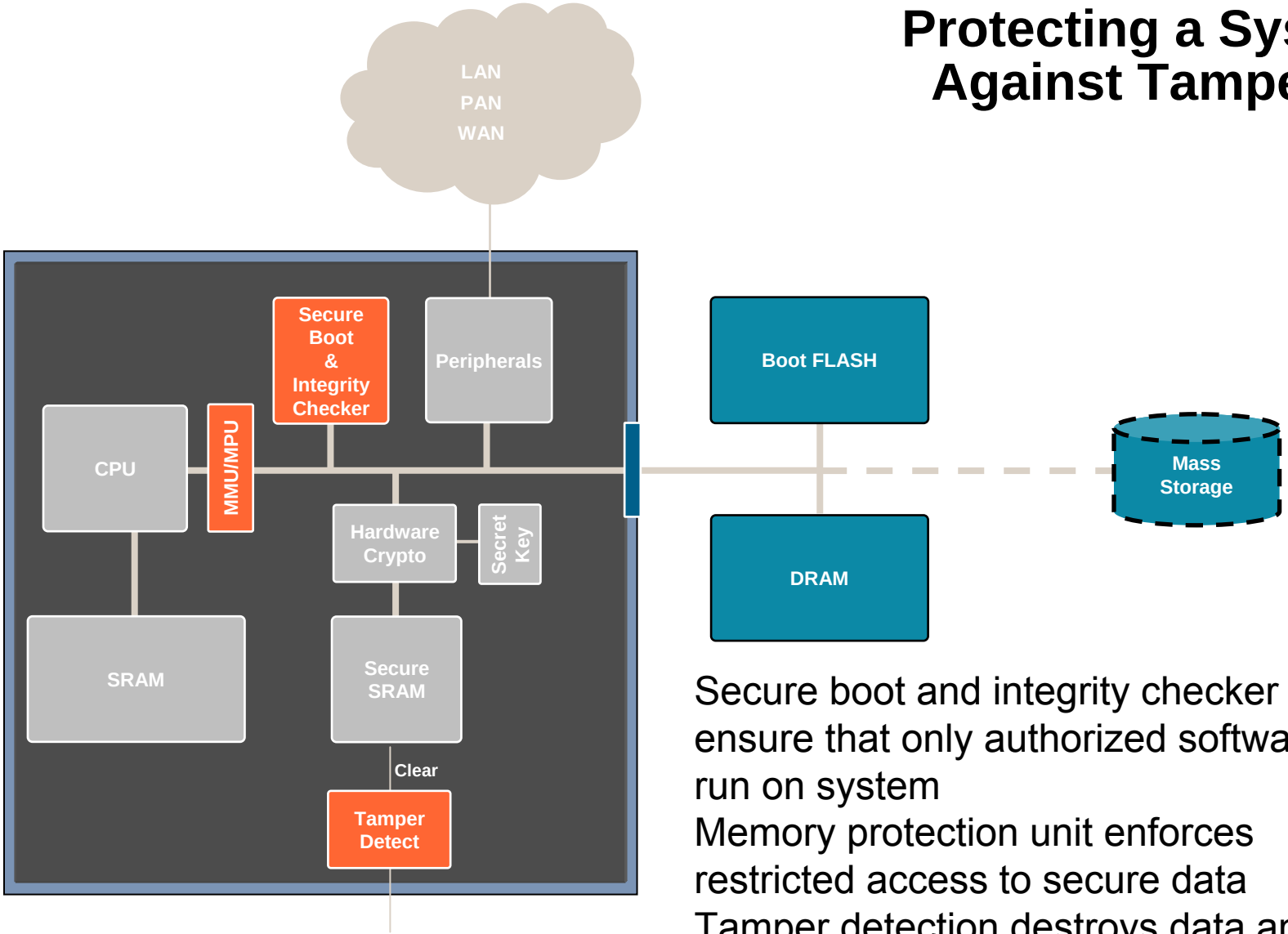
Securing Data in External Memory



Secret key in combination with hardware crypto and secure RAM enables secure data storage in external memory

freescale semiconductor

Protecting a System Against Tampering



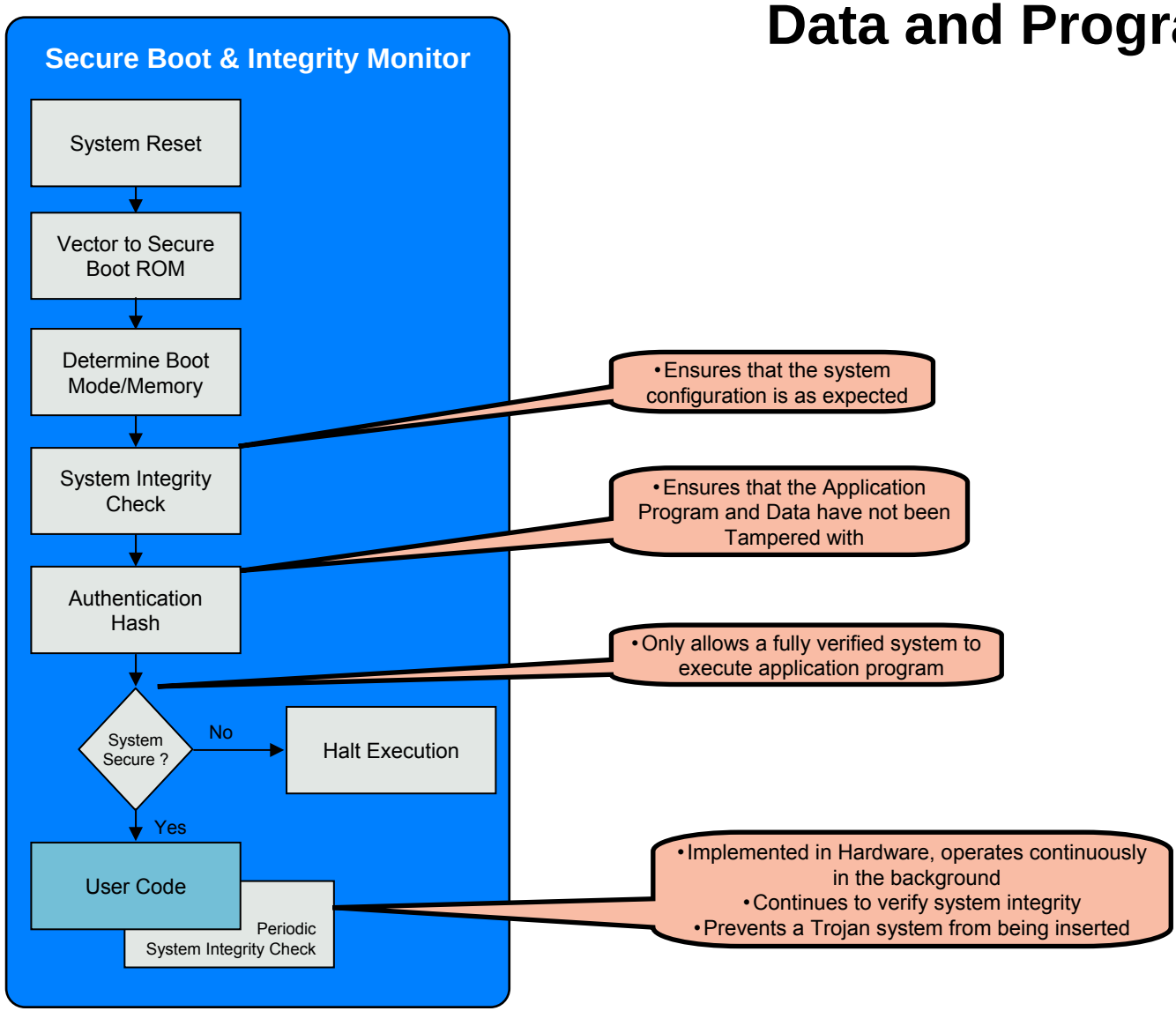
Secure boot and integrity checker ensure that only authorized software will run on system

Memory protection unit enforces restricted access to secure data

Tamper detection destroys data and keys when system is threatened

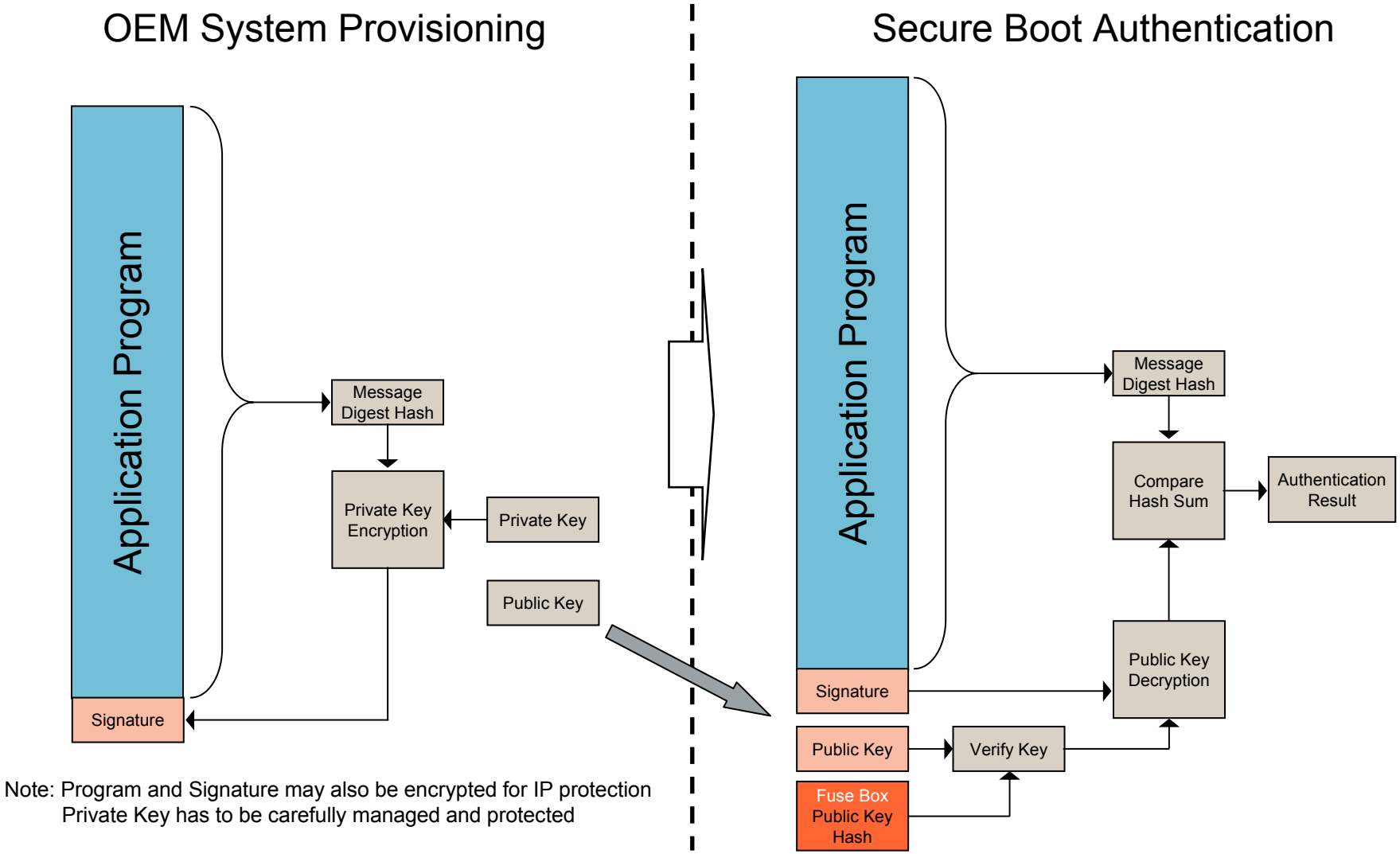
freescale semiconductor

Data and Program Integrity



freescale semiconductor

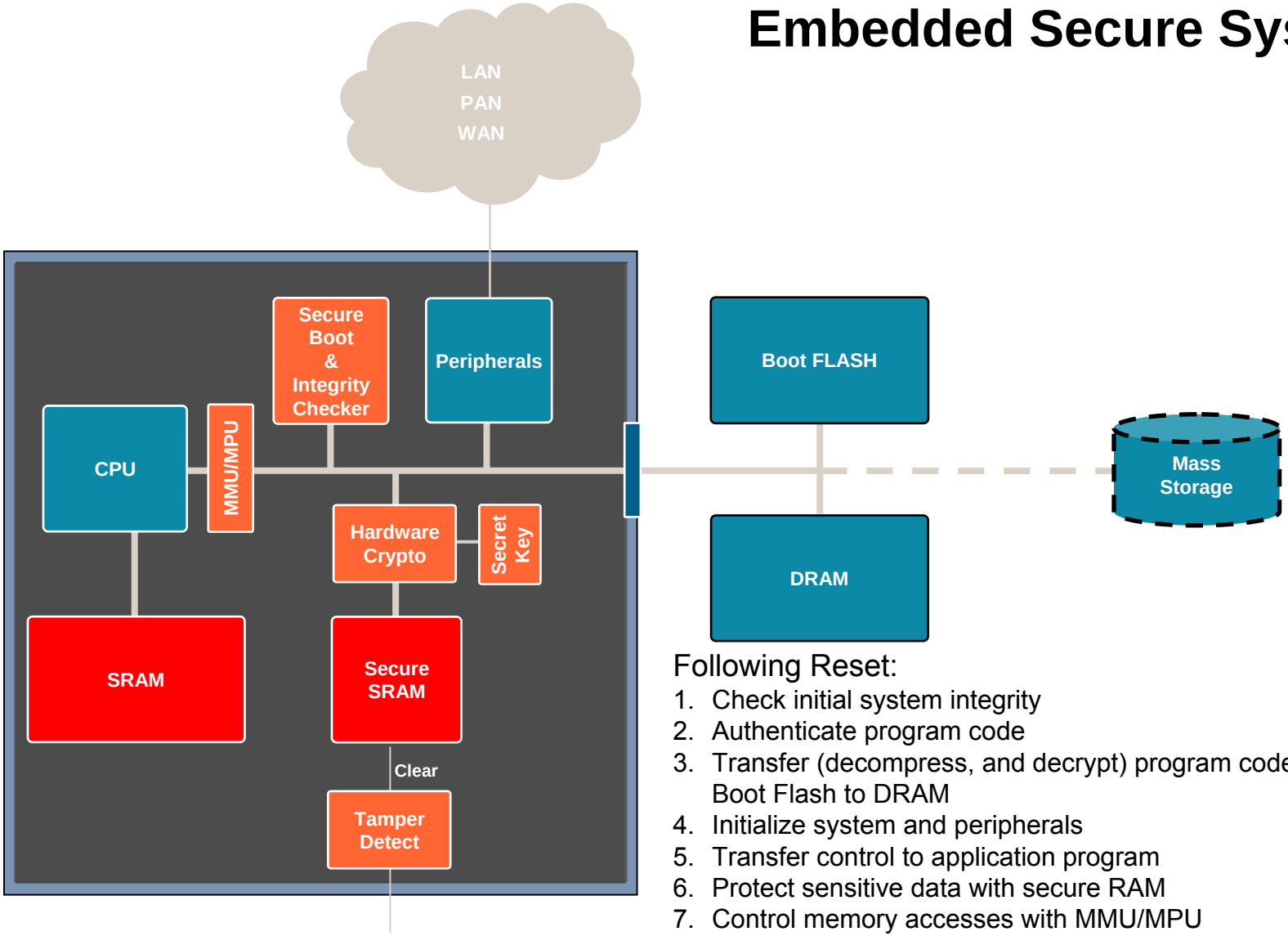
Program Authentication



Note: Program and Signature may also be encrypted for IP protection
Private Key has to be carefully managed and protected

freescale semiconductor

Embedded Secure System

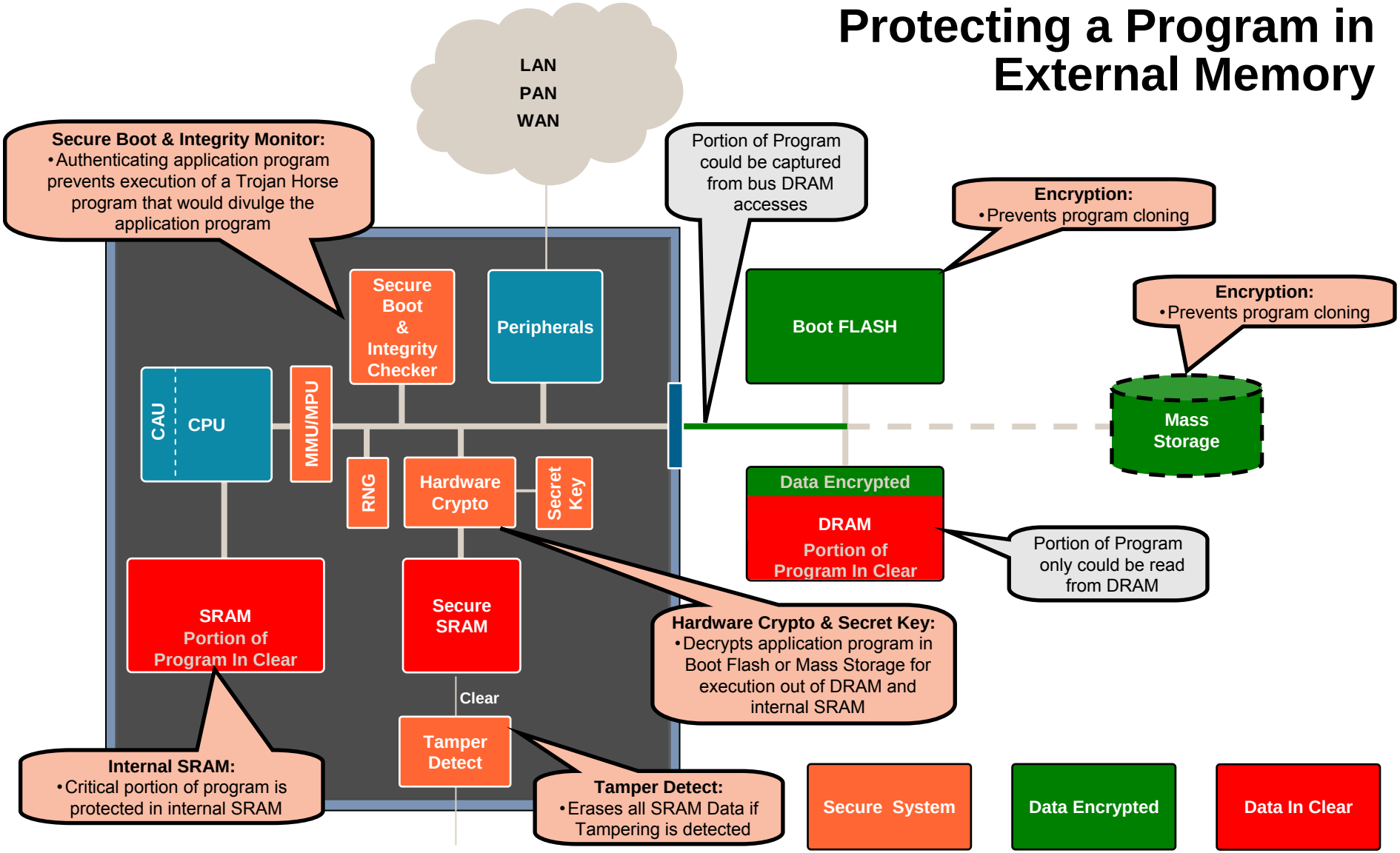


Following Reset:

1. Check initial system integrity
2. Authenticate program code
3. Transfer (decompress, and decrypt) program code from Boot Flash to DRAM
4. Initialize system and peripherals
5. Transfer control to application program
6. Protect sensitive data with secure RAM
7. Control memory accesses with MMU/MPU
8. Encrypt communications with CAU
9. Continuously hash memory with integrity checker

freescale semiconductor

Protecting a Program in External Memory



freescale semiconductor

Software Overview

Well architected and developed application software will require minor adaptations for use in a secure system:

- All commonly used embedded system RTOSes may be used
- Application software should be evaluated for security weaknesses
- Access to sensitive data needs to be carefully assigned
- Movement of sensitive data has to be setup for correct encryption/decryption
- Security exceptions must be handled according to application requirements
- Changes to authenticated data must be re-hashed
- System memory allocation may need to be optimized for data and program protection
- Support for field system analyses requirements must be designed into the application
- Appropriate code signing procedures must be followed

Secure System Tools

Tools for supporting the development, maintenance and provisioning of Secure Systems

Required Functions:

- Code signing using private key
- Public/Private key generation, management and secure storage
- Password management
- Controlled environment for application software development
- Controlled environment for production Flash programming
- System deployment tracking, and update management
- Server authentication of valid systems

Secure System Management Phases

Application Development	Code Signing	Production Programming	Maintenance
Need to restrict source code availability. Prevent un-authorized distribution. Prevent insertion of un-authorized code. **Options:** Trust. Secure computer systems.	Requires public/private key pair generation and management. Application code signing (Code hash and private key encryption of message digest). **Options:** Locally on a secure computer. Contracted to a Code Signing service. Use run-time server authentication.	Prevent un-authorized system (clone) programming. Ensure correct configuration of on chip secure system (fuses). Prevent un-authorized software distribution. **Options:** Trusted premises programming. Secured production programmer. Production tracking system. Use run-time server authentication.	Allow field firmware updates/upgrades. Prevent un-authorized system (clone) programming. Prevent un-authorized software distribution. Prevent un-authorized system use. **Options:** Use Code signing process together with standard field firmware updates. Use run-time server authentication with software update.

freescale™ semiconductor

Related Session Resources

Session Location – Online Literature Library

http://www.freescale.com/webapp/sps/site/homepage.jsp?nodeId=052577903644CB

Sessions

Session ID	Title

Demos

Pedestal ID	Demo Title

freescale™ semiconductor

Q & A

freescale™ semiconductor


freescale™
semiconductor