Flash Memory SUMMIT

How to secure storage devices and Embedded Systems?

Reid Augustin and WeiTi Liu

LucidPort Technology, Inc.

www.lucidport.com

sales@lucidport.com

Topics:

- ❑ Why all storage devices need encryption?
- ❑ Understanding the security risks of different storage devices and embedded systems
  - ❑ Flash drive, External Hard drive ,Cloud and Embedded systems
  - ❑ Risks of unsecured Embedded Systems
    - ❑ Protection of Embedded system's Firmware-Flash Memory content
- ❑ Solutions and Recommendations

Why all storage devices need encryption

Embedded Systems Security Breach examples

Printers

Tens of millions of HP LaserJet printers vulnerable to remote hacking

By Sebastian Anthony on November 29, 2011

Cars

Car hacking: The next global cybercrime?
Holly Ellyatt | @HollyEllyatt
CNBC.com

MY Cloud - A storage device can access files through Internet

It's Crazy What Can Be Hacked Thanks to Heartbleed

By Robert McMillan

Ref: http://www.wired.com/2014/04/heartbleed_embedded/
http://www.extremetech.com/computing/106945-tens-of-millions-of-hp-laserjet-printers-vulnerable-to-hacking
http://www.wdc.com/en/heartbleedupdate/

Understanding of the security risks of different storage devices and embedded systems

Many embedded devices and systems which engineered pre-internet era, the usages of embedded devices and systems were intended for standalone and lacking of security features. Today, all the devices and systems are used as internet devices increasing security vulnerability.

- Flash drive
- External Hard drive
- Cloud
- Embedded systems

Ref:
1. EndPoint Device Secures Cloud Storage, Flash Memory Summit, 2013, Santa Clara, CA
   http://www.flashmemorysummit.com/English/Collaterals/Proceedings/2013/20130813_103A_Liu.pdf
2. 2014 Data Breach Investigations Report, Verizon
   Verizonenterprise.com
3. http://www.wired.com/2014/04/heartbleed_embedded/
4. http://www.wdc.com/en/heartbleedupdate/

Secure Embedded System– Why?

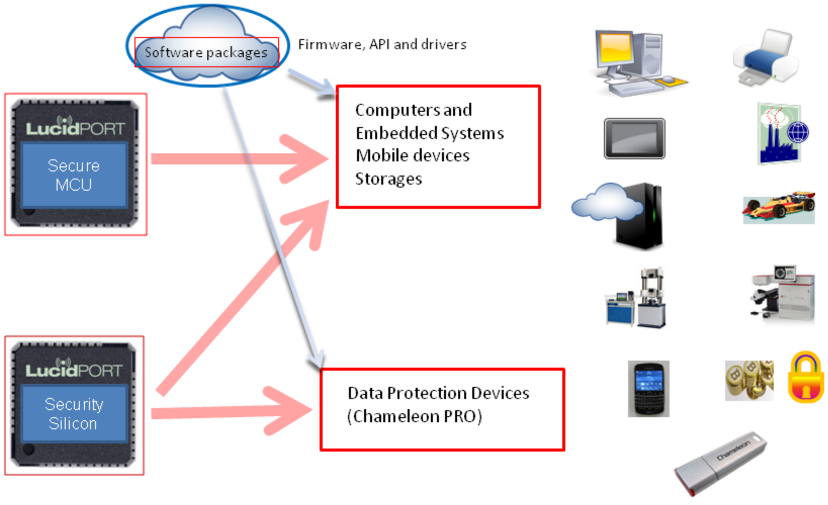
- Embedded system firmware and design data base need protection
  - Hacking and tempering
  - Copy
  - Cloning
  - Protection of product IPs
- Contents of Embedded System Storage Devices need protection
  - Data stored on Printer, MFP, Testing instrument and Manufacture equipment

Secure Embedded System– Why? (2)

- Hacker can access many Embedded Systems through internet connections
  - Printers, Firewalls, Video consoles and Hospital Equipments
  - Test equipment, cars and others
- Unsecured non-volatile storage devices containing Embedded Systems firmware that are vulnerable to security breaches
  - Flash, FRAM and MRAM
- Conventional MCU has build-in security blocks for customers' applications but such internal security block is not able to protect hacking of MCU's own firmware

Secure Embedded system– Actions

- Secure embedded system's on-board firmware, the contents of storage elements (Flash, RAMs, etc.)
  - Unique
  - Encrypt (AES)
- Strong Key Management
  - Generating the Key
  - Managing the Key
- Authentication
- Advance blocking I/O connectivity, USB and internet etc.



Software packages

Firmware, API and drivers

LucidPORT Secure MCU

Computers and Embedded Systems Mobile devices Storages

LucidPORT Security Silicon

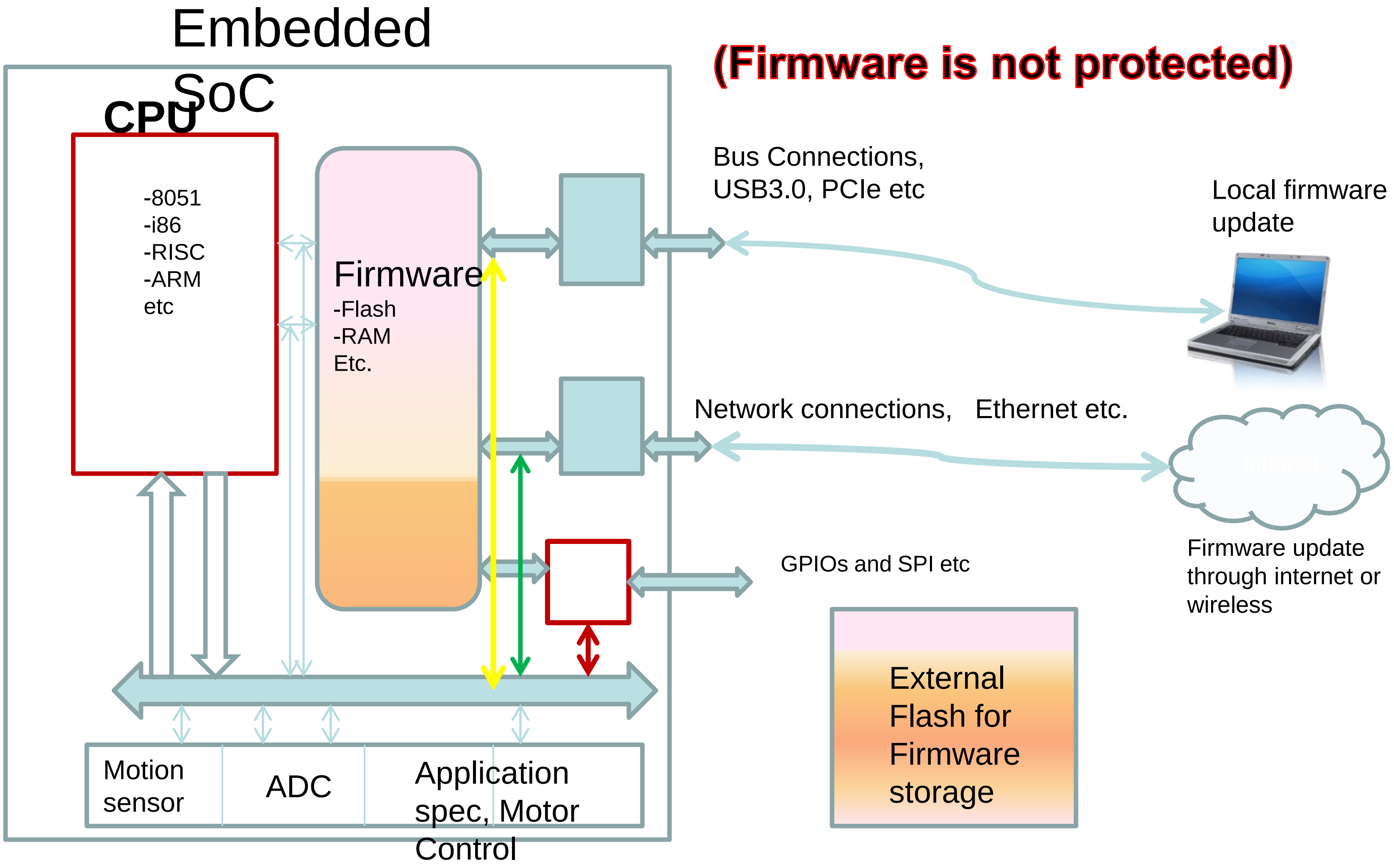
Data Protection Devices (Chameleon PRO)

Proposed Solutions

Embedded Systems On-Board firmware protection

Embedded Systems Data Content protection

Typical Embedded System Design(SoC) block diagram



Embedded SoC

CPU

-8051
-i86
-RISC
-ARM
etc

Firmware
-Flash
-RAM
Etc.

(Firmware is not protected)

Bus Connections, USB3.0, PCIe etc

Local firmware update

Network connections, Ethernet etc.

Firmware update through internet or wireless

GPIOs and SPI etc

External Flash for Firmware storage

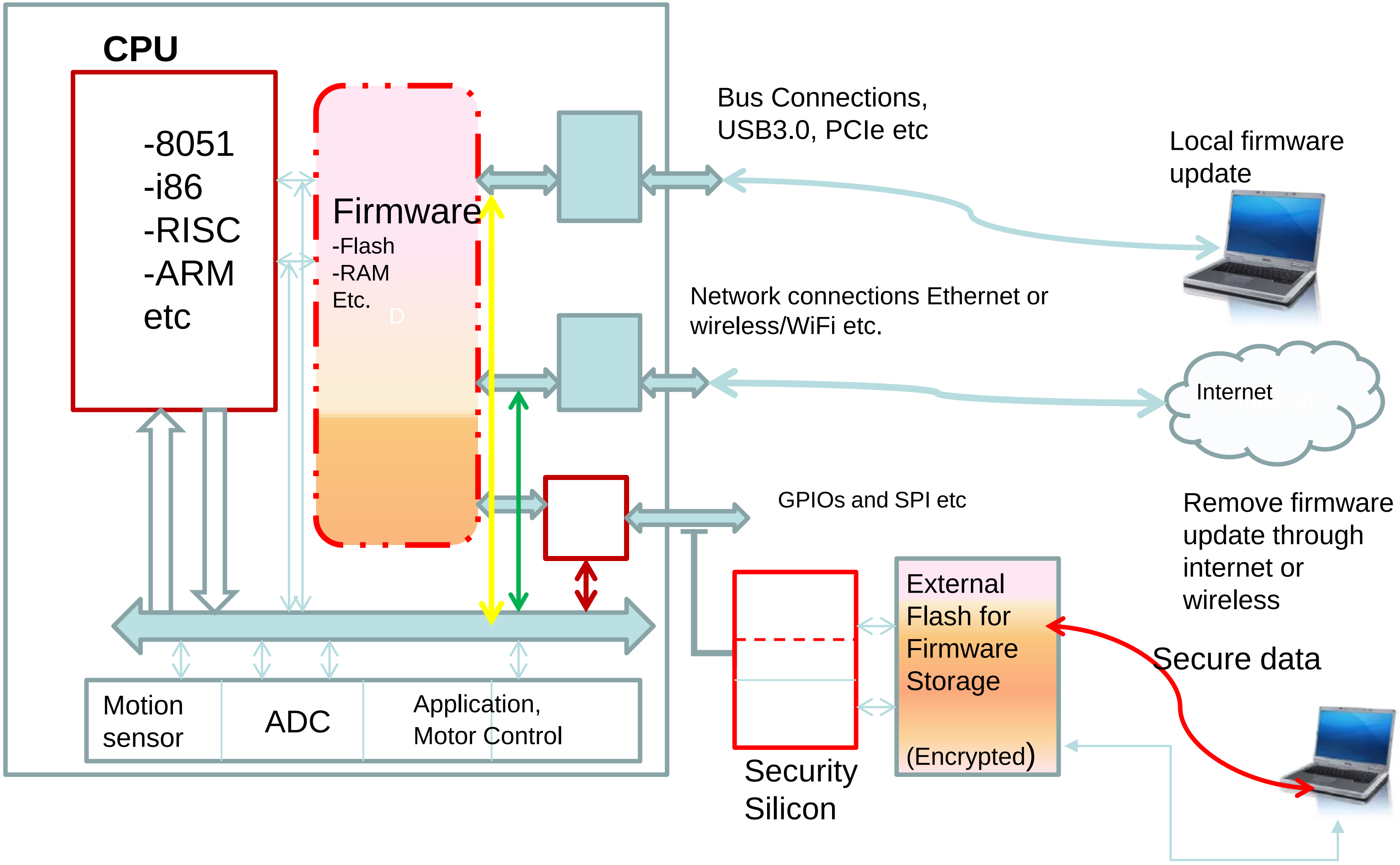
Motion sensor

ADC

Application spec, Motor Control

Embedded System Design(SoC) with Secure features

Embedded SoC



CPU

-8051
-i86
-RISC
-ARM
etc

Firmware
-Flash
-RAM
Etc.

Bus Connections, USB3.0, PCIe etc

Local firmware update

Network connections Ethernet or wireless/WiFi etc.

Internet

GPIOs and SPI etc

Remove firmware update through internet or wireless

Motion sensor

ADC

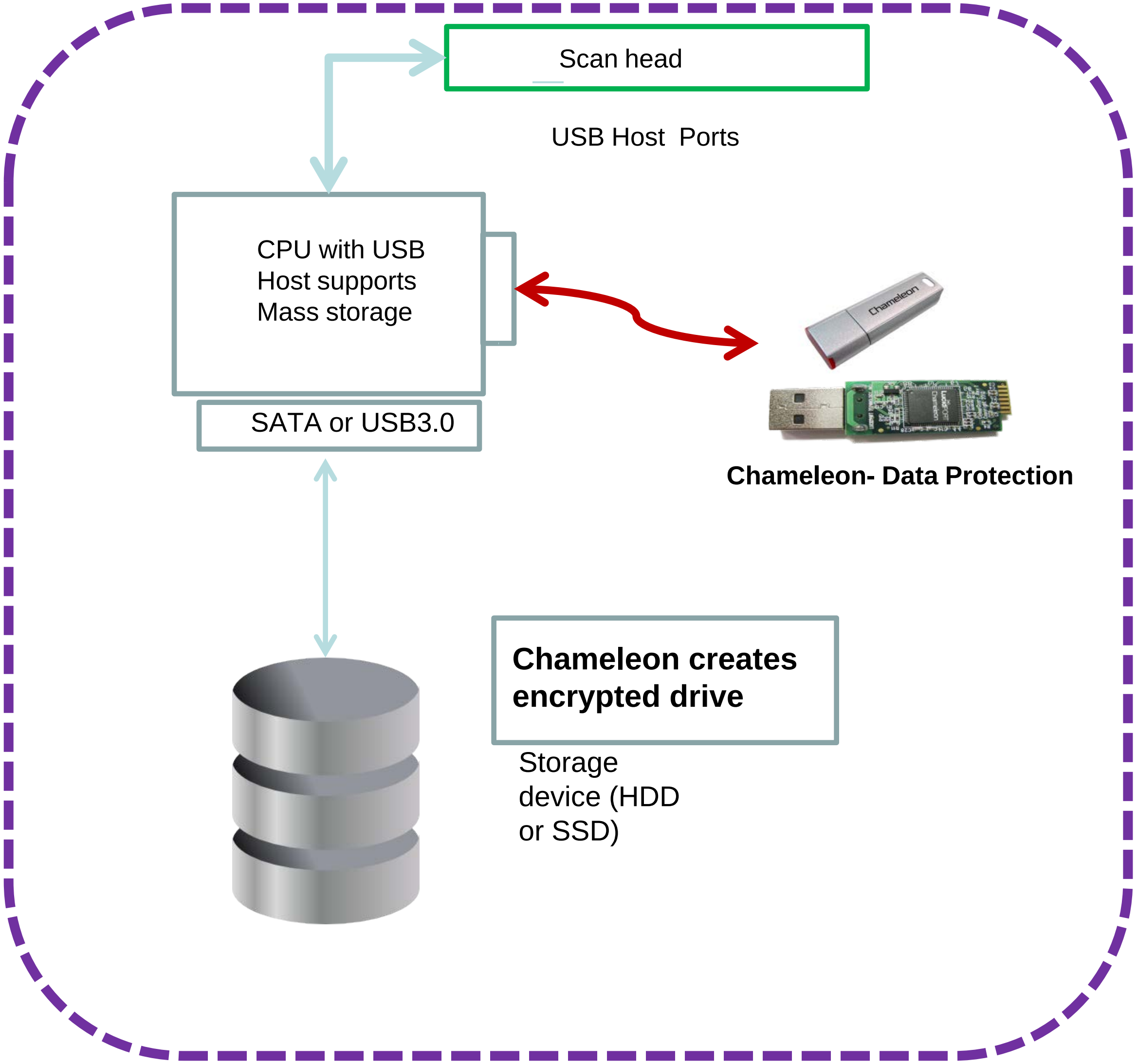
Application, Motor Control

Security Silicon

External Flash for Firmware Storage

(Encrypted)

Secure data



Scan head

USB Host Ports

CPU with USB Host supports Mass storage

SATA or USB3.0

Chameleon- Data Protection

Chameleon creates encrypted drive

Storage device (HDD or SSD)

Chameleon Secures MFP and Printers Contents

Chameleon Features:

Protect storage space to 2TB
Chameleon Pro: Centralized control
Password: support
Recovery (lost device): Yes.
Back up: encrypted back up
Required Internet connection: NO
Vulnerable virus and malware attack: No
Backdoor solution: No
Class supported: Mass storage
OS(s): Windows

Unlike flash drives, the encrypted data is not stored on the Chameleon. It remains in your storage device. In the event of a lost Chameleon, your data is still recoverable and remains safe in your computer, external hard drive, or flash drive. The optional Recovery Passphrase that is created at initial setup can be used to access your encrypted data in such cases. The Chameleon is a physical key that locks away your sensitive information when you are away and easily accesses it when you need it.

Encrypted Flash Drives features and Security risks

	RISKS
Application Objectives	Single storage device with encryption function. Not able to support any other application in secure matter
Protected storage space- Protected Device	Limited by flash memory size, cost will increase when Flash memory size increase
Internet security, Cloud security	None (protects files only on the Flash drive)
Management/Control- Password (Key Password) Recovery (Lost device) Back up Trace on PC	None- Supported, Password unlocks the files, No, if you forget your device or Password, Flash drive is useless Unencrypted backups, requires Flash drive plugged in and unlocked Traces of private files still on the PC’s hard drive
Vulnerable to virus and malware attack?	Yes
Who designed it? Who owns the device’s source code? Who manufactures the devices?	Flash drive manufacture may outsource from third party code developers
Back door solutions	Many Flash may have back door solutions

Summary

- Storage devices need to add data protection features
  - Encrypted Flash Drive exposed high security risks
  - Cloud storage needs strong data protection solutions
- Embedded Systems are vulnerable to security breach
  - Risk factors are high
  - Users are not aware of the potential risk factors
- Securing Embedded system
  - Solutions are proposed
    - Data protection
    - New concept and design to protect onboard firmware
- No silver bullets