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/
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


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.
Proposed Solutions

Embedded Systems On-Board firmware protection
Embedded Systems Data Content protection
Typical Embedded System Design (SoC) block diagram

- 8051
- i86
- RISC
- ARM etc

CPU

Firmware
- Flash
- RAM
- Etc.

Bus Connections, USB3.0, PCIe etc

Network connections, Ethernet etc.

GPIOs and SPI etc

Motion sensor

ADC

Application spec, Motor Control

External Flash for Firmware storage

(Firmware is not protected)

Local firmware update

Firmware update through internet or wireless
Embedded System Design (SoC) with Secure features

CPU
- 8051
- i86
- RISC
- ARM
etc

Firmware
- Flash
- RAM
Etc.

Bus Connections,
USB3.0, PCIe etc

Network connections Ethernet or wireless/WiFi etc.

GPIOs and SPI etc

Motion sensor
ADC
Application, Motor Control

External Flash for Firmware Storage (Encrypted)

Secure data

Internet

Local firmware update

Remove firmware update through internet or wireless

Security Silicon

Embedded SoC
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

<table>
<thead>
<tr>
<th>Feature</th>
<th>RISKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Objectives</td>
<td>Single storage device with encryption function. Not able to support any other application in secure matter</td>
</tr>
<tr>
<td>Protected storage space- Protected Device</td>
<td>Limited by flash memory size, cost will increase when Flash memory size increase</td>
</tr>
<tr>
<td>Internet security, Cloud security</td>
<td>None (protects files only on the Flash drive)</td>
</tr>
<tr>
<td>Management/Control-</td>
<td>None- Supported, Password unlocks the files, Flash drive is useless</td>
</tr>
<tr>
<td>Password (Key Password)</td>
<td></td>
</tr>
<tr>
<td>Recovery (Lost device)</td>
<td></td>
</tr>
<tr>
<td>Back up</td>
<td>Unencrypted backups, requires Flash drive plugged in and unlocked</td>
</tr>
<tr>
<td>Trace on PC</td>
<td>Traces of private files still on the PC’s hard drive</td>
</tr>
<tr>
<td>Vulnerable to virus and malware attack?</td>
<td>Yes</td>
</tr>
<tr>
<td>Who designed it?</td>
<td>Flash drive manufacture may outsource from third party code developers</td>
</tr>
<tr>
<td>Who owns the device’s source code?</td>
<td></td>
</tr>
<tr>
<td>Who manufactures the devices?</td>
<td></td>
</tr>
<tr>
<td>Back door solutions</td>
<td>Many Flash may have back door solutions</td>
</tr>
</tbody>
</table>
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