Embedded Systems Silicon Valley 2011

ESC-202

Implementing Secure Remote Firmware Updates

Tuesday May 3rd, 8:00 – 9:15

Loren Shade
loren@allegrosoft.com

PERVASIVE

Home • Work • Play

Pervasive (Home)

CONTROL4
www.control4.com

MOXI
www.moxi.com

YAMAHA neoHD
usa.yamaha.com

BAINULTRA
www.bainultra.com

Pervasive (Work)

BROCADE
www.brocade.com

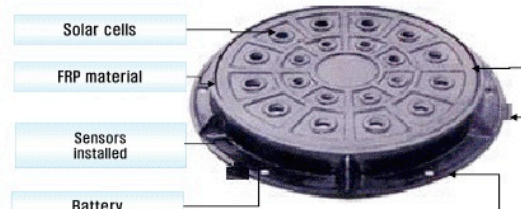
iPhone 4
www.control4.com

CISCO VOIP PHONE
www.cisco.com

Verizon FIOS ONT
www.verizon.com

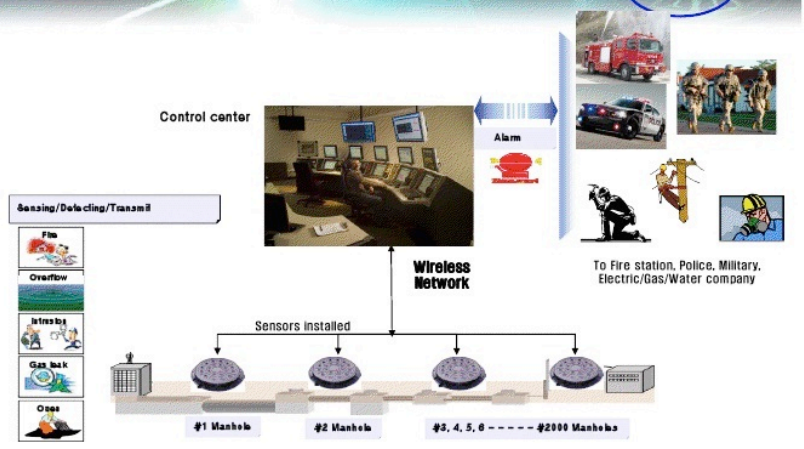
XEROX PRINTER
www.xerox.com

What is Wireless Manhole



Subjects	How to	Features
Self Charging	Solar cells	Self power
FRP	Fiber Reinforced Plastic	Easy production
Remote Locking	By Key, Electronics Access or Control center	To avoid stolen
Wireless Modules	Bluetooth, Zigbee, CDMA Wireless Mesh Network	Remote control
Sensors	Fire, Electricity, Intrusion, Gas, Water	Detection
Dual Sealing	Secure installation	Reliability

How it works

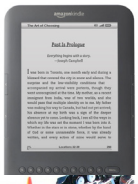


Pervasive (Play)

GARMIN
www.garmin.com

MARKIV DiskLavier PRO
usa.yamaha.com

FRETLIGHT
www.fretlight.com



THUNDER-MAX
www.thunder-max.com

FAD or FOREVER

Microsoft Expects 10 Year Lifecycle for Xbox 360

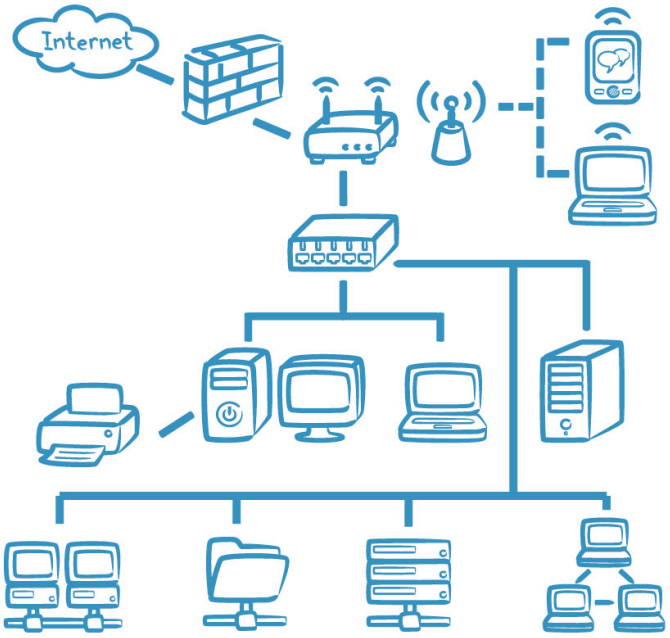
Microsoft Expects 10 Years Lifecycle for Xbox 360 : Microsoft Xbox 360 to Have 10 Years Lifecycle, Anton Shilov, Xbit Laboratories, June 2009, http://www.xbitlabs.com/news/multimedia/display/20090603230547_Microsoft_Expects_10_Years_Lifecycle_for_Xbox_360.html

Changes in Business Model

- Product Business Models Endorse Updates
  - Extend Product Lifecycle
  - Engage Customers (Cross sell and upgrades)
  - Support and Service
  - $$$$$$$$$$

Security and Remote Updates

- Remote Update Implementations often Proprietary
  - Often None Standard Protocols
  - Often NO Security



Security is a PROCESS!!

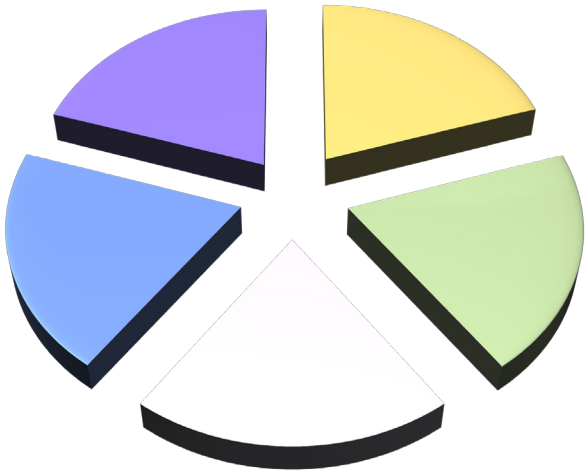
"Security is a chain; it is only as secure as the weakest link …"

"Security is a process, not a product"

Bruce Schneier
Secrets & Lies

Example - Defense Contractors working with DOE/DOD classified material

Implementation Areas



Hardware
Software (RTOS, Application)
Operational
Security
Communications

Requirements

- Leverage Established Standards
- Authenticate Downloads
- Validate Downloads
- Versatile Communications Solution
- Scalability
- Cancel update on failed Authentication or Validation

Simple Communications Framework

Security, Validation and Authentication

- Key Pair – Public (*pk*) and Secure Private (*sk*)
- Calculating Signature (FIPS 186-3)
  - Hash (FIPS 180-2)
  - Signature Calculation
  - Append Result

Digital Signature Process

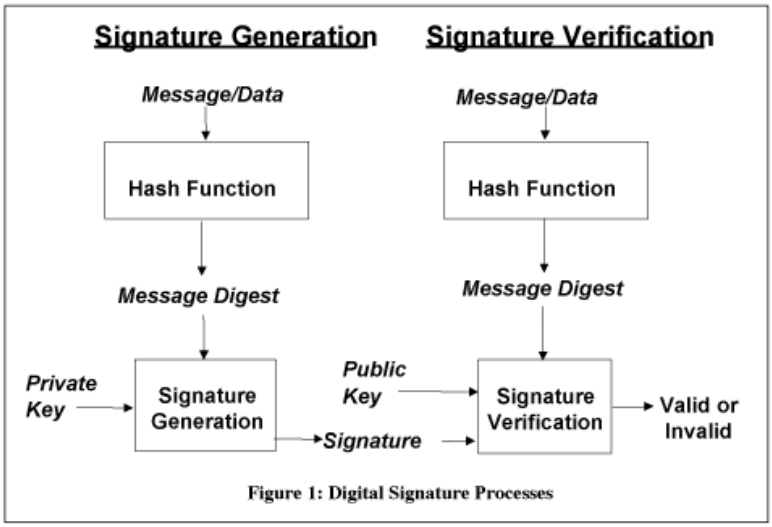
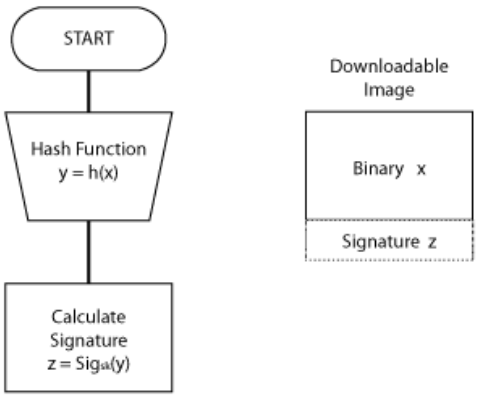


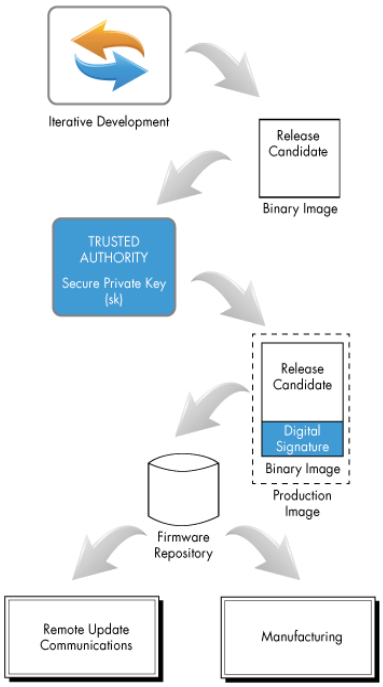
Figure 1: Digital Signature Processes

SOURCE: FIPS 186-3 (pg 9)

Implementation

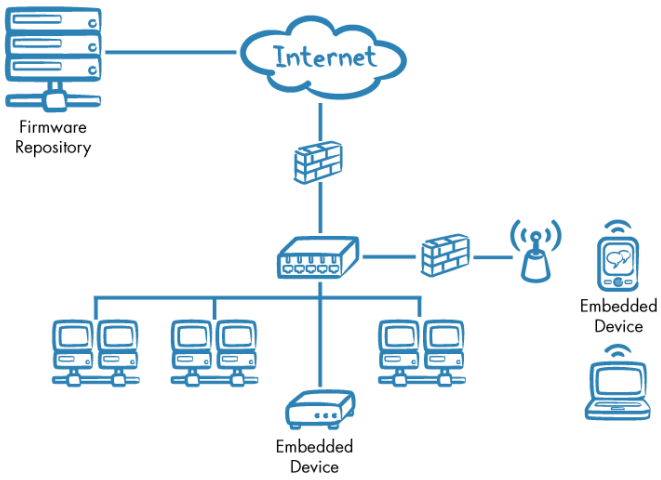


Trusted Authority in Development Cycle



Communications Architecture

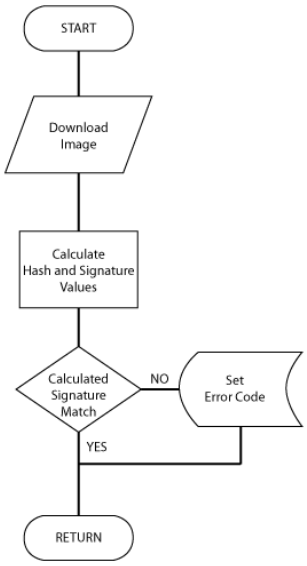
- HTTP
- HTML/XHTML
- XML



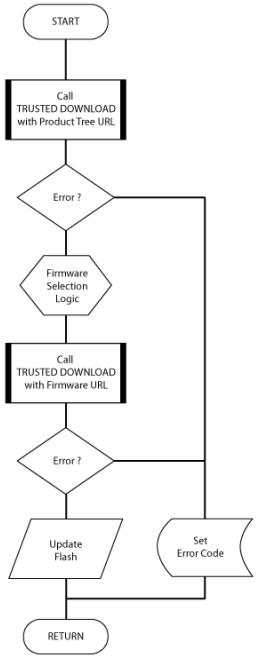
Embedded Software Logic

- TRUSTED DOWNLOAD (Subroutine)
- DOWNLOAD LOGIC

Trusted Download



Download Logic



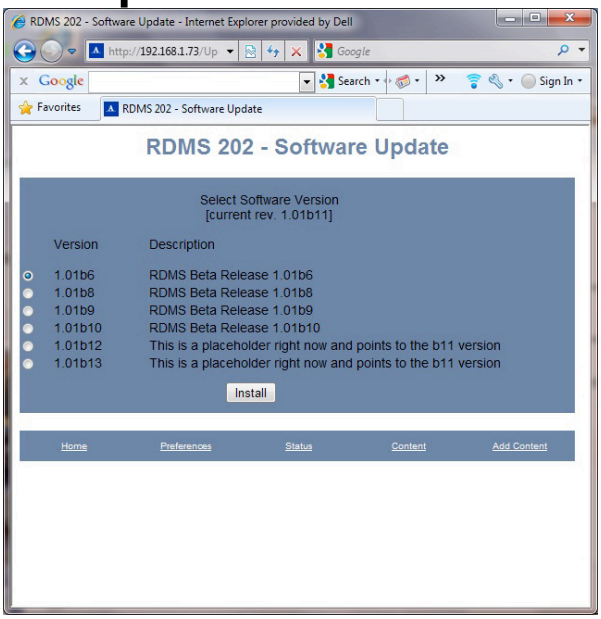
Firmware Repository Organization

- Simple XML
- Variations employ server side logic

Example XML

```
<?xml version="1.0"?>
<Revisions>
 <Product>
  <Name>RDMC 101</Name>
  <Major>1</Major>
  <Minor>50</Minor>
  <Beta>34</Beta>
  <Path>/files/RDMCv150b34.bin</Path>
  <Description>Beta 34 for RDMC 101 v1.5</Description>
 </Product>
<Product>
  <Name>RPLAY 303</Name>
  <Major>1</Major>
  <Minor>00</Minor>
  <Beta>10</Beta>
  <Path>/files/rplay.100b10</Path>
  <Description>Beta 10 for RPLAY 303</Description>
 </Product>
</Revisions>
```


Example Update Screen



Questions & Comments

loren@allegrosoft.com - 203-542-8166

Slides, Notes and Paper available at

www.allegrosoft.com/escsv2011