



IBM

Trusted Computing and Netted Sensors

2005-10-25

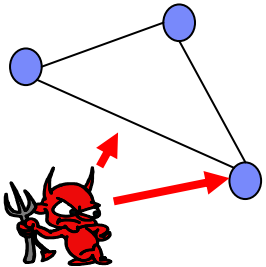
Jeffrey W. Leach / IBM United States

Seiji Munetoh / IBM Tokyo Research Lab

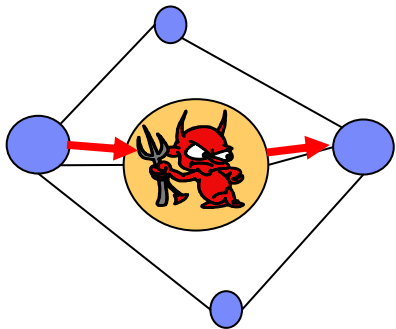
Agenda

- Brief Threat Analysis of Netted Sensors
- Hardware-based Security
- TCG Overview
- Example Implementation - TPod

Brief Threat Analysis of Netted Sensors



- Protection from outside attack
 - Eavesdropping
 - Unauthorized access



- Protection from inside attack
 - Spoofing by malicious sensor in the net
 - Denial of Service
 - Disturbance

**Authentication
Secure Channel
(Encryption)**

**But
How to keep the secret
or sensitive info in the device?
And
How to trust the devices?**

Hardware-based Security Enhancement

- Protected storage
 - Secure Storage for Key and Sensitive data
- Protected operations
 - Encryption/Decryption
 - Sign/Verify
 - Random number generation
- Validations
 - FIPS140-2 Level 3, 4(Max)
 - Common Criteria EAL3,4
- Trusted Computing (New capability)
 - Root of trust measurement
 - Root of trust reporting

Security Module/Chip

Security Level/ Cost ↑



**Secure Co-Processor
(IBM4758)**

Certification of the hardware under FIPS PUB 140-1 at levels 3 and 4 assures a high-integrity processing environment.
BUT Expensive for small devices



SmartCard

**Inexpensive (<\$10)
BUT Just keep the (users) Identity**



**Trusted Platform Module
(TPM)**

+ Platform

**Inexpensive (<\$5)
Protected storage
Protected Crypto operations
Holds/Reports Platform Measurements**



TCG for embedded devices



- Embedded devices, smart sensors and other intelligent, networked controllers are becoming pervasive on wired and wireless networks. As these devices become more closely integrated with corporate IT networks security considerations become critical. TCG can help address significant platform identity and integrity issues.



Why standards in security?

Standards for infrastructure and technology are generally good!

- Critical for creating end to end solutions as part of ecosystem
- Broaden and accelerate the technology rate of adoption
- Broaden market
- Avoid custom development
- Independence from supplier
- Demonstrate required level of quality
- Simplify regulatory compliance

Security standards!

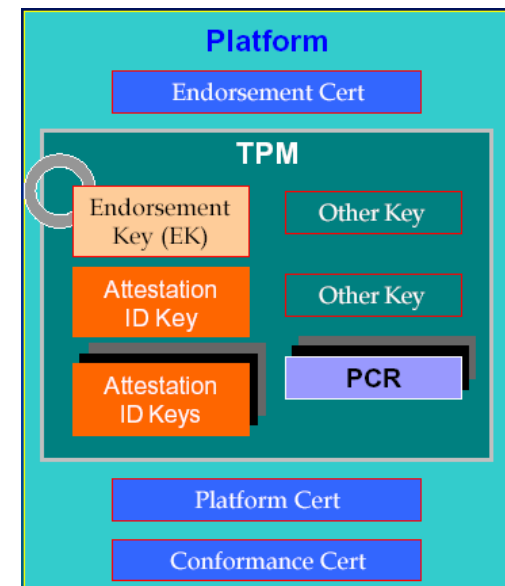
- Security is notoriously error prone, standardization enables:
 - Creation of a componentized architecture for Security
 - Expanded population for technical expert review and evaluation
- Security standards need special care
 - Security standards must be proven concepts
 - implement and evaluate first

TCG Specifications

- The TCG standard is divided into multiple documents including TPM, TSS, Infrastructure, and platform specific specifications.
- The **TPM** and **TSS** specifications are platform independent
- Platform specific specifications provide a reference implementation for a class of devices
- Platform specific work is underway to apply the TCG standard (TPM/TSS) to PCs, servers, peripherals, storage, and mobile phones
- Currently there is no embedded device specific workgroup, but embedded devices can still benefit from the capabilities offered by TCG

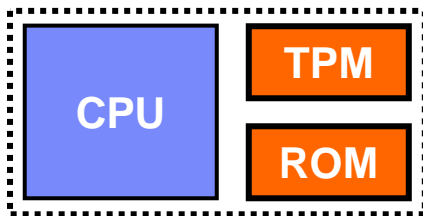
Trusted Platform Module (TPM)

- Enhances many aspects of platform security
 - Specified by Trusted Computing Group (TCG)
- Major functions today:
 - *Protected non-volatile storage* of platform secrets (e.g. encryption/signature keys, etc.)
 - *Special purpose protected processing* (e.g. key generation, digital signatures, etc.)
 - *Spoof-resistant platform authentication* capability (e.g. platform integrity measurement & reporting)

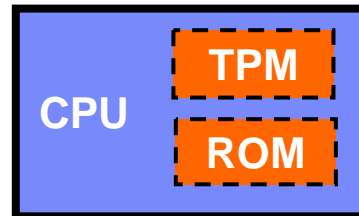


TCG Implementation – Hardware-based Root of Trust

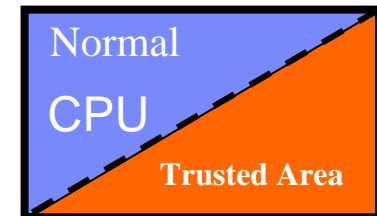
- TPM and Initial Boot Code must be Physically Protected
- for Embedded Platform...
 - Discrete TPM
 - ◆ TPM for PC Platform (LPC bus)
 - ◆ Atmel AT97SC3201S supports I2C bus!
 - CPU Embedded TPM
 - ◆ E.g. Intel PXA27x (Also supports Trusted ROM)
 - Software TPM with Strong Separation
 - ◆ E.g. ARM11 TrustZone



Discrete TPM
(Current PC Platform)



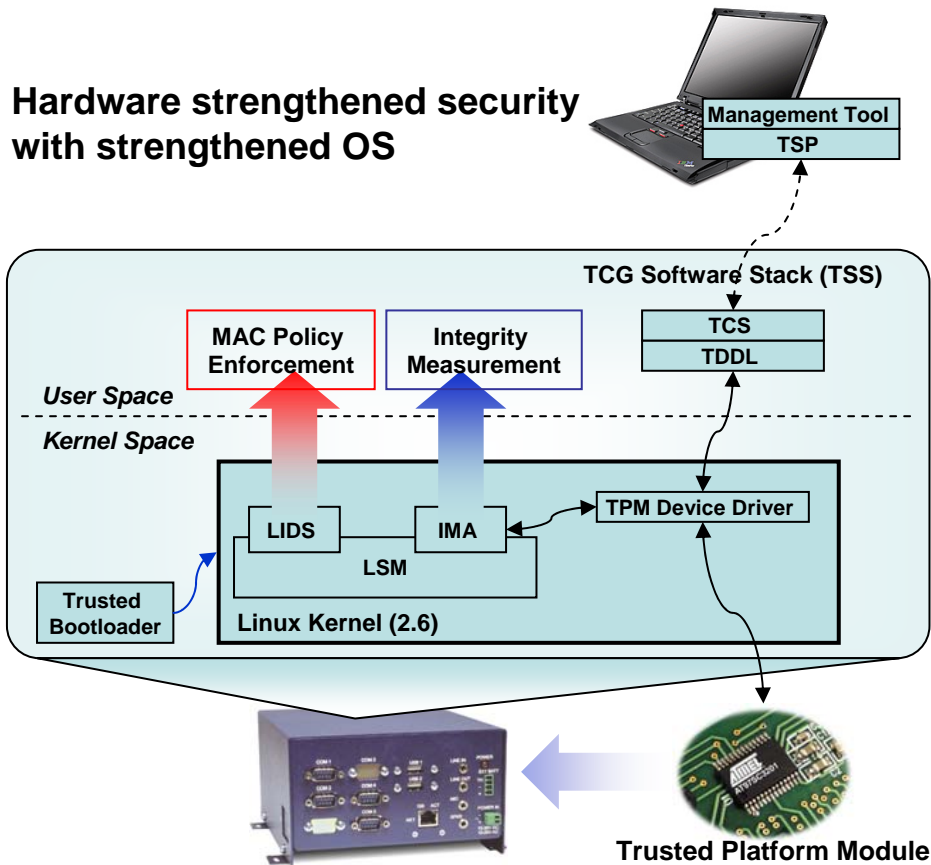
Embedded TPM



Software TPM

Example Implementation - TPod

Hardware strengthened security with strengthened OS



- 🔒 **Mandatory Access Control (MAC)** improves security of CE Devices connected to the Internet by minimizing influence of malicious attacks.
- 🔒 **TPM protects Identity and Integrity of software.** Enables reliable remote device management and minimizes administrative costs of Mobile, Embedded and CE devices.
- 🔒 **Protected Persistent Storage.** Sensitive data is encrypted based on platform integrity, and protected even if Mandatory Access Control is disabled.
- 🔒 **Performance.** Secure-Hash calculation of file/image in the Trusted Bootstrap process increases boot up time from 45sec to 66sec (incl. measurement of Java Middleware).

CPU: XScale PXA255 400MHz
 Memory: 32MB Flash/64MB SDRAM
 TPM: Atmel AT97SC3201S (on I2C bus)

TPM device driver is available in 2.6.12
 IMA patch submitted to LKML
 LIDS <http://www.lids.org>
 TSS (Trousers) <http://sourceforge.net/trousers>

SOAP Message with Platform Integrity

```

- <soapenv:Header>
- <w:Security xmlns:w="http://schemas.xmlsoap.org/ws/2003/06/secext" soapenv:mustUnderstand="1">
  <w:BinarySecurityToken xmlns:u="http://schemas.xmlsoap.org/ws/2003/06/utility" xmlns=""
    EncodingType="w:Base64Binary" ValueType="w:X509v3"
    u:Id="ST_4324564437189652379_1089806298916">MIIDbiCCAlaQAwIBAgICA0OwDOYJKoZIhvcNAOEFB0AwIiELMA
    X.509 Certificate of AIK
  - <tcg:AttestationToken xmlns:u="http://schemas.xmlsoap.org/ws/2003/06/utility"
    xmlns:tcg="http://www.trustedcomputinggroup.org/" u:Id="ST_7006790277265804579_1089806298916">
    Attestation Token
    <tcg:Measurement xmlns:tcg="http://www.trustedcomputinggroup.org/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema" tcg:ValueType="tcg:PCRComposite"
    tcg:EncodingType="xsd:hexBinary">000212010000003C03F2DB3C521C991682F9826CAE2B9873DA4C73EFE5F08C
    Measurement
  - <w:SecurityTokenReference>
    <w:Reference xmlns="" URI="#ST_4324564437189652379_1089806298916" />
  - <w:SecurityTokenReference>
  - </w:SecurityTokenReference>
  - </tcg:AttestationToken>
- <d:Signature xmlns:d="http://www.w3.org/2000/09/xmldsig#">
  Signature
  - <d1:SignedInfo xmlns:d1="http://www.w3.org/2000/09/xmldsig#">
    <d1:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <d1:SignatureMethod Algorithm="http://www.trustedcomputinggroup.org/2004/02/xmldsig#rsa-sha1-
    pcr" />
    Signature Algorithm
    + <d1:Reference URI="#sign_8677982348579964772_1089806299357">
    + <d1:Reference URI="#sign_135439407900327171_1089806299358">
    + <d1:Reference URI="#sign_2503163924570652626_1089806299358">
    </d1:SignedInfo>
    <d:SignatureValue>AQEABIFVT1QDnjr5g54Cso1gWg7qbiFhr6McrGIV1O1mthjbGavIrKGAaIHX0sW/bylia8gUyDfmgD
  + <d:KeyInfo>
  - </d:Signature>
  - </w:Security>
  - <u:Timestamp xmlns:u="http://schemas.xmlsoap.org/ws/2003/06/utility">
  - </u:Timestamp>
  - </soapenv:Header>
- <soapenv:Body xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:u="http://schemas.xmlsoap.org/ws/2003/06/utility" u:Id="sign_8677982348579964772_1089806299357">
  - <ns1:getQuoteResponse xmlns:ns1="http://service.stock.wss.service.wsosgi.ibm.com">
    <getQuoteReturn xmlns="">33.0</getQuoteReturn>
  - </ns1:getQuoteResponse>
  - </soapenv:Body>
- </soapenv:Envelope>

```

Links

- Trusted Computing Group
<https://www.trustedcomputinggroup.org/home>
- Linux Intrusion Detection System
<http://www.lids.org/>
- Integrity Measurement Architecture
http://www.research.ibm.com/secure_systems_department/projects/tcglinux/
http://www.research.ibm.com/compsci/project_spotlight/security/
(The patch is available from LKML)
- TPM Device Driver for LINUX (GPL)
<http://sourceforge.net/projects/tpmdd/>
(TPM is supported by Linux kernel $\geq 2.6.12$)
- TSS (TCG Software Stack) for LINUX (CPL)
<http://sourceforge.net/projects/trousers>

Thank you!

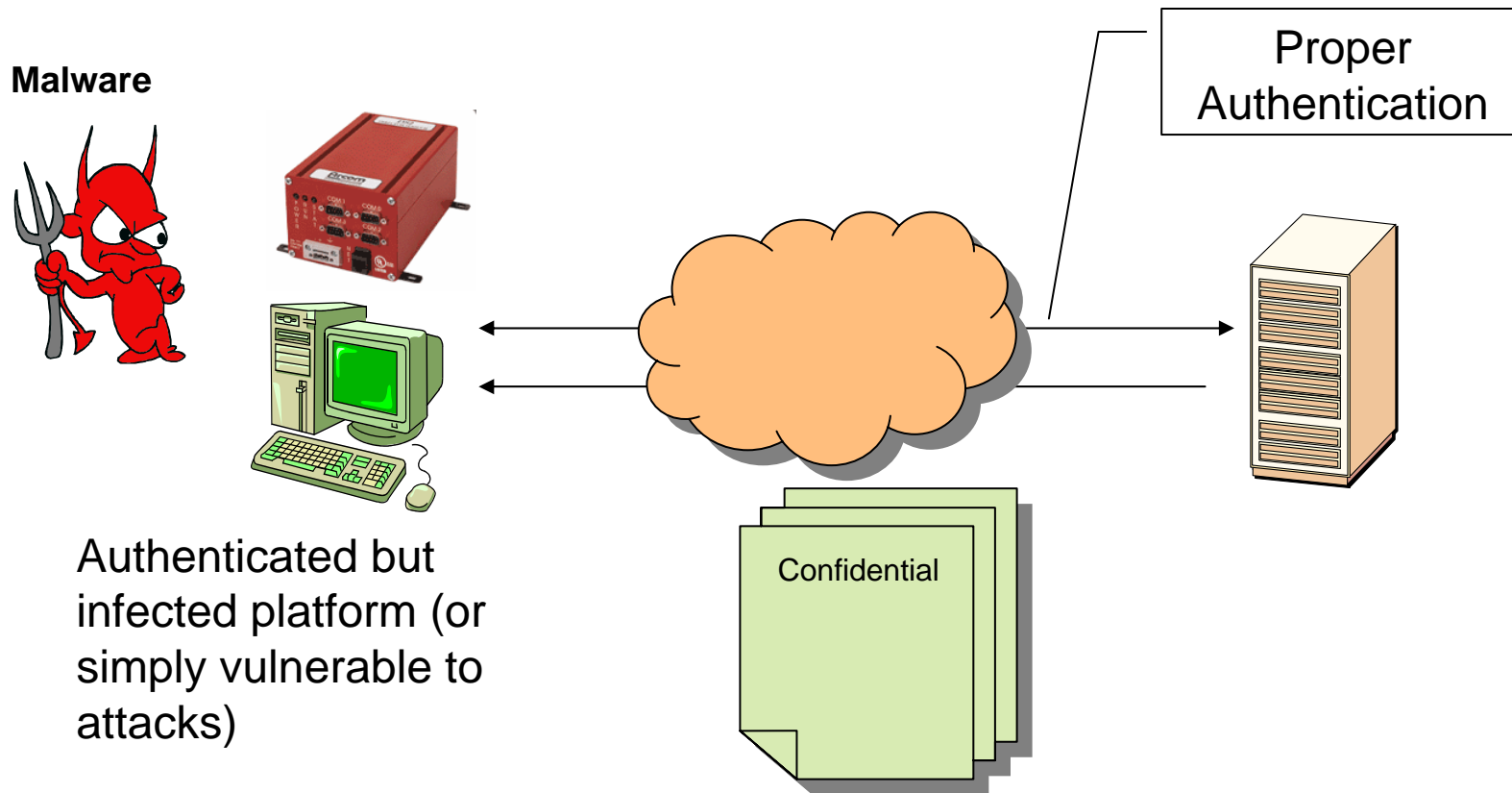


Trusted RFID Gateways

Backup

- Integrity Protection by TPM/TCG
- Implementation Details

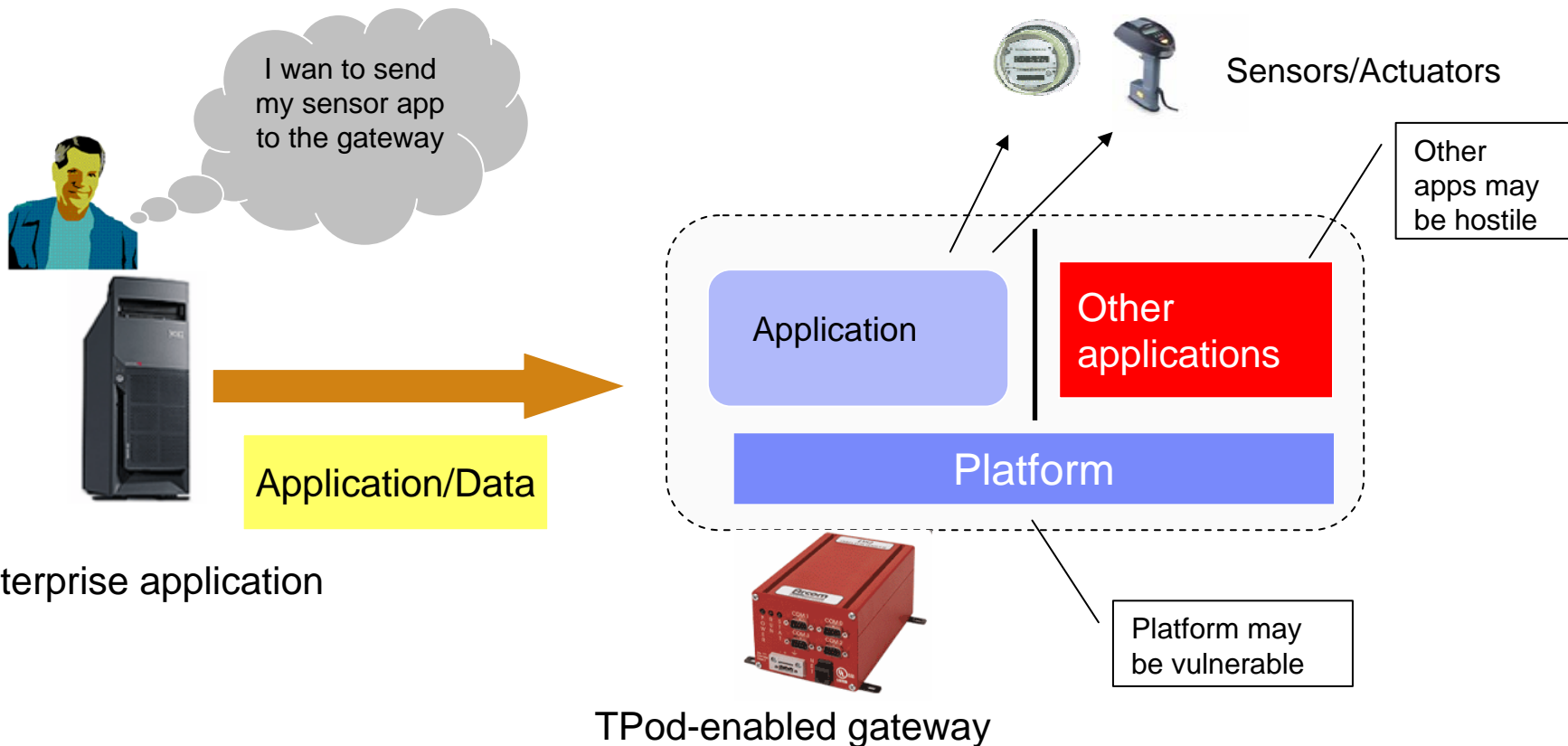
Limitation of Authentication



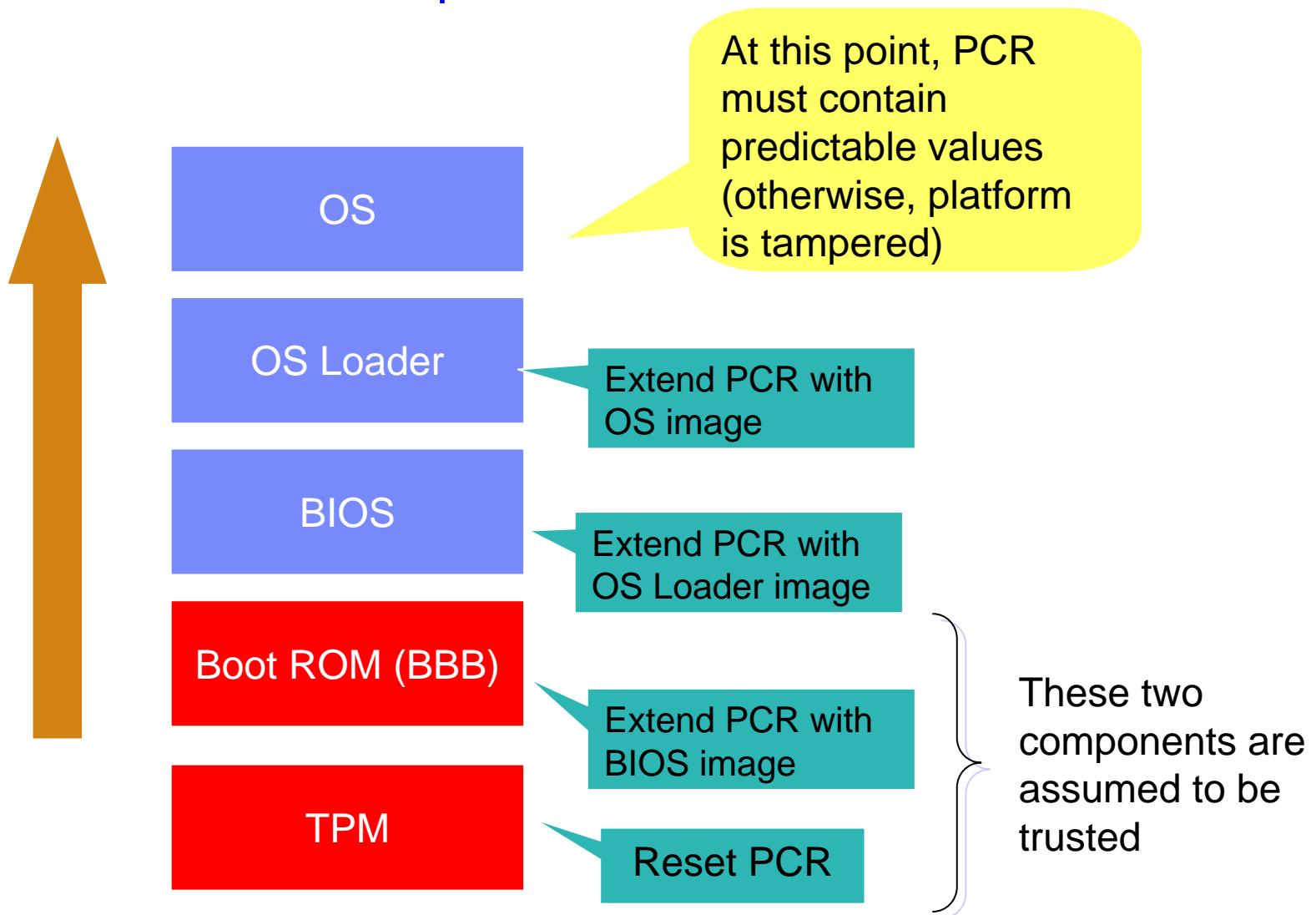
If the platform is general purpose, there is no way to prevent malware from simulating the proper authentication

Trusted Platform on demand (TPod) provides a secure way to execute software on a remote platform

- *Remote Protected Execution Environment* – Its data and execution is protected
 - ◆ Other apps may be hostile
 - ◆ Platform may be vulnerable

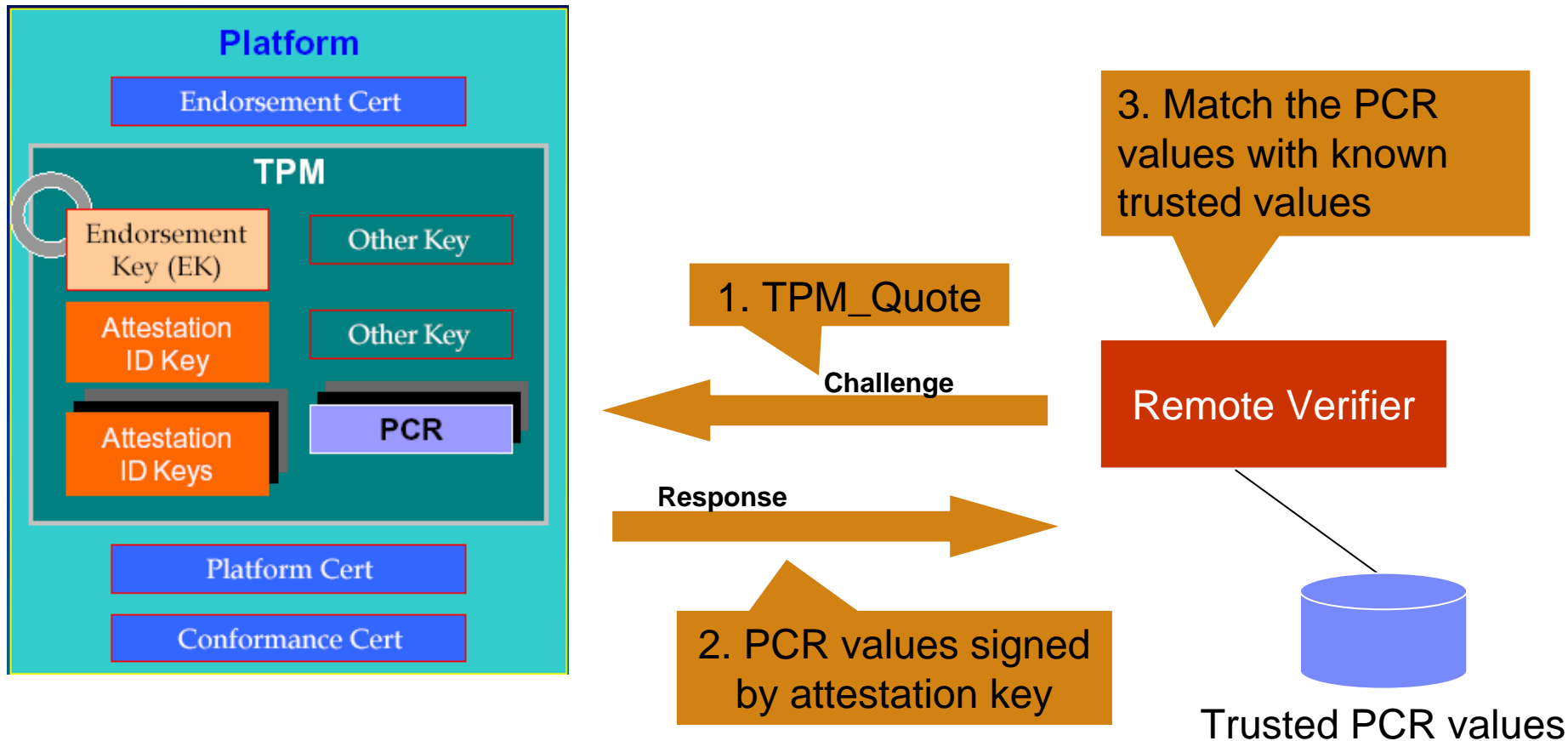


Measured Bootstrap with PCR



TPM Quote Function

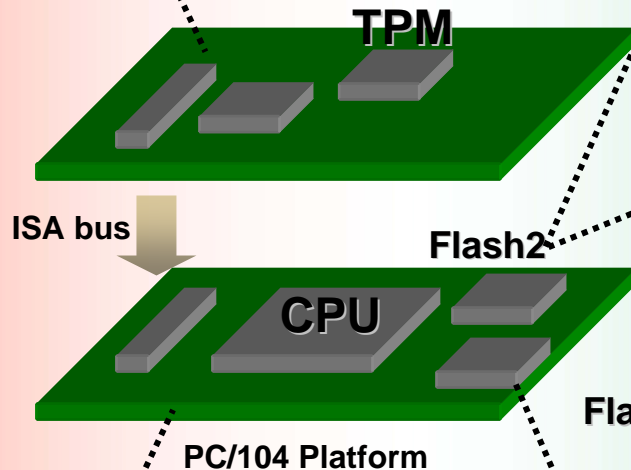
- Integrity of the platform can be remotely verified



Trusted Linux Gateway – Components

PC104 TPM Daughter Board

TPM : Atmel AT97SC3201S
 I2C bus controller : Philips PCA9564
 Battery backup (for RTC)



Arcom Viper

CPU: Intel XScale (PXA255 400MHz)
 Memory: 32M Flash, 64MB SDRAM
 Platform: PC104

Java Middleware

With Integrity Check Capability

TCG Enabled Linux

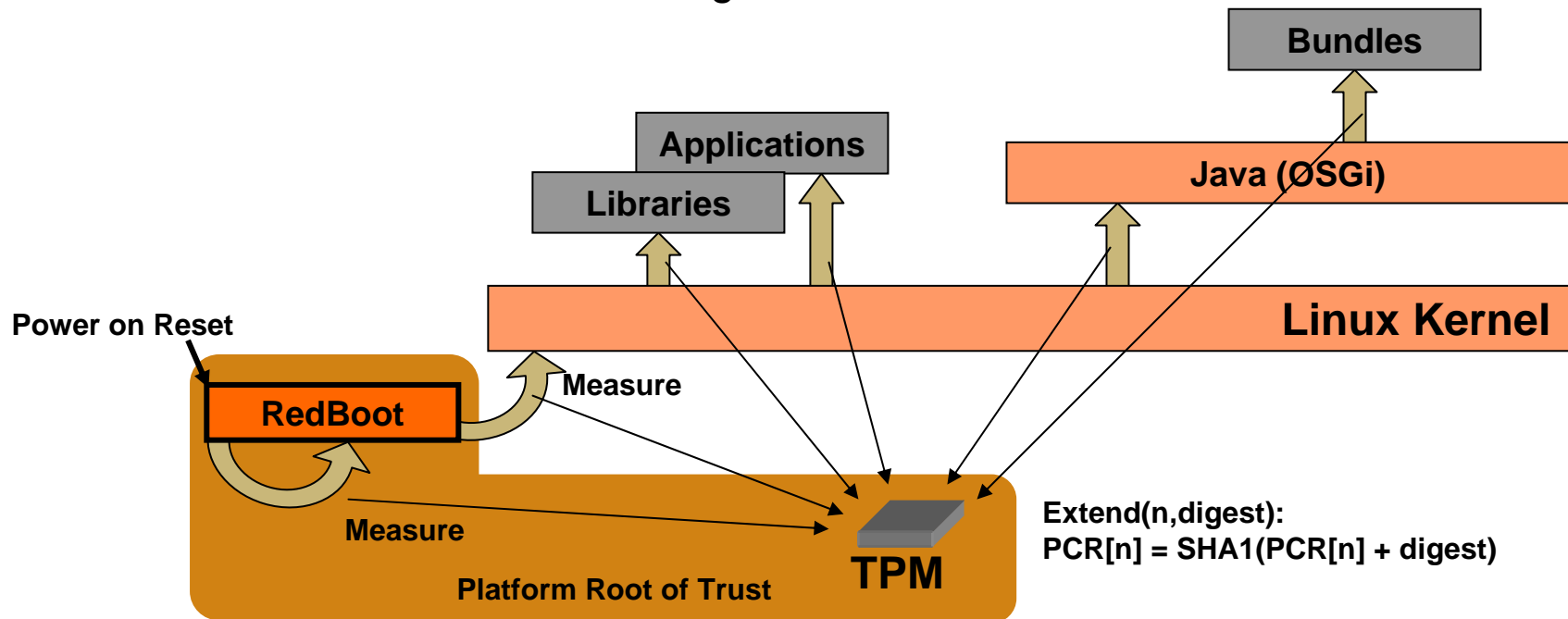
TPM Device Driver and TSS
 LSM Modules: IMA and LIDS

Boot Flash

Work as CRTM
 (Core Root of Trust Measurement)
 TCG Enabled RedBoot

Transitive Trust

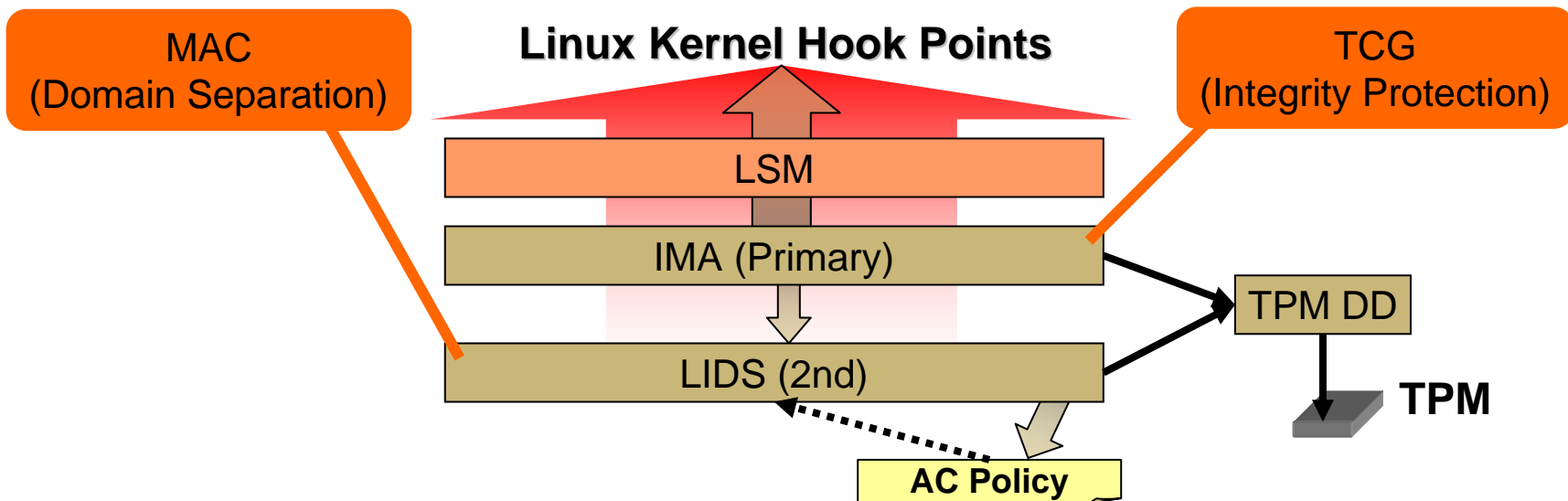
- Integrity Measurement Strategy
 - RedBoot measure itself and Kernel Image
 - Kernel measures Executables, Shared libraries and Loadable Kernel Modules
 - The OSGi bundle loader measures integrity of each bundle JAR file before loading it



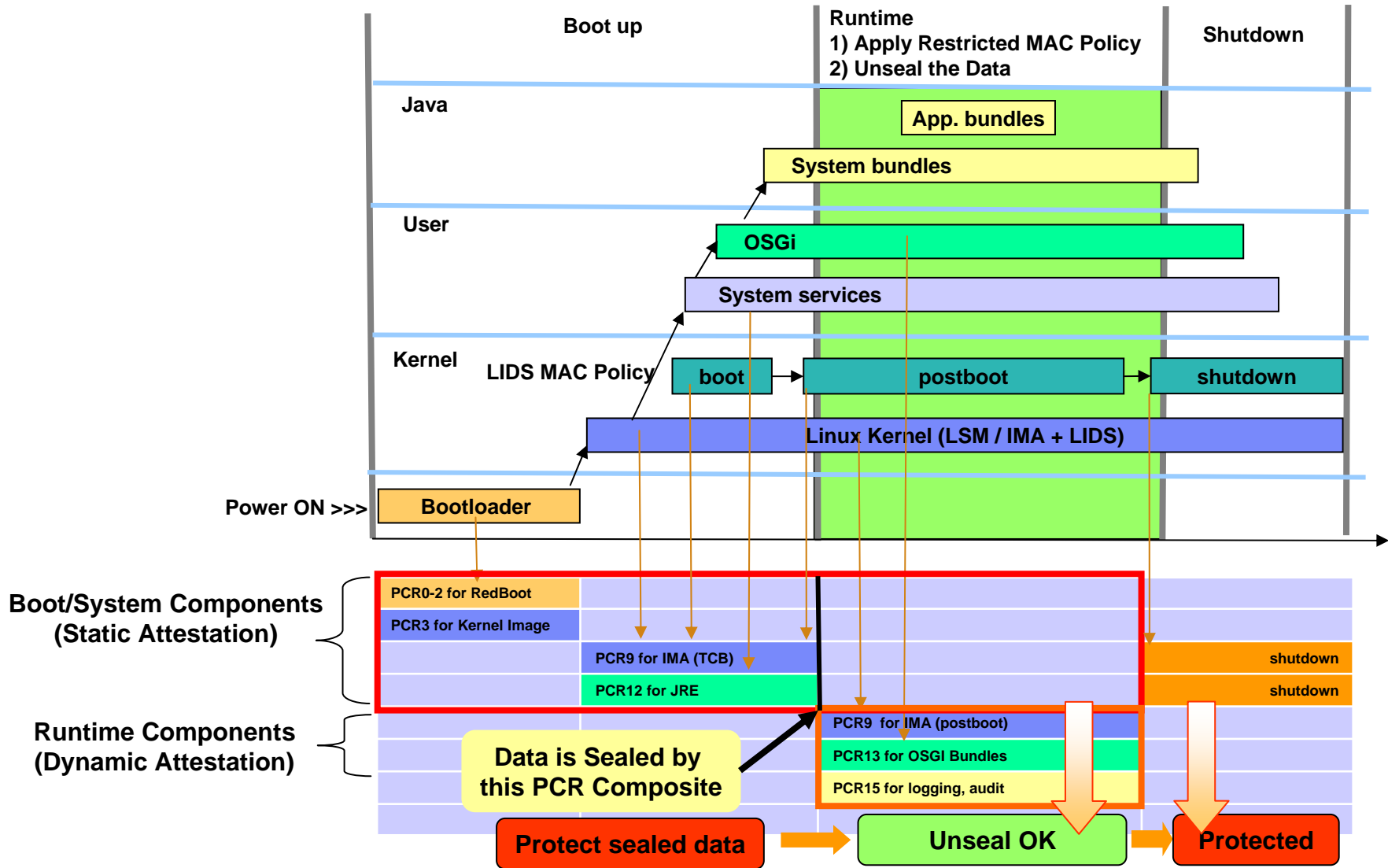
Linux - Security Enhancement

- LSM (Linux Security Module)
 - LIDS (Linux Intrusion Detection System)
 - ♦ MAC Policy Enforcement
 - IMA (Integrity Measurement Architecture)
 - ♦ Integrity Measurement

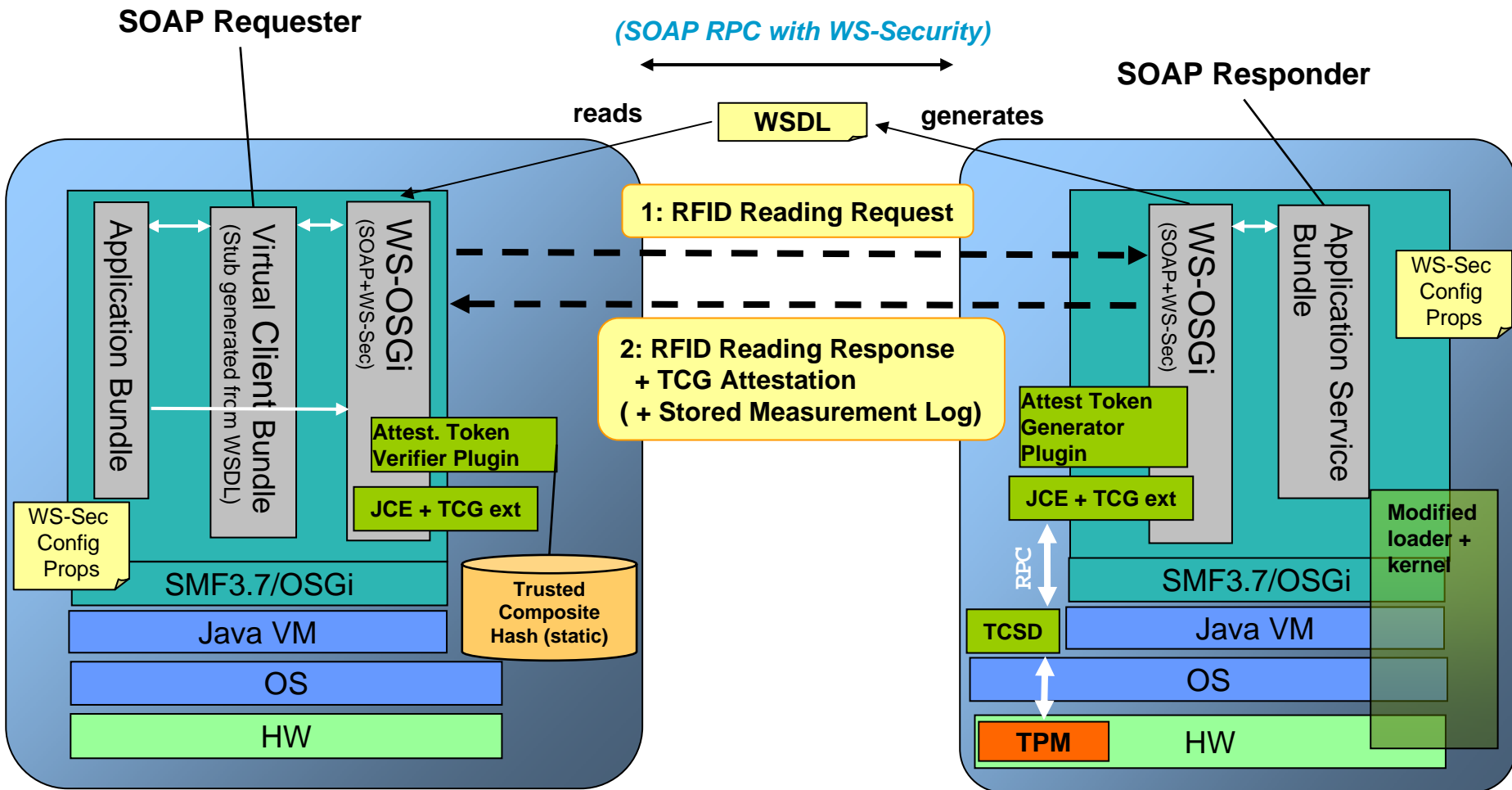
Stacked!



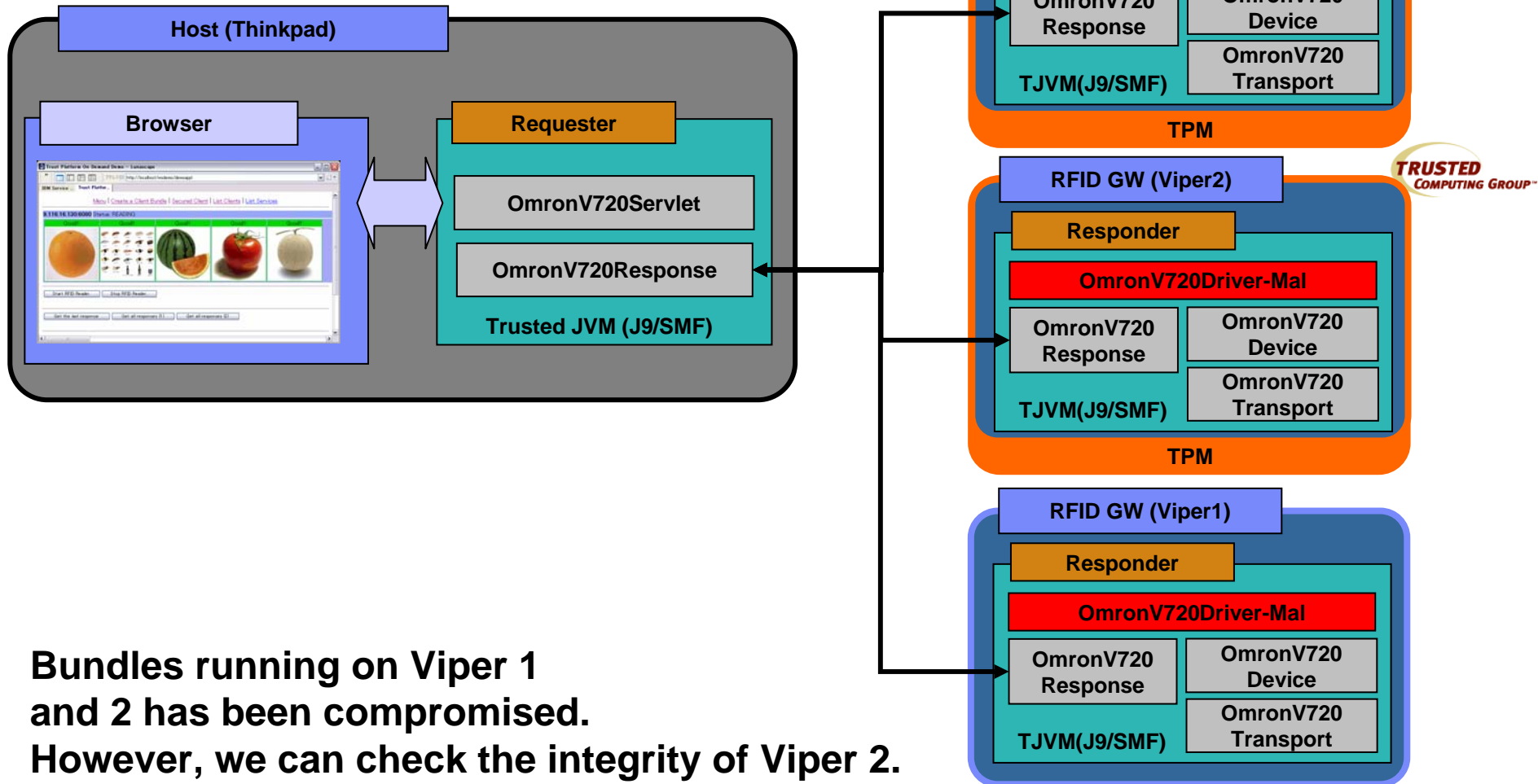
State transition, PCR usage and Data Protection



WS-Assurance: Prototype WS-Attestation Implementation



Demo System Configuration: OSGi RFID Bundles



Bundles running on Viper 1 and 2 has been compromised. However, we can check the integrity of Viper 2.