ハードウェアと連係した高信頼コンピューティング
～Trusted Boot を使ったルートキット検出～

ソフトウェアセキュリティ研究チーム
須崎有康

Research Center for Information Security

高信頼コンピューティング≠安全

- 安全であることを保証するものではなく、意図した処理が確実に行なわれること確認する。
  - 意図しない処理(ルートキットなど)を見つけることができる。

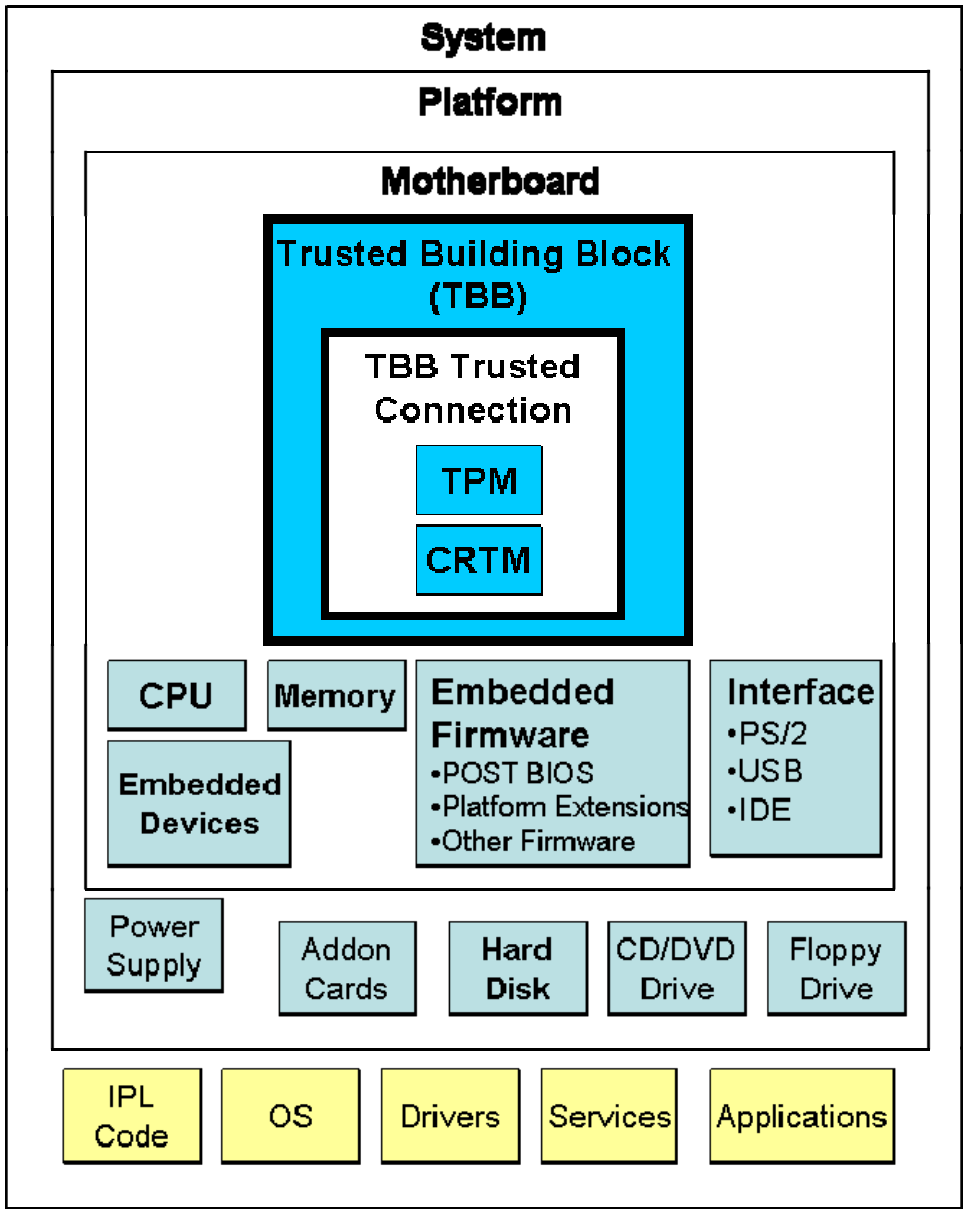
- 高信頼コンピューティングのために
  - 個々のPC内処理を確実に記録する。
    - CPUとは独立したデバイスで保障する。
  - 記録は信頼できる第三者機関(Trusted Third Party)によって検証される。

高信頼コンピューティングの基盤

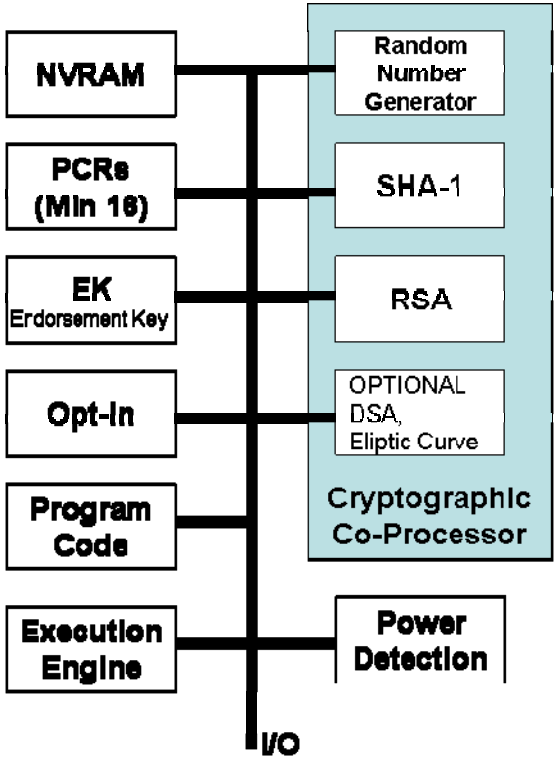
- 標準化団体 TCG (Trusted Computing Group)により規格さている
  - Promoter: ディレクタになれる。8社
    - Intel, HP, IBM, Microsoft, AMD, SUN, Infenion, Lenovo
  - Contributor: 投票権あり。73社
    - Fujitsu, Hitachi, NEC, Panasonic, Renesas, Sony, Toshiba
  - Adaptor:　情報にアクセスできる。

- セキュアチップTPM (Trusted Platform Module)などハードウェアを信頼の基として意図した実行を行なう。

高信頼コンピューティング行なうためのPC構成

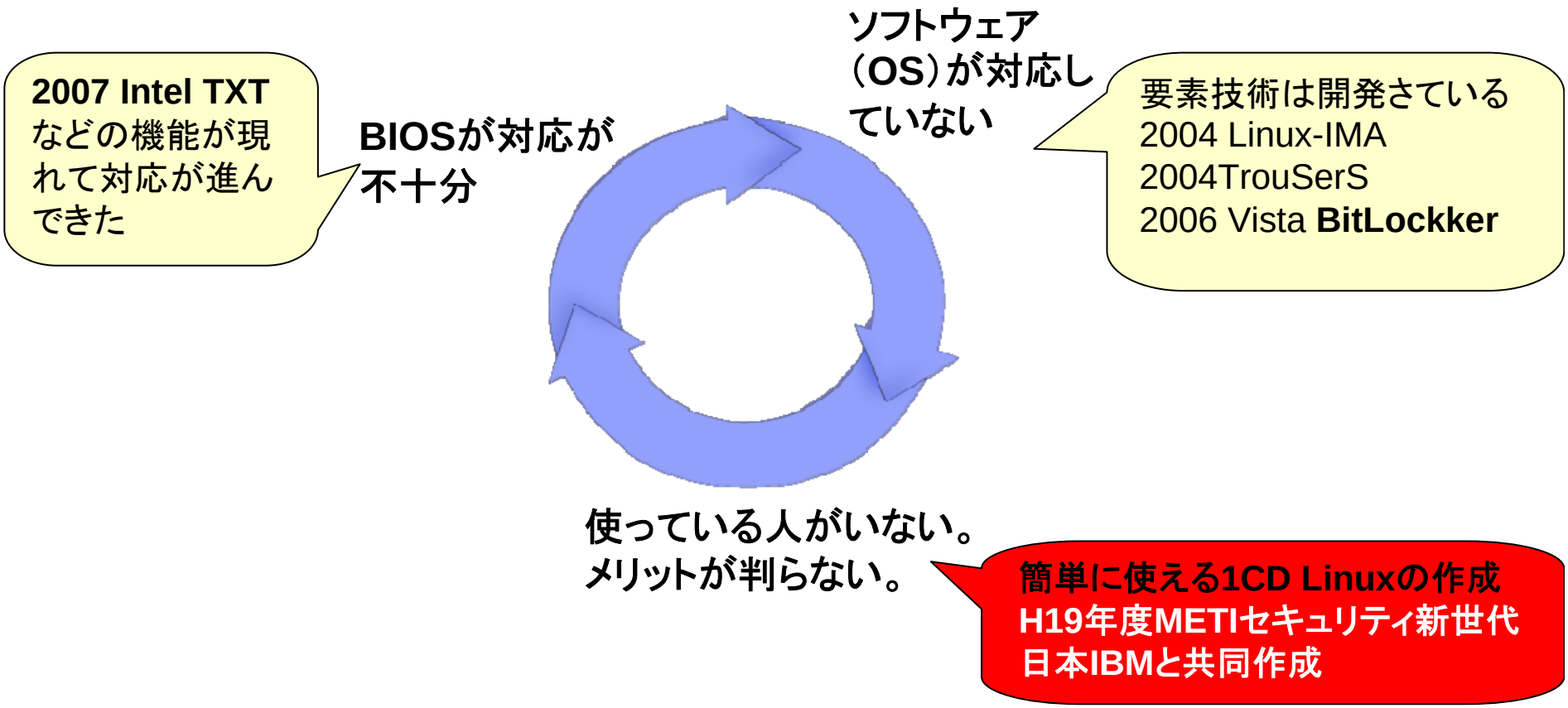


TPM内の構成



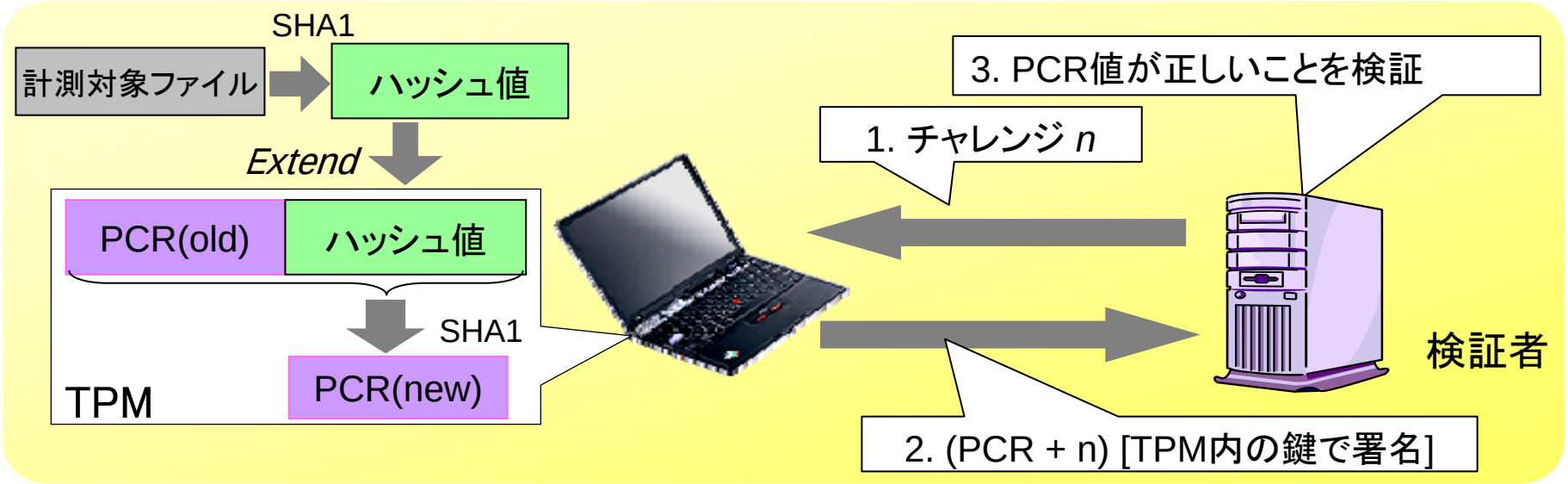
高信頼コンピューティングの現状

- TPMは普及しているが、その活用は不十分。



提供する高信頼コンピューティングのシナリオ

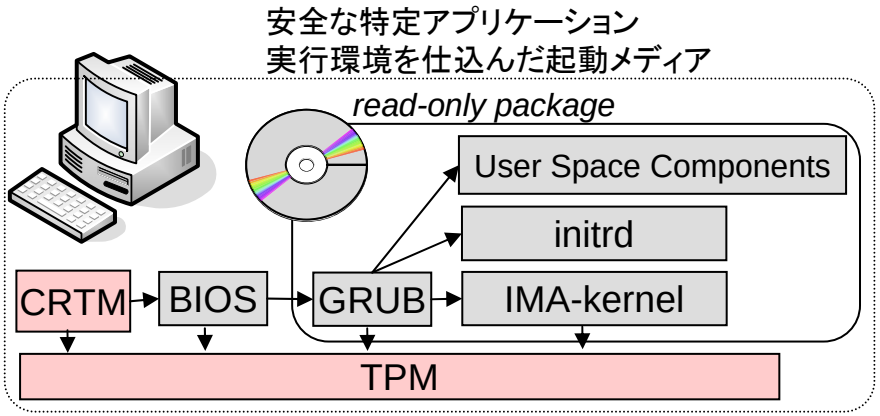
- クライアント側で正しくブートシーケンスを計測
  - TPMによる記録
- 外部のサーバ(Remote Attestation)での検証
  - 意図した起動 (Trusted Boot)であることの検証
    - これにより、ルートキットなど混在を発見する。
  - アプリケーションの脆弱性データベース検証
    - 脆弱性のあるアプリケーションがインストールされているか確認

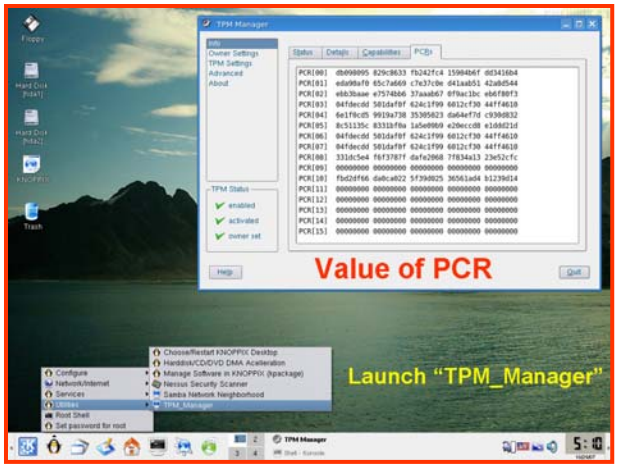


KNOPPIX for Trusted Computing Geeks

- クライアント (KNOPPIX TC-Geeks)
  - GRUB-IMA (Bootloader with Integrity Measurement Architecture)
  - Linux-IMA (kernel with Integrity Measurement Architecture)
  - TrouSerS (Open-source TCG Software Stack)
  - OpenPTS (Open-source Platform Trust Services)

- サーバ (Remote Attestation)
  - OpenPTS (Open-source Platform Trust Services)
  - 完全性情報データベース
    - IIDB (Integrity Information Data Base)
  - アプリケーションの脆弱性情報データベース (DSA: Debian Security Advisory)
    - VULDB (Vulnerability Data Base)

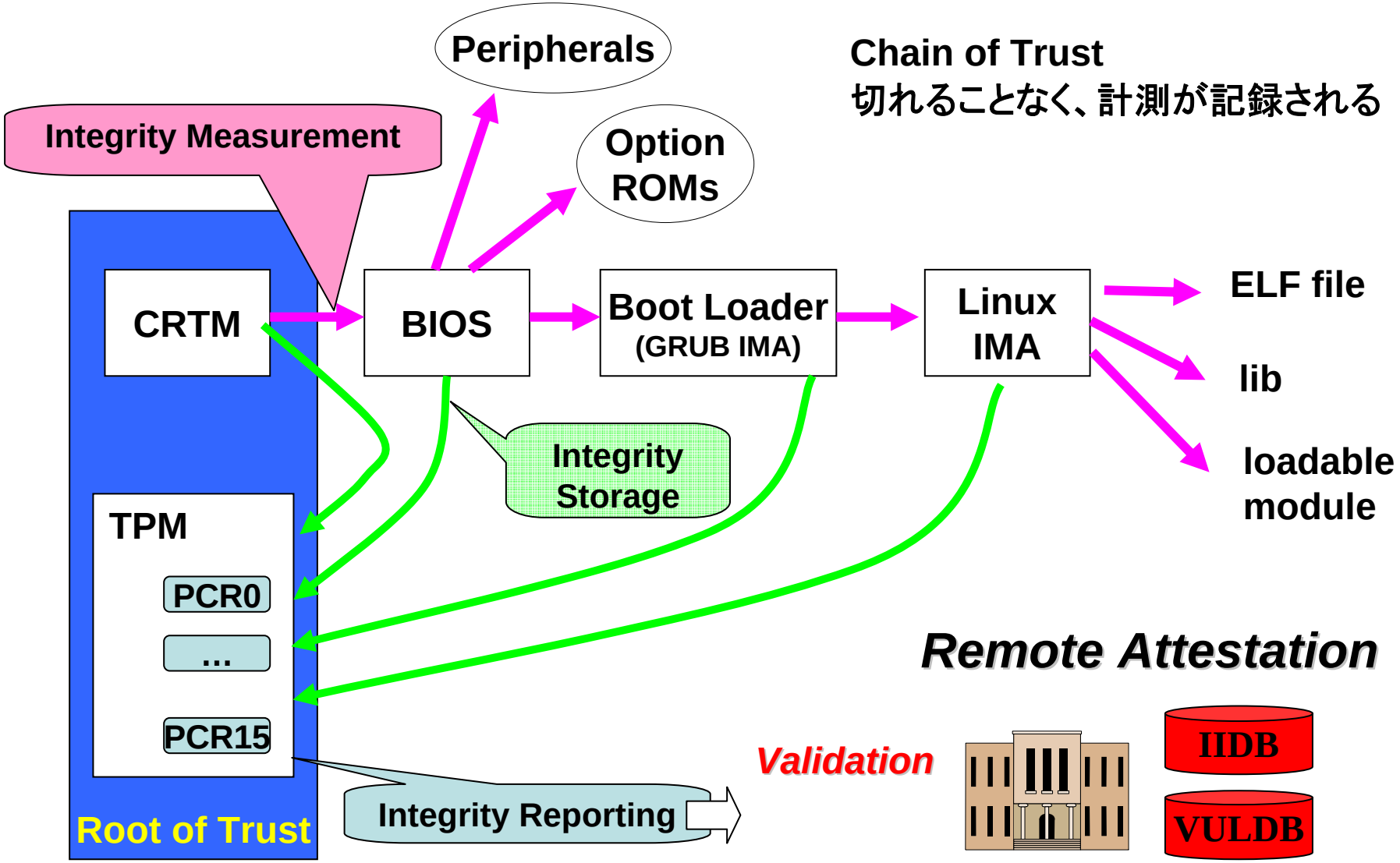




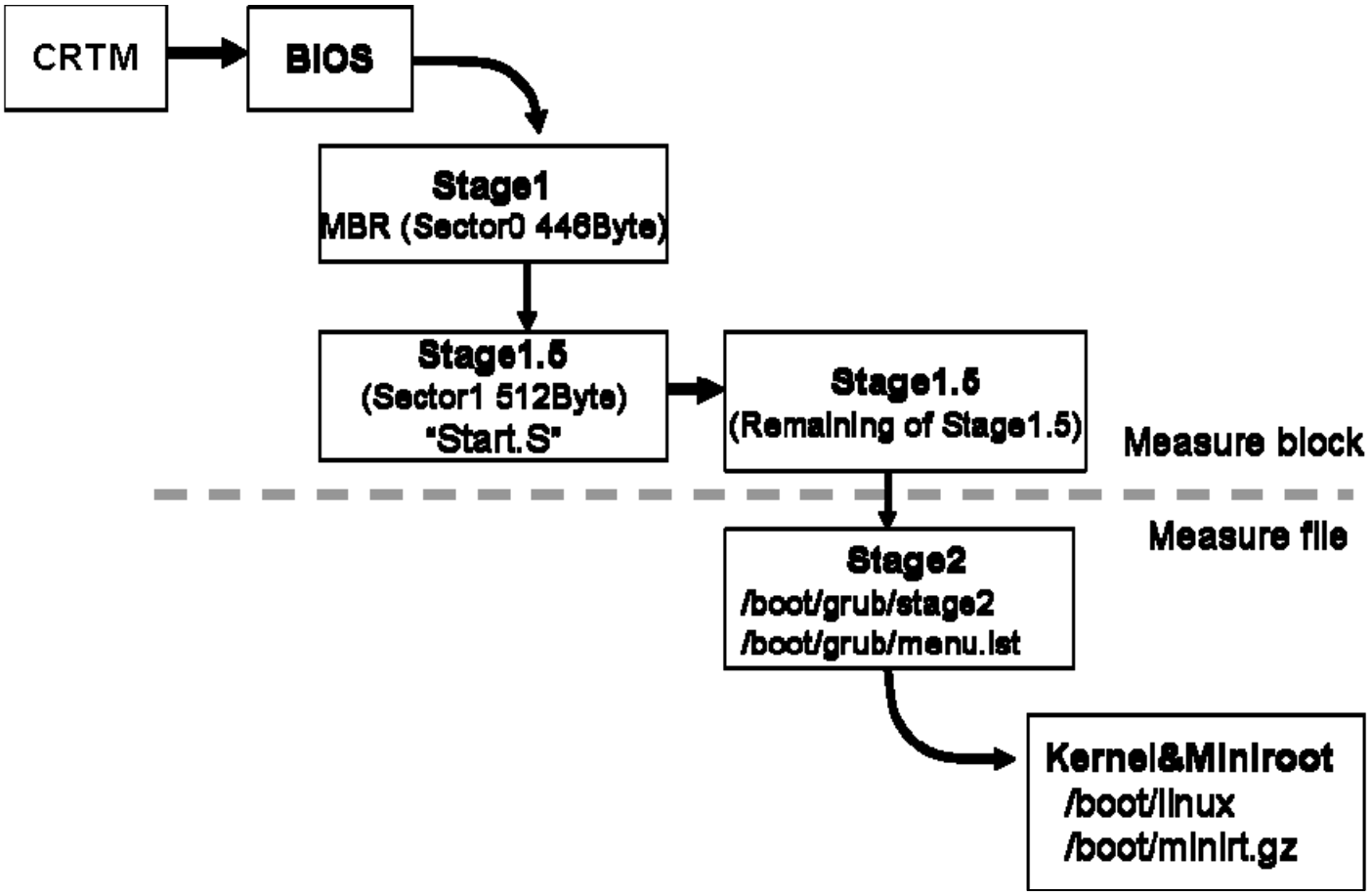
Trusted Boot

- TPM を基点とする高信頼な起動方法
  - TPMはpassive deviceであり、TPM自体が能動的なセキュリティを確保するものではない。
    - 外部に出ない固有の鍵、内部での暗号化などを行なう。
      - **CPUとは独立**しており、暗号化はTPM固有のものとして外部に伝達できる。
    - 外部の検証機関(Remote Attestation)を通して、**起動の完全性検証**が可能。
  - 個々の各デバイスやファイルを計測し、TPM内のPCR (Platform Configuration Register)に保存

Trusted BootでのTPMの役割



GRUB-IMAによる計測



計測: Measurement

- 各デバイスやファイルは起動時に計測され、そのSHA1 digestをTPMのPCR (Platform Configuration Register)に “Extend” により記録する。
  - **Extend**
    - **PCR(i) = SHA1(PCR(i) +Digest)**
- PCR の利用法はTCGにより規格化されている。

PCR	Function
0	CRTM, BIOS, and Platform Extensions
1	Platform Configuration
2	Option ROM Code
3	Optional ROM Configurations and Data
4	IPL Code (Usually the MBR)
5	IPL Code Configuration and DATA (for use by the IPL code)
6	State Transition and Wake Events
7	Reserved for future usage. Don't use.
8-15	Flexible use

Trusted BootのBIOS/ブートローダログ

– **/sys/kernel/security/tmp0/ascii_bios_mesurements**

PCR ↓　SHA1 ↓　Event ↓

```
3 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
4 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
5 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
6 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
7 2907b0a74e2e025f863bda3dd55a9ada385dcf28 04 [Event Separator]
4 c1e25c3f6b0dc78d57296aa2870ca6f782ccf80f 05 [Calling INT 19h]
4 38f30a0a967fcf2bfee1e3b2971de540115048c8 05 [Returned INT 19h]
4 7ca42b22324927c400263bae94e1e7cc28655532 05 [Booting CD ROM]
4 5c3eb80066420002bc3dcc7ca4ab6efad7ed4ae5 01 [POST CODE]
4 1cdac212c5342627905cfcc4931972a8b4a09996 0d [IPL]      /boot/grub/stage2_eltorito
4 2cedbf54913d69d027c5b97e02763f921b16e345 06 []
4 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 f1f74d078d57197ee9cd9205995a6ba5e6a68cbf 0e [IPL Partition Data]   /boot/grub/grub.conf
5 aed235d4ddb5fed00156f4991f2c1d1330c97694 1105 []
8 94c417906f8d383b811d918dce6bafdbc650ed42 1205 []    /boot/isolinux/linnux-ima
8 793eb4a591229afe35d60d5c2b66cee9dc33225c 1405 []   /boot/isolinux/minirt-ima.gz
5 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 fac33a1fc0ad42c07d00322d64c23f67567f334a 1005 []
```

Measured files

Trusted BootでのOSの役割

- Linux IMA (Integrity Measurement Architecture)カーネルによる計測
  - ELF, lib, module ファイルがオープンされるとその値をPCRに保存すると共にログを残す。

  - **/sys/kernel/security/ima/ascii_runtime_mesurements**

PCR SHA1 Event

↓ ↓ ↓

```
10 eeb9e57fc3a66e85858585329c7291a2e138d695 boot_aggregate
10 4cd410cbd7766b0672dfeb0b73756c490c1262b6 /static/ash
10 449c076c8bbde638c37e075d63ccd7a6ac6602a0 /static/insmod
10 06dd0a423bd7d35ea2388c481a329b34552db3c0 pas16
10 23a1ba028254b2d5c14f7d6240764706f83bcaa9 psi240i
10 0fa2ec2a67a3e33ea062f4715b1a0d566fe5ce83 t128
10 b55dfa9b2ab368b7f2d839b39dd69613c69a0d56 u14_34f
10 c68b8de398d26abf41989364eb77be153464cd87 wd7000
10 cccf8dc1ff3748dcfa8c4d145a461a3deda6431d usbcore
10 0a2447092eb5d5b337cccfe2afb75dcdae7c40de ehci_hcd
10 bbaa6a8dfb5fe4046c4dec4b6d3d98db15067491 uhci_hcd
```

PCR

- **/sys/devices/platform/tpm_atmel/pcrs**

```
PCR-00: 87 31 03 3F DD DB 3F DA 05 F5 07 63 21 50 B9 9B BF 6D 45 15
PCR-01: 13 02 B2 55 28 E4 B7 06 35 04 F2 6A 74 6E D2 E1 1D 17 24 3B
PCR-02: EB B3 BA AE E7 57 4B B6 37 AA AB 67 0F 9A C1 BC EB 6F 80 F3
PCR-03: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-04: 11 AF B4 D2 CC 62 91 18 80 D3 3E 51 BA 18 8A EE E9 E8 0A D3
PCR-05: 3D D4 62 3E 57 34 78 B1 EB A3 89 FE 24 5B 44 DB D0 79 70 52
PCR-06: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-07: 04 FD EC DD 50 1D AF 0F 62 4C 1F 99 60 12 CF 30 44 FF 46 10
PCR-08: 78 F7 B8 1C 1B 69 DD 24 10 4E 0C 81 59 70 FE 66 1B DD 93 46
PCR-09: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Remote Attestationによる検証

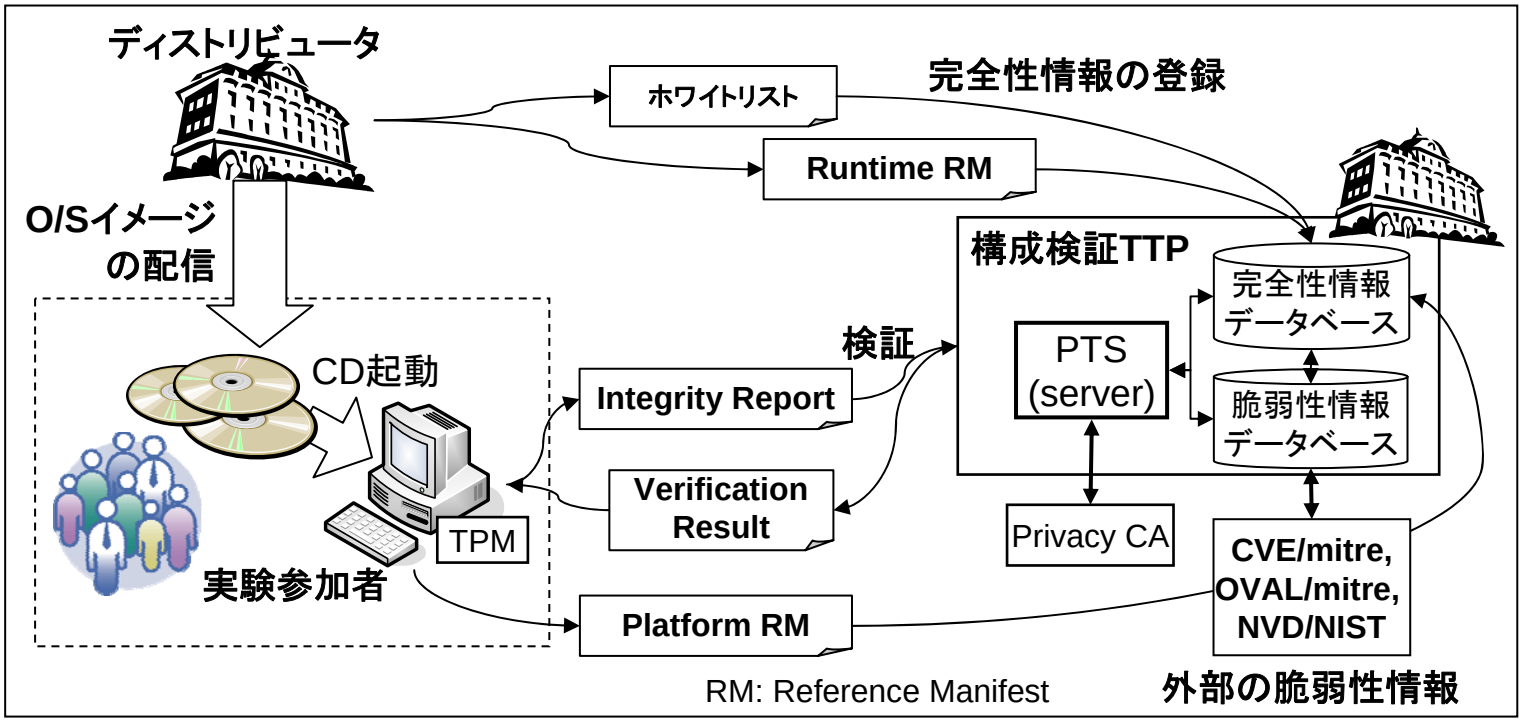
- サーバ(Remote Attestaion)によるクライアントのTrusted Bootの完全性(Attestation)検証
  - 「TPM内のPCR値」と「OSが持つ計測ログ」をRemote Attestationに送り、ログを用いてPCR値を検算する。
  - PCR値はTPM内のAIK (Attestation dentity Key)により署名されるのでCPUには干渉されない。

二つのデータベース

- IIDB (Integrity Information Data Base)
  - ルートキットが混入されてもRemote Attestationによる検出が可能。
- VULDB (Vulnerability Data Base)
  - DSA (Debian Security Advisory)の脆弱性データベースがサーバで用意されているため、脆弱性のあるパッケージも検出可能。

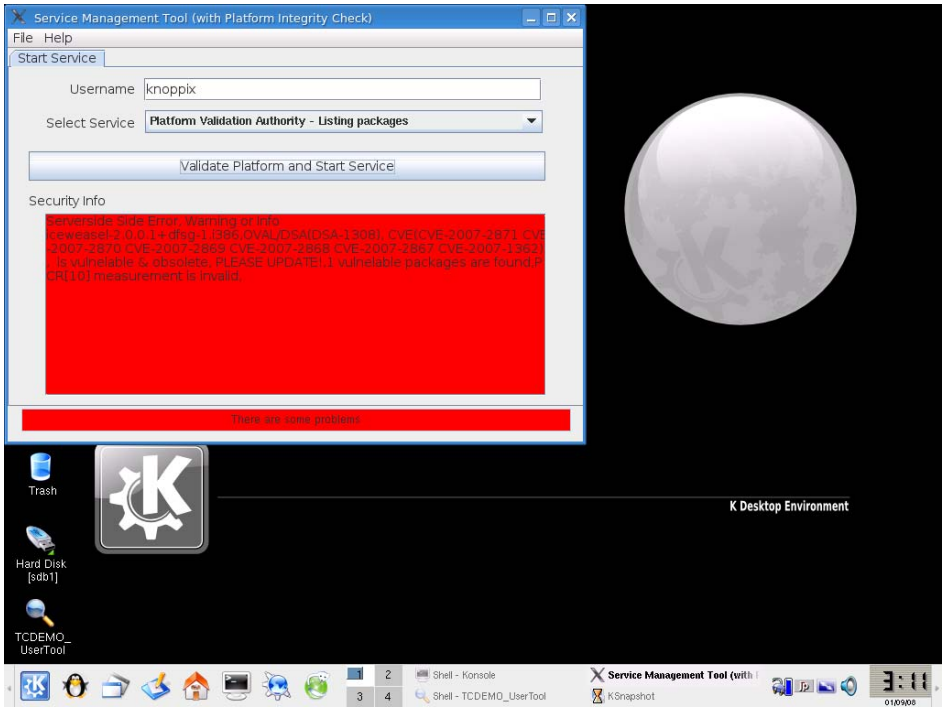
検証

- OpenPTS (Platform Trust Service) を使った完全性検証

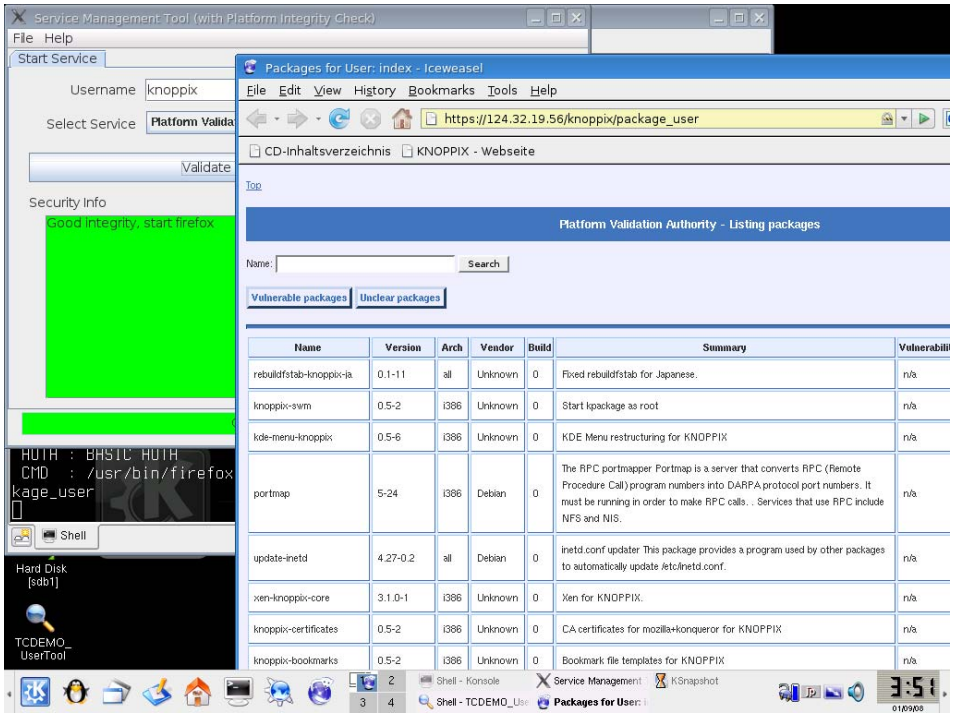


検証結果

FAIL



SUCESS



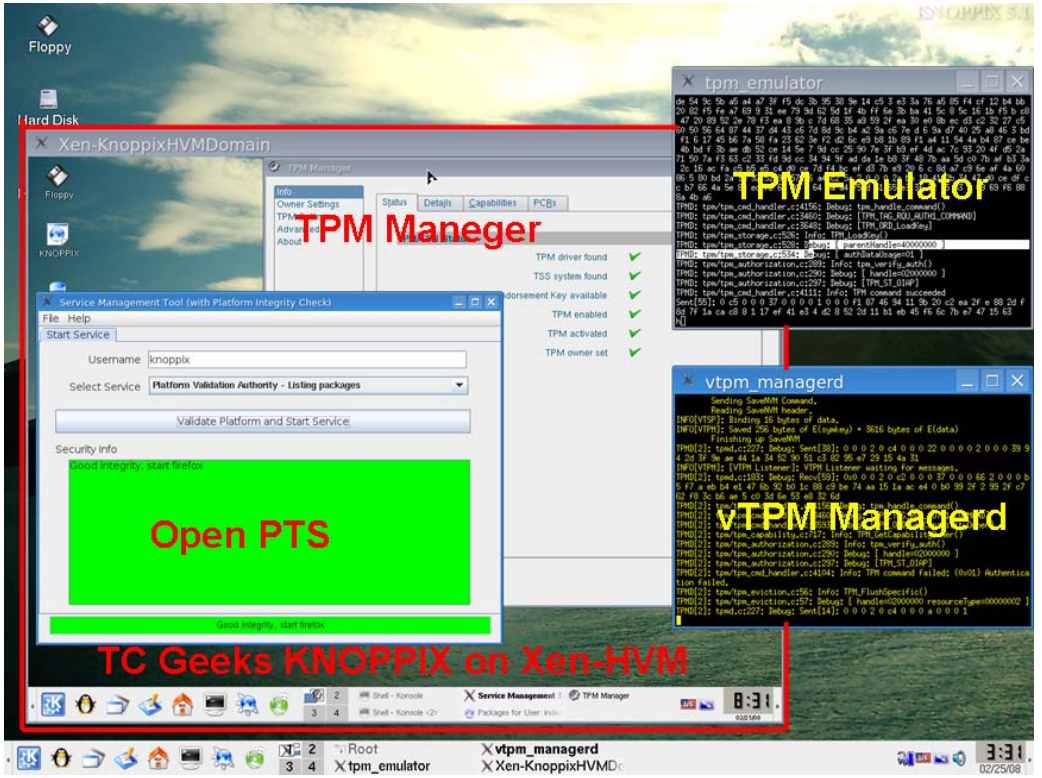
実行環境

- KNOPPIX for Trusted Computing GeeksのCDイメージは下記よりダウンロード可能
  - http://unit.aist.go.jp/itri/knoppix/iso/knoppix511-TC-Geeks-101.iso
- TCG-BIOS対応のPC
  - TPMの普及は進んでいるがBIOSの対応は不十分
  - 仮想マシンを使って対応
    - VMKnoppix

VMKnoppix with vTPM

- vTPMを使ったXen
  - 仮想化ソフトウェアを収録しているVMKnoppixではTPM-EmulatorとXen-HVMを整備して、vTPM(VirtualTPM)が使える仮想マシンを提供。
  - 物理的なTPMが無くともTPMの動作確認可能

TCG MM (2008/02 Tokyo)
でデモ展示



新しい技術/開発している技術

- DRTM (Dynamic Root of Trust Measurement)
  - 現在のSRTMではシステムの起動時のみにしかトラストチェーンを構築できないのに対し、任意の時点でトラストチェーンを作成する技術。
    - Intel TXT (Trusted eXecution Technology)で対応可能
- Trusted Internet Virtual Disk
  - ブロック単位で検証可能なネットワークデバイス”HTTP-FUSE CLOOP”を開発。
    - 科学技術振興調整費H18-20「組込みシステム向け情報セキュリティ技術」
- TCG-BIOS Checker
  - BIOSがTrusted Bootに対応できるか検査するツール
    - Nguyen Anh Quynh (AIST)が開発

まとめ

- 高信頼コンピューティングにより、改ざんされていないかを監視することで安全な計算機環境を提供する技術を構築する
- 高信頼コンピューティングは使えるハードウェアが出始めたところで、ソフトウェアの開発・運用をこれから整備しなければならない

本研究は、経済産業省 新世代情報セキュリティ研究開発事業の委託研究の一環として行っているものです