Knoppix を利用した Trusted Computing 技術の体験

宗藤誠治[†]中村めぐみ[†]八木豊志樹[††] Nguyen Anh Quynh[††] 須崎有康[††]

1. はじめに

プラットフォームのセキュリティを強化する技術として Trusted Computing (TC) 技術が注目されている．TC 技術ではハードウェアによる物理的なセキュリティ保護機能をプラットフォームの信頼の源として利用することで，そのプラットフォーム上で稼動するソフトウェアの信頼性を保障する．このためハードウェアとソフトウェアの連携が重要となる．ハードウェアについては Trusted Computing Group (TCG)[1]で仕様の標準化が進められており，セキュリティチップ（Trusted Platform Module, TPM）は現在多くの PC に搭載されている．また TC 技術を使った仮想化技術のセキュリティ確保の動きも CPU ベンダーを中心として進められている．しかしながらソフトウェア側の TC 機能への対応はまだ不十分である．そこで我々は，ソフトウェア側の対応する O/S として Linux に注目して，Linux の CD 起動拡張である Knoppix を利用した誰でも利用可能な TC 端末の実現[2]を進めている．

2. Trusted Computing 技術の概要

従来のセキュリティ技術では O/S や仮想化技術は RootKit などによる攻撃に対して決定的な対策法が無く信頼性の確保には限界があった．Trusted Computing 技術では，安価なハードウェアレベルでの保護機能により，従来のソフトウェアのみのセキュリティ対策では難しかったこうした問題に対応する．TPM と呼ばれるセキュリティチップにはソフトウェアの完全性(Integrity)を記録するために Platform Configuration Registers (PCR)と呼ばれる領域を持ち，PCR は電源投入時にのみリセット可能で，PCR への書き込みは Extend と呼ばれる特殊な命令でのみ可能である．Extend では

PCR = HASH(PCR + Digest)

という操作が本レジスタに対して行われる．したがって，起動時から記録したハッシュ値の畳み込み値が PCR であり，この PCR 値を任意の値に操作することは困難である．これが，TPM を使ったソフトウェアの完全性記録と保護の基本的な仕組みである．PCR は 16 個もしくは 24 個あり，BIOS と仮想化での PCR の割り当ては TCG により定められている．

2.1 計測技術（Trusted Boot）

TPM にソフトウェアの完全性情報を記録する方法は Trusted Boot と呼ばれる．最初に起動するコードは Core Root Of Trust Measurement（CRTM）と呼ばれ，物理的に保護されており Root of Trust の一部である．CRTM は自身と次に起動する BIOS のコードの計測と，TPM への記録を行い、BIOS へ制御を移す．このように，コードを計測し，TPM へ記録してから起動するステップを繰り返すことで，CRTM から始まる信頼の鎖をソフトウェア全体につなげる事が可能となり，結果としてハードウェア由来の信頼性をソフトウェアに与えることが可能となる．PC で動作する Linux で Trusted Boot を利用するためには，まず，BIOS が TCG 仕様に準拠していることが必要である．Linux については，Bootloader（Grub-IMA）や Kernel（Linux-IMA）を TCG の計測対応にするパッチはリリースされており，これらを組み込むことで，Trusted Boot に対応させることが可能[2]である．

2.2 検証技術

計測した結果の検証には２つの方法がある．一つは PCR の値を直接確認する方法で，PCR へのハッシュ値の記録順序が固定の場合に利用可能である．もう一つは PCR への記録をイベントログとして記録し，PCR 値自体はイベントログの検証に利用し，次にログ上の個々の記録を確認してゆく方法である．TPM には Quote と Seal/Unseal と呼ばれるコマンドがあり，Quote は PCR 値に署名を行いその結果を外部への報告に利用する（Remote Attestation）．その結果第三者による検証が可能になる．TCG ではそのために必要となる各種 XML フォーマットを規定している．Seal/Unseal は PCR の値をチェックする暗号/復号であり，データをある特定の PCR の値のときにのみ利用可能にすることができる．

† 日本 IBM 東京基礎研究所

†† 産業技術総合研究所

3. Knoppix Trusted Computing Geeks

TC 技術は本格的に利用可能な状態になりつつあるが，実際の市販 OS でのサポートには至っていない．問題点としては，1) 従来の PC では TCG 仕様への準拠が不十分で BIOS の TCG 機能の未実装やバグにより，TPM 搭載 PC でも正しい Trusted Boot が可能なマシンが限られること，2) Linux の計測手法の組み込みに Kernel の再構成が必要になること，3) O/S の振舞いすべてが計測できるわけではないこと，などの制約があげられる．

1)については TCG の仕様の向上，OS ベンダー要求により TPM Version1.2 搭載の PC から改善している．2)については，Linux Integrity Module（LIM）という，アクセス制御（LSM）とは別のフックが用意されることで，例えば SELinux と Linux-IMA を同時に利用することが可能になる．3)については通常のデスクトップ O/S では利便性との兼ね合いとなるが，CD 起動やネットワーク起動の O/S に関しては O/S 全体の計測が可能となる．Knoppix に Trusted Computing 機能を搭載した“KNOPPIX5.1.1 for Trusted Computing Geeks”を作成し公開した[2]．この利用により，インストール済み OS には変更を加えることなく，CD 起動するだけで TC 機能を体験することが可能である．

現在公開している Version では，Bootloader から Kernel, Loadable Kernel Module, アプリケーション（ELF）まですべての実行形式が TPM に記録される． また TPM Manager により，Linux-IMA でのユーザーランドの計測に伴う PCR[10]の値の変更がリアルタイムで確認できる．

表 1，収録コンポーネント一覧

Bootloader	Grub 0.97 + Grub-IMA v1.1.0.0
Linux	Kernel 2.6.19+Linux-IMA
TSS	TrouSerS v0.2.9.1
CLI	Tpm-tools v1.2.5.1
GUI	TPM Manager v0.4

今後，計測技術に関しては HTTP-FUSE による，RootFS のブロック検証[3]や，仮想化で利用可能になる Intel TXT や AMD-SVM(skinit) の Dynamic Root Of Trust Measurement (DRTM)にも対応を広げてゆく予定である．また検証技術に関しては，TCG で仕様策定中の Platform Trust Services（PTS）の搭載と Remote Attestation で必要となる検証サーバーの構築を予定している．

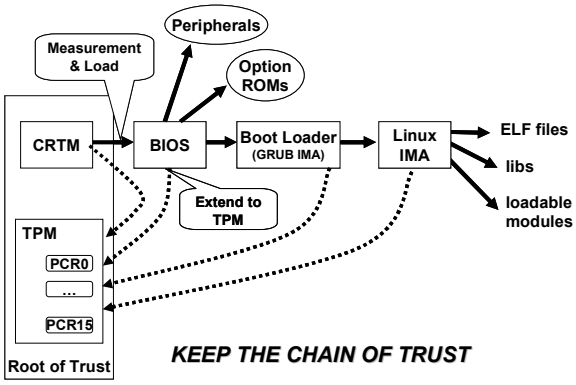

図 1， トラストチェイン

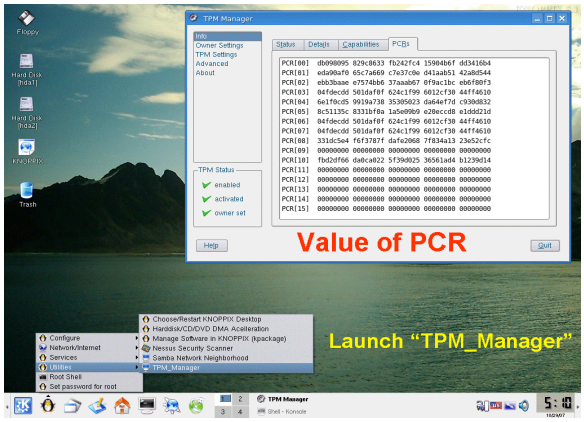

図 2， 起動画面，PCR 値の確認

4. 謝辞

TPM Manager の利用に際して，Christian Stüble とAnoosheh Zaerin に感謝します．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研究として行われたものである．

参 考 文 献

[1] https://www.trustedcomputinggroup.org/

[2] http://unit.aist.go.jp/itri/knoppix/index.html.

[3] 八木 豊志樹，須崎 有康，宗藤 誠治，中村 めぐみ，飯島 賢吾，大澤 一郎，"ブロック検証によるセキュアなインターネット起動"，第 18 回コンピュータシステム・シンポジウム(ComSys2006)，2006 年 11 月

Linux は，Linus Torvalds 氏の日本およびその他の国における登録商標または商標です．本文中の会社名，製品名およびサービス名等はそれぞれ各社の商標です