

KNOPPIX Trusted Computing Geeks での OpenPlatformTrustServices の使い方

2008-02-25 Version 1.1 for

KNOPPIX 5.1.1 Trusted Computing Geeks v1.0.1

OpenPlatformTrustServices v0.1.1

Copyright IBM Japan, Ltd. 2008

*) 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。

*) 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

変更履歴

版	日付	概要
V1.0	2008/1/29	初版 Geeks V1.0 に対応
V1.1	2008/2/25	Geeks V1.0.1 に対応、CD 作成ガイドへのリンク、6-2-4 追加

概要	4
1. OS イメージの作成	5
2. USB の準備	5
3. PC のセットアップ	6
3-1. BIOS のセットアップ画面に入り、TPM を有効化する	6
3-2. TPM を初期化する（オプション）	7
4. KNOPPIX TC Geeks 起動と初期設定	8
4-1. TPM のオーナーシップ取得とデモの初期化.....	8
4-1-1. CD を起動.....	8
4-1-2. TPM のオーナーシップ取得	8
4-1-3. デモ環境のセットアップ	9
4-2. その他の設定	12
4-2-1. キーボード.....	12
4-2-2. 画面の背景.....	12
5. デモ.....	13
5-1. 検証失敗 & アプリの更新 編.....	13
5-1-1. 最初の検証（失敗します）	13
5-1-2. 脆弱性にあるパッケージの更新.....	14
5-1-3. 設定の USB への保存.....	14
5-1-4. 再起動	14
5-2. 検証成功 & デモサービス 編.....	15
5-2-1. 起動.....	15
5-2-2. 検証成功.....	15
5-2-3. デモサービスについて.....	16
6. 既知の問題点、トラブル対策	17
6-1. 既知の問題点	17
6-1-1. TPM Manager で TakeOwnership すると、SRK 認証で失敗.....	17
6-2. トラブル対策	17
6-2-1. KNOPPIX (Grub) が起動しない	17
6-2-2. KNOPPIX (OS) が起動しない.....	17
6-2-3. ユーザーツールが起動しない.....	18
6-2-4. ユーザーツールの Select Service で Listing Measurement を選ぶと、サーバーに接続しない.....	18
付録 プラットフォーム情報	19

概要

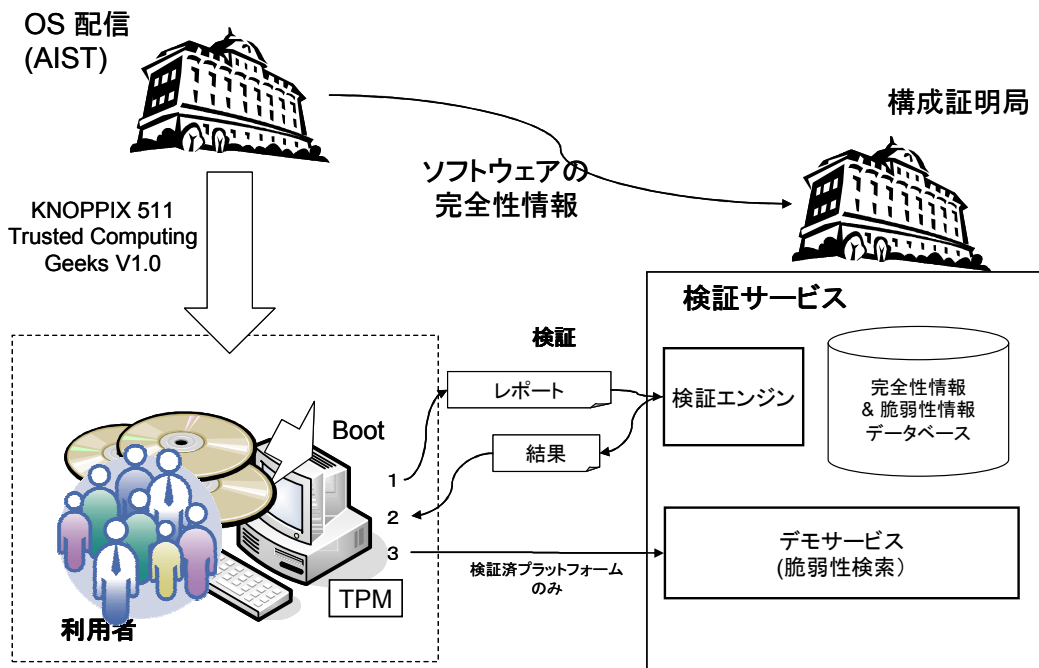
CD 起動型 OS、KNOPPIX を利用した、Trusted Computing の基本技術の一つ、Remote Attestation を体験するデモです。実験で利用する KNOPPIX には Trusted Boot の機能と、Remote Attestation の Client 側の機能が組み込まれており、インターネット上の Remote Attestation 検証サーバーによる検証が可能です。検証が成功した場合(脆弱性や不正な改ざんが無い場合)には、デモのサービス(脆弱性の検索サービス)を利用することが可能です。

利用者は KNOPPIX の OS イメージをダウンロードし、起動用の CD を作成します。初期設定が終わった端末は、下図に示すように、計測結果のレポートを作成し、検証サーバーに送付します。検証サービスでは、KNOPPIX に含まれる各種ソフトウェアの完全性(ホワイトリスト)が保存されており、レポートに含まれている情報を元にユーザーが利用している端末とソフトウェア完全性を確認します。また、データベースを用いて脆弱性の有無も確認します。今回、この検証が OK だった場合には、実証実験サーバーで稼動している脆弱性検索デモ・データベースの利用が可能となります。

また、動いた、動かない、などの情報を、下記メーリングリストなどに寄せていただくと助かります。

日本語 <http://lists.sourceforge.jp/mailman/listinfo/openpts-jpusers>

英語 <http://lists.sourceforge.jp/mailman/listinfo/openpts-users>



1. OS イメージの作成

TCG 関連機能と OpenPlatformTrustServices を組み込んだ KNOPPIX が <http://unit.aist.go.jp/itri/knoppix/> からダウンロードできます。

利用できる PC ですが、

- TPM 搭載の PC であること
- トラステッドブートに対応していること (BIOS の対応が必要、対応の状況は付録の「プラットフォーム情報」に一覧があります)
- TPM をまだ利用していないこと (すでに Windows の BitLocker などを利用している場合は、同時に利用することが出来ません)

上記の PC をお持ちの場合、まず、ISO イメージを上記サイトからダウンロードし、CD を作成します。付録の「プラットフォーム情報」に記載されている情報は限定的です。記載されていない PC でも試すことは可能です。

ISO イメージから CD を作成する方法は下記の Ubuntu のガイドが参考になります。

「Ubuntu Tips/インストール/ISO イメージを CD-R(W)に書き込むには」
<https://wiki.ubuntulinux.jp/UbuntuTips/Install/BurningISO>

2. USB の準備

TPM 内部に保存される RSA 鍵は EK と SRK の 2 つのみでその他の鍵は TPM の外で管理されます (外部保存される鍵は SRK で暗号化されていますので安全です)。こうした鍵は TSS で管理されますが、CD には保存できないため、USB メモリを利用します。KNOPPIX の場合、UNIONFS を利用することで、書き込み可能なファイルシステムを実現していますので、TSS の管理する鍵ファイルも UNIONFS 上で管理すると、再起動の際にも継続して TPM と TPM の鍵を利用することが可能になります。USB の容量は 以下の実験を行うのであれば 128MB あれば十分ですが、継続して利用する場合は、容量の大きなものが望ましいです。また、高速な USB ですと動作が速くなりますのでお勧めです。

3. PC のセットアップ

製品出荷時に TPM の機能は無効化されています。まず、PC 起動時に BIOS セットアップメニューに入り、TPM を有効にします。

(すでに TPM を有効化している場合は、いったん、BIOS のメニューで TPM をクリアしてから以下のセットアップ作業を進める事をお勧めします。)

3-1. BIOS のセットアップ画面に入り、TPM を有効化する

起動時に F1 (IBM, Lenovo 社製 PC 等) ,F2(Panasonic 社製 PC 等) キーを押すと BIOS の設定画面になります。一般には、セキュリティのメニューに TPM の有効化の設定があります。標準状態では無効化されているため、有効化しておきます。

ベンダー	BIOS メニューの起動キー	TPM 設定メニュー	その他
IBM/Lenovo	F1	Security -> IBM Security Chip	
Panasonic	F2	Security tab -> Embedded Security (TPM)Sub-Menu -> Embedded Security Chip -> Enable	TPM を有効化する場合、スーパーバイザー PW の設定が必要
HP	F10	Security menu -> System Security -> Embedded Security Device Support	TPM を有効化する場合、セットアップ PW の設定が必要
DELL	F2		
NEC	F2		

その他の PC については以下のサイトを参考にしてください

http://www.michaelstevensstech.com/bios_manufacturer.htm

3-2. TPM を初期化する(オプション)

すでに TPM を有効化している場合には、TPM の初期化が必要になる場合があります。この場合、初期化前の TPM で作成された鍵はすべて利用不可能になりますので、現在も利用中の場合については初期化を行わないでください。

TPM の初期化の方法は、まず PC をコールドブート(電源 OFF の状態から起動)します。次に BIOS メニューに入り、TPM のクリアを行います。

注意: Panasonic 社製 PC の場合、TPM をクリアすると、TPM が無効化になるので、再起動時にもう一度 BIOS メニューに入り、TPM を有効化します。

4. KNOPPIX TC Geeks 起動と初期設定

デモを始める前に、TPM のオーナーシップの取得とユーザー環境のセットアップを行います。

4-1. TPM のオーナーシップ取得とデモの初期化

4-1-1. CD を起動

Grub の画面で、以下のどれかを選択し、起動してください。

GRUB のメニューエントリー	コメント
KNOPPIX (2.6.19.1+ima)	通常、例) Thinkpad T60, Panasonic W7
KNOPPIX (2.6.19.1+ima, fdev 1024x768)	新しいグラフィックチップの PC
KNOPPIX (2.6.19.1+ima, vesa 1024x768)	新しいグラフィックチップの PC、例) Thinkpad X60, Dell OptiPlex 755, HP dc7800 等

しばらく待つと、標準のデスクトップ画面が表示されます。

4-1-2. TPM のオーナーシップ取得

コンソールを起動し、TPM のオーナーシップの取得と管理用 GUI ツールを起動します。

```
$ tpm_takeownership
Enter owner password: *****
Confirm password: *****
Enter SRK password:
Confirm password:
```

注意: SRK のパスワードは Enter だけ入力してください(この場合、パスワード無しの SRK が生成されます)。収録されている GUI ツール、TPM Manager でオーナーシップの取得を行うことも可能ですが、その場合には、既知のパスワードを用いた SRK が生成されるため、互換性がありません。そのため、tpm_takeownership コマンドを利用してください。

4-1-3. デモ環境のセットアップ

以下のコマンドをコンソールから入力し、デスクトップ上のアイコン作成との管理者ツールを起動します。

```
$ cd /opt/OpenPlatformTrustServices/tcdemo
$ make setup-desktop
$ sudo make start-client-admin-gcj
```

- Platform Information タブ
 - PCの情報が表示されています。上からSMBIOSから得られるマシンの情報、各種PCRの値、BIOSとブートローダーが計測したイベントログの一覧です
 - ボタンを押すと最新情報に更新されます

The screenshot shows the 'Platform Trust Service - Client (Debug)' application window. The 'Platform Information' tab is active, displaying the following information:

- Platform Vendor: Matsushita Electric Industrial Co., Ltd.
- Platform Name: CF-W7BWH4JS
- BIOS Version: V1.00L10
- BIOS Date: 2007/09/28

Below the information fields is a table of PCR Values:

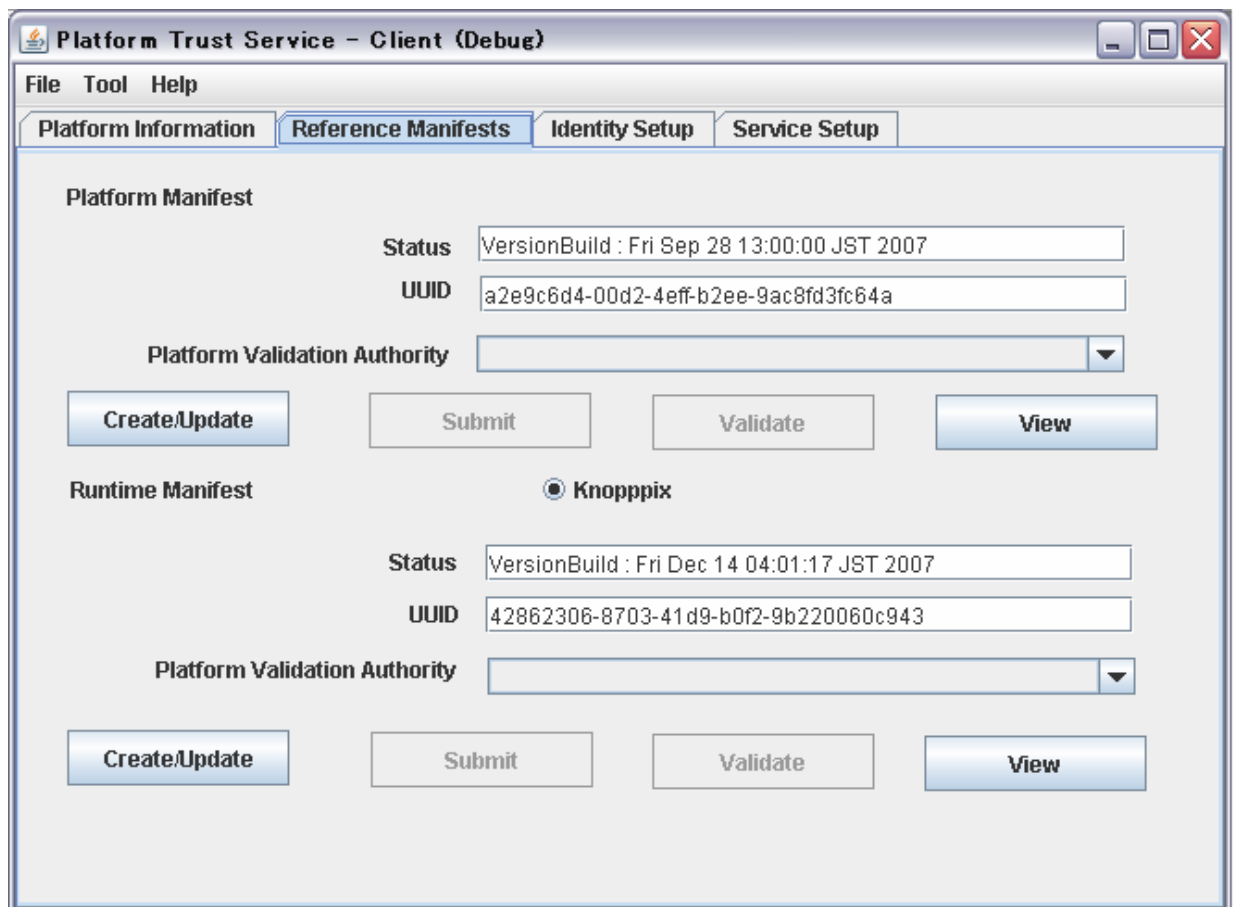
Index	Digest(hex)	Usage
0	ac550f26880157a59eec57a8b048966cdecce814	CRTM, POST BIOS, and ...
1	122c069b2cb7fcf21a3e0705c1f4a3f0c414b7bd	Host Platform Configurat...
2	d98637dbd94d00e2334d9aa9cac3bcf92fe2e413	Option ROM Code
3	3a3f780f11a4b49969fcaa80cd6e3957c33b2275	Option ROM Configurati...
4	da4426fc6cf403d5c166535f65aa417158cb5c21	IPL
5	9b687d3ca0c167b27774c88edabc3e1598ebecc6	IPL Configuration and D...
6	4adc69796769989eb7f6db94fc0f9657d7725044	State Transition

Below the PCR table is an Event Log table:

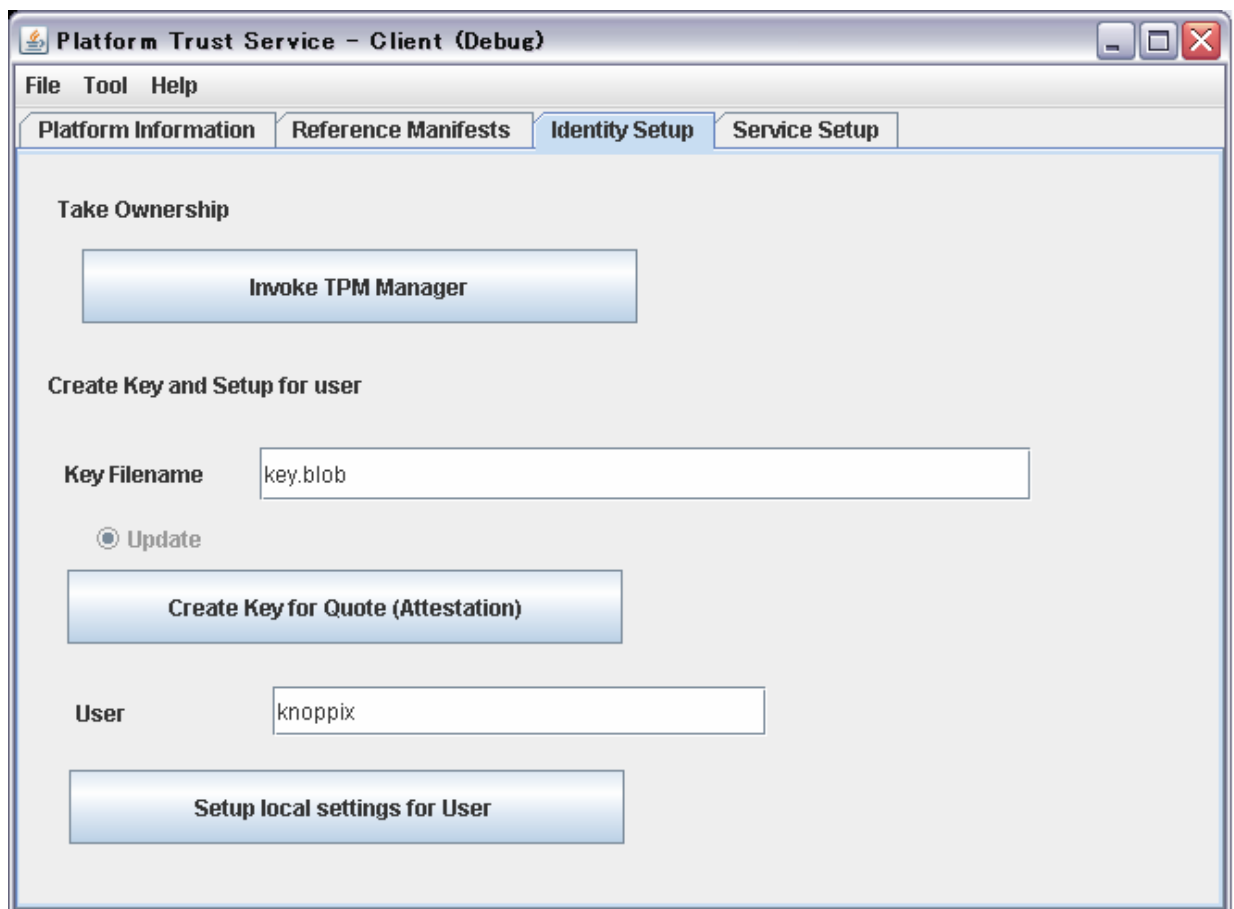
PCR Index	Digest(hex)	Name
0	dac03d111ddc84c9bb9d6b8b1c855b6dbe510bb0	EV_S_CRTM_VERSION[...
0	baacbcadc52f9b280a2702ab9b1baf99c835e513	EV_POST_CODE
0	ed4f61be338185bc947012c9925bb8ce404994fc	EV_POST_CODE
0	a2d1382881274950d1d31dac9df5f7d735747630	EV_POST_CODE
0	fdb581db7efd01b4b241e8156a18c3ec4d11c99f	EV_POST_CODE
0	5d85221a5ac161cca4d33ce72b7d39d927b1e2c8	EV_POST_CODE
0	f0f26d6c7f6c6b58f53257088cf1f33ce65bc418	EV_POST_CODE

At the bottom of the window, there is a 'Refresh Platform Information' button.

- Reference Manifest タブ
 - Platform Manifest と Runtime Manifest の更新を行います
 - Create/Update ボタンを押して、新たにマニフェストを作成します。Platform と Runtime の2つ作成します。更新が成功すると UUID の表示が変わります。実行環境(GCJ のバグ)の問題で更新が失敗する場合があります。その場合はもう一度更新ボタンを押してみてください (必須)
 - 更新確認のダイアログが出た場合は、OK を選択してください
 - 補足:View ボタンで生成されたマニフェストの XML をブラウザで見ることが出来ます。



- Identity Setup タブ
 - ユーザーが利用する鍵と環境の設定を行います
 - 注意: Invoke TPM Manager ボタンは使わないでください。
 - Create Key for Quote ボタンを押して、署名用の鍵を作成します。パスワードを聞いてくるので設定します。このパスワードがユーザーのパスワードになります(必須)
 - Setup local settings for User ボタンを押して、Knopix User の環境設定を行います。(必須)



- Service Setup タブ
 - そのままで OK です

以上で、デモ環境のセットアップは完了です。

4-2. その他の設定

以下、この時点で設定しておく、便利になる項目を説明します。

4-2-1. キーボード

標準は英語キーボードですので日本語に対応させるには

- メニューバーの右にある国旗を右クリック
 - Configure
 - Layout タブ
 - Available Layout で Japan を選択し Add ボタン
 - Keyboard model は Japanese 106-key を選択
 - Xkb Option タブ
 - CTRL キーの配置の変更などが出来ます

4-2-2. 画面の背景

変更しておく、KNOPPIX.IMG が正しくマウントされたのか起動画面で確認できます。

- Desktop でマウスを右クリック
 - Configure Desktop
 - 好きな背景を選択

5. デモ

最初に構成検証のデモと KNOPPIX の更新について説明し、次に通常の動作について説明します。

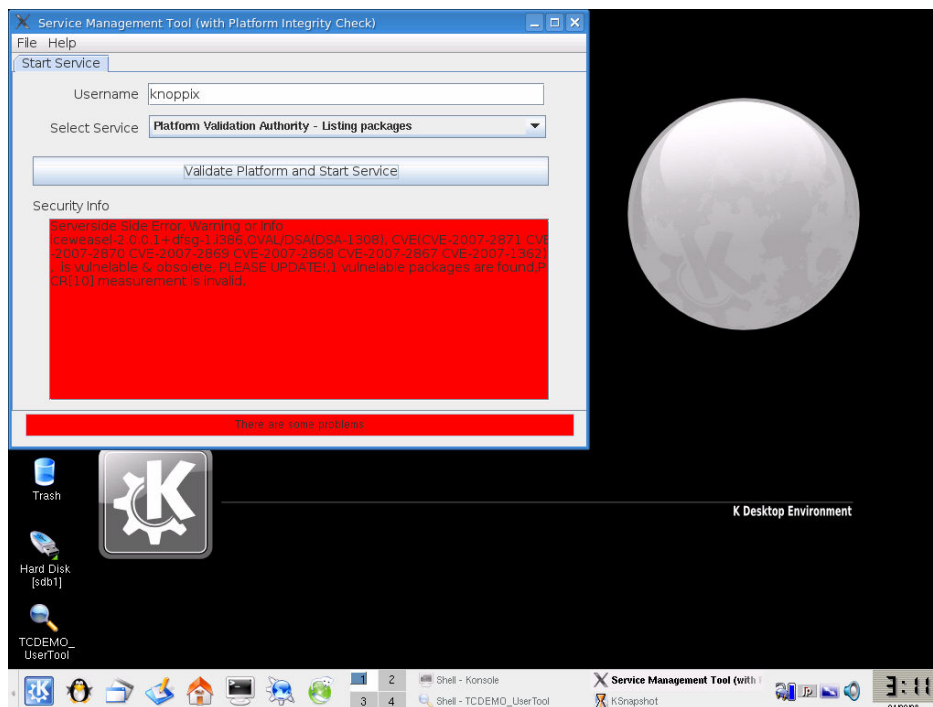
5-1. 検証失敗 & アプリの更新 編

5-1-1. 最初の検証(失敗します)

デスクトップの TCDEMO_UserTool アイコンをクリックするか、コマンドラインでデモのアプリを起動します。

```
$ /opt/OpenPlatformTrustServices/bin/pts-cu-swing
```

- Validate Platform and Start Service ボタンを押します
 - 署名鍵のパスワードの入力のダイアログがポップアップするので、パスワードを入力します
 - 数秒後に Security Info が赤くなり、iceweasel/firefox)の脆弱性が指摘されると OK です



5-1-2. 脆弱性にあるパッケージの更新

iceweasel を新しい Version に Update します。新しい Version は CD に含まれていますので、以下のコマンドで更新します。

```
$ cd /cdrom/KNOPPIX/updates
$ sudo dpkg -i iceweasel_2.0.0.12-0etch1_i386.deb
<snip>
```

注意) 脆弱性情報はたえず更新されるため、上記の iceweasel が使えなくなる場合があります。

5-1-3. 設定の USB への保存

以上の変更を行った、UNIONFS のイメージファイルを USB に保存します。次回の起動では、保存したイメージの入った USB を挿入して KNOPPIX を起動すれば、(ダイアログが出るので OK とすれば自動でマウントされます) これまでの設定が利用できます。

- KNOPPIX (Menu バーの左から 2 個目のペンギン)
 - Configure
 - Create a persistent KNOPPIX disk image
- Create persistent KNOPPIX home directory ダイアログが Popup
 - Yes
 - USB デバイスを選択
 - No (AES 暗号化は選択しない)
 - 100 (容量指定、100MB 以上に)
 - OK (完了)

5-1-4. 再起動

今の検証サーバーは計測に脆弱性のあるコンポーネントが含まれていると、たとえ更新しても INVALID となります。すべてのソフトウェアが新しい状態で記録されるように、一度再起動します。

5-2. 検証成功 & デモサービス 編

検証が OK な場合には、検証サーバーからデモサーバーにアクセスするためのアカウント情報が送られてきます。その後、Firefox が起動し、デモのサーバーに接続します。デモサーバーでは KNOPPIX に含まれるパッケージやハッシュ値、脆弱性の検索が可能です。

5-2-1. 起動

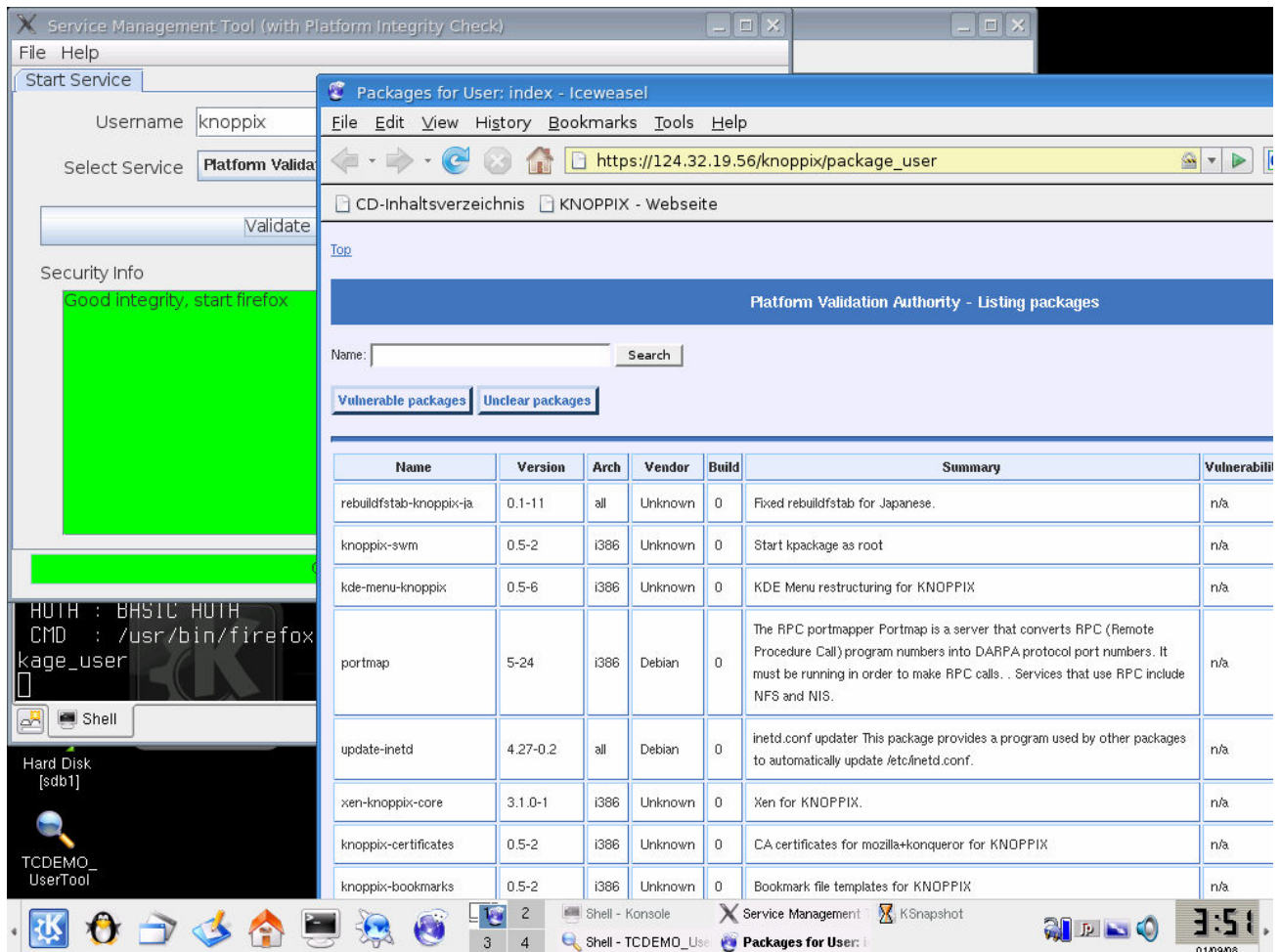
- Grub の画面で IMA を選択
- KNOPPIX-CONFIGURATION (USB に保存したデータのマウントになります)
 - OK(Default) を選択

5-2-2. 検証成功

5-1-1 同様に、デスクトップの TCDEMO_UserTool をクリックしてデモを起動します。ボタンを押して、署名鍵のパスワードの入力を行い、数秒待つと今度は表示が緑になり、iceweasel(firefox)が起動を開始します。

- SSL 証明書(CN 124.32.19.56)の確認ダイアログ Accept 選択肢 OK
- Guest アカウントで Login の確認ダイアログ、OK
- Security Warning のダイアログ OK

で、Platform Validation Authority の検索サービスを利用することが可能です。



実は、再起動後のデスクトップで Iceweasel (Firefox) のアイコンの色が緑から青に変わっています。TCG の技術を使った構成証明では、ソフトウェアの情報はそのハッシュ値の形で記録され、かつ、記録は TPM チップで保護されています。そのため、Iceweasel が改ざんされ、このアイコンが巧妙な偽者であったとしても、確実な検証が可能です。

5-2-3. デモサービスについて

KNOPPIX に含まれるハッシュ値の情報や脆弱性情報の検索が可能です。

たとえば、iceweasel で検索すると Version 2.0.0.1 には DSA-1424 で指摘されている脆弱性が含まれている事がわかります。

6. 既知の問題点、トラブル対策

このデモはまだ不完全なため、以下のような問題があります。もし問題が発生した場合は参考にさせていただけると助かります。また、以下に無いトラブルについては [メーリングリスト](#) や [フォーラム](#) に投稿していただくと、大変助かります。

6-1. 既知の問題点

6-1-1. TPM Manager で TakeOwnership すると、SRK 認証で失敗

tpm_takeownership コマンドを使ってください。これは SRK のパスワードの取り扱いが tpm-tools v1.2.5.1 と TPM Manager v0.4 で異なる為です。

6-2. トラブル対策

6-2-1. KNOPPIX(Grub)が起動しない

BIOS の TCG サポートに問題がある可能性があります。最新の BIOS への Update を行うと、起動出来る場合があります。

6-2-2. KNOPPIX(OS)が起動しない

BIOS の TCG 機能、Kernel の TPM ドライバの問題が考えられます。また、最新の機種では KNOPPIX が起動できない場合があります。この場合、Kernel の起動オプションの指定で解決する場合があります。起動オプションの指定について下記のサイトを参考にしてください

http://www.knoppix.net/wiki/Cheat_Codes (英語)

<http://www.kernel.org/pub/dist/knoppix/KNOPPIX-FAQ-EN.txt> (英語)

<http://www.alpha.co.jp/biz/products/knoppix/faq/starting.shtml> (日本語)

6-2-3. ユーザーツールが起動しない

コンソールに以下のようなエラーが出る場合は、ユーザー環境の設定が正しく出来ていません。
/home/knoppix/.pts ディレクトリが存在しますでしょうか？ 存在しない場合は ステップの 4-1-3.
を参照してください。

```
Exception from Config
java.lang.Exception: Need to create /home/knoppix/.pts?
set --new flag, and try again
    at tcdemo.Config.<init>(pts-cu-swing)
```

6-2-4. ユーザーツールの Select Service で Listing Measurement を選ぶと、サーバーに接続しない

OpenPlatformTrustServices のバグです、以下のファイルを修正して、4-1-3 節の管理者ツールで
“Setup local settings for User” ボタンを押し設定を更新してください。

/opt/OpenPlatformTrustServices/tcdemo/tcdemo.properties

```
service.1.url=https://124.32.19.56/knoppix/measurement_user
#service.1.url=http://124.32.19.56:80
```

付録 プラットフォーム情報

最新の情報については <http://sourceforge.jp/projects/openpts/wiki/PlatformInfo> を参照してください。

Vendor	Type	P/N	BIOS Version	BIOS Date	TPM	HDD Boot	USB Boot	CD Boot	Comments
IBM	Thinkpad X31	2672CBJ	1QET78WW (2.15)	11/18/2004	Atmel v1.1b	OK(3)		NG(1)	
IBM	Thinkpad T42	2373J8J	1RETDNWW (3.19)	10/13/2005	Atmel v1.1b	OK(3)		NG(1)	
DELL	OptiPlex GX620	OptiPlex GX620	A07	03/31/2006	ST Micro v1.2?	?	NG(7)	NG(6)	
IBM	Thinkpad T43	266872J	1YET65WW (1.29)	08/21/2006		NG(2, 3)		NG(1, 2)	
Lenovo	Thinkpad T60	20076EJ	79ETC9WW (2.09)	12/22/2006	Atmel v1.2	OK(3)		NG(1)	BIOS 更新で対応
Lenovo	Thinkpad T60p	8741JMJ	7IET23WW (1.04)	12/27/2006	Atmel v1.2	OK(3)		NG(1)	BIOS 更新で対応
Panasonic	Y7	CF-Y7A WDAJS	V1.00L11	04/11/2007	Infineon v1.2	OK	OK?	OK	
IBM	Thinkpad T42	2373J8J	1RETDRWW (3.23)	06/18/2007	Atmel v1.1b	OK(3)	NG?	NG(1)	
Fujitsu	Lifebook S2210	CP32730 1	V1.09	06/21/2007	Infineon v1.2	OK?	OK?	OK?	(8), AMD SKINIT
DELL	OptiPlex 755	OptiPlex 755	A01	08/10/2007		?		NG(5)	(9)
HP	dc7800p	GC760A V	786F1 v01.04	08/27/2007		NG(4)		NG(6)	
Lenovo	Thinkpad T60	20076EJ	79ETD9WW (2.19)	09/19/2007	Atmel v1.2	OK(3)	OK	OK	
Lenovo	Thinkpad T60p	8741JMJ	7IET31WW (1.12)	09/19/2007	Atmel v1.2	OK(3)	OK	OK	
Panasonic	W7	CF-W7B WHAJS	V1.00L10	09/28/2007	Infineon v1.2	OK?	OK?	OK	

注釈

1. TCGBIOS による CD Boot Image の計測が間違っています
2. TCGBIOS が PCR の 8 以上を使えません
3. MBR の最初の 446 bytes が計測されます
4. TCGBIOS の Int 1Ah Call に問題があります (MS BitLocker(R) は動きます)
5. CD の Boot Image が計測されません
6. Knoppix511 が起動しません
7. BIOS が TPM/TCG 対応ではありません
8. Linux 2.6.19 の TPM driver が動きません
9. Kernel オプション `xmodule=vesa screen=1024x768` で Knoppix を起動