How to use OpenPlatformTrustServices with KNOPPIX Trusted Computing Geeks

2008-01-29 Version 1.0 for
KNOPPIX 5.1.1 Trusted Computing Geeks v1.0
OpenPlatformTrustServices v0.1.1

*) This work is sponsored by the Ministry of Economy, Trade and Industry, Japan (METI) under contract for the New-Generation Information Security R&D Program.

Overview....3
1. Creation of OS image....4
2. Preparation of USB Memory Device....4
3. Setup the PC....4
3-1. Enter the BIOS setup menu....5
3-2. Enable the TPM....5
3-3. Clear the TPM Ownership (option)....5
4. KNOPPIX TC Geeks boot and initial setting....6
4-1. Initialize the TPM and setup the demo environment....6
4-1-1. Boot the CD....6
4-1-2. Take the TPM ownership....6
4-1-2. Setup of a demonstration environment....7
4-2. Other settings....10
4-2-1. Keyboard Settings....10
4-2-2. Desktop background image....10
5. Demonstration....11
5-1. Validation failure & Update vulnerable app....11
5-1-1. First Remote Attestation (it fails)....11
5-1-2. Update the vulnerable package....12
5-1-3. Save changes to USB memory....12
5-1-4. Restart....12
5-2. Validation success & Demo Services....13
5-2-1. Startup....13
5-2-2. Validation success....13
5-2-3. Demo service....14
6. Known problems and Trouble shootings....15
6-1. Known problems....15
6-1-1. Incompatible TakeOwnership with TPM Manager....15
6-2. Trouble shootings....15
6-2-1. KNOPPIX does not boot - GRUB....15
6-2-2. KNOPPIX does not boot - OS....15
6-2-3. User tool does not start....16
Appendix. Platform Information....17

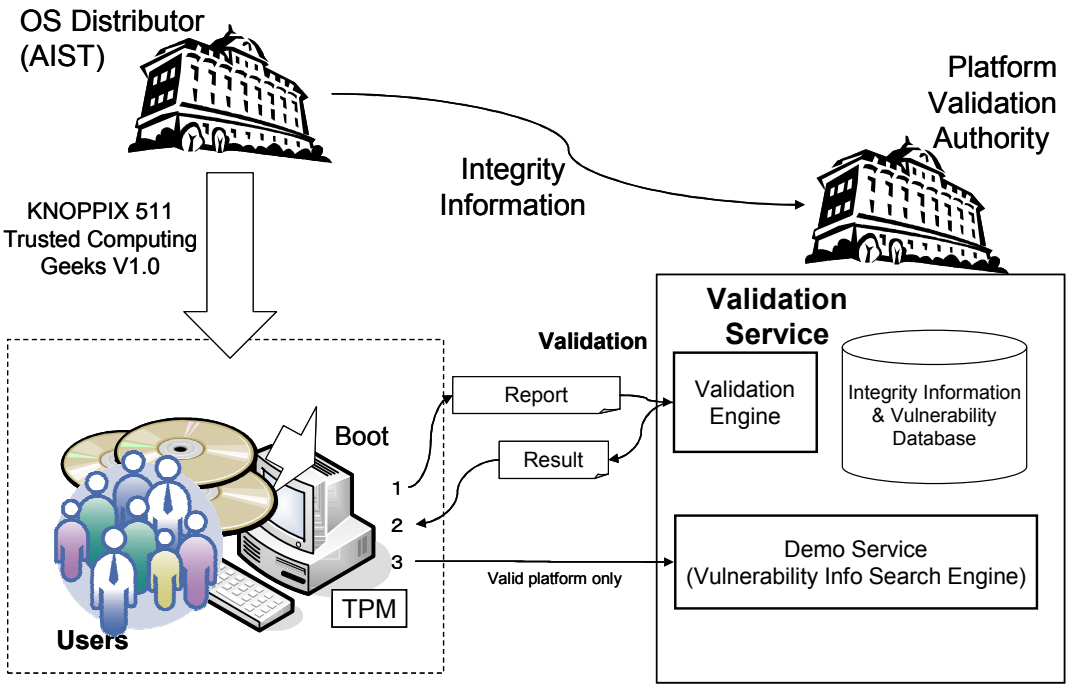
Overview

This is a demonstration which experiences Remote Attestation, fundamental capability provided by Trusted Computing Technology, just using CD bootable OS – KNOPPIX. This KNOPPIX supports Trusted Boot and client software for Remote Attestation., and can be validated by demo Validation Service on Internet. When the validation success (without any known vulnerability), the client will be able to use a service (demonstration of vulnerability search service)

Users just download the KNOPPIX OS image and create the bootable CD. After initial setup procedure is finished, the demo application on the client creates a report which contains software integrity information on the client and sends it to validation service. The validation service maintains integrity (white-list) and vulnerability information regarding to this KNOPPIX, and validates the given report with them. The validation includes integrity and vulnerability checking. In this demonstration, the server provides integrity and vulnerability search service which only accessible by the valid client.

Any information, including your test result and trouble, you can provide us will be very helpful and appreciated. The following mailing-lists are available for such reporting.

Japanese http://lists.sourceforge.jp/mailman/listinfo/openpts-jpusers
English http://lists.sourceforge.jp/mailman/listinfo/openpts-users



1. Creation of OS image

KNOPPIX with various TCG functionalities including OpenPlatformTrustServices can be downloaded from http://unit.aist.go.jp/itri/knoppix/.

Supported PCs,

- PC with TPM security chip
- PC has BIOS which support Trusted Boot capability (See the table at Appendix. Platform Information)
- TPM is not used yet (when MS BitLocker or other software which use TPM are already used, probably this KNOPPIX cannot use simultaneously).

If you have above-mentioned PC, first, please download the ISO image from the site, and create the CD. The platform information indicated at Appendix. Platform Information is limited. PC which is not indicated might be work.

2. Preparation of USB Memory Device

Only two RSA keys, EK and SRK, are saved inside of the TPM, and other keys are managed outside of the TPM. (The key-data is safe since it is encrypted by SRK), and such a key is managed by TCG Software Stack (TSS,). Thus, we use USB Memory device to store the key since it cannot save at CD media.

The KNOPPIX supports UNIONFS which enable seamless write through a RAMDISK or a filesystem image on USB memory. To achieve the following experiments, the required size of USB Memory is 128MB. Also fast USB Memory is highly recommended to get the better performance.

3. Setup the PC

The TPM function is disabled at the initial shipment state. Please try to go to BIOS setup menu, and enable the TPM.

(If you already enabled the TPM, to avoid any troubles, please clear existing TPM ownership if possible, ref. 3-3.)

3-1. Enter the BIOS setup menu.

At the boot time press F1 (IBM, Lenovo), F2 (Panasonic) key, then you went to BIOS setup menu.

3-2. Enable the TPM.

Generally, TPM setup menu exist at security menu.

Generally, the menu of a security has a setups of validation of TPM. In reference condition, since it is cancelled, it comes into effect.

3-3. Clear the TPM Ownership (option).

CAUTION: When TPM is already owned, an initializing of TPM ownership may be needed. In this case, all the keys created by the TPM before are destroyed. Thus please do not clear the ownership if you need to use previous configuration.

The way of an initializing of TPM ownership carries out the cold boot (boot from the power OFF state). Next, please go into the BIOS menu, and clear the TPM ownership.

NOTE: In case pf Panasonic PCs, TPM will be disabled if TPM ownership was cleared. Please go into the BIOS menu again, and enable the TPM.

4. KNOPPIX TC Geeks boot and initial setting

Before beginning a demonstration, an acquisition of the TPM ownership and the setup of a user environment are required.

4-1. Initialize the TPM and setup the demo environment

4-1-1. Boot the CD.

At the Grub screen, Please choose IMA. Then, please wait for a while, and then KNOPPIX desktop window will be displayed.

4-1-2. Take the TPM ownership

Please start a console and take the TPM ownership as follows:

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

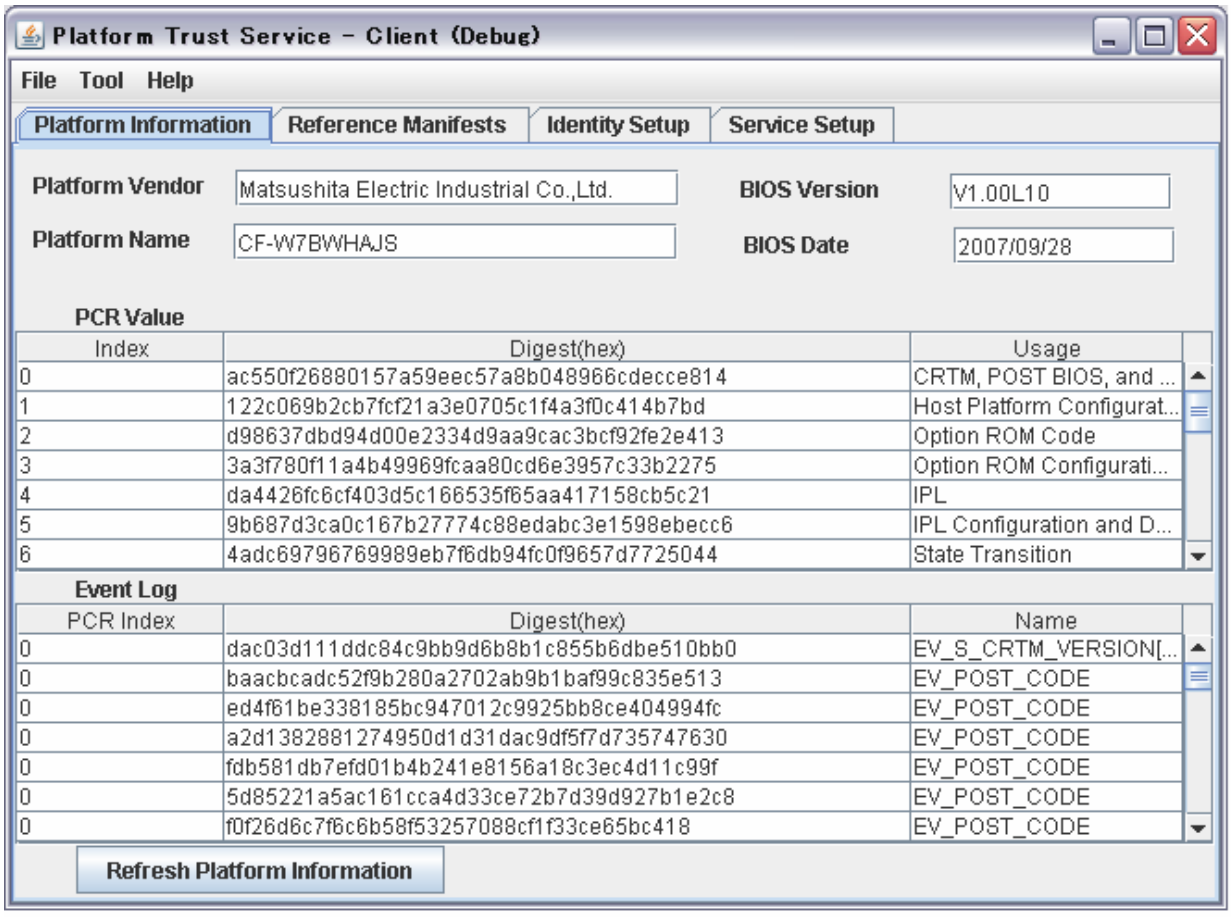
CAUTION: For the password of SRK, please just inputs Enter only (it generates SRK without an authentication). Although it is also possible to take ownership by the GUI tool, TPM Manager, but it generates a SRK with authentication by well known password. This is not compatible. Therefore, please use a **tpm_takeownership** command.

4-1-2. Setup of a demonstration environment

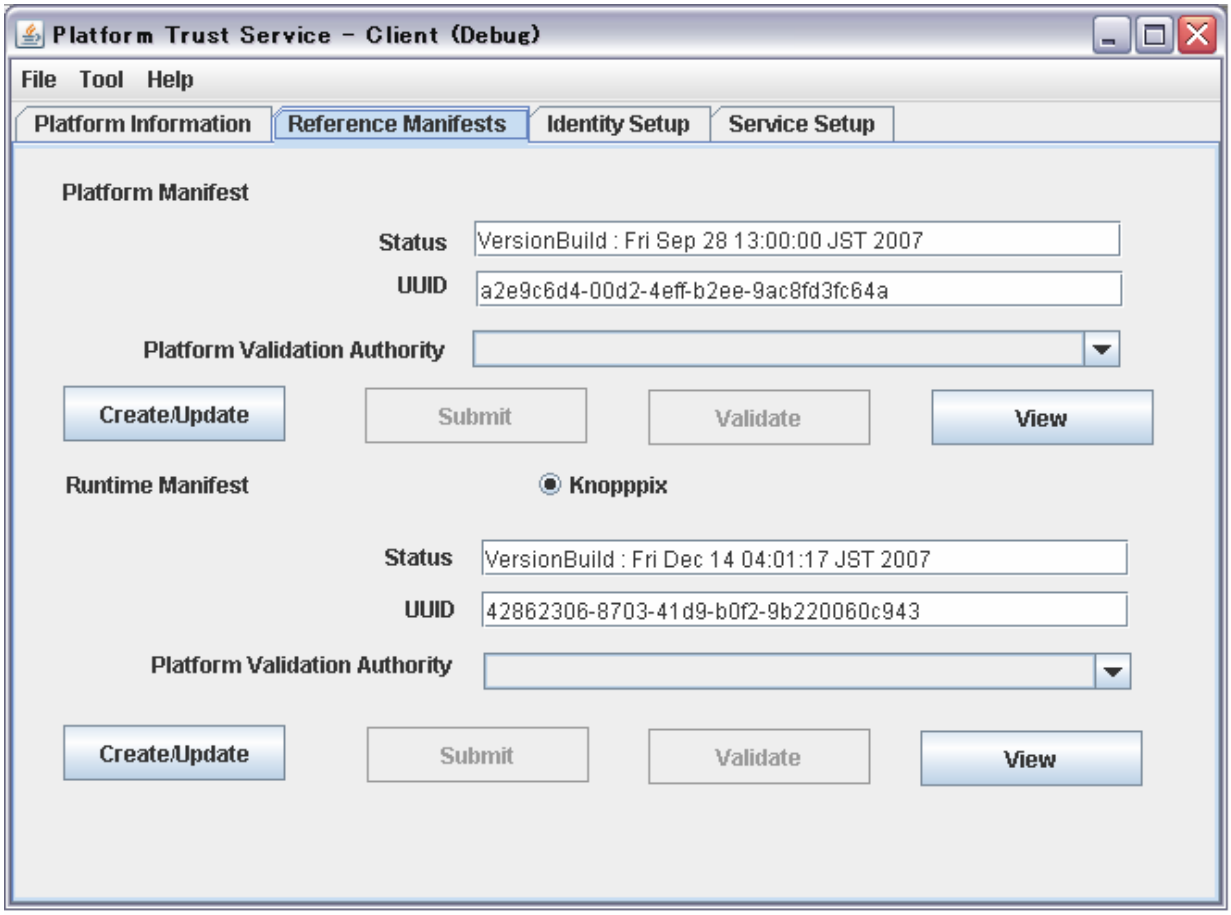
Please execute the following commands from a console to create icon on desktop and start admin GUI tool.

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

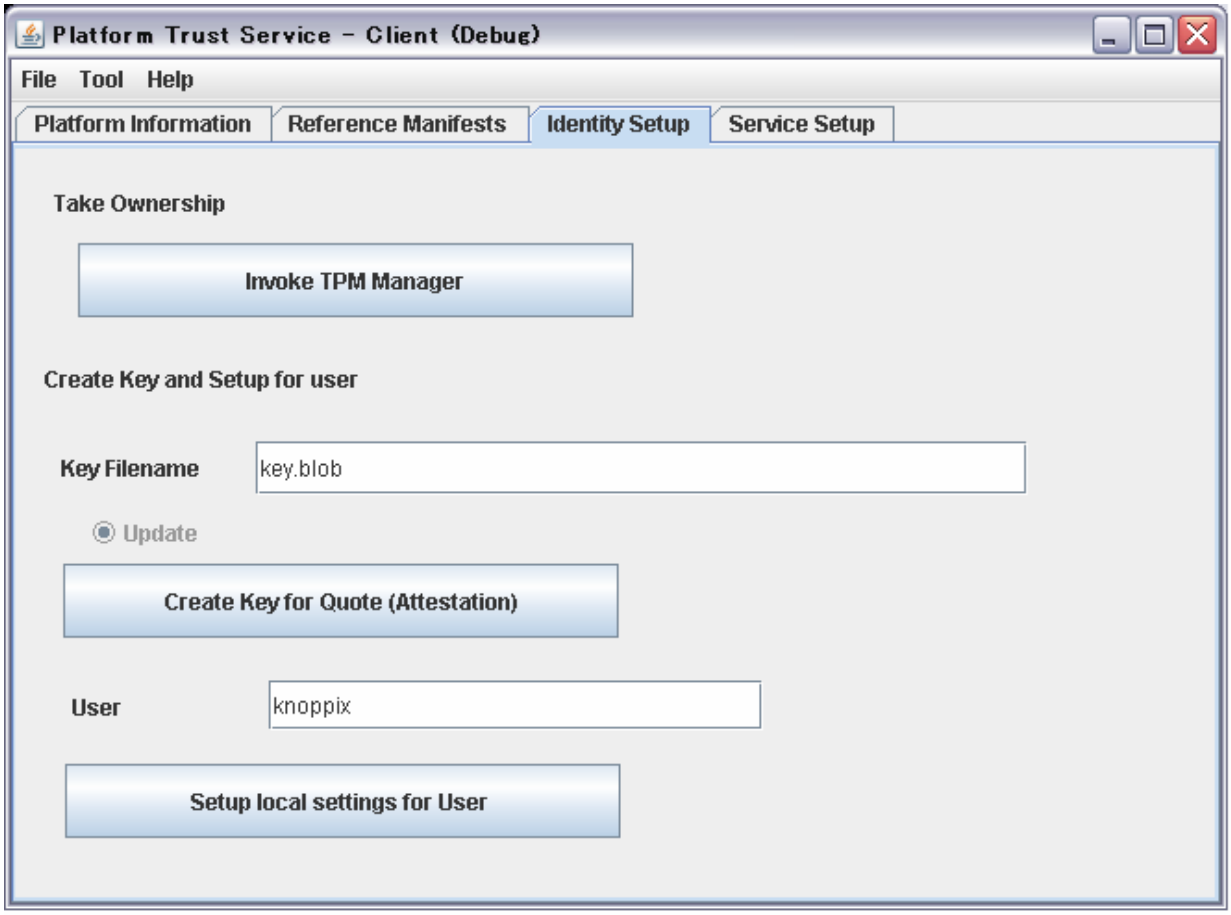
- Platform Information Tab
  - Shows current PC information. Machine info obtains from SMBIOS data、PCR values, Eventlog measured by BIOS and Bootloader.
  - Press the “Refresh Platform Information” button to update the data



- Reference Manifest Tab
  - Update Platform Manifest and Runtime Manifest
    - Press Create/Update button to update the manifest. we need to update both Platform and Runtime manifest. When update was succeed, the UUID will be changed. Some time update is failed due to the bug in GCJ runtime, in such case. Please try again. (mandatory operation)
    - Dialog will be displayed, please press OK button.
    - Note: To see the manifest (XML), press the "View" button, then firefox is starting up and display the manifest.



- Identity Setup Tab
  - Create the user's attestation key and setup the user environment
    - CAUTION: Don't use the Invoke TPM Manager button to take TPM ownership, sorry.
    - Press the"Create Key for Quote" button, it create the key for attestation. The dialog for password enters will popup, please set user password. (mandatory operation)
    - Press "Setup local settings for User" button, it create the environment for KNOPPIX User (mandatory operation)



- Service Setup Tab
  - Don't touch this tab. Not work at this time. sorry.

With that, the setup of a demonstration environment is completed.

4-2. Other settings

Hereafter, the following settings might be convenient for you

4-2-1. Keyboard Settings

Since a standard is an English keyboard, for other languages

- Crick the national flag on right side of menu bar.
    - Configure
        - Layout Tab
            - Available Layout, select the language and press Add button
            - Select Keyboard model
        - Xkb Option tab
            - you can change the CTRL location etc

4-2-2. Desktop background image

It is easy to confirm the UNIONFS operation with the desktop's background image. Since sometime the mount of UNIONFS was fail...

- Left crick the mouse on Desktop
    - Configure Desktop
        - Select your favorite image

5. Demonstration

First, the demonstration of remote attestation (this will fail due to the obsolete package), and the updating the KNOPPIX are explained

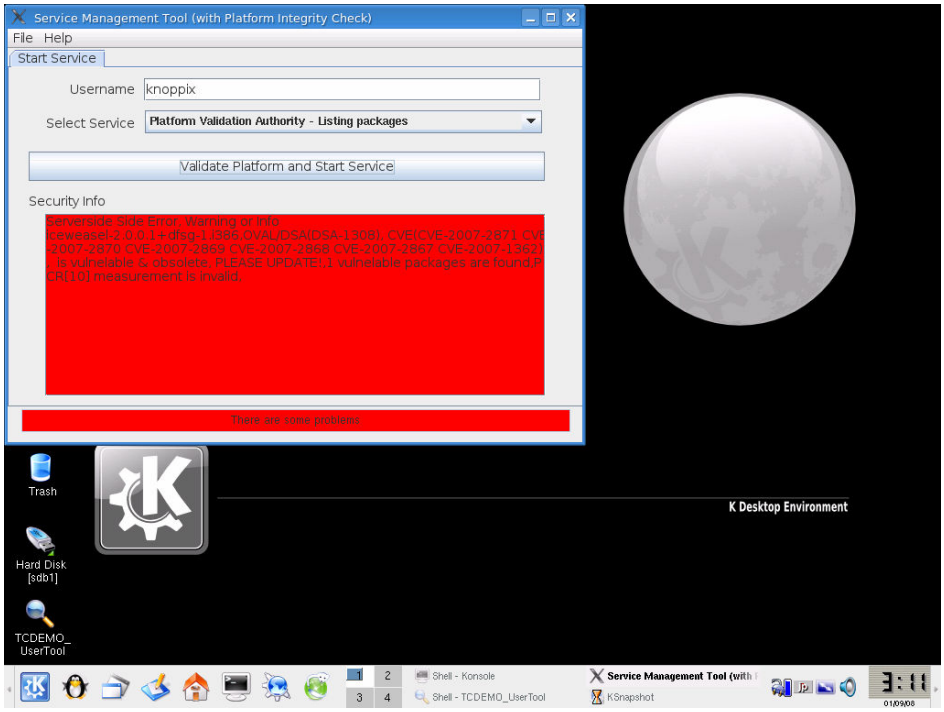
5-1. Validation failure & Update vulnerable app

5-1-1. First Remote Attestation (it fails)

Please click TCDEMO_UserTool icon on the desktop or use the following command-line to start up the GUI User Tool.

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

- Press “Validate Platform and Start Service” button .
  - The password input dialogue of signature key pops up, please enter your password.
  - Wait for several seconds, then “Security Info” becomes red and the problem of iceweasel (firefox) is pointed out.



5-1-2. Update the vulnerable package

Let's update the iceweasel to the new version (is available on CD) by the following commands.

```
$ cd /cdrom/KNOPPIX/updates
$ sudo dpkg -i iceweasel_2.0.0.10-0etch1_i386.deb
<snip>
```

NOTE: This new version will become obsolete when new vulnerability was found.

5-1-3. Save changes to USB memory

Let's save the image file of UNIONFS which made the above change to USB memory. The changes are preserved if booting the KNOPPIX with this USB memory.,

- KNOPPIX (penguin icon on menu bar)
  - Configure
    - Create a persistent KNOPPIX disk image
- "Create persistent KNOPPIX home directory" dialogue is popup.
  - Yes
  - Select USB memory device (e.g. /dev/sdb1).
  - No (an AES encryption is not chosen)
  - 100　(the image size, 100MB or more)
  - O.K. (completion)

5-1-4. Restart

Even update the packages, If the existence of vulnerable component has been recorded, the validation server returns the result, INVALID. Please reboot once, then all the software may be recorded in the new status.

5-2. Validation success & Demo Services

When validation successes, the account information for accessing demo service is sent from validation server. Then, Iceweasel (Firefox) starts and it connects with the demo service. In demo service, you will be able to search the package and hash values included in the KNOPPIX, and also vulnerability information.

5-2-1. Startup

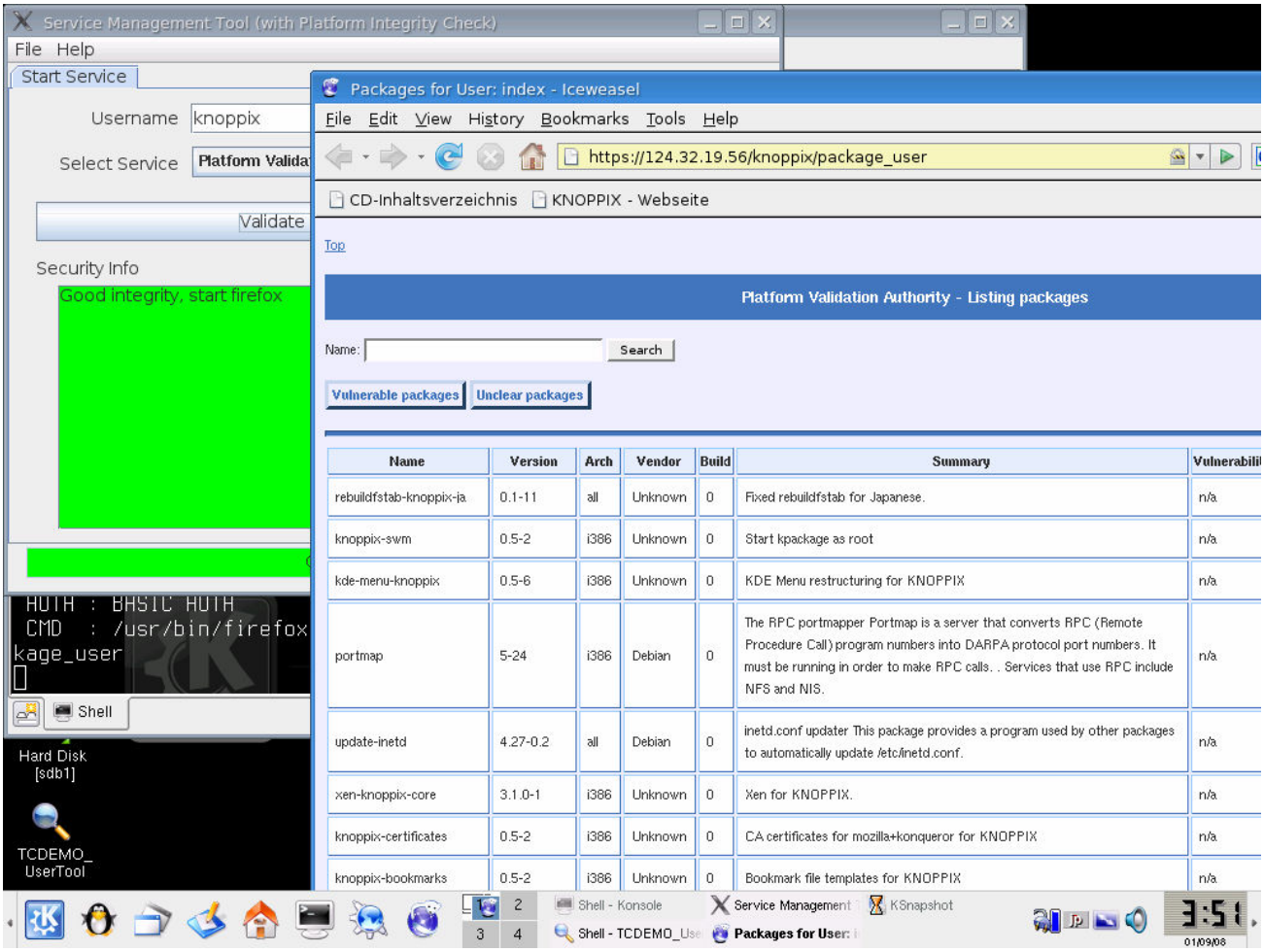
- IMA is chosen on the Grub menu.
- "KNOPPIX-CONFIGURATION" dialog (for mounting UNIONFS image onUSB memory)
    - O.K. (Default) is chosen.

5-2-2. Validation success

Like section 5-1-1, TCDEMO_UserTool of desktop is clicked and the GUI tool is started.　Press the button, and enter the password., and wait for several seconds. Then ,the tool become in green shortly and iceweasel (firefox) will start.

- Verification dialogue of a SSL certificate (CN 124.32.19.56) popup, select "Accept"
- Verification dialogue of Login as Guest,　select OK
- Security Warning dialog, select O.K.

It is possible to come out and to use the retrieval service of Platform Validation Authority.



In fact, the color of the desktop icon of Iceweasel (Firefox) has changed to blue from green after rebooting the KNOPPIX. In the Remote Attestation using the technology of TCG, the integrity of software is recorded in the form of the hash value –– and the record is protected by the TPM chip. Therefore, the validation is possible even if the icon (and software) was modified artfully.

5-2-3. Demo service

It is possible to search hash value or vulnerability information included in the KNOPPIX.

For example, Search package name, “iceweasel”, then the result shows the version 2.0.0.1 contains the vulnerability pointed out by DSA-1424.

6. Known problems and Trouble shootings

Since this demonstration is still imperfect, there are the following problems. If you have any trouble please let us know and thank you for your help.

6-1. Known problems

6-1-1. Incompatible TakeOwnership with TPM Manager

Please use **tpm_takeownership** command to take your TPM ownership. Since the handling of the SRK authentication is different between tpm-tools V1.2.5.1 and TPM Manager V0.4.

6-2. Trouble shootings

6-2-1. KNOPPIX does not boot - GRUB.

There may be a problem in a BIOS TCG support. If BIOS update is available, please try with the latest BIOS.

6-2-2. KNOPPIX does not boot - OS.

The problem of the BIOS TCG functionality and the TPM driver of Linux Kernel can be considered. Moreover, KNOPPIX (kernel 2.6.19) may be unable to boot with the newest PC model. A kernel boot option may help for such problems. For more detail about kernel option, please refer the following sites:

http://www.knoppix.net/wiki/Cheat_Codes (English)
http://www.kernel.org/pub/dist/knoppix/KNOPPIX-FAQ-EN.txt (English)
http://www.alpha.co.jp/biz/products/knoppix/faq/starting.shtml (Japanese)

6-2-3. User tool does not start.

When the following errors appear in a console, the setups of the user environment has not been performed correctly.　Does a directory /home/knoppix/.pts exist?　When it does not exist Please refer to section 4-1-3.

```
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)
```

Appendix. Platform Information

For the latest info, please refer to http://sourceforge.jp/projects/openpts/wiki/PlatformInfo.

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)	Pls. update the BIOS
Lenovo	Thinkpad T60p	8741JMJ	7IET23WW (1.04)	12/27/2006	Atmel v1.2	OK(3)		NG(1)	Pls. update the BIOS
Panasonic	Y7	CF-Y7AW DAJS	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	GC760AV	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	

Notes)

1. TCGBIOS do wrong measurement of CD Boot Image
2. TCGBIOS can't use PCR #>7
3. Measure 446 bytes of MBR
4. Some trouble around TGCBIOS Int 1Ah Call (but MS BitLocker(R) may work)
5. Do not measure El Torito Boot Image
6. Knoppix511, Boot Fail
7. No TCGBIOS?
8. Linux 2.6.19, TPM driver is not work
9. Use kernel option, xmodule=vesa screen=1024x768, to boot the KNOPPIX.