

Usage of TPM under the Xen

Michal Prochazka, Daniel Kouril
{michalp,kouril}@ics.muni.cz

¹Institute of Computer Science
Masaryk University

²CESNET
Czech Republic

Hamburg 17. 1. 2007

What is a TPM?

- Trusted Platform Module
- Microcontroller affixed to the motherboard
- Secured key store, RNG
- Remote attestation, sealing
 - Similar concept as smart cards, but unlike smart cards the TPMs identify the host computer not the user.

Functionality of TPM

- Endorsement Key
- Attestation - provide information about state of the system
 - Platform Configuration Registers, Attestation Information
 - BIOS, kernel, applications, conf. files can be check if they are correct
- Remote attestation - provide above information for remote clients
- Data sealing - secure the I/O, memory, files
 - Secured typing the password on the keyboard
 - Secured part of the system can be accessed only by authorized processes
- Key exchange - exchange of keys between TPMs
 - Storage Root Key
 - Exchanged key can never be seen in the clear text form

Restriction run of VM image

- The VM is restricted to run only on the selected machines
- User can choose on which machine(s) VM can be run
- Absolute assurance of running the VM on selected machine(s)
- In the event of use of PCR, machine can be checked for integrity

Encrypted VM image

- Use of eCryptFS together with ability of exchange keys
- VM can be run only on one or a set of machines which have the same key in the TPM
- VM can not run outside the group of authorized machines

Secured web services/applications

- Use of the vTPM and PKCS#11 interface to the TPM
- X.509 certificates for web services and applications
- User has assurance she is working with the right web service/application
- It complicates making a fake web services/applications
- Highest level of security with good level of robustness

Secured sensitive data

- Use of the vTPM and PKCS#11 interface to the TPM and PCR
- Kerberos tickets, proxy certificates, host certificates
- Secured on both levels dom0 and domU
- Sensitive data can be accessed only by applications complying with the conditions

Migration of VM

- By using TPM and secured VM there is no loss on migration
- Key never leaves the secured storage
- Migratable vs. non-migratable keys

TPM in the Grid

- Project Daonity
- SEMP

Thank you for your attention.