Trusted Infrastructure Cloud

Norbert Schirmer (Sirrix AG)

Trustworthy Cloud Workshop
ESORICS 2013, London
Trust in Clouds

- Outsourcing of resources (computing, network, storage) to cloud provider
- Pay-per-use
- Scalability

- *Shared responsibility* between cloud customer and cloud provider
- How to gain trust in cloud resources?
**Trusted Infrastructure Cloud**

- **Trust in remote resources**: built on top of Trusted Computing technologies
  - Integrity ensured by hardware anchor, trusted boot, security kernel, remote attestation
- **Protection against insider attacks**: administration is controlled by infrastructure
  - No administrators with elevated privileges
- **Separation of tenants**: Trusted Virtual Domains (TVD)
  - Trustworthy isolation of computing / storage / networking
TrustedServer: Security Kernel

- Isolation and Virtualisation
- Trusted Virtual Domains
- Integrity of Platform

Diagram:
- TURAYA™ Security Kernel
- Isolation
- Policy Enforcement
- Hardware
Ensuring Integrity

- **Essential Preconditions**
  - Tamper Proof Hardware module
  - Integrity during boot

- **Integration into Infrastructure**
  - Remote Attestation
    - Trustworthy integrity for remote resources
    - Communication only between trustworthy systems
    - Isolation of faulty / malicious systems
  - Secure Binding
    - Binding of boot process to trusted configuration
    - Only untampered security kernel is booted
**Chain of Trust**

- **Execution**
  - App
  - OS

- **Turaya™ Security Kernel**

- **Bootloader**

- **Hardware**
  - CRTM
  - TPM

- **Measurements**
  - $m_X: \text{hash}(X)$
  - Measurements of binary code $X$

- **Trustworthy Components**
  - BIOS
  - Bootloader

- **Turaya™ Security Kernel**
  - measures the virtual machines

- **BIOS$^{TC}$**
  - measures Bootloader

- **CRTM**
  - measures BIOS

---

**Core Root of Trust for Measurement (CRTM)**

**Trusted Platform Module (TPM)**
Trusted Virtual Domains (TVD)

- Core concept for
  - Simple but pervasive information flow control
  - Trustworthy isolation of shared computing / storage / networking resources

- Association of compartments (VMs) with security domains
  - Direct information flow only within same TVD
  - Control of all interfaces between TVDs
  - Used to separate tenants, but can also be used to separate security domains of a single tenant
TVD: Physical Network Layer
TVD: VPN-based Virtual Network Layers
Workflow Illustration
Step 1: Trusted Boot

TURAYA™ Security Kernel

TrustedServer

https

TURAYA™ Security Kernel

TrustedDesktop

TOM
Step 2: TrustedChannel & Remote Attestation
Step 3: Start Compartments

TURAYA™ Security Kernel

TrustedServer

TrustedChannel

TOM

TrustedDesktop

TClouds (No. 257243)
Trustworthy Clouds - Privacy and Resilience for Internet-scale Critical Infrastructure

12.09.13
Integration of Commodity Cloud Storage

Commodity Cloud Storage (e.g. Amazon S3)

Apps + OS

Virtual Volume

dec/enc

mount

PE

Share TVD B

Hardware

PE = Policy Enforcement
Conclusion

- Establish trust in remote resources by Trusted Computing technologies
  - Hardware trust anchor
  - Trusted boot ensures integrity
  - Security kernel

- Protection against insider attacks
  - Automated management / maintenance via controlled remote interfaces
  - No administrators with elevated privileges

- Trusted Virtual Domains (TVD)
  - Trustworthy isolation of computing / storage / networking
  - Information flow control
  - Transparent encryption
  - VPN
"The TClouds project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-257243.”

If you need further information, please contact the coordinator:

Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55  Fax: +43 4242 233 55 77
E-Mail: coordination@tclouds-project.eu

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.