Extending user controlled security domain with the TPM/TCG

Yuri Demchenko
University of Amsterdam

MWSG10 meeting
November 14-15, 2006, CERN

www.eu-egee.org

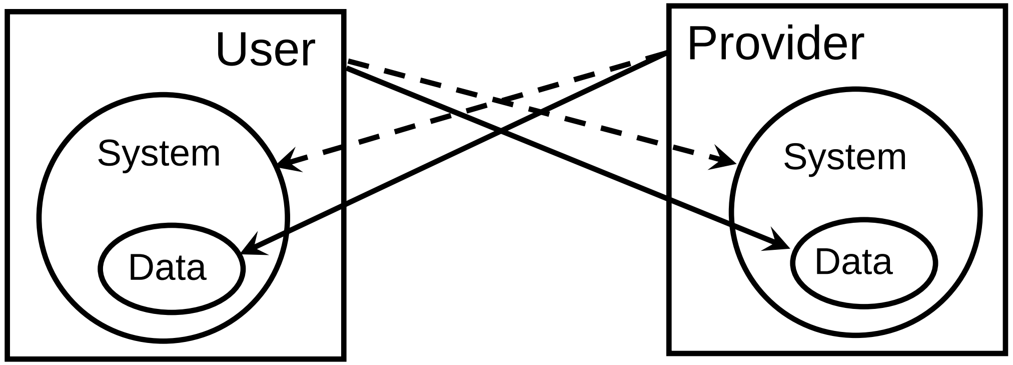
Information Society and Media

Outline

- **Different sides of the Security and Trust**
  - User and Service Provider vs System and Data
  - Secure Credentials Storage
- **Trusted Computing Platform and Trusted Platform Module**
- **User controlled Virtual Workspace organisation**
- **Discussion – Vision for use of this technology**

Different sides of the Security and Trust

- **Modern paradigm of remote distributed services and digital content providing makes security and trust relations between User and Provider more complex**
- **User and Service Provider – two actors concerned with own Data/Content security and each other System/Platform trustworthiness**
- **Two other aspects of security/trust**
  - Data stored vs Data accessed/processed
  - System Idle vs Active (with User session)
- **Think about real life analogy: *Diplomatic/President's visit***



Security in SOA Collaborative Environment – Use Cases

- **Virtual Laboratory (VL) as Business Collaborative Environment**
  - Implementing Utility Computing paradigm
  - Can a VL provider offer a trusted experiment environment from the competitor’s point of view
    - Extreme usecase: *Will Pepsi Company trust to do analysis on the Coca-Cola VL facility?*
    - Common sense: *Remote System can be trusted as much as the administrator can be trusted*
- **Content providers (music, movie)**
  - Content played at the user PC/player should be protected from copying or useable during the service contract

Secure User Credential Storage

- **EGEE1 MJRA3.5 Deliverable "Secure Credential Storage" - https://edms.cern.ch/document/638872/**
  - Overview and security analysis of available credential storage methods
  - Suggested pro-active and countermeasures against identified security threats
- **Smartcard together with One-time Password (OTP) identified as a preferable solution**
  - Provides also solution for User/AuthZ session credentials storage
  - But this solution again as much secure as the user client/portal can be secured

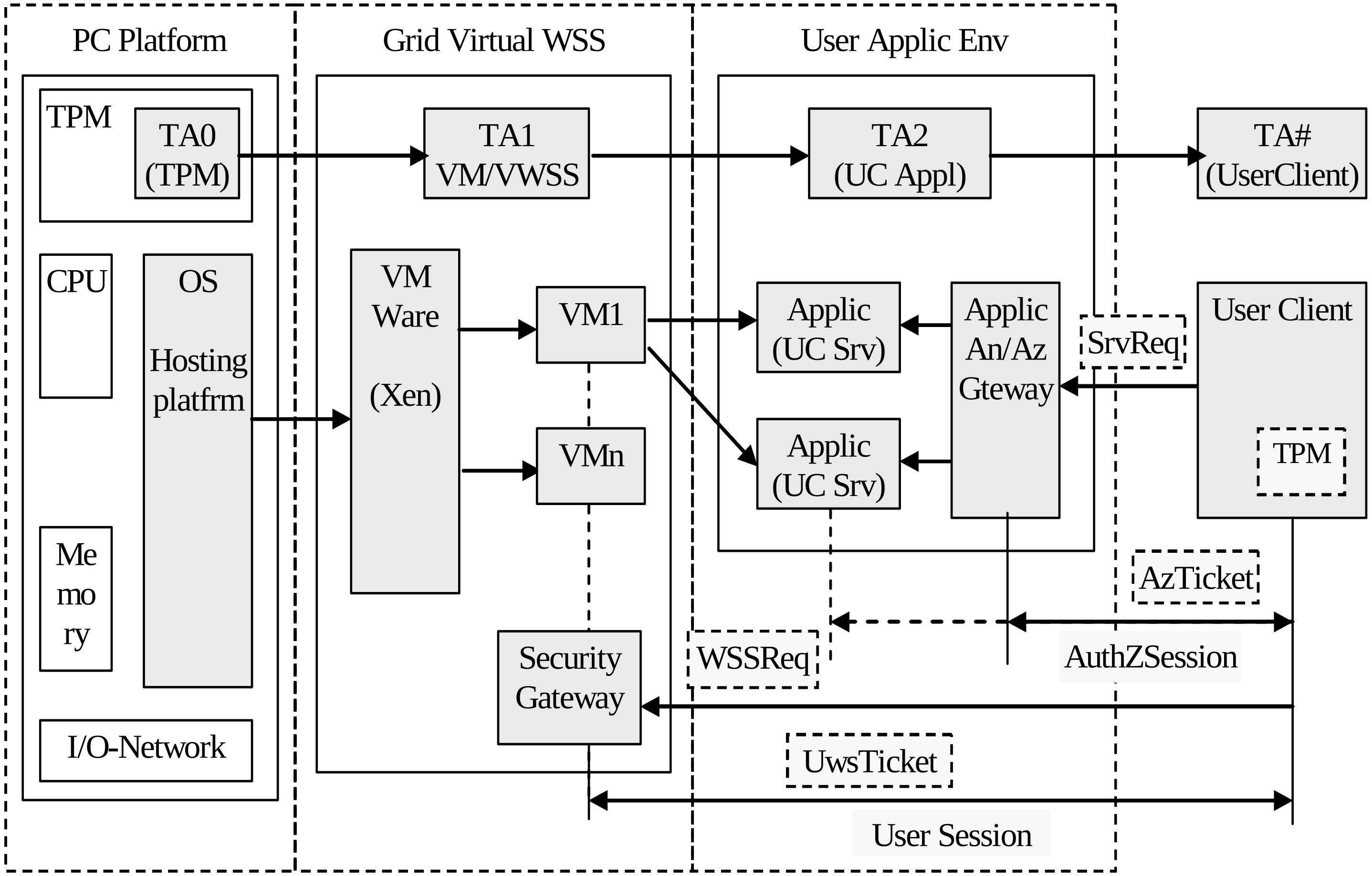
TCG Trusted Computing Platform

- **Promoted by the Trusted Computing Group (TCG)**
  - Basis for building and managing controlled secure environment for running applications and processing (protected) content
    - https://www.trustedcomputinggroup.org/home
  - Standards for trusted network, client, server and mobile agent
  - TMP software stack (TSS) defines API's for remote access, Identity Mngnt, PKI, Secure e-mail, file/folder encryption, etc.
- **TCG components**
  - **Trusted Platform Module (TPM)**
  - "Curtained memory" in the CPU
  - Security kernel in the OS and security kernel in each application
  - Back-end infrastructure of online security servers maintained by hardware and software vendors
- **Trusted Network Connect (TNC) – to enforce security policies before and after endpoints or clients connect to multi-vendor environment**

Trusted Platform Module (TPM)

- **Chip built-in into the computer system or a smartcard chip**
  - Can be considered as a platform tied “root-of-trust” and used for trusted platform registration and integrity assurance
- **Provides a number of hardware-based cryptographic functions**
  - **Asymmetric key functions** for on-chip key pair generation using hardware random key generation; private key signatures; public key encryption and private key decryption
  - An **Endorsement key** that can be used by a platform owner to establish that identity keys were generated in a TPM, without disclosing its identity
  - **Direct Dynamic Attestation (DAA)** that securely communicates information about the static or dynamic platform configuration, which is internally stored in TPM in the form of hashed values
  - Monotonic counter and the tick counter to enable **transaction timing and sequencing**
  - Protection of communication between two TPM
  - Secure key/data backup to another TPM

User-controlled Virtual Workspace Service (VWSS-UC) - 3 layer model



- Trust Anchors: T0 (TPM) – TA1 (VM/VWSS) – TA2 (Appl) – TA# (User)
- User and AuthZ Sessions

VWSS-UC – Implementation Suggestions

- **TPM Enabled computer platform**
  - http://www.tonymcfadden.net/tpmvendors.html
- **Xen v3.0 has already so-called Virtual TPM module**
  - http://www.cl.cam.ac.uk/Research/SRG/netos/xen/readmes/user
- **Grid Virtual Workspace Service (VWSS) – GT4 candidate component**
  - http://workspace.globus.org/
- **GAAA-AuthZ Authorisation session management supported by GAAAPI**
  - Proprietary and SAML based AuthZ ticket formats

Discussion

- **What is the vision for use of this technology?**