TERRA

Authored by: Garfinkel, Pfaff, Chow, Rosenblum, and Boneh

A virtual machine-based platform for trusted computing

Presented by: David Rager
November 10, 2004

Why there exists a need

- Commodity OS too complex to build securely upon
- Commodity OS poorly isolate apps
- Only weak mechanisms for peer authentication, making secure dist. apps difficult
- No trusted path between users and programs (authentication)

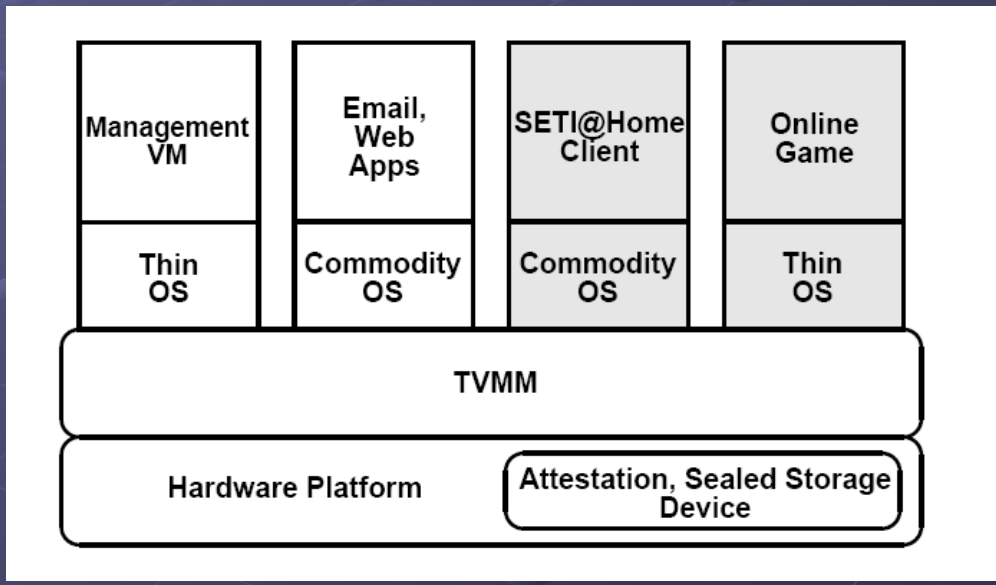
Current Solutions

- “Closed box” systems
- Good for limiting interaction but inflexible

Terra

- *Trusted Virtual Machine Monitor*
- “Secure” applications
  - *High-assurance*
  - *Tamper-resistant*
  - *General-purpose platform*
- Provide “open” or “closed-box” VMs
- Run existing software – highly compatible
- Trusted Quake to come….

Architecture



Features List

- Isolation – multiple applications in isolation
- Extensibility – small vs. large OS
- Efficiency – virtualizable hardware costs very little
- Compatibility – can run many OS's
- Security – relatively simple program
- Root Secure – cannot enter modify closed boxes
- Attestation – verifiable binaries
- Trusted Path

3 Means to Attestation

- Certifying the Chain
  - Private key embedded
  - Signed by hardware vendor
  - Hardware certifies firmware
  - Firmware certifies bootloader
  - Bootloader certifies TVMM
  - TVMM certifies VMs

3 Means to Attestation

- A component wanting to be certified:
  - Component generates public/private key
  - Component makes ENDORSE API call to lower level component
  - Lower level component generates and signs certificate containing:
    - SHA-1 hash of attestable parts of higher comp.
    - Higher comp's public key and application data

3 Means to Attestation

- Certifying VM itself
  - TVMM signs hash of all persistent data that defines the VM
  - Includes: BIOS, executable code, constant data of the VM
  - Does not include: temporary data
  - This difference is application defined

An Attestation Example

- Remote server verifies:
  - Hardware vendor's certificate
  - All hashes in certificate chain in remote server's list of authorized software
  - Hash of VM's attested storage is on list of authorized applications (valid version of Quicken)

Concerns

- Vendor key revocation
  - Extracting the vendor key from tamper-*resistant* hardware and publishing
- Privacy
  - Use Privacy Certificate Authority (PCA)?
  - PCA translates Hardware ID into random num
  - Group signatures (allows revocation)
- Interoperability of software
  - Attestation allows software to only operate under limited conditions (monopoly power)
- Digital Rights Management
  - Only play music on software that enforces limits

Platform Security

- “root” secure
- Independent OS/application vulnerability
- Attested software !--> Secure software (duh)

Storage Options

- Encrypted disks
  - HMAC
  - Encryption
- Integrity-checked disks
  - HMAC
- Raw disks
- A disk's hash makes up the primary ID of a VM

Storage Attestation

- Ahead-of-Time attestation
  - done during bootup
  - Computations for 1 GB of data take 8 seconds on 2.4 gHz
  - Single corrupt bit prevents booting
- Optimistic attestation
  - Assumes will attest correctly
  - Halts VM immediately on failed attestation

Device Drivers

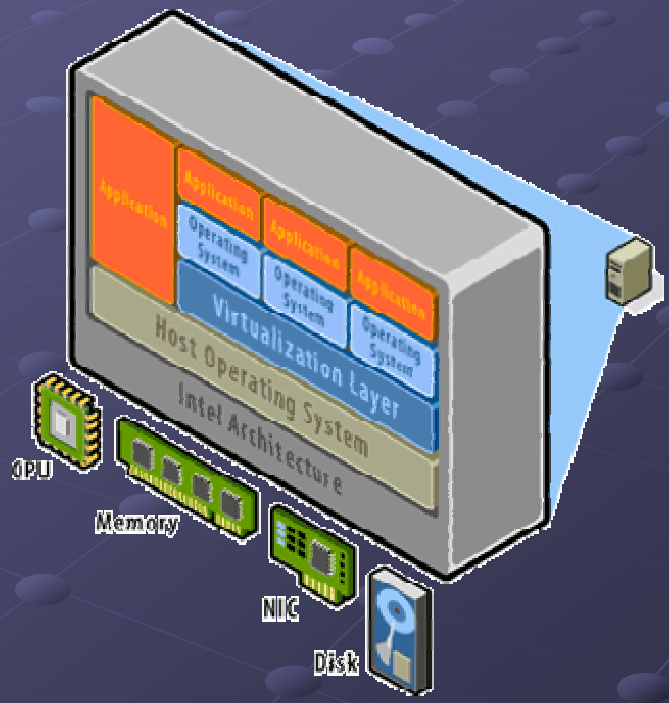
- Too large to be correct
- Protect TVMM via hardware memory protection and restricting access to sensitive interfaces
- Inherently insecure when outside TVMM (other OS's could spy on comm by exploiting drivers)

Hardware Support

- Sealed storage (key saved on disk)
- Can attest booted OS
- HW virtualization (make graphics cards and gigabit NICs fast)
- Secure counter (ideally a secure clock)
- Real-time resource management

Prototype Implementation

- VMware GSX Server 2.0.1 w/ Debian
- Comm btw VMs and TVMM's done with VMware serial device
- Secure storage
  - Ahead-of-Time trivial
  - Optimistic must hash entire block
- OpenSSL Library for certificate mgmt



Trusted Quake

- Closed-box VM boots Quake directly
- Attests to each other that hosts (clients and servers) running same version
- Boot times:
  - No attestation: 26.6 seconds
  - Ahead-of-Time: 57.1 seconds
  - Optimistic: 27.3 seconds
  - Optimistic + encryption: 29.1 seconds
  - No subjective difference in performance between ahead and optimistic

Trusted Quake (cont'd)

- Quake maintains shared secret for comm
  - Prevents aiming proxies
- Binary client integrity
  - Prevents mods that make characters further away seem larger than they are
- Server integrity
  - Prevents server from offering unfair advantages to some
  - Only allows trusted clients to connect

Trusted Quake (cont'd)

- Can't prevent:
  - Bugs
  - Network DOS attacks (lag help)
  - Out-of-band collusion (telephone)

Trusted Access Points (TAPs)

- Can secure corporate VPN endpoints
- Prevents source forging
- Prevents DOS attacks
- Scalability

Conclusion

- Both “open-box” and “closed-box”
- Hardware support helpful and even required
  - Requires tamper-resistant hardware
- Optimistic attestation better
- Like current VMware products, but with emphasis on security
- Provides peer attestation

Resources

- http://www.vmware.com/products/server/gsx_features.html
- Terra: A Virtual Machine-Based Platform for Trusted Computing