Transparent Mobile Storage Protection in Trusted Virtual Domains

Luigi Catuogno[1], Hans Löhr[1], Mark Manulis[2], Ahmad-Reza Sadeghi[1], Marcel Winandy[1]

[1]Ruhr Universität Bochum (Germany)
[2]Technische Univ.Darmstadt – Center for advanced Security Research Darmstadt (CASED)

Mobile Storage Devices (MSD)

- Memory devices used as “portable hard disks”.
  - Pluggable into a wide variety of equipments (e.g., cameras)
  - Robust, reliable and flexible
- However
  - Raise several security issues

Security Issues with MSD

- Can be intercepted by outsiders
  - Unauthorized read & manipulation of sensitive data
- However
  - Usage policy and restrictions not sufficient
    - Impacts on flexibility
    - Policies are often error prone

Goals

- Flexible and transparent deployment of MSDs within the same organizational network
  - Guaranteeing data confidentiality and integrity
    - Prevention of unauthorized access by outsiders
    - Prevention of unintentional keys/data disclosure by insiders
  - Enforcing access policy also when the platform is off-line.

Trusted Virtual Domains (TVD)

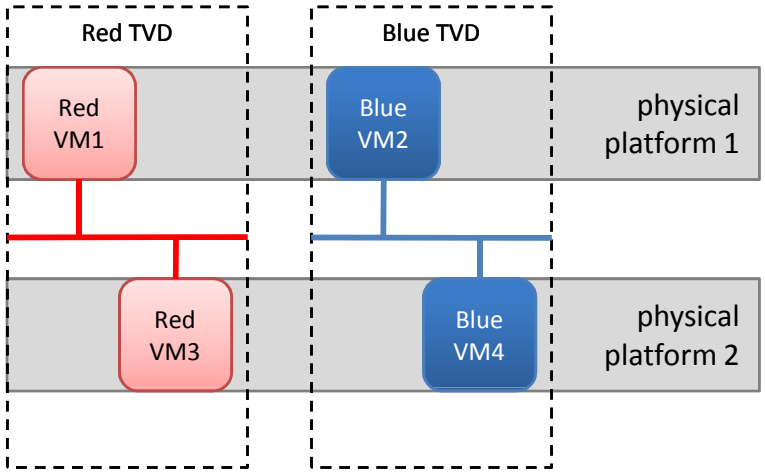
- The forthcoming framework to implement multi-domain/single-infrastructure computer networks
  - Externalized data centers
  - Organizational intranets which require the separation of different data flows.

Trusted Virtual Domains

Trusted Virtual Domains (TVD)

- Coalition of Virtual Machines that:
  - Trust each other
  - Enforce a common security policy (TVD Policy)
  - Span over a physical infrastructure, shared with other TVDs

Trusted Virtual Domain



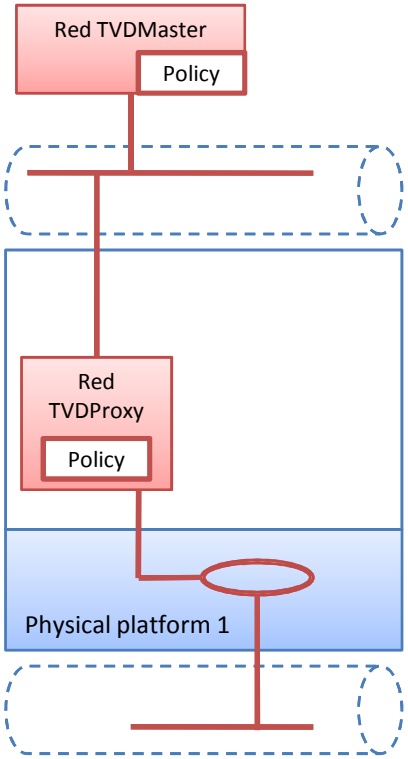
- Virtual machines of different TVDs are separated even if running on the same platform
- Virtual machines of the same TVD are connected through a dedicated and isolated VLAN

TVD Architecture

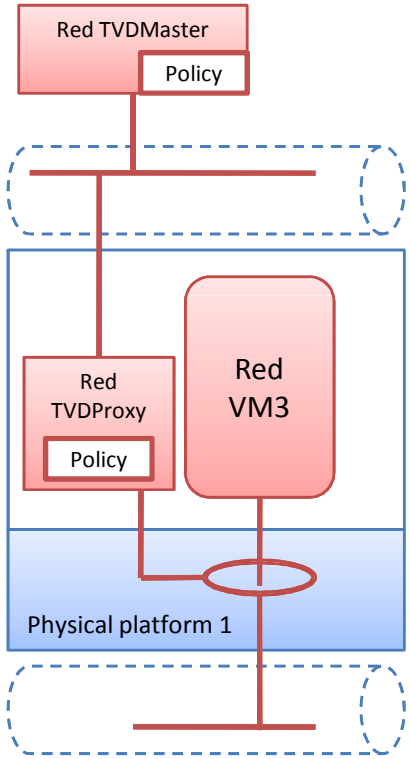
- TVD Master
  - A special node that controls the access to the TVD is done by following the admission control rules specified in the TVD Policy
- TVD Proxy
  - A compartment deployed on each platform to locally enforce the TVD Policy

Trusted Virtual Domain

Deployment & Joining



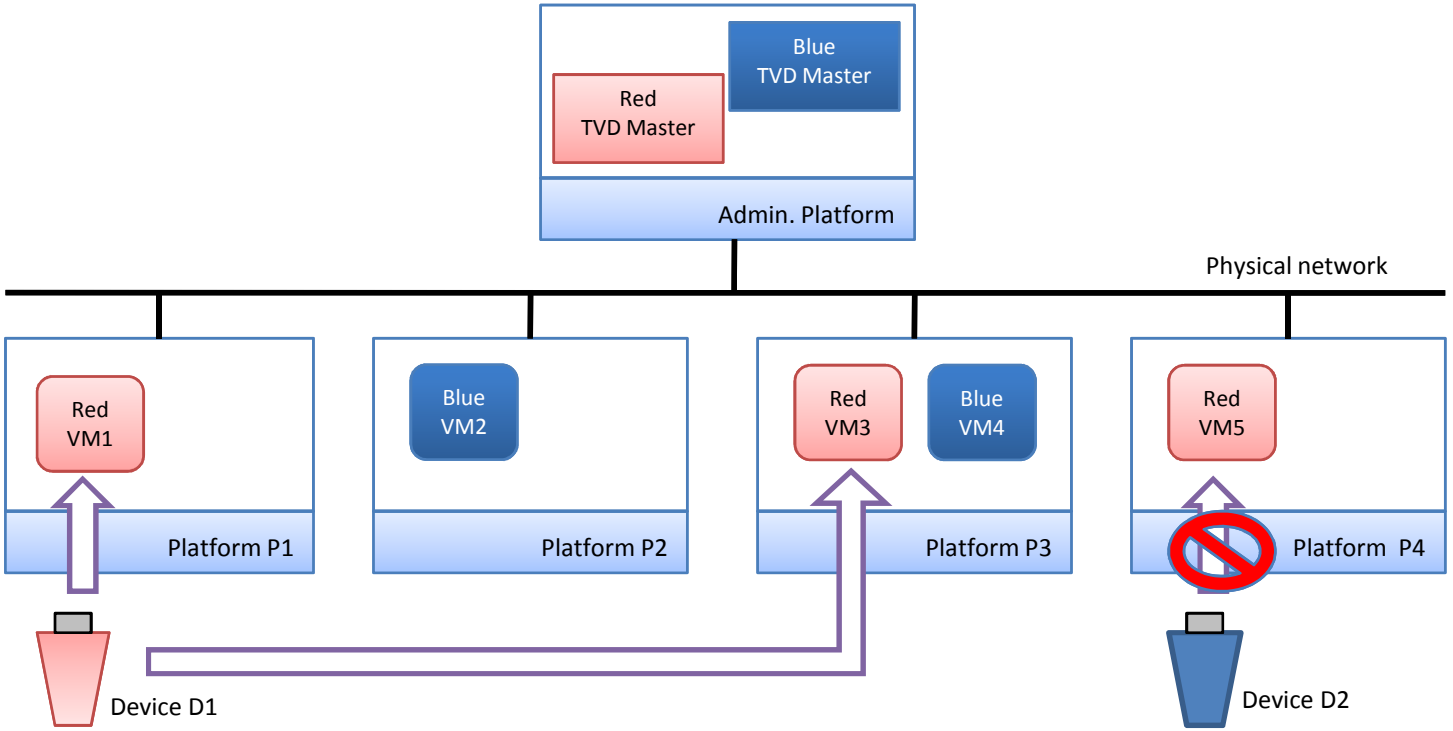
TVD Deploy



TVD Join

Our Proposal: System operation

Handling Mobile Storage Devices



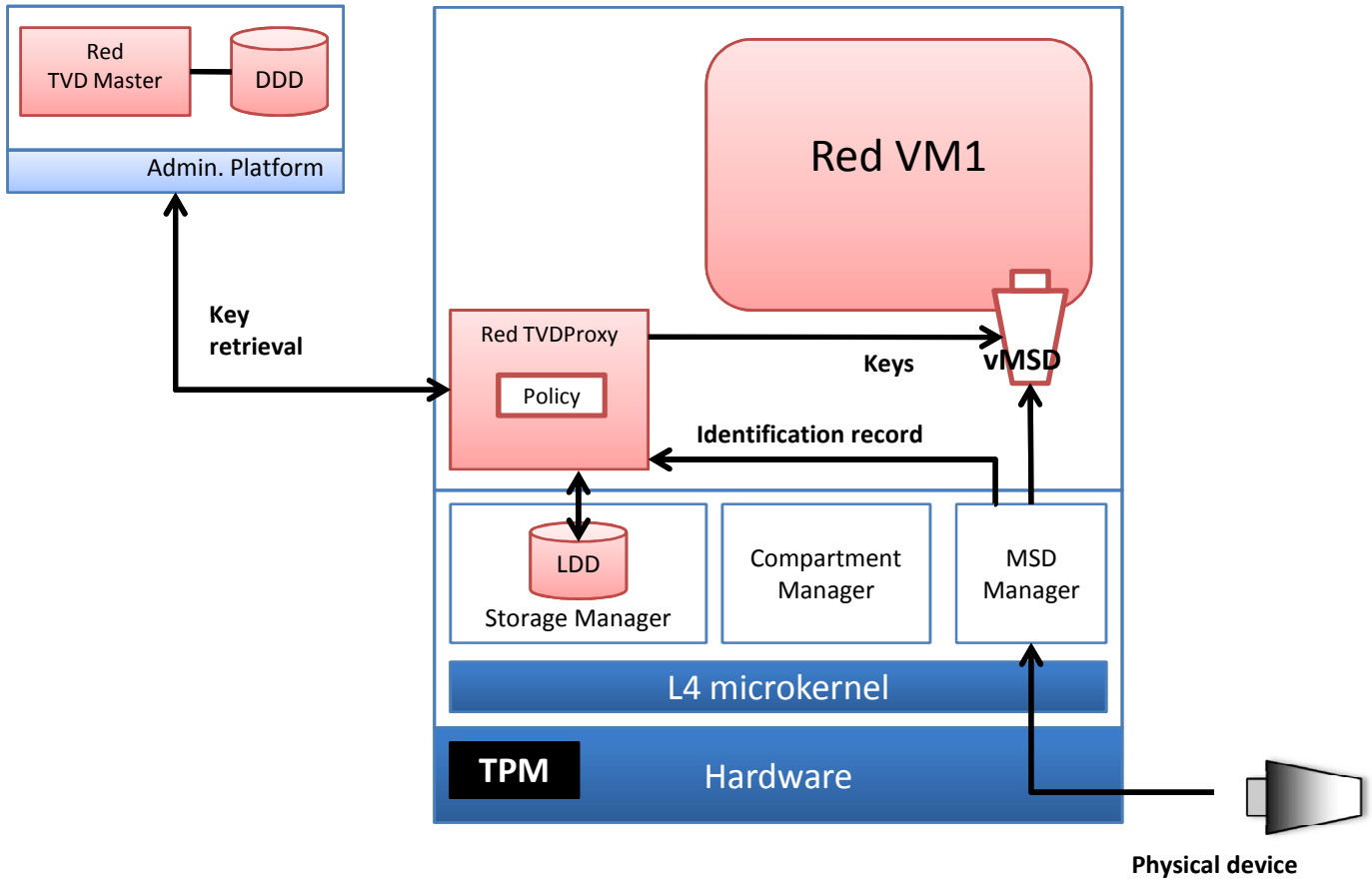
Requirements

- Different MSDs may unpredictably appear and disappear within the TVD
  - **Device identification.** Whenever an MSD is plugged in, the platform should be able to distinguish the device and the domain this device belongs to.
  - **Dynamic device management.** The architecture should be able to enforce the policy and deliver the correct encryption keys wherever the device is plugged-in
  - **Transparent and mandatory data encryption and signature.**

Our Solution

- **Device identification.** A unique identification record (IR) is assigned to the device when it is *initialized*
- **Key retrieval.** Encryption (and signing) keys are indexed with the IR and stored in a two level database (Local/Domain Device Directory)
- **Access Policy Enforcement** Is accomplished by the TVD infrastructure. Device access policy is incorporated into the TVD Policy.
- **Device Access.** Data encryption/integrity verification is transparently done by a specific component on the platform and is not in charge to the “user” VM.

The Platform Architecture



Our Proposal:
Data Encryption and Storage

Accessing data

- Each device is associated to a unique encryption key
- Each platform has an individual signing key for each device and a shared public key
- Written data are encrypted and signed
- Reads succeed only if data has a valid signature

Encryption Scheme

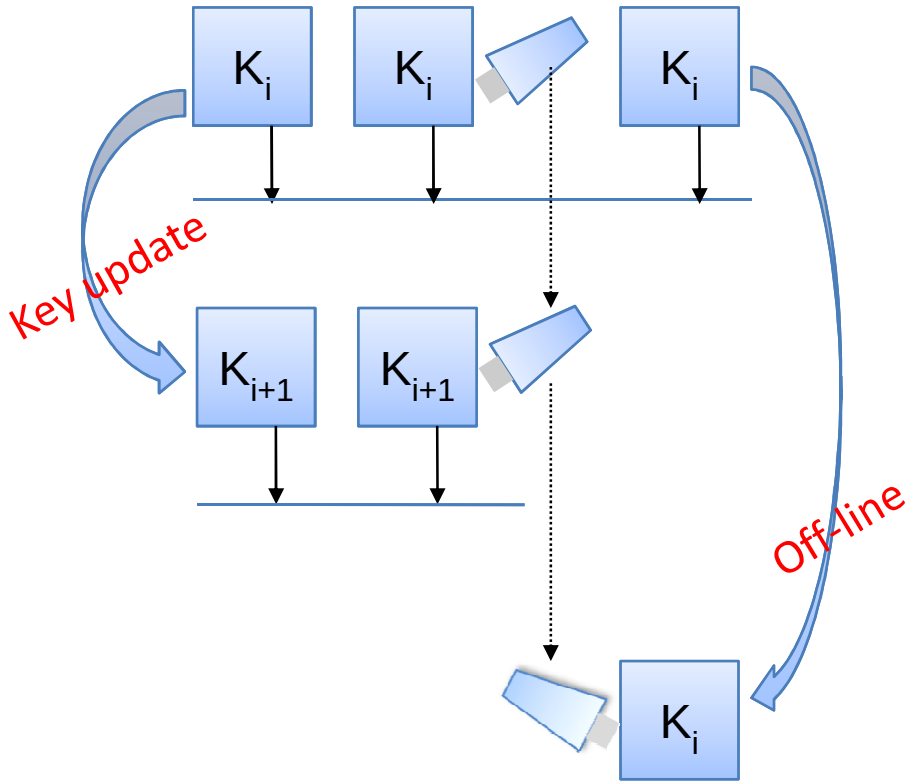
- Lazy revocation:
  - Triggers re-encryption of only newly modified data
  - Not all distributed data has to be re-encrypted
  - Whenever a user is revoked
    - A new key is delivered to remaining users
    - Encryption is done always with the most recent key

Off-line access to MSDs

Off-line scenario: requirements

- **Delegation.** Off-line platforms should be able to enforce the access control policy
- **Delayed re-encryption.** Off-line platforms should be enabled to access data written up to the time they were on-line
- **Traceability and recovery.** Domain member should be able to track ad revert unauthorized data changes

Off-line scenario: our solutions



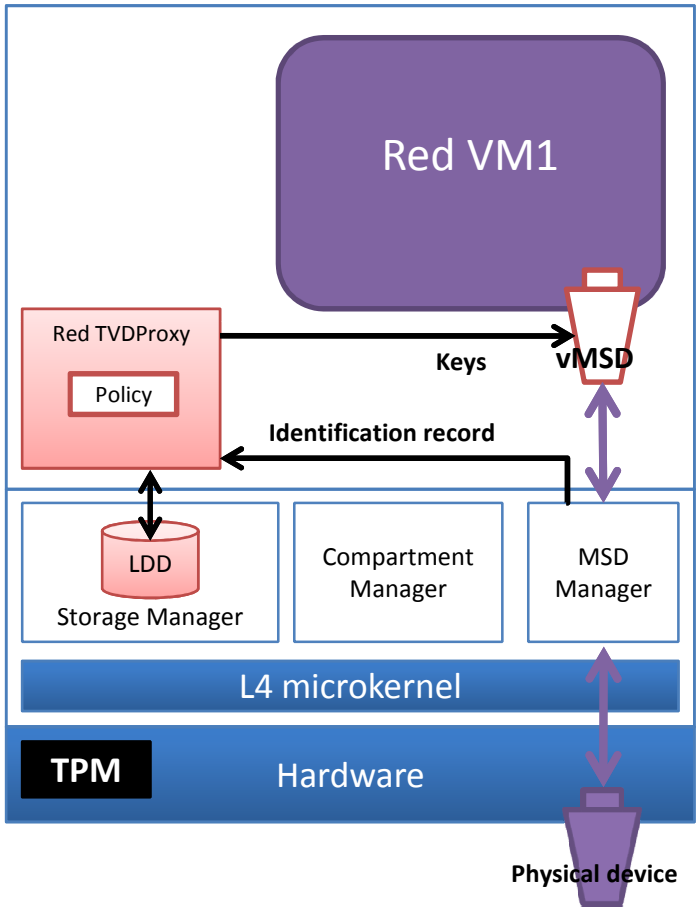
- **Delegation:** off-line platforms store keys into their LDD
- **Delayed re-encryption:** Lazy revocation of encryption keys allows off-line platform to access (at less) old-data.

Off-line scenario: our solutions

- **Traceability and recovery**: Employing a versioning file system to keep track of all modifications.
  - Off-line platforms are enabled to access the most recent version they can decrypt
  - Whenever a revocation occurs it is possible to revert all changes done by revoked platforms

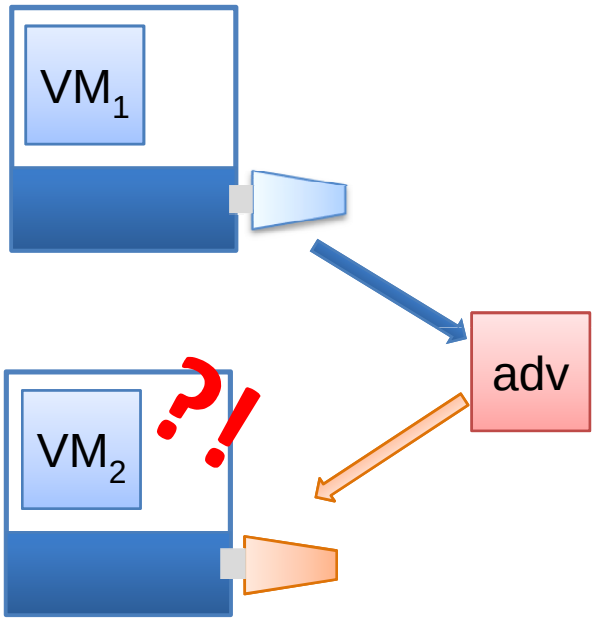
Security considerations

Attacks to the “user machine”



- The adversary could exploit any VM:
  - Enjoys its data access privileges
  - cannot access or handle the keys
  - Cannot override the TVD Policy
  - Keys in the LDD cannot be accessed by corrupted compartments
  - Cannot tamper the device’s IR

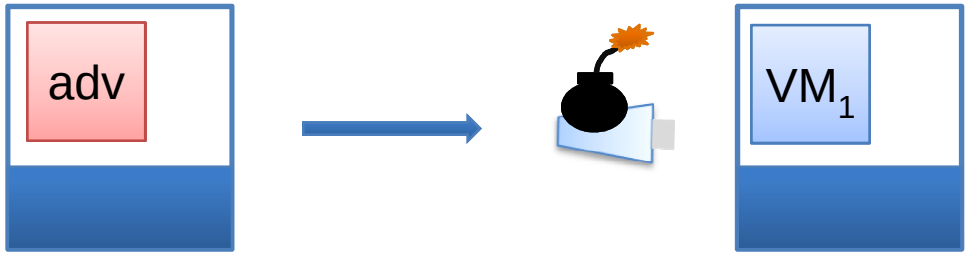
Attacks to MSDs



- Denial of Service
  - file deletion/corruption
  - device re-initialization
- Roll-back
  - Bringing back the device at a certain time in the past by overwriting the current file system with an older (though legitimate) image

Attacks to off-line platforms

- Revoked platform can exchange data with unaware off-line platforms.
  - Provide corrupted data



Conclusion

Results

- Free and transparent deployment of MSDs within the same TVD
  - Coherently incorporated into the TVD infrastructure
  - Data confidentiality and integrity through transparent and mandatory encryption and signature
  - Decentralized Access Policy enforcement
    - Even while data is accessed by an off-line platform

Future Direction

- File system improvement
- Preventing the diffusion of malware through MSDs

Further Info

- System Security Lab at Ruhr Universität Bochum (DE)
  - http://www.trust.rub.de
- Turaya Security Kernel
  - http://www.emscb.org
- OpenTC: EU Project featuring an implementation of Trusted Virtual Domain
  - http://www.opentc.net

Thank you!