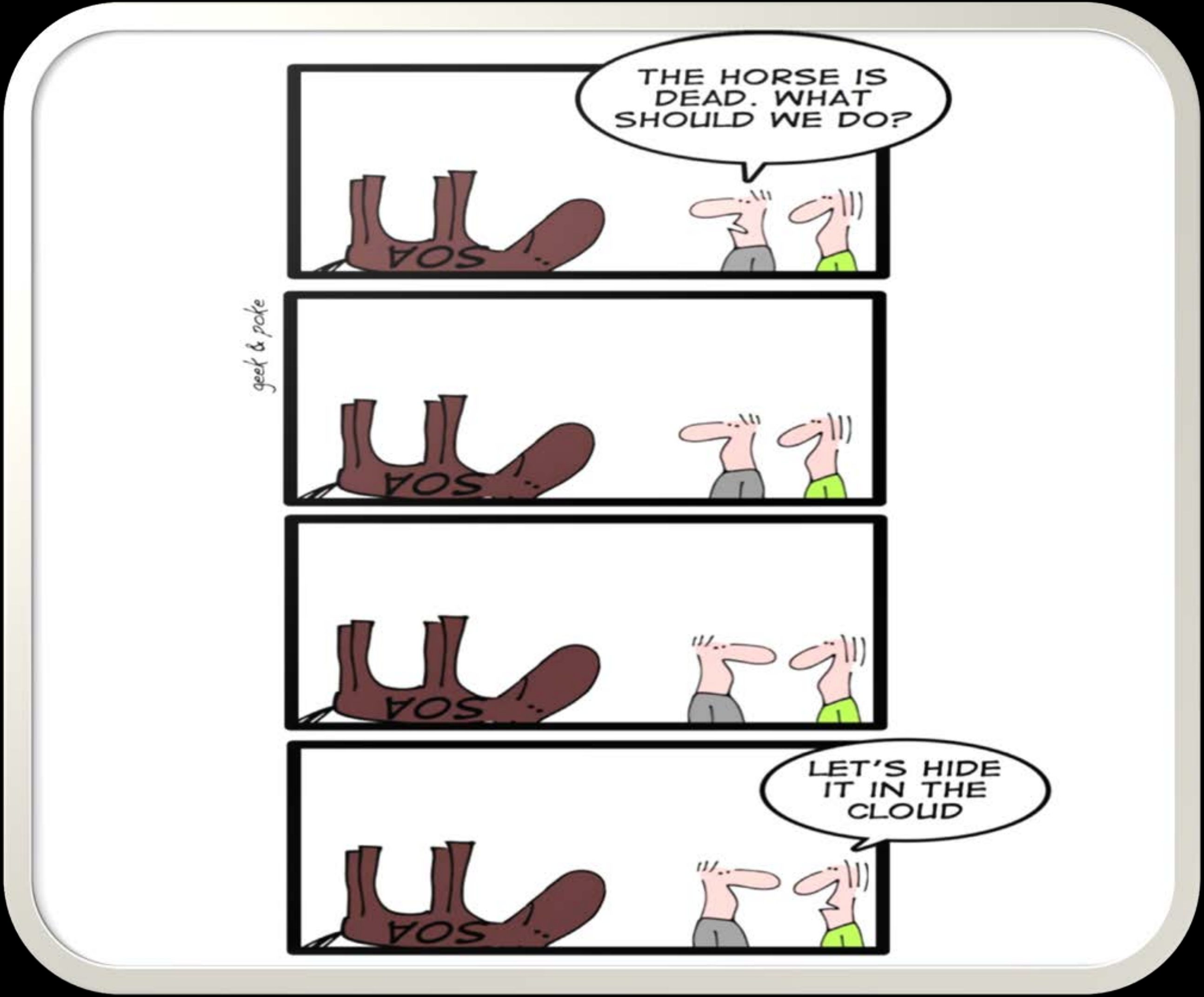
Mobile Trusted Virtual Domains

Ahmad-Reza Sadeghi

ahmad.sadeghi@trust.cased.de

System Security Lab
Technische Universität Darmstadt,
Fraunhofer SIT, Darmstadt,
Germany

The Monolithic Cloud!

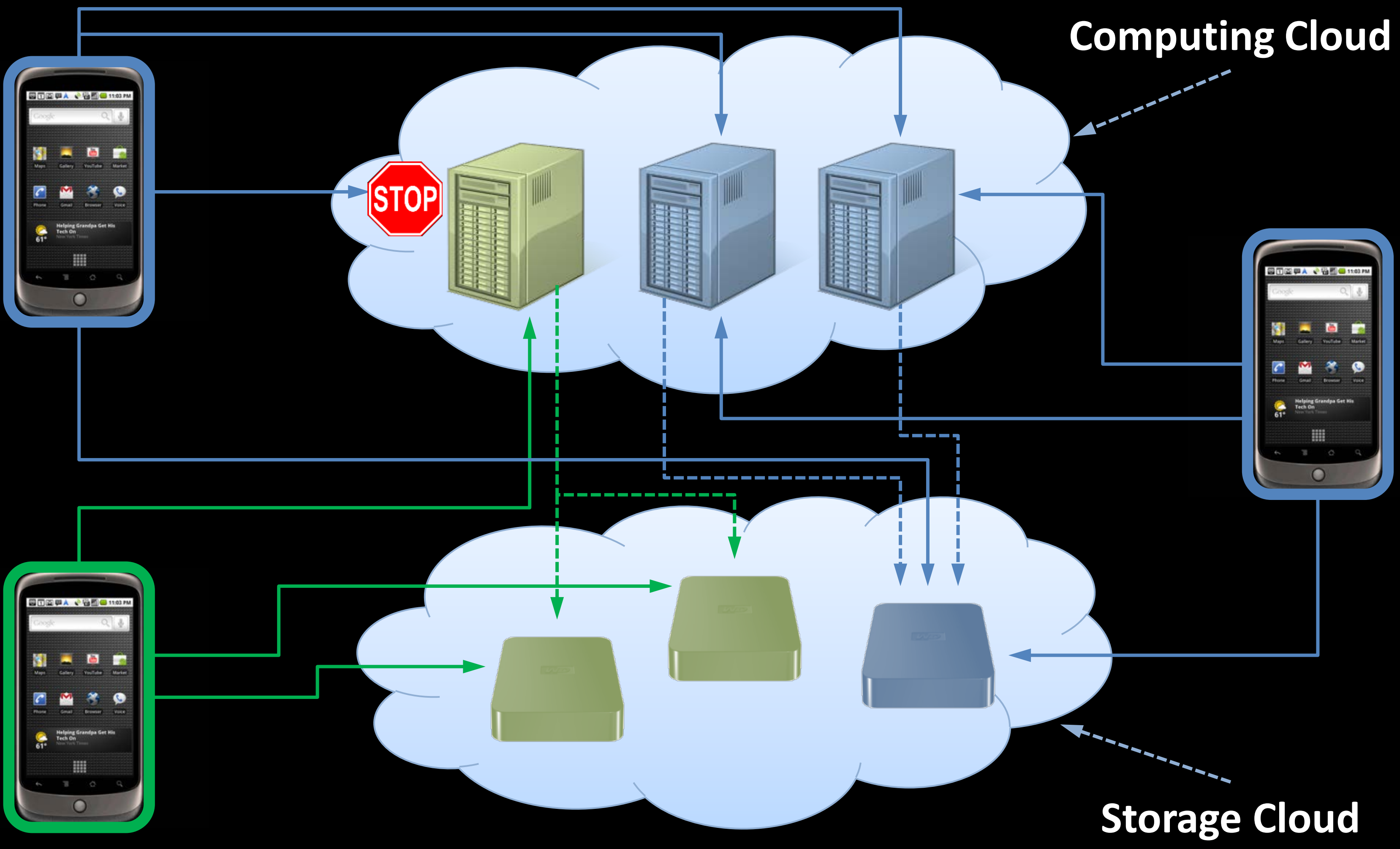

THE HORSE IS DEAD. WHAT SHOULD WE DO?
SOA
SOA
SOA
LET'S HIDE IT IN THE CLOUD
SOA
geek & poke

The Buzzword Jungle

Secure and Trusted Computing,
Virtualization,

Hypervisor, Microvisors, Virtual Box, EC2,
VM Leakage, Mobile Clouds, ….

Summary and Conclusion

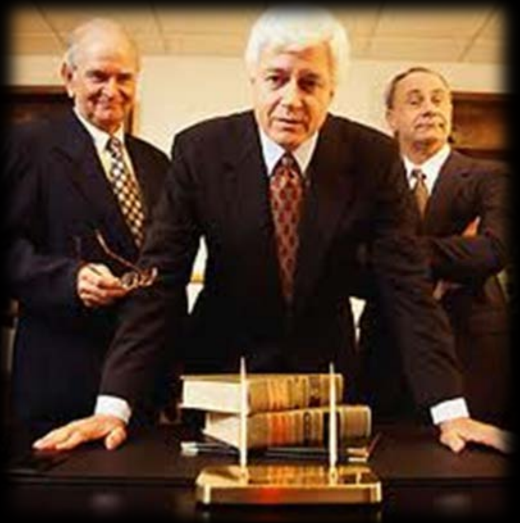


A Note on Notions

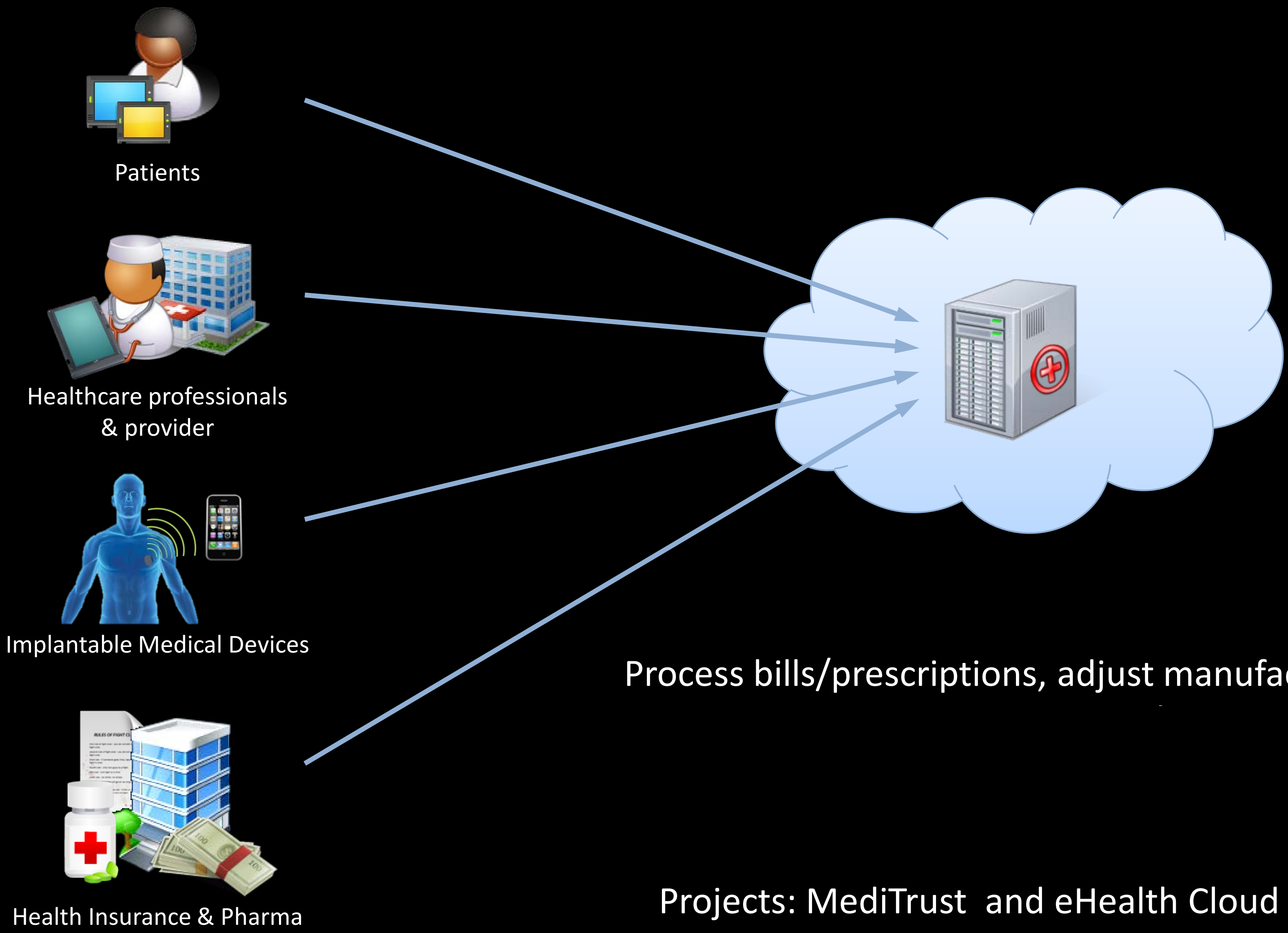
Secure (Multiparty) Computation (no TTP) The Ultimate Solution for Clouds?

“Trustworthy” Computing

A Frustrating Application Scenario: eHealth Cloud



Advanced e-Health Cloud



Patients

Healthcare professionals
& provider

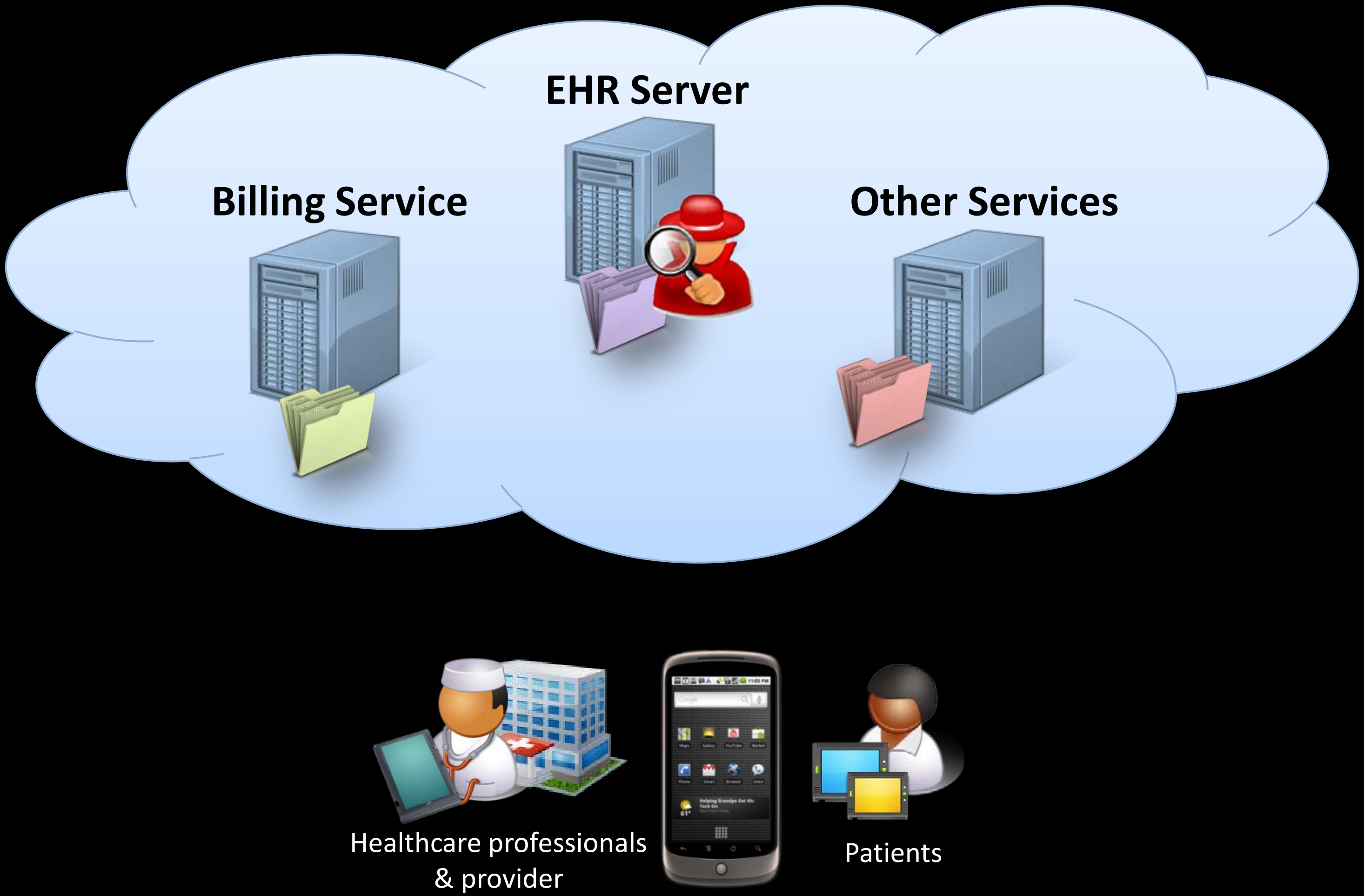
Implantable Medical Devices

Health Insurance & Pharma

Process bills/prescriptions, adjust manufacturing,…

Projects: MediTrust and eHealth Cloud

Platform Security (Server)



EHR Server

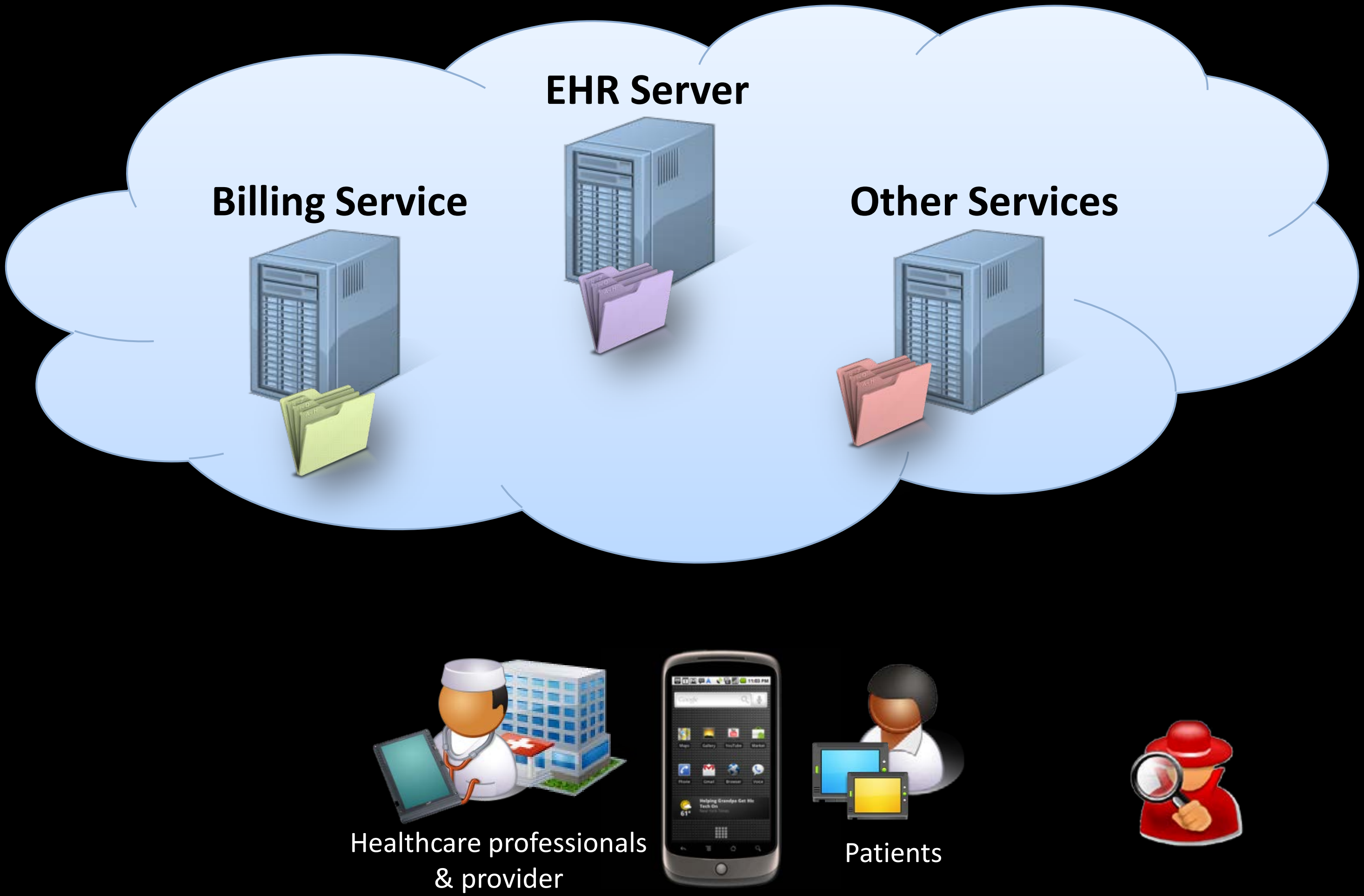
Billing Service

Other Services

Healthcare professionals & provider

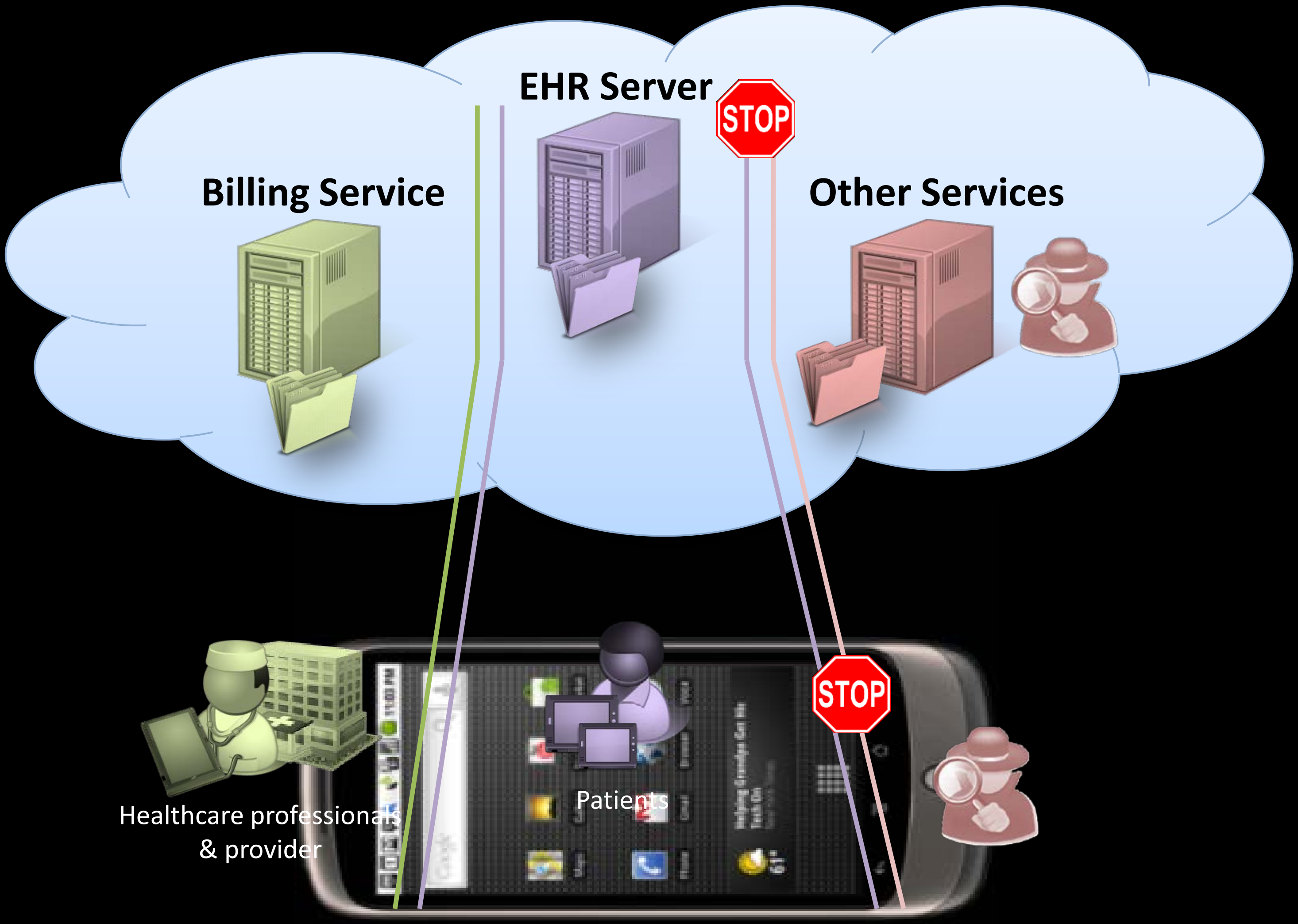
Patients

Platform Security (Client)



unauthorized access
(read/modify)

Privacy Domains



H. Löhr, A.-R. Sadeghi, M. Winandy. Securing the E-Health Cloud. IHI 2010

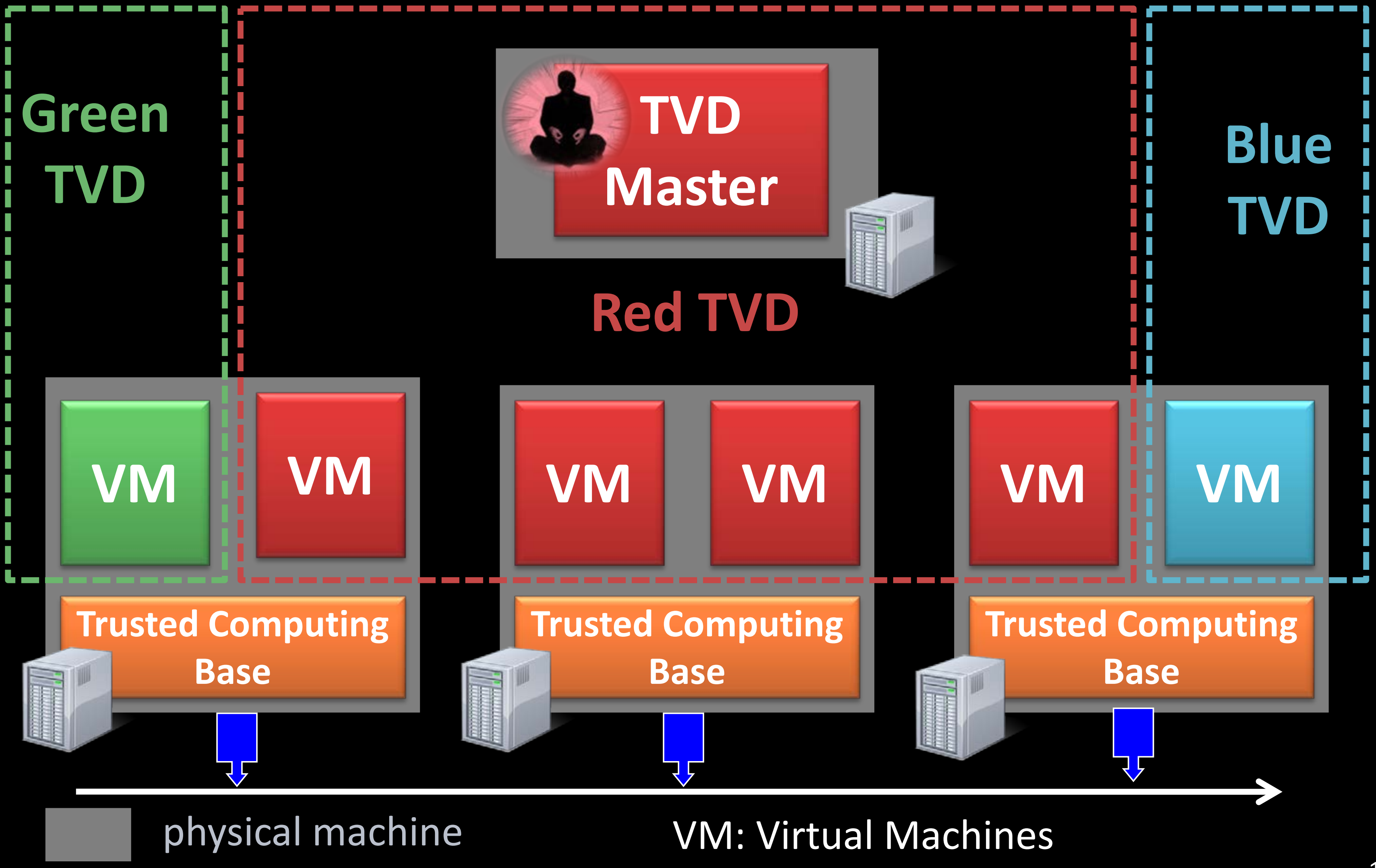
Background on TVDs

- S. Cabuk, C. I. Dalton, H. Ramasamy, M. Schunter. Towards automated provisioning of secure virtualized networks . CCS 2007
- Towards Automated Security Policy Enforcement in Mlti-Tenat Virtual Data Centers: Ahmad-Reza Sadeghi, Christian Stüble, Serdar Cabuk, Chris I. Dalton, Konrad Eriksson, Dirk Kuhlmann, Hari Govind V. Ramasamy, Gianluca Ramunnok, Matthias Schunter *Journal of Computer Security* 2010

Trusted Virtual Domains (TVD)

- **A coalition of virtual and/or physical machines**
  - Trust based on a security policy beyond physical boundaries
- **TVD members can ``see'' and access each other but are closed to non-members**
  - Separation of workflows and workloads
- **More abstract than typical access control mechanisms**
  - Platform independent, suitable for large distributed systems
- **Use mainly existing technologies**
  - E.g., isolation among TVDs using virtual LAN (VLAN) and VPN

Logical TVD Architecture



VM: Virtual Machines

Security Objectives & Requirements

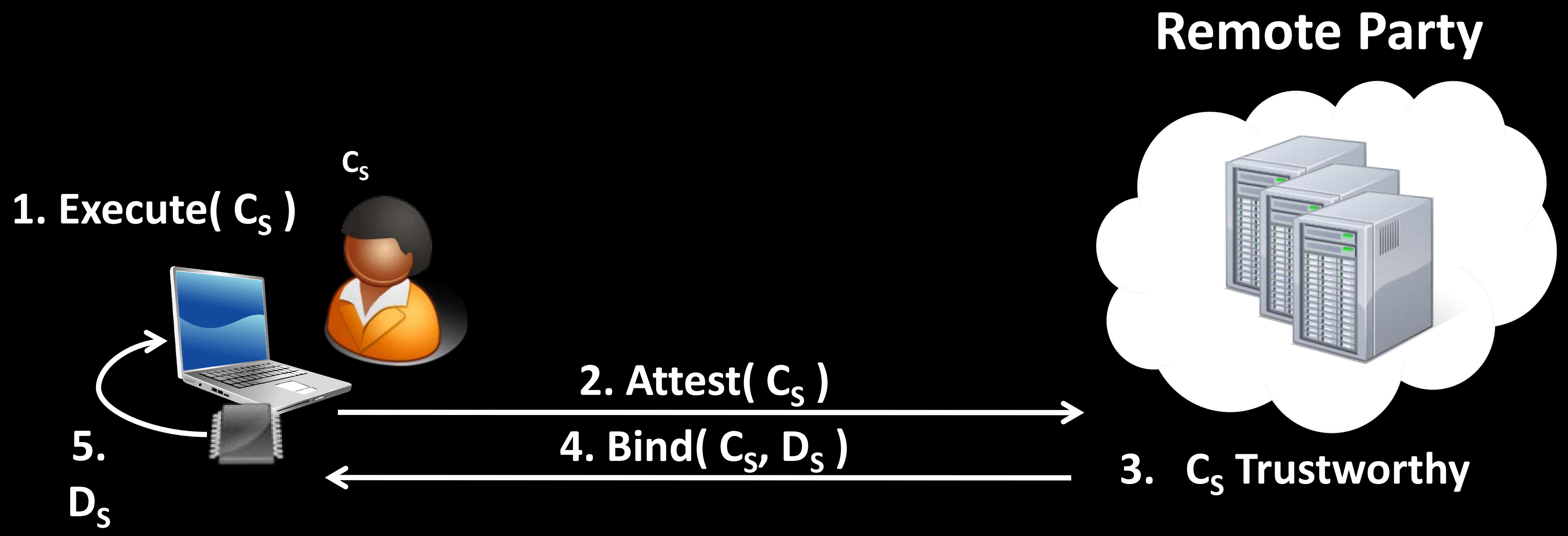
- **Secure TVD membership and revocation**
  - Platforms, VMs, …
- **Secure intra-TVD communication**
  - However, some members of TVD may have more privileges than others
- **Secure inter-TVD communication**
  - Usually undesired (due to isolation) to control information flow

Challenges

- **How to determine, represent, and verify trustworthiness of platforms / virtual machines**
  - Even a secure OS cannot verify its own integrity
- **How could common computing platforms support such a functionality?**

The TCG Approach (Simplified)

1. System Integrity Report and Verification (Attestation)
2. Access Control based on System State (Binding/Sealing)



C_S Initial System State (Hard- und Software)

D Sensitive Data

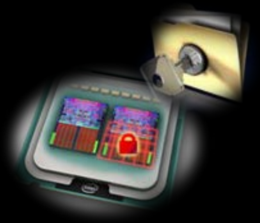
Main Components of TVD

- **TVD Policy**
  - Admission control for virtual/real machines to join TVD
  - Inter/Intra-TVD communication policy

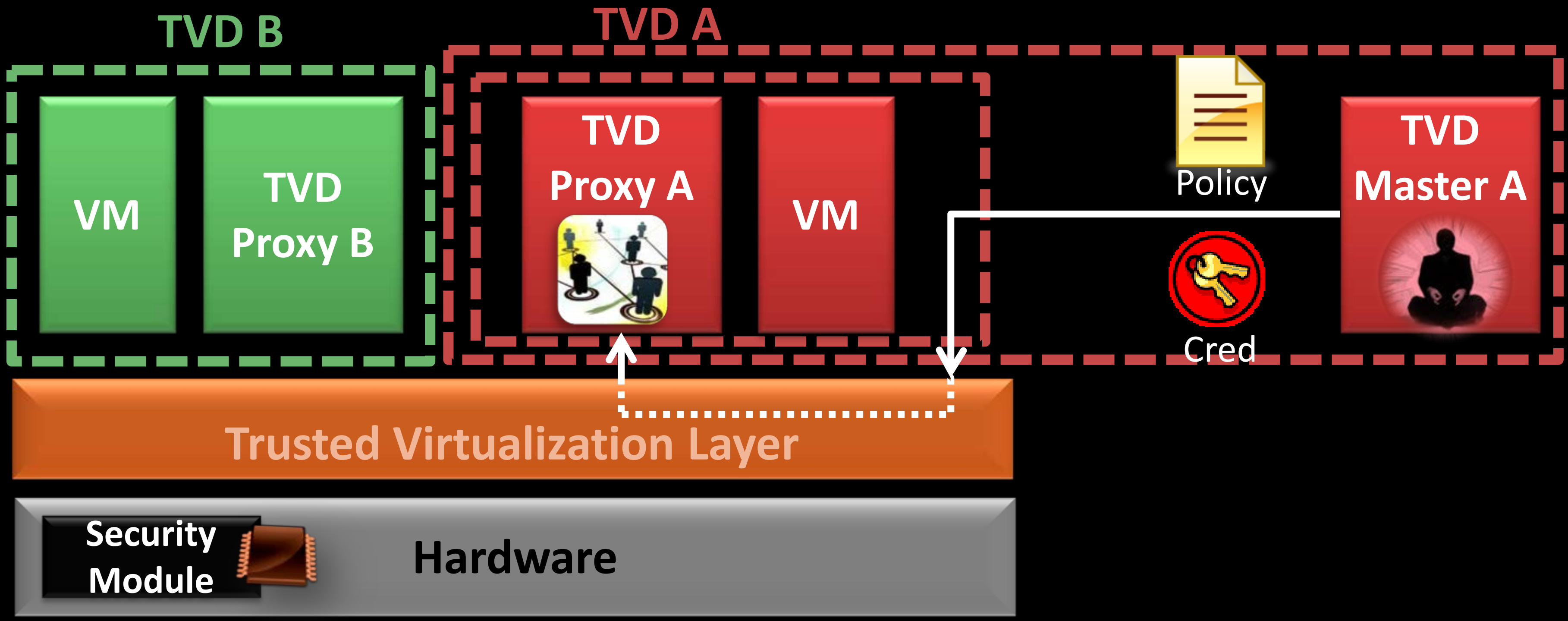
- **TVD Master**
  - Controls access to TVD according to TVD policy
  - Rules include platforms integrity measurements

- **TVD Proxy**
  - Local proxy of TVD Master on each physical platform
  - Responsible for local enforcement of TVD policy
  - Several TVD proxies can reside on one physical platform

- **Trusted Computing functionality**
  - TPM/MTM support

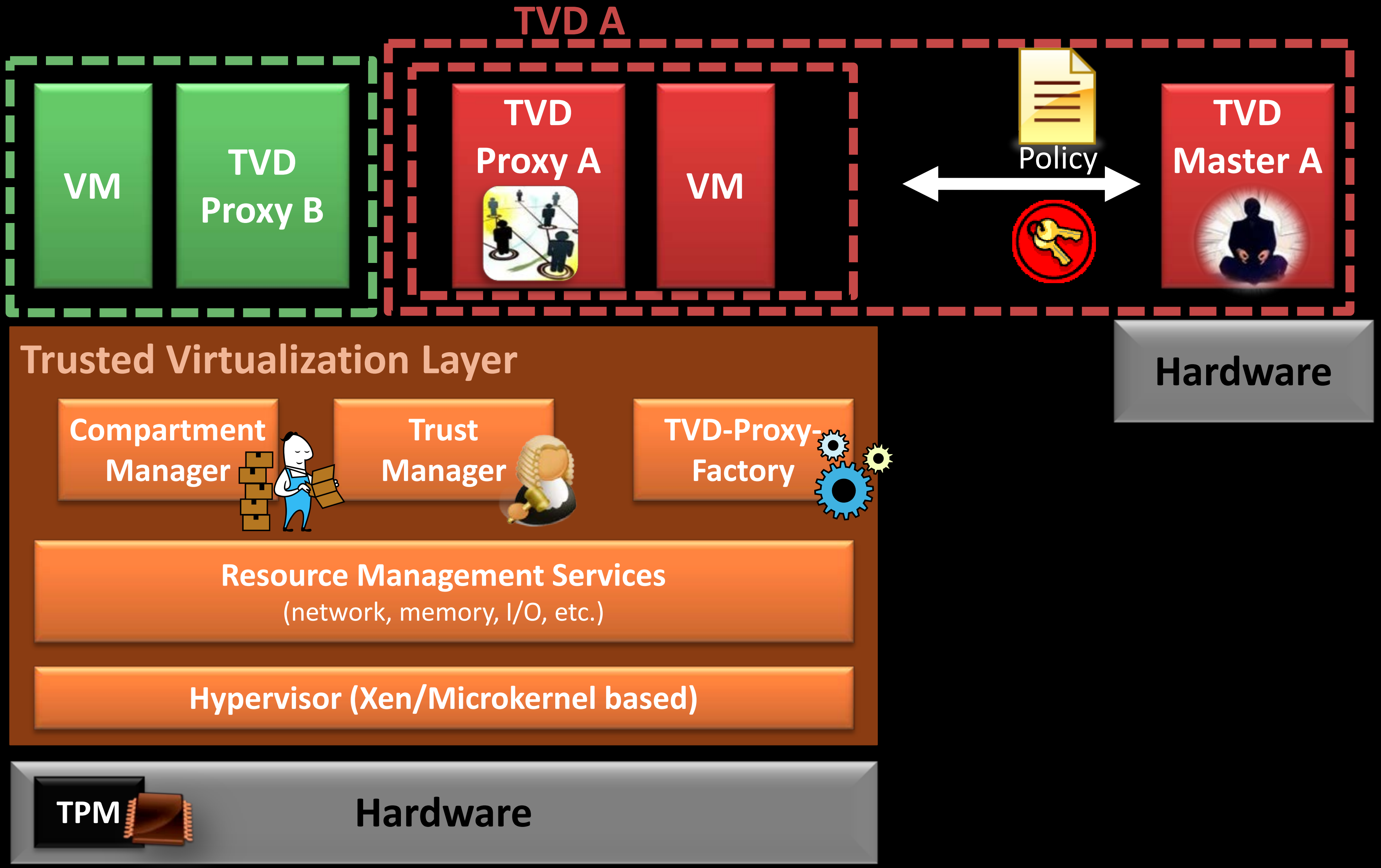


TVD Architecture



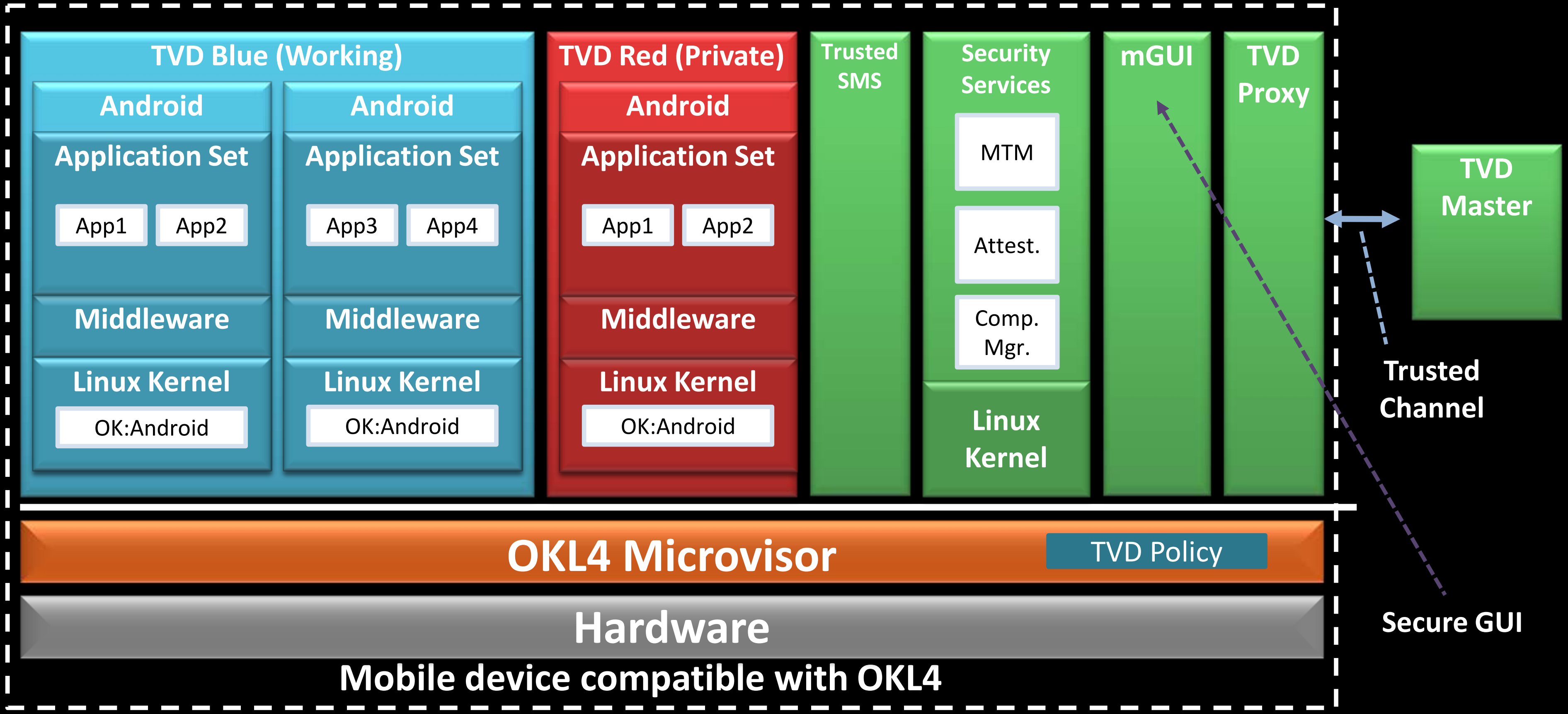
1. Create TVD Master and initialize it with TVD requirements and policy
2. Setup a trusted channel to TVD Master and receive policy
3. Create and configure TVD Proxy (local representative of TVD)
4. TVD Proxy instantiates and configures required TVD specific modules (e.g., vSwitches, VLAN tagging module, VPN,…)
5. VM asks TVD Proxy to join the TVD based on TVD policy (if positive connect VM)

TVD Implementation Architecture


TVD A
VM
TVD Proxy B
TVD Proxy A
VM
Policy
TVD Master A
Hardware
Trusted Virtualization Layer
Compartment Manager
Trust Manager
TVD-Proxy-Factory
Resource Management Services
(network, memory, I/O, etc.)
Hypervisor (Xen/Microkernel based)
TPM
Hardware

Mobile TVDs
based on Microvisors

Integration of TVD Main Components

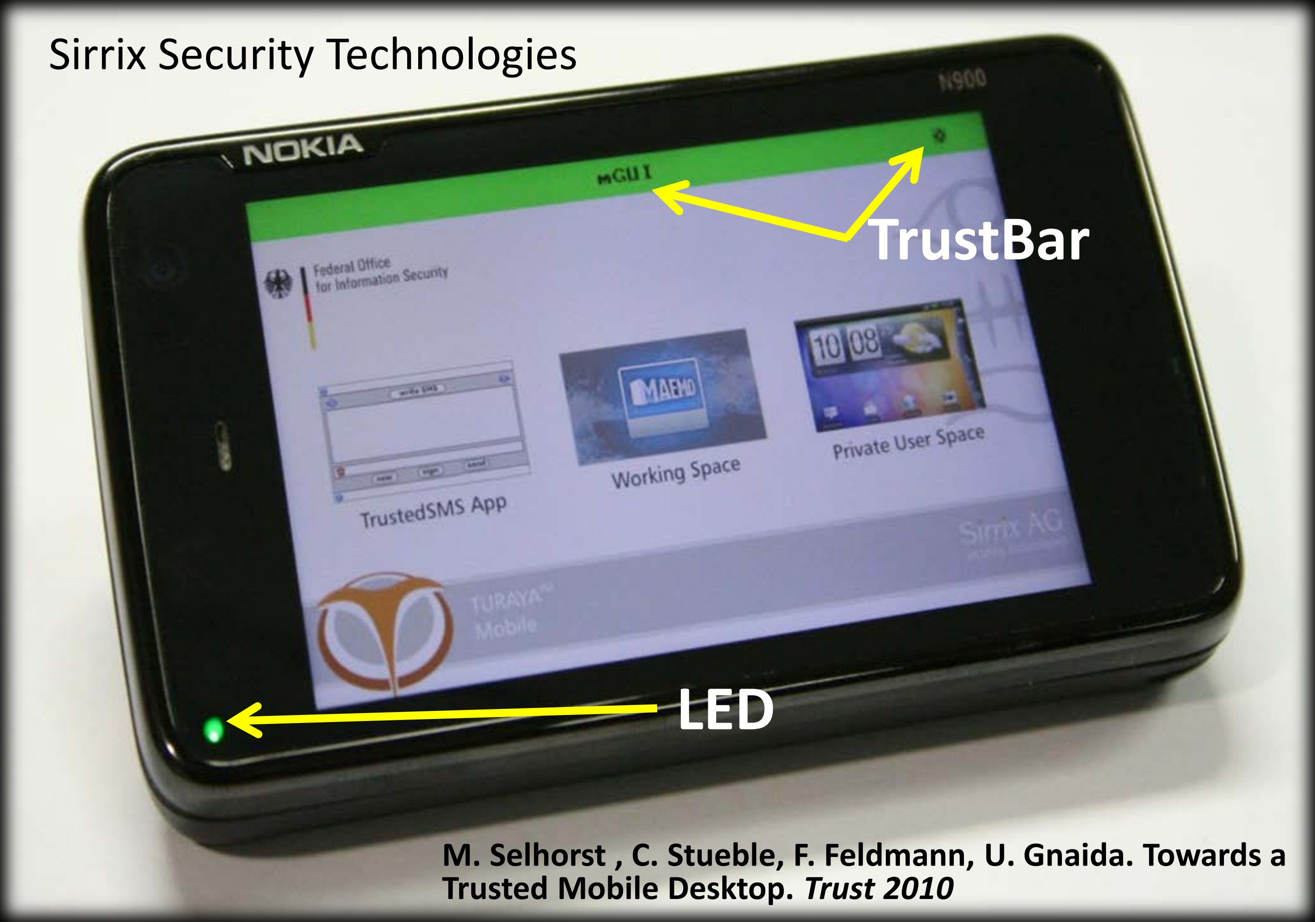


Pro and Contra

- **Pro:**
  - Supports different operating systems (Linux, Symbian, Android)
  - Very fast switching between different Compartments and TVDs
- **Contra:**
  - Short development cycles

Towards Mobile TVDs

- **Trusted Mobile Desktop**
  - Provides secure GUI and isolation of operating systems and stand-alone trusted applications (e.g., SMS application)

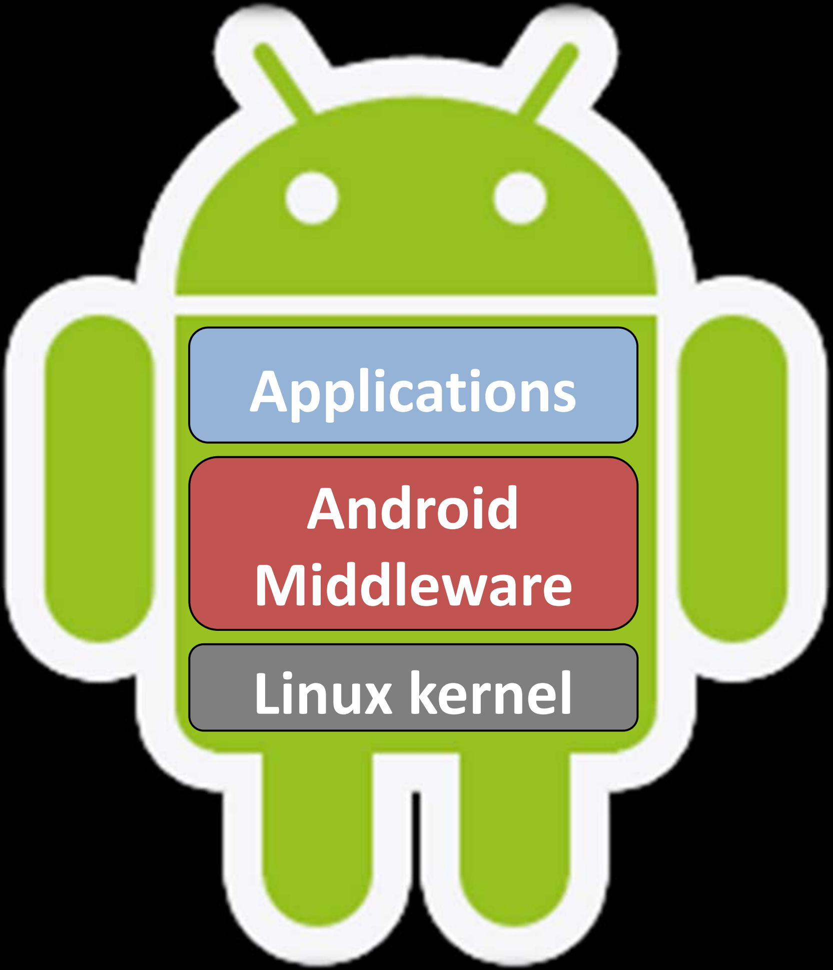


M. Selhorst , C. Stueble, F. Feldmann, U. Gnaida. Towards a Trusted Mobile Desktop. *Trust 2010*

Mobile
TVDs based on Android

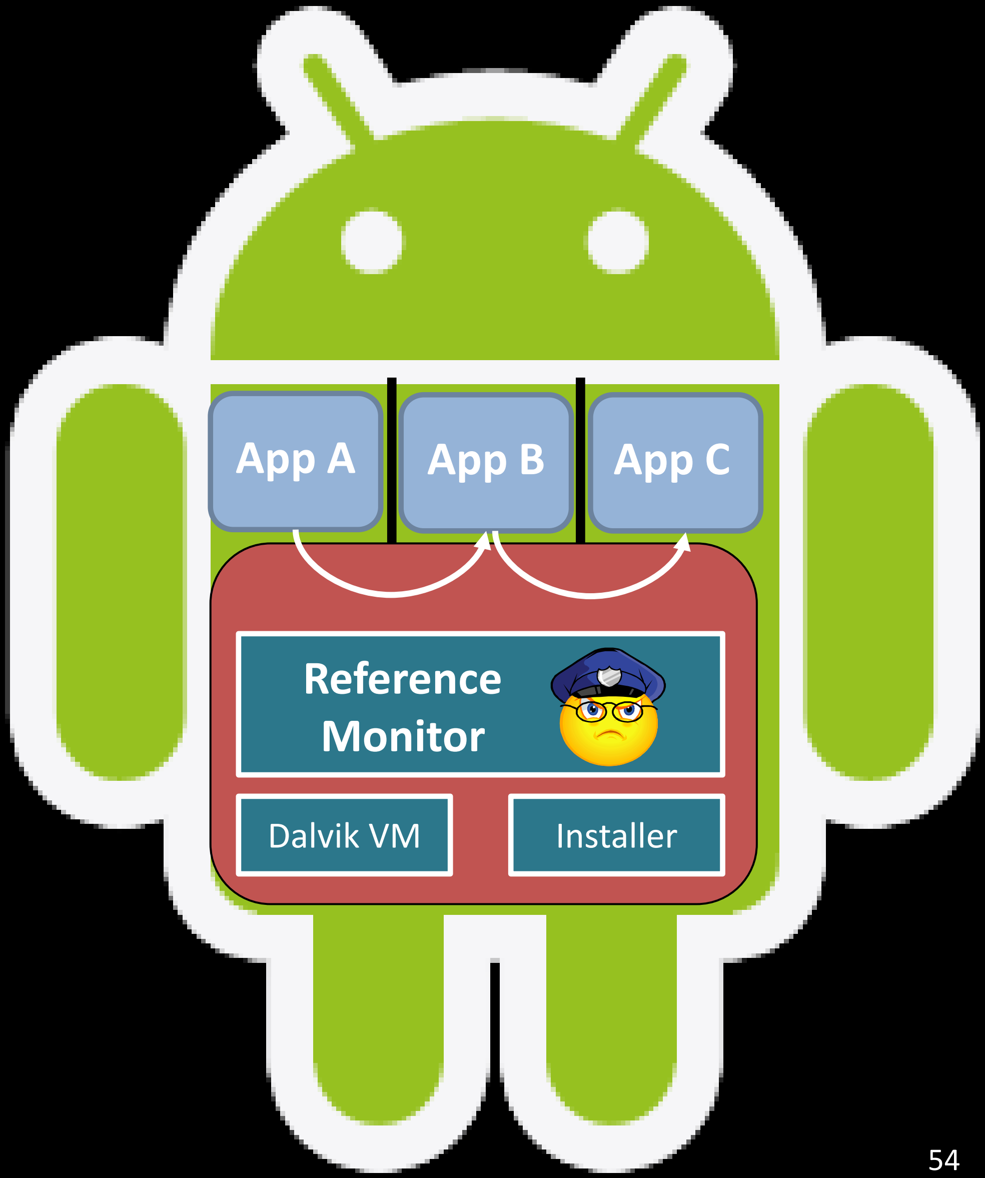
Android Architecture: Basics

- **Linux kernel:**
  - Network, storage, memory, processing …
- **Android middleware:**
  - Java Virtual Machine, Application framework, Libraries, …
- **Application layer:**
  - Each app runs within its own virtual machine instance

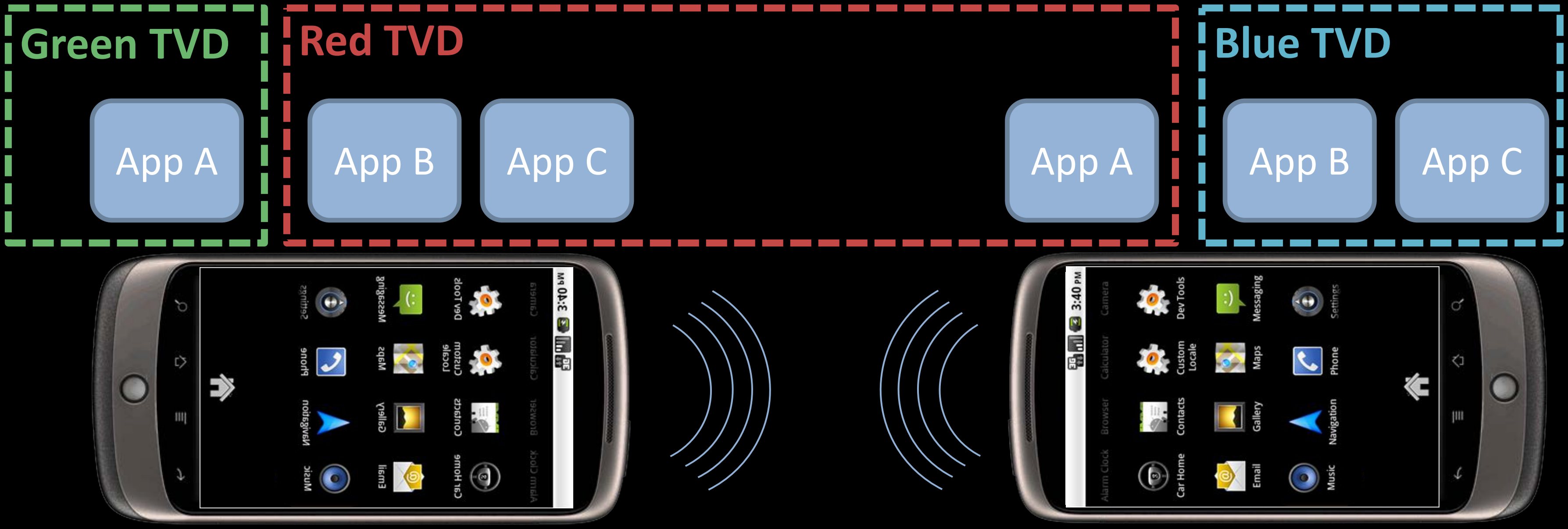


Android Middleware

- **Android Installer for Apps**
  - User grants new applications their rights
  - Every application has been assigned own user ID and one/several Group ID(s)
- **Java Dalvik Virtual Machine**
  - Special Java Virtual Machine for Android
  - Interprets Java Code of Apps
- **Inter Component Communication (ICC)**
  - Apps communicate via ICC
- **Reference Monitor (RM)**
  - ICC calls are mediated by a middleware reference monitor (mandatory access control)



Android TVD: Color your Apps!



Green TVD

App A

Red TVD

App B

App C

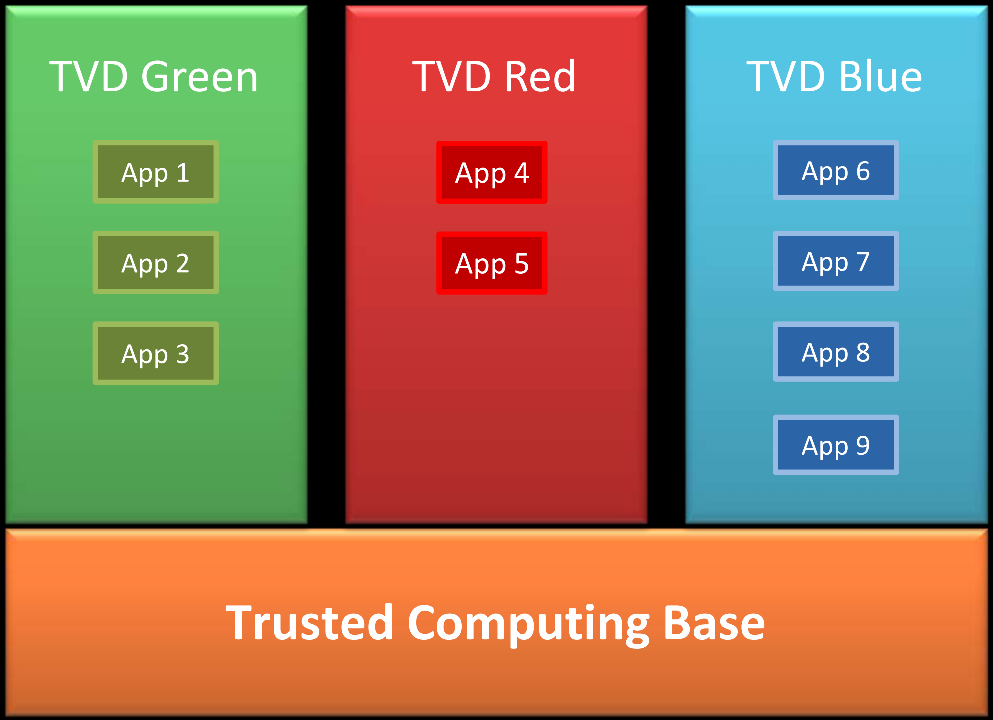
App A

Blue TVD

App B

App C

Android TVD: Color your Apps!



TVD Green

App 1

App 2

App 3

TVD Red

App 4

App 5

TVD Blue

App 6

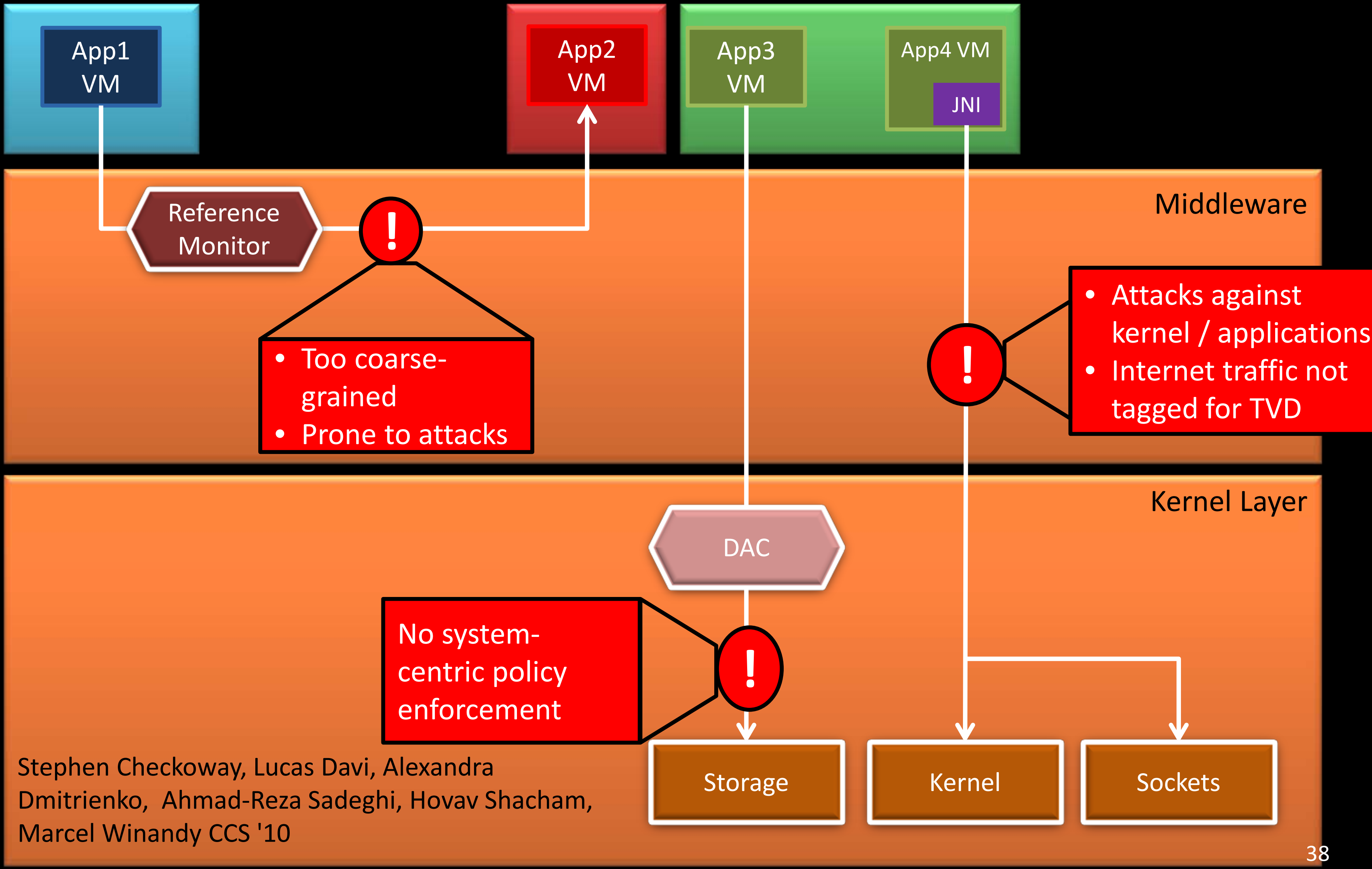
App 7

App 8

App 9

Trusted Computing Base

Current Android Security Model



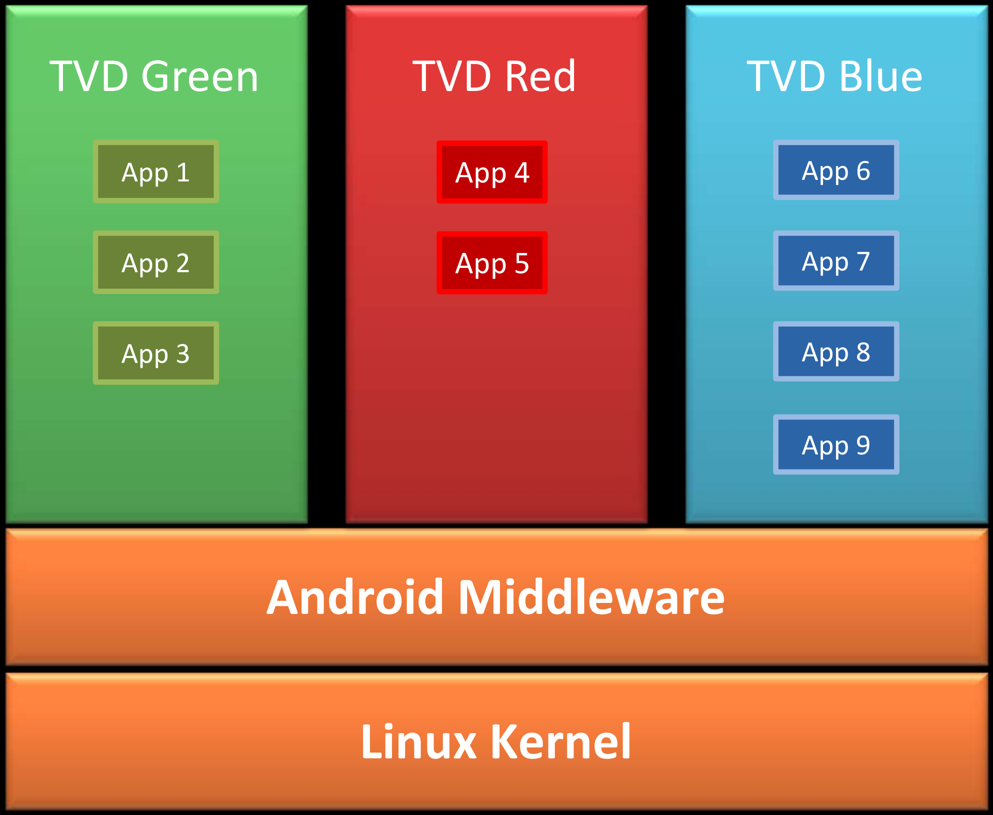
- Too coarse-grained
- Prone to attacks

- Attacks against kernel / applications
- Internet traffic not tagged for TVD

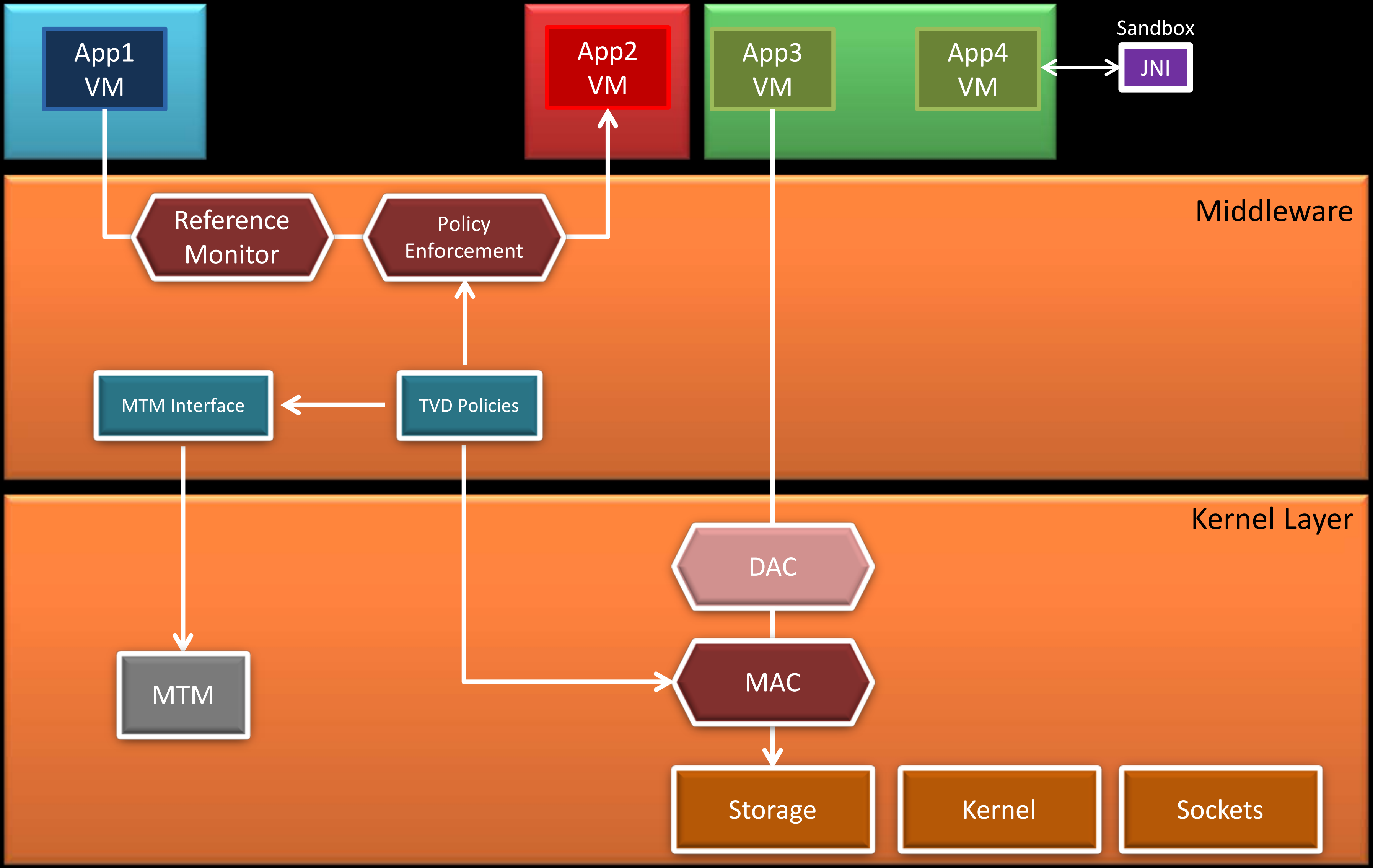
No system-centric policy enforcement

Stephen Checkoway, Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi, Hovav Shacham, Marcel Winandy CCS '10

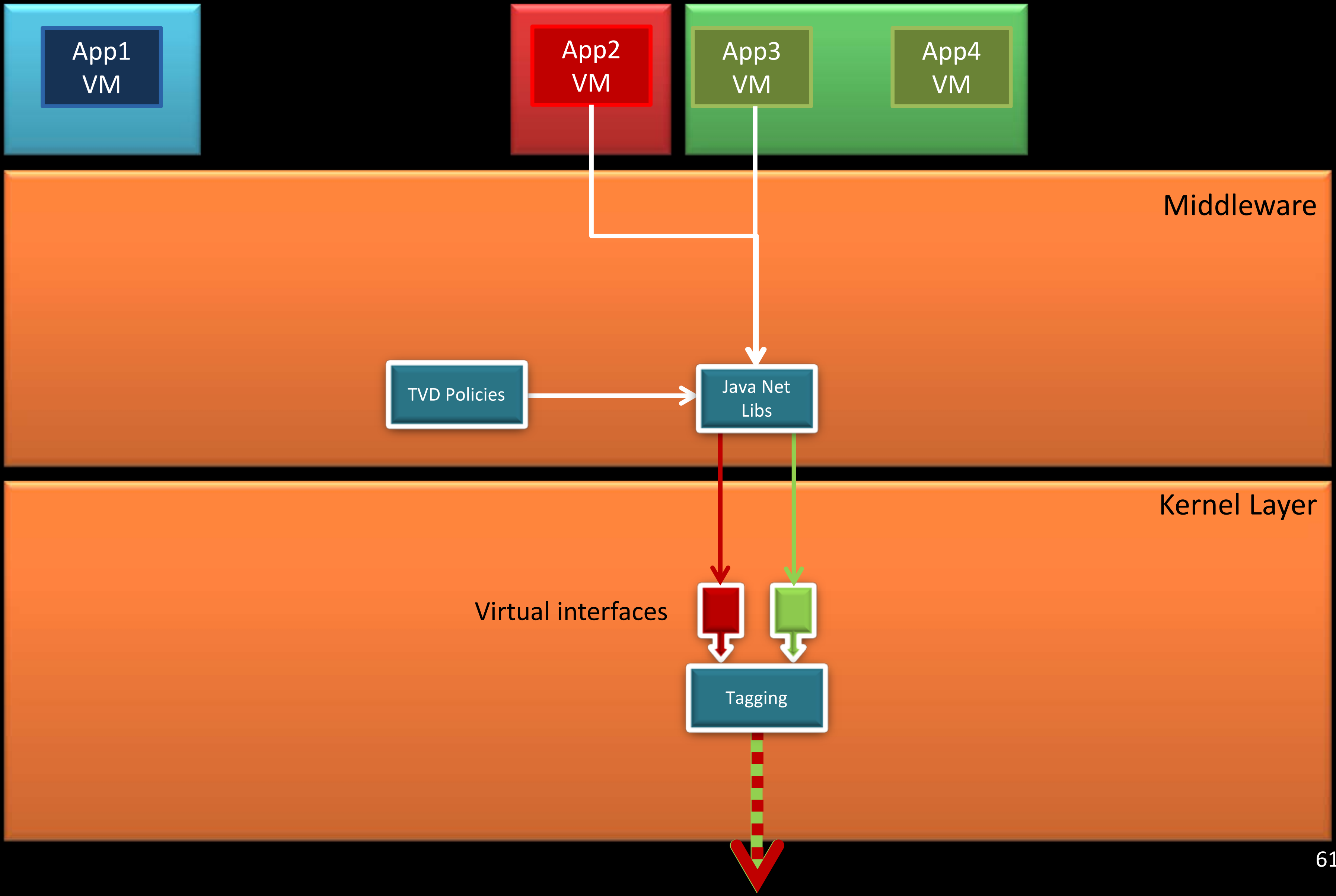
Concept 1: Extended Policy Framework



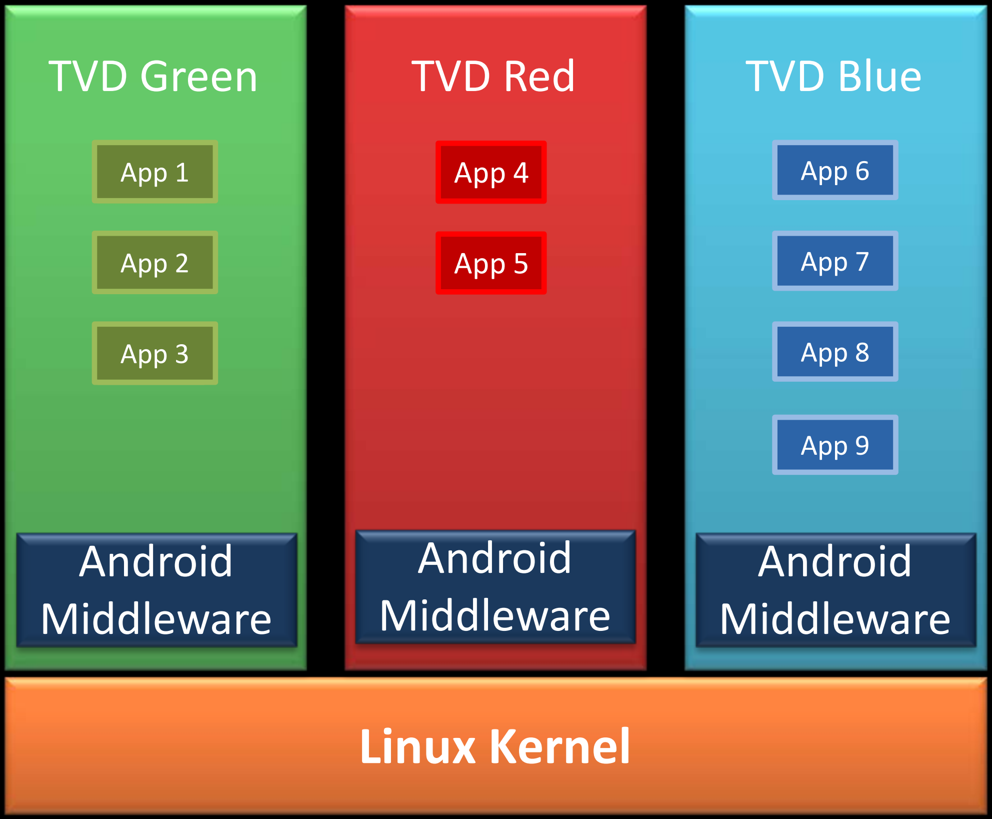
Isolation with Policy Framework



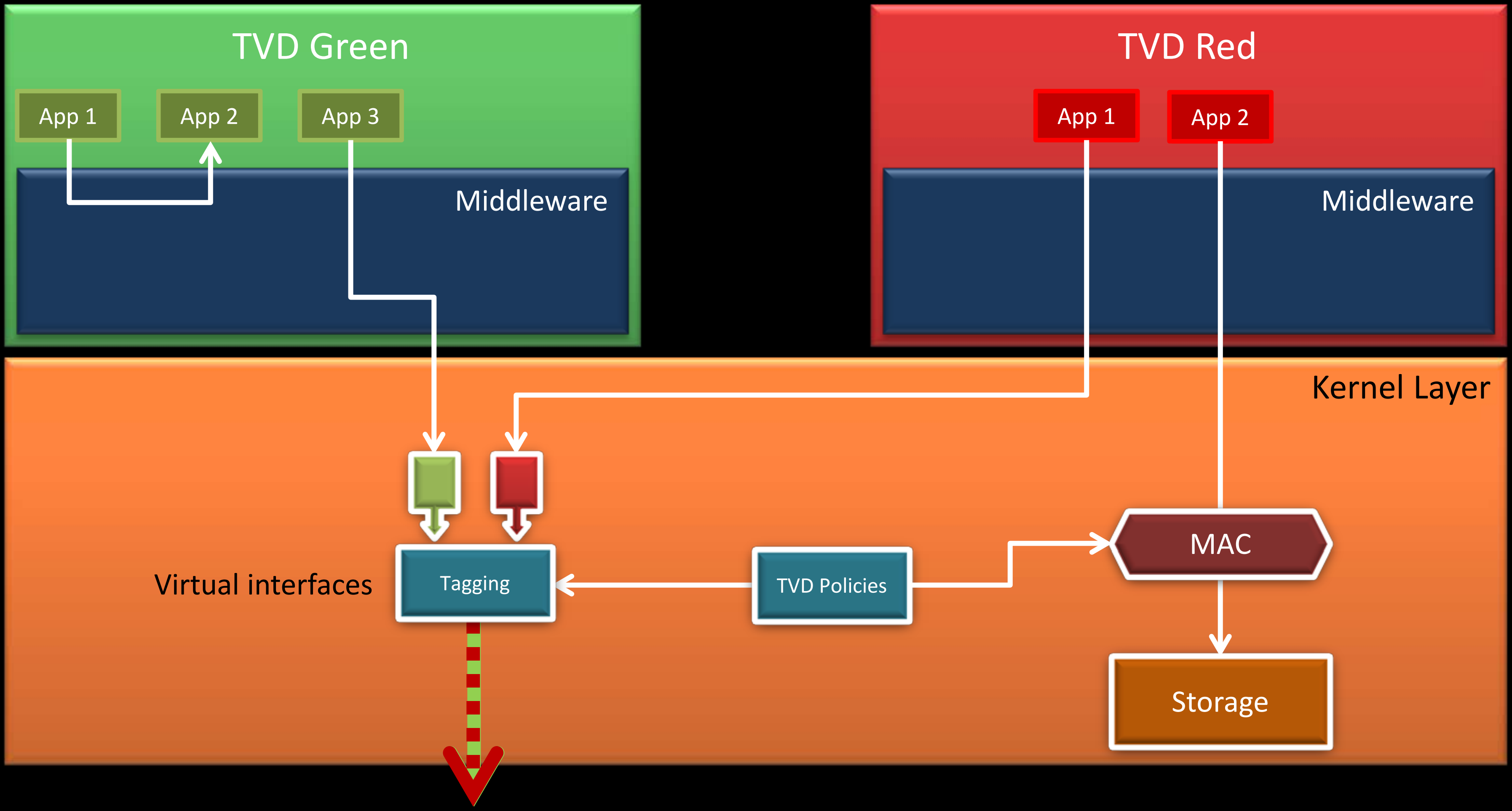
TVD Network Tagging



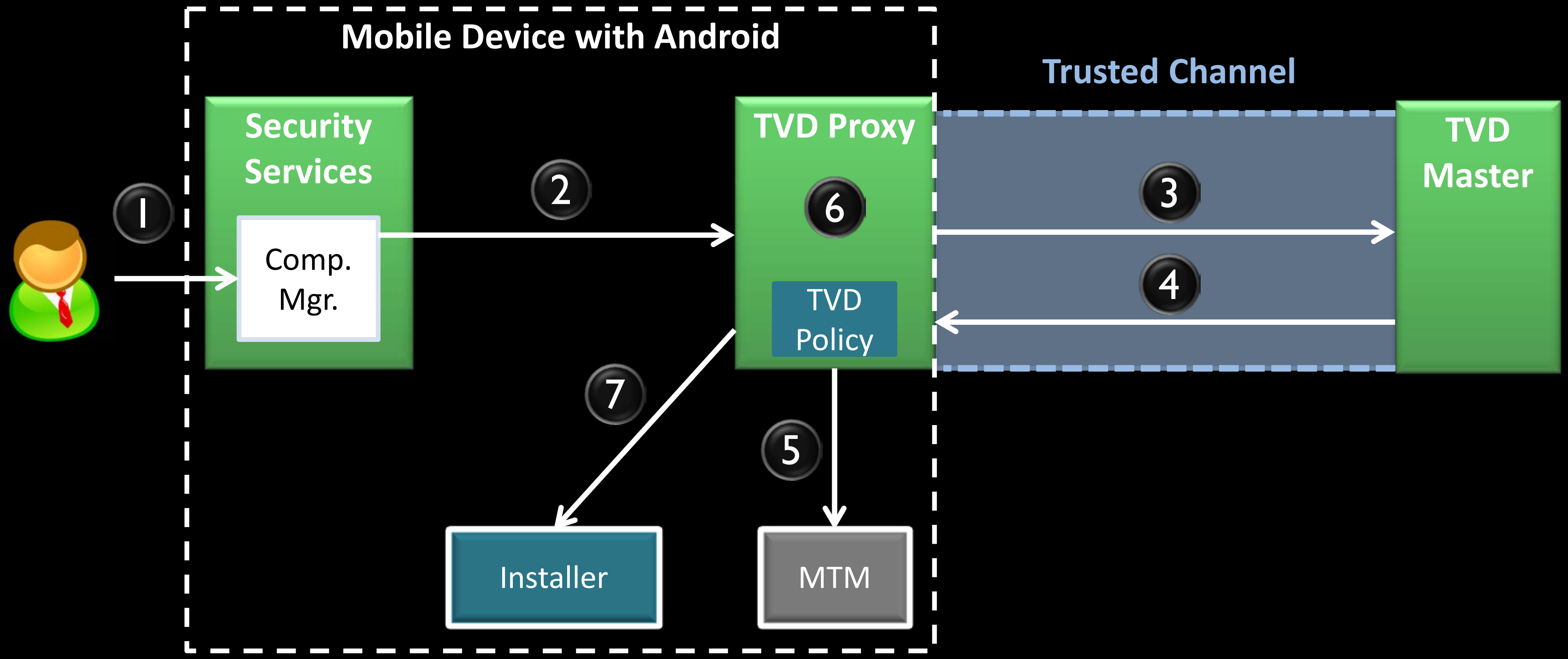
Concept 2: Container Isolation



Isolation with Containers



How to Color Applications



1. User selects new application
2. The Compartment Manager (Comp. Mgr.) forwards the request to TVD Proxy
3. TVD Proxy requests the new application from TVD Master
4. TVD Master sends the application installation package (with RIM Certificate)
5. TVD Proxy verifies the Remote Integrity Metrics (RIM), (Certificates)
6. TVD Proxy determines the TVD (color) for the new application
7. TVD Proxy issues the installation of the new application

Current and Future Work

- **Trust but verify**
  - Trusted Execution Environment in the Cloud (e.g., TXT?)
  - Malicious insiders (in particular remote admnistrators)
- **Fine-grained advanced policy enforcement**
- **Migration and attestation of VMs**
- **Efficiency**
- **Evaluating security provided by current clouds**
- **Most important:**
  - Useable security
  - Legal issues