Is Smart also Secure?

On the (In)Security of Smartphones

Prof. Dr.-Ing. Ahmad-Reza Sadeghi
ahmad.sadeghi@trust.cased.de
System Security Lab
Technische Universität Darmstadt,
Fraunhofer SIT, Darmstadt,
Germany

Smartphones Applications Today

Mobile Phone Features

Call, SMS, MP3, Video

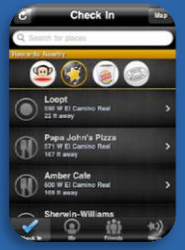
Interfaces

GPS, WiFi, Bluetooth, Infrared

Online Services

Browsing, E-Mail, E-Shopping,

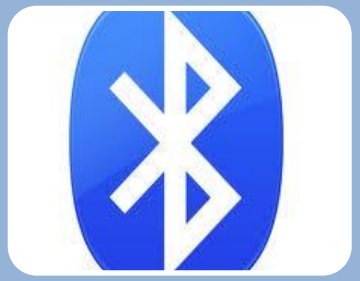
Social Networking, Medical



Location Services

Navigation, Recommendation

Context-Based Policies & Applications



Bluetooth Discovery

- Bluetooth interface should only be discovered at home
- Requires **location recognition**

Lend Phone

- Access control to sensitive data (e.g., SMS) when lending to others
- Requires **user recognition**

Application Restriction in Company

- A company restricts the set of applications which can be used while the employee is working
- Requires **policy enforcement by trusted third parties**

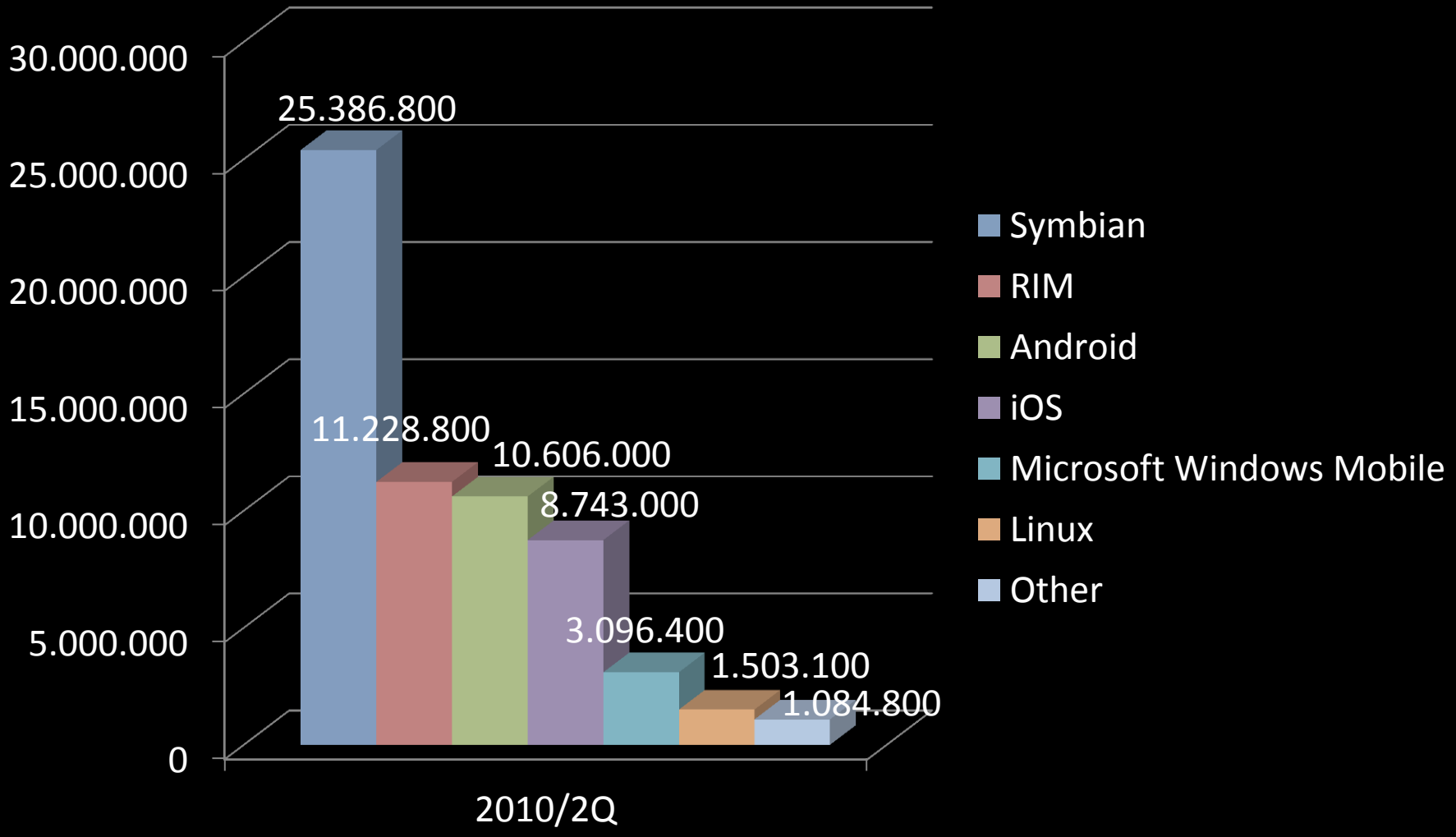
Enterprise Solution: Restricting Application Set

Model

- Different & more complicated than PC world
  - Many stakeholders, resource constraints, …

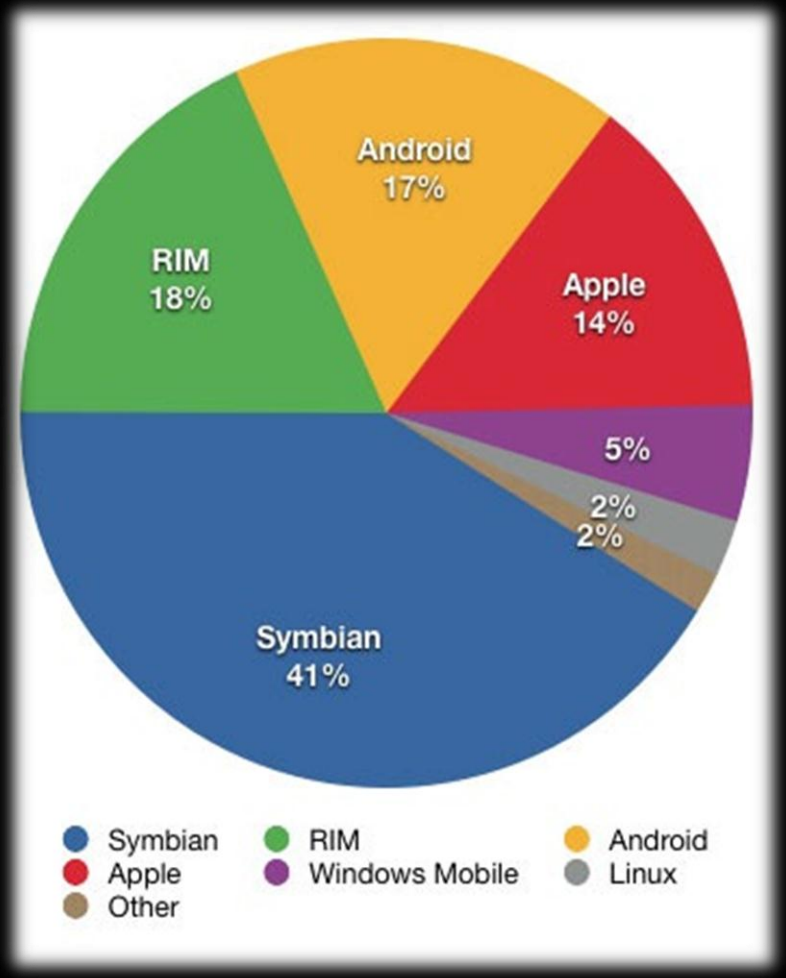
Security:
An Enabling Technology for New Business Models?

Worldwide Smartphone Sales to End Users by Operating System Sold Units Q2/2010



Based on Gartner Statistics (August 2010)
http://www.gartner.com/it/page.jsp?id=1421013

Worldwide Smartphone Sales to End Users by Operating System Market Share Q2/2010



Based on Gartner Statistics (August 2010)
http://www.gartner.com/it/page.jsp?id=1421013

What Aspects of Security Do We Need on Smartphones?

Smartphones Target of Attacks

Nokia phones hit by malware attack

NEWS **Posted 8th July 2010 at 1:01pm by Matt Dixon**

A malware campaign is targeting smartphones based on the Symbian platform from a handful of manufacturers, potentially posing a threat to millions of users worldwide.

If you have a smartphone running Symbian S60 3rd or 5th edition from Samsung, Nokia or Sony Ericsson then it could be at risk of infection, according to security software vendor NetQin.

the BlackBerry which allows users to listen in on other people's calls.

Threat Classification

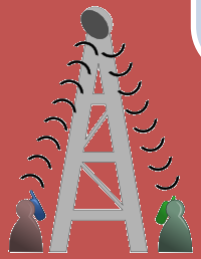
Attacks on Privacy

Location, E-Mail, Contacts

Runtime Attacks

Code Injection, Return-Oriented Programming, Kernel Exploits

Attack Vectors



Hardware Attacks

GPS, GSM Module, Base Station

Malware

Trojans, Viruses, Worms

Security Features of Modern Smartphones

Overview of Selected Smartphones

iPhone

- Closed Source
- Sandboxing
- Code Signing
- Code Inspection
- Non-Executable Memory

Android

- Open Source
- Strict Sandboxing
- Java Dalvik Virtual Machine
- Java Apps
- Lightweight Code Signing
- Permission Framework

MeeGo

- Open Source
- Security Framework based on Role-Based Access Control
- Detailed information not yet published

Blackberry

- Closed Source
- Apps and main part of the OS in Java
- End-to-End Encryption
- Code signing and digital certificates

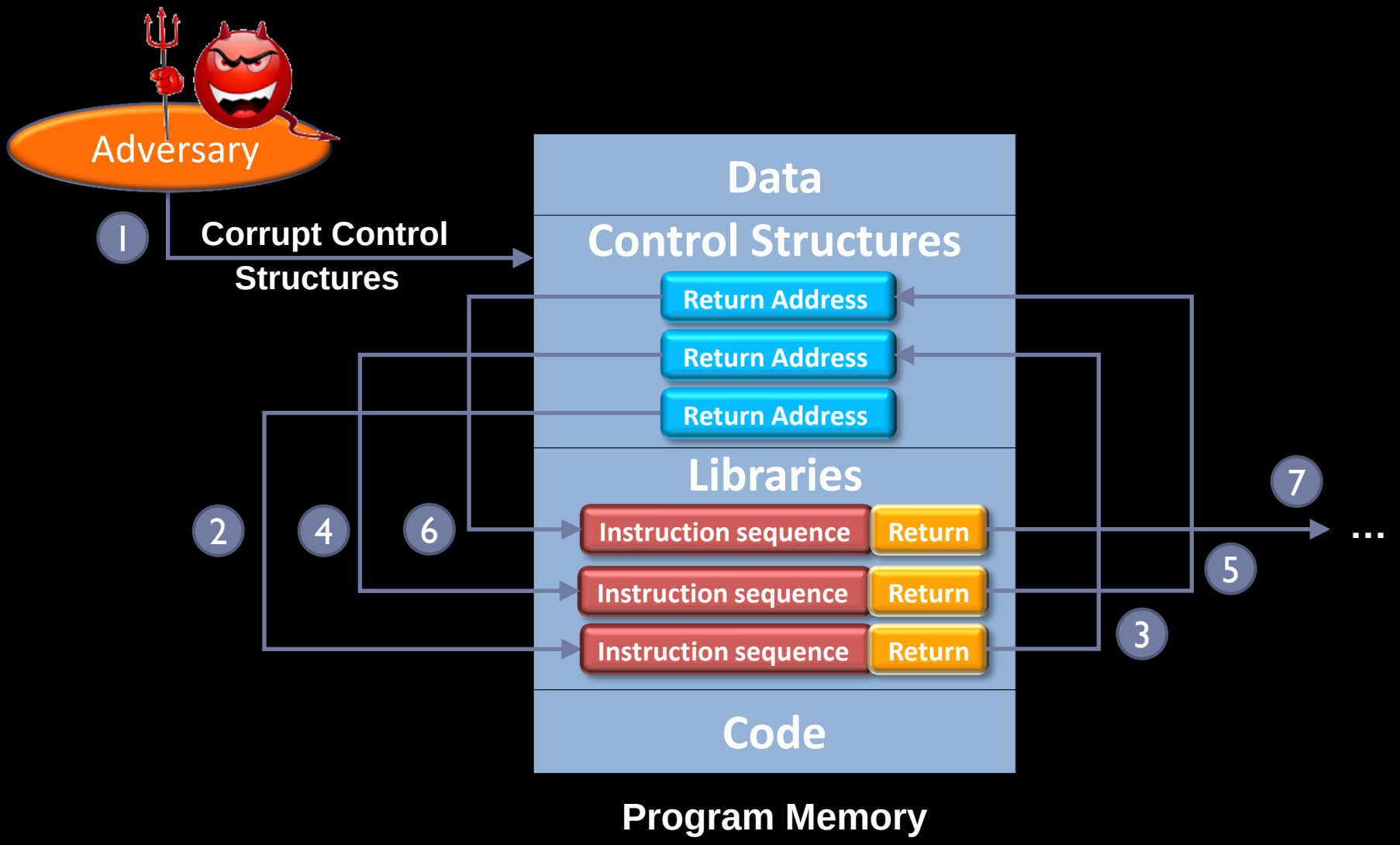
The Newcomer: Windows 7 Phone

A new competitor for iPhone and Android?

- **Security Aspects**
  - Strict Application Sandboxing
  - Isolated Storage
    - Applications can only access own data
    - Applications are not allowed to access OS storage
  - Application Signing
    - Application are signed by Microsoft
    - Microsoft also enforces code inspection
  - No native code in applications allowed
  - Phone features (SMS, E-Mail,…)
    - Only indirect access through launchers and choosers
    - Launcher and Choosers start central built-in applications

Some Recent Attacks

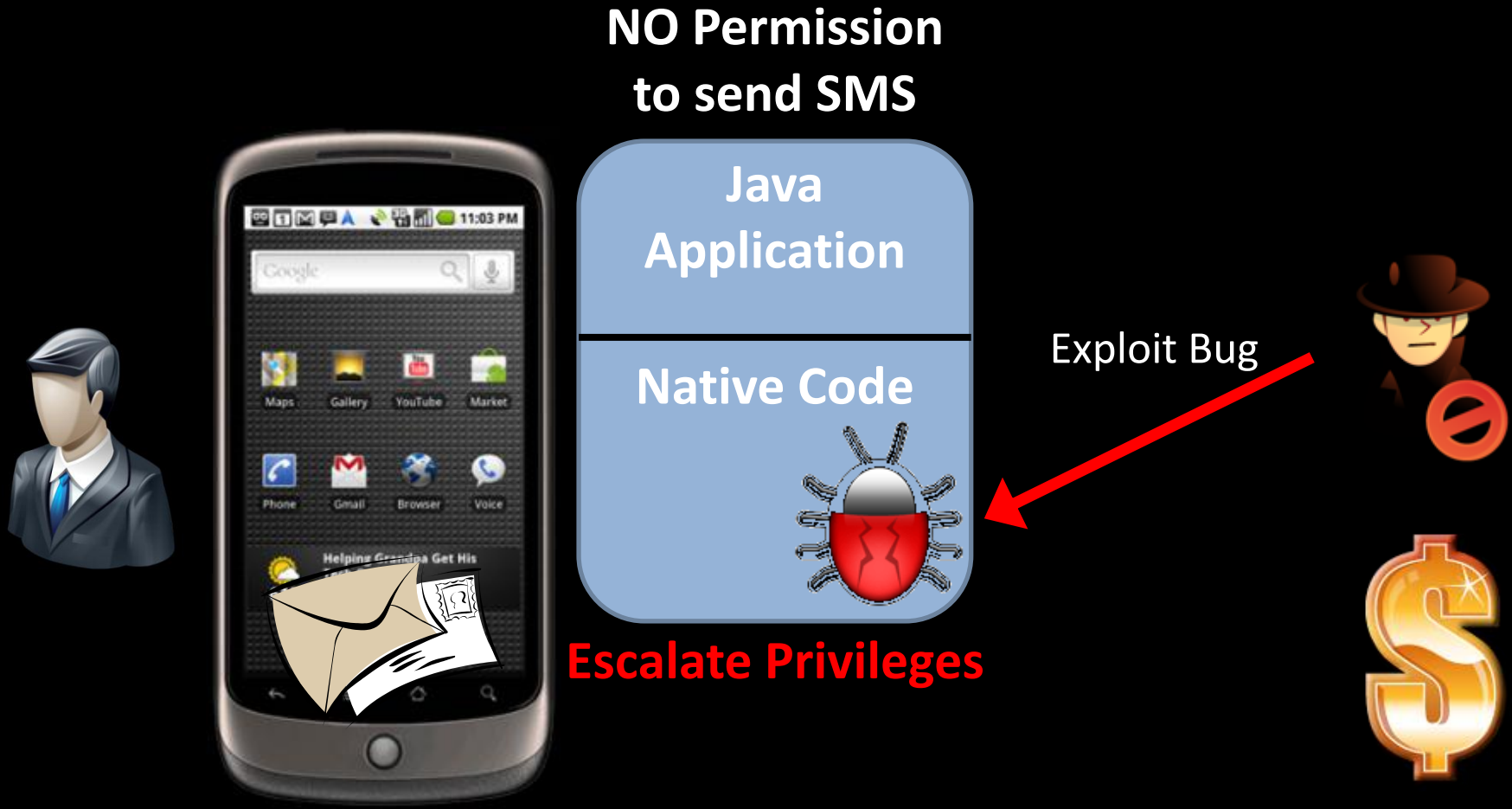
Attack Technique: Return-Oriented Programming



Apple iPhone: Stealing SMS Database

Iozzo and Weinmann: Pwn2own Contest 2010

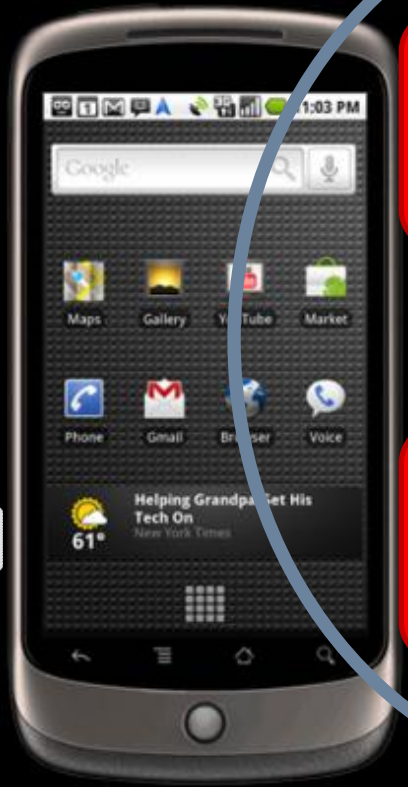
Privilege Escalation on Google Android



Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi, Marcel Winandy:
Information Security Conference (ISC 2010)

Google Android:

Soundminer: A stealthy and context-aware sound Trojan



APP_B

Permission:
Internet

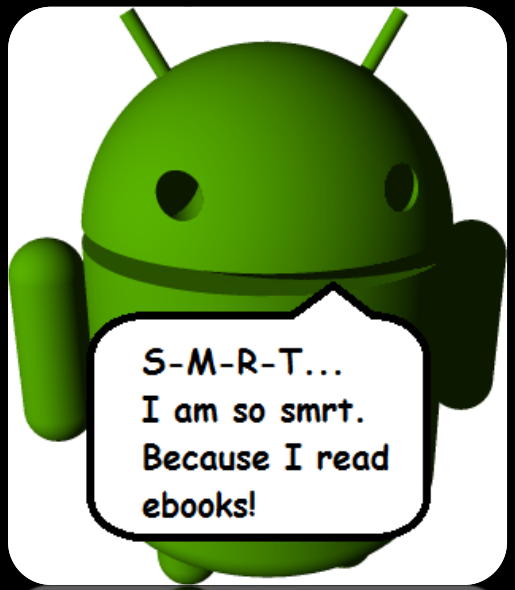
APP_A

Permission:
Record Audio

1) Call Credit Institute
2) Credit Card Number is extracted from the speech

SCHLEGEL, R., ZHANG, K., ZHOU, X., INTWALA, M., KAPADIA, A., AND WANG, X. Soundminer: A stealthy and context-aware sound trojan for smartphones, NDSS'11

Google Android is Cool

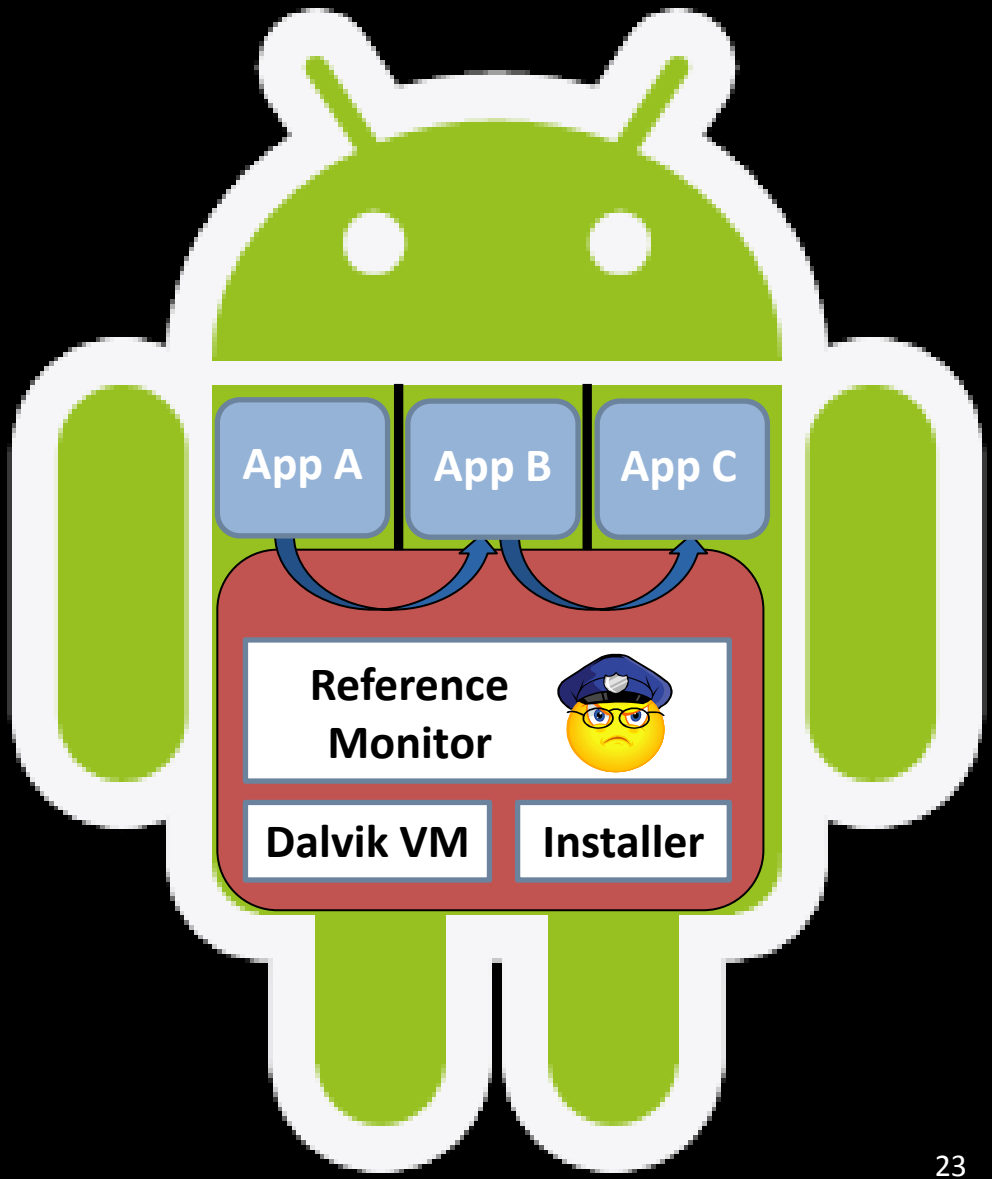


Android Architecture

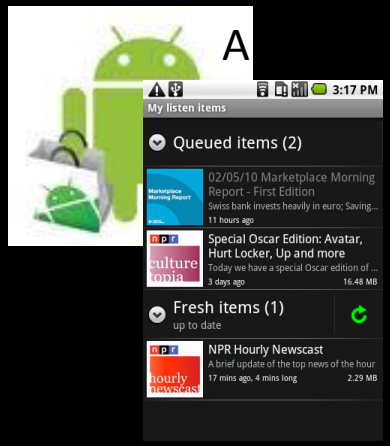
- **Linux kernel:**
  - Network, storage, memory, processing …
- **Android middleware:**
  - Java Virtual Machine, …
- **Application layer:**
  - Each app runs within its own virtual machine instance

Android Middleware

- **Android Installer**
- **Java Dalvik Virtual Machine (DVM)**
  - Special Java Virtual Machine for Android
  - Interprets Java Code of Apps
- **Inter-process communication (IPC)**
  - Apps communicate via IPC Calls
  - IPC messages are called Intents
- **Reference Monitor (RM)**
  - IPC calls are mediated by a middleware reference monitor



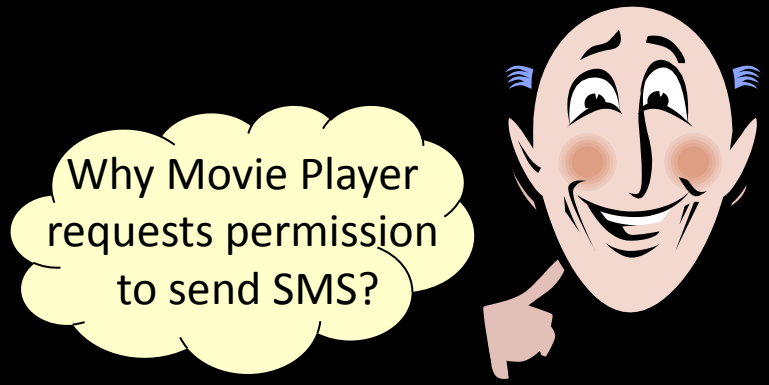
Android Installer: Installation of a Security-Critical App



Download app

Permissions

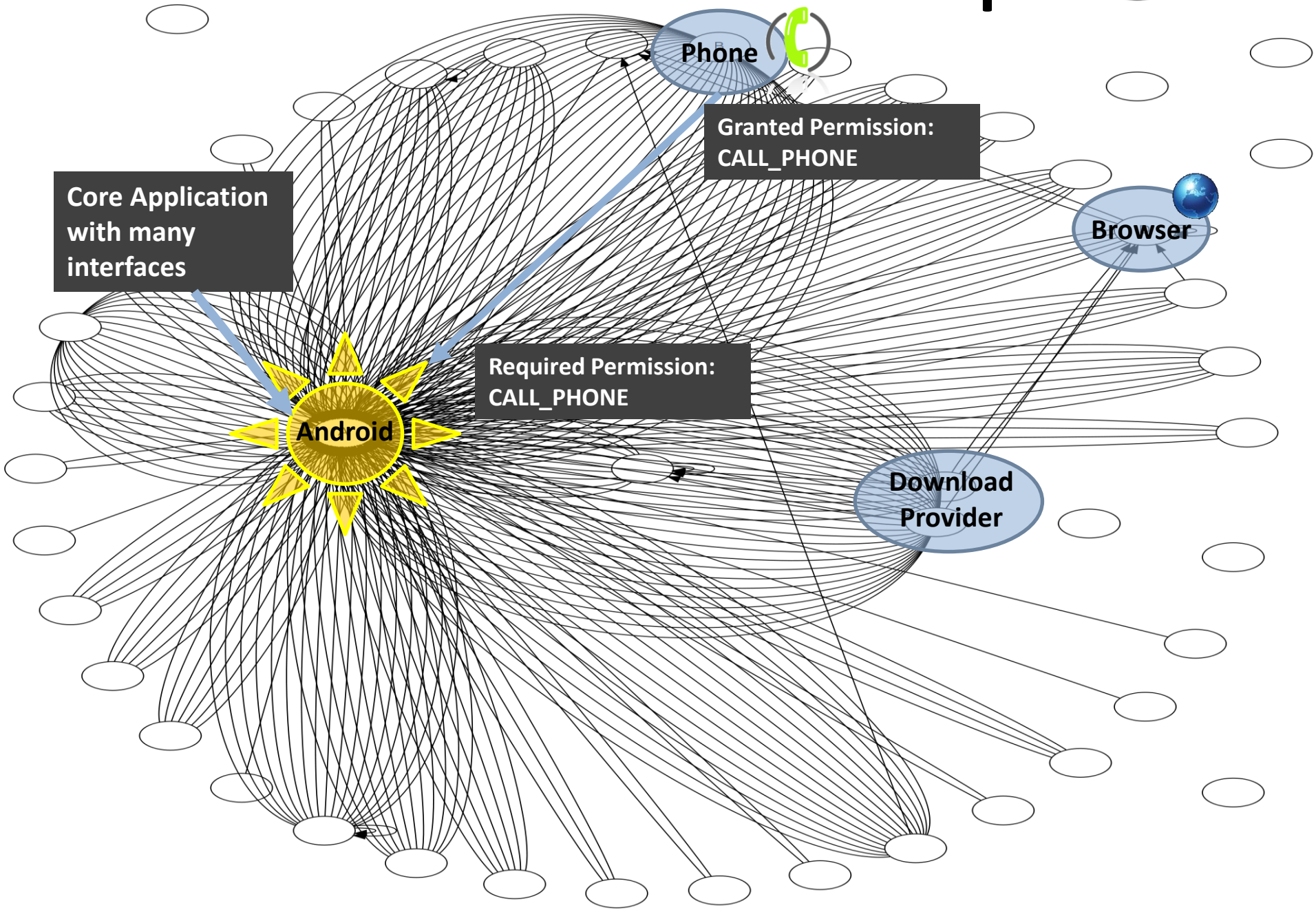
Deny install



Android Permission System

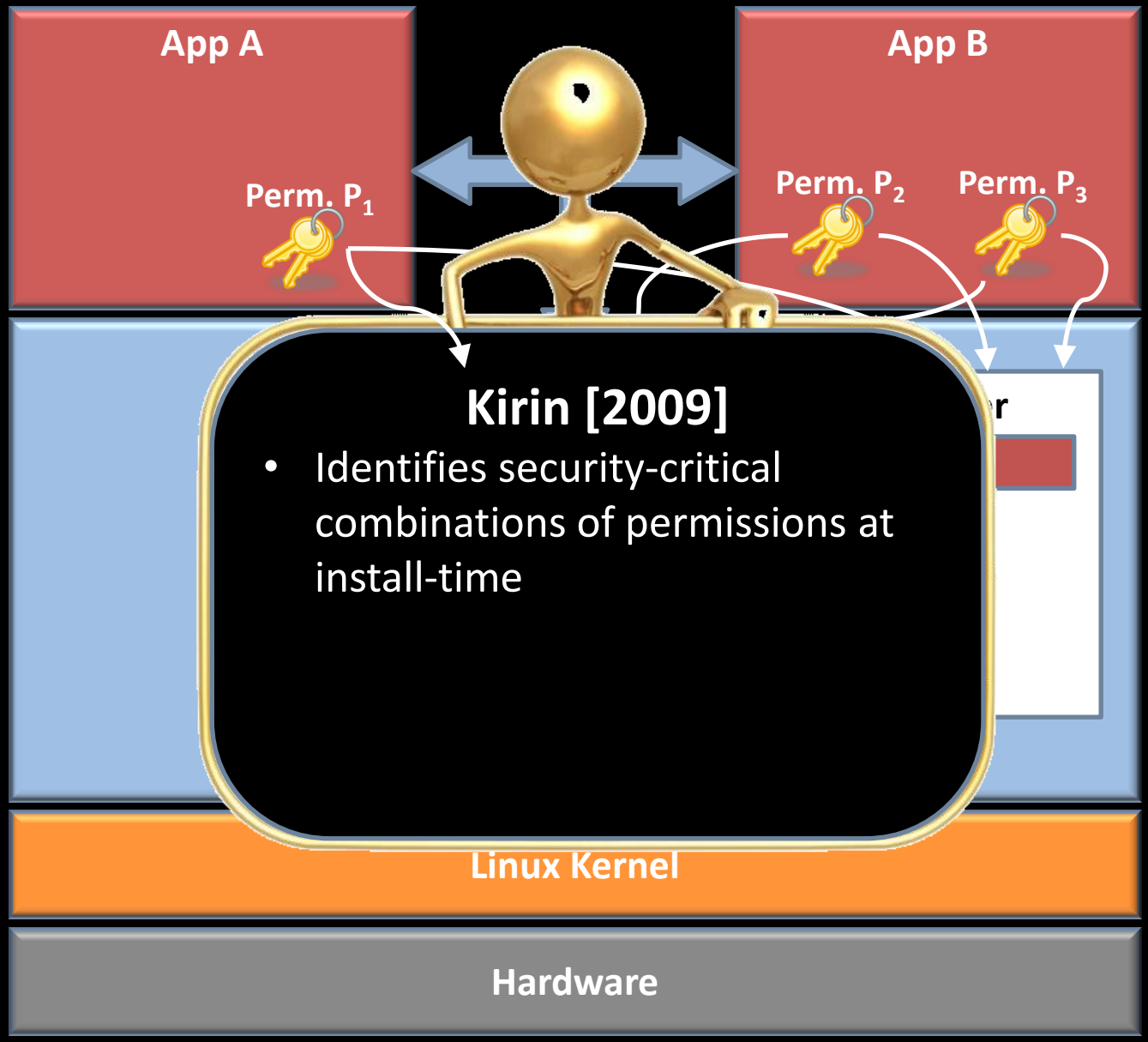
- **Application are assigned permissions**
- **Permissions are needed to control access**
  - System resources (logs, battery, etc.)
  - Sensitive data (SMS, contacts, e-mails, etc.)
  - System interfaces (Internet, send SMS, etc.)
- **Application (developers) can also define own permissions to protect application interfaces**

Android Permission Graph

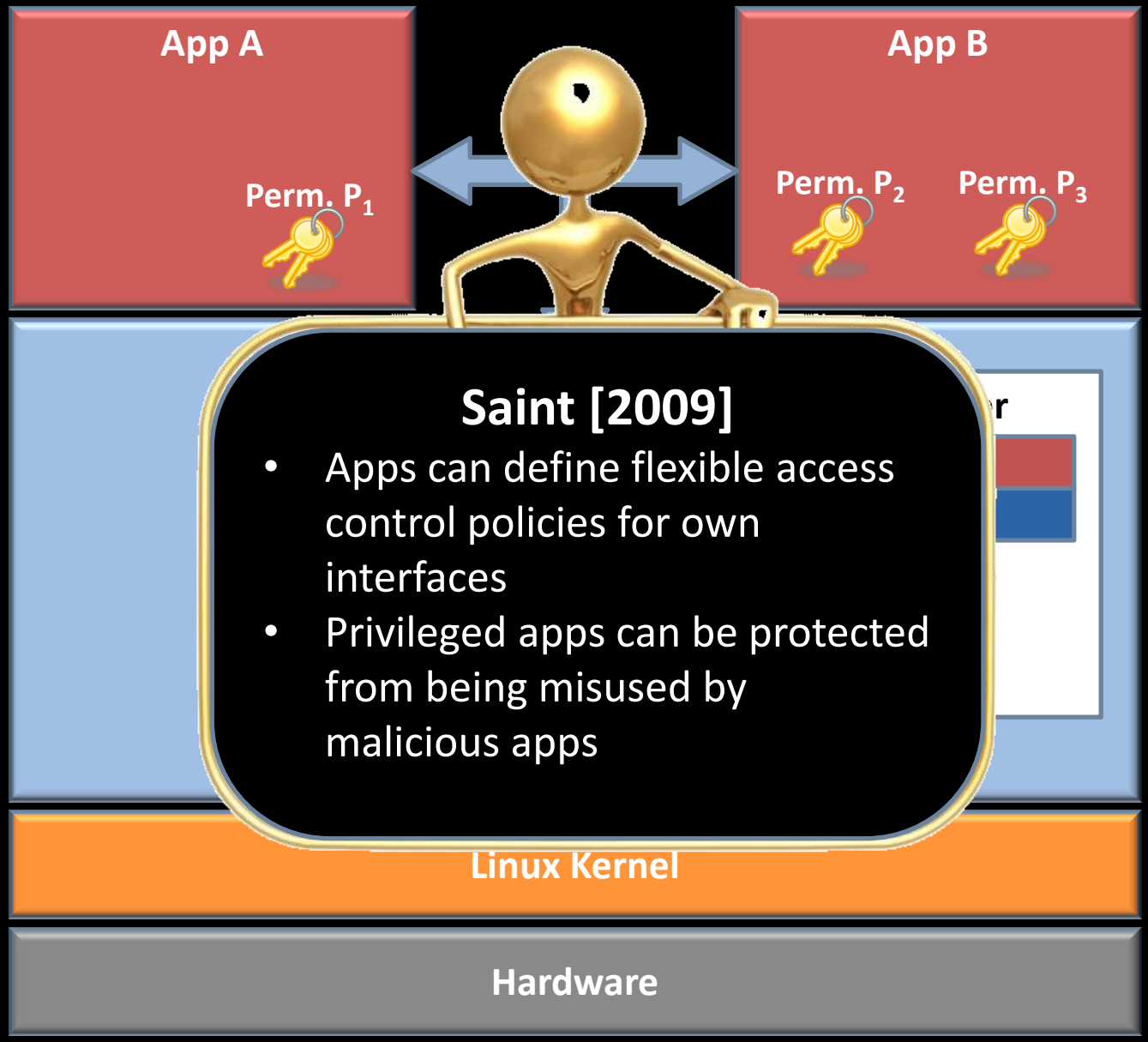


Research on Android

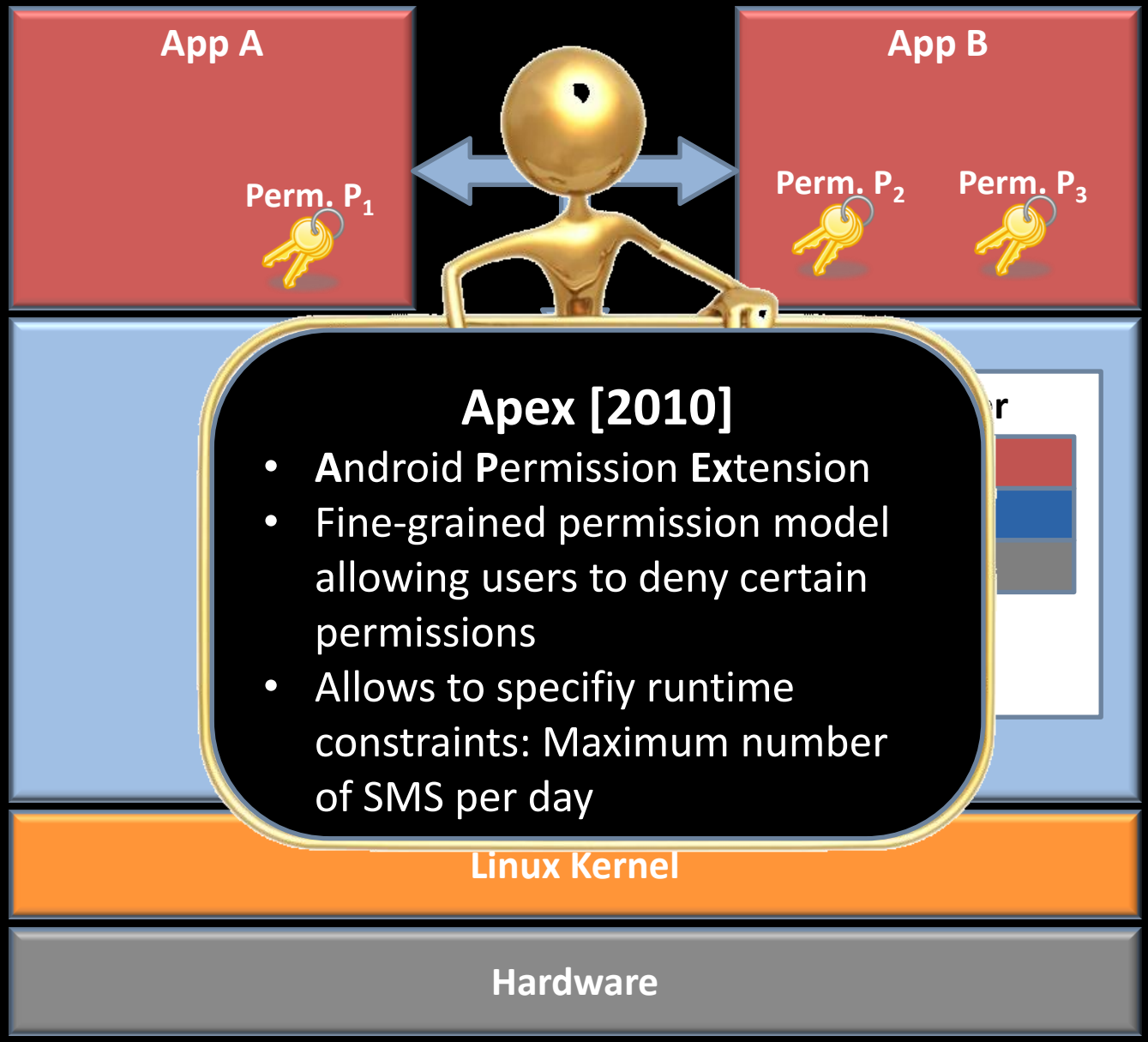
Security Extensions for Android



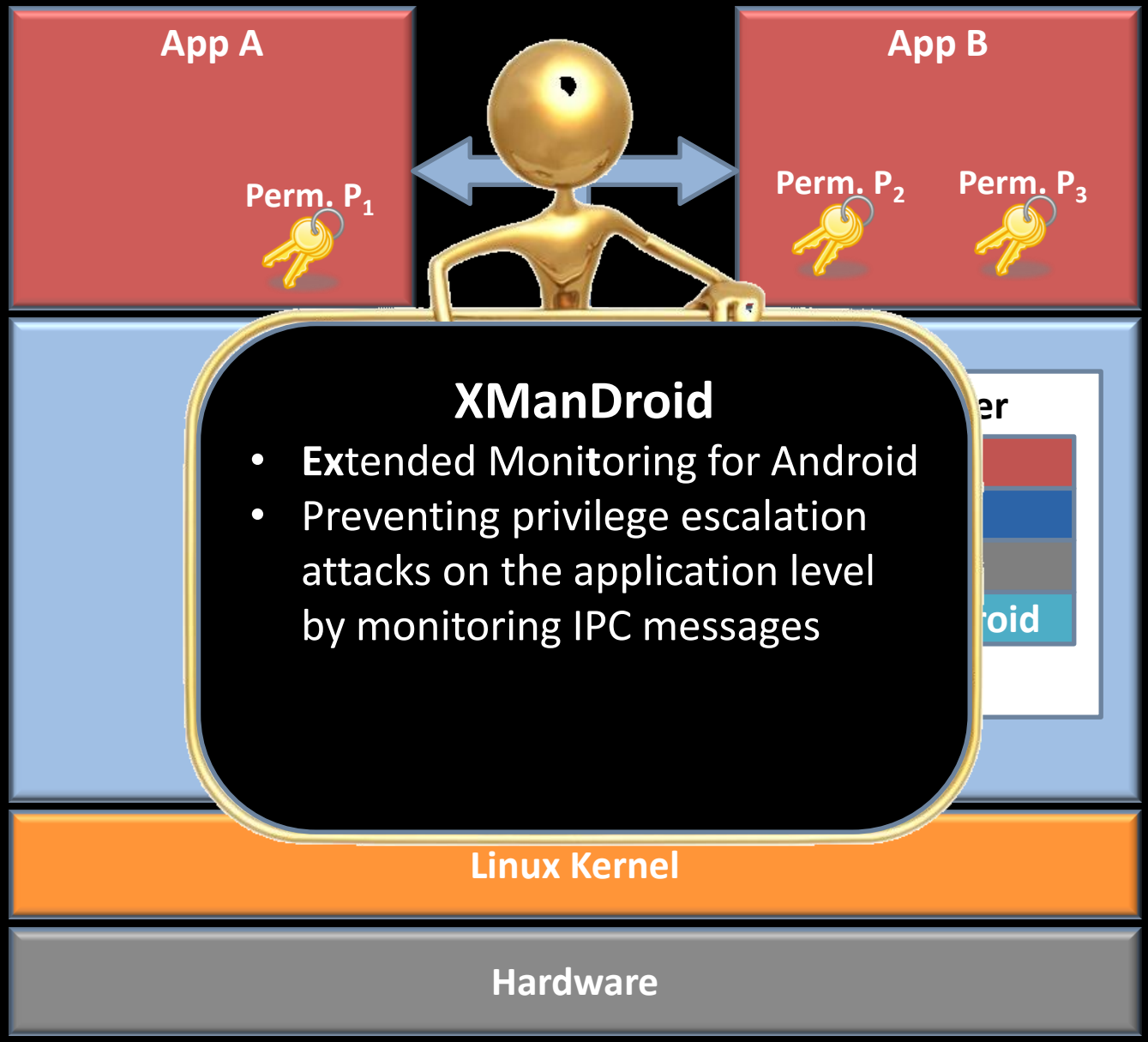
Security Extensions for Android



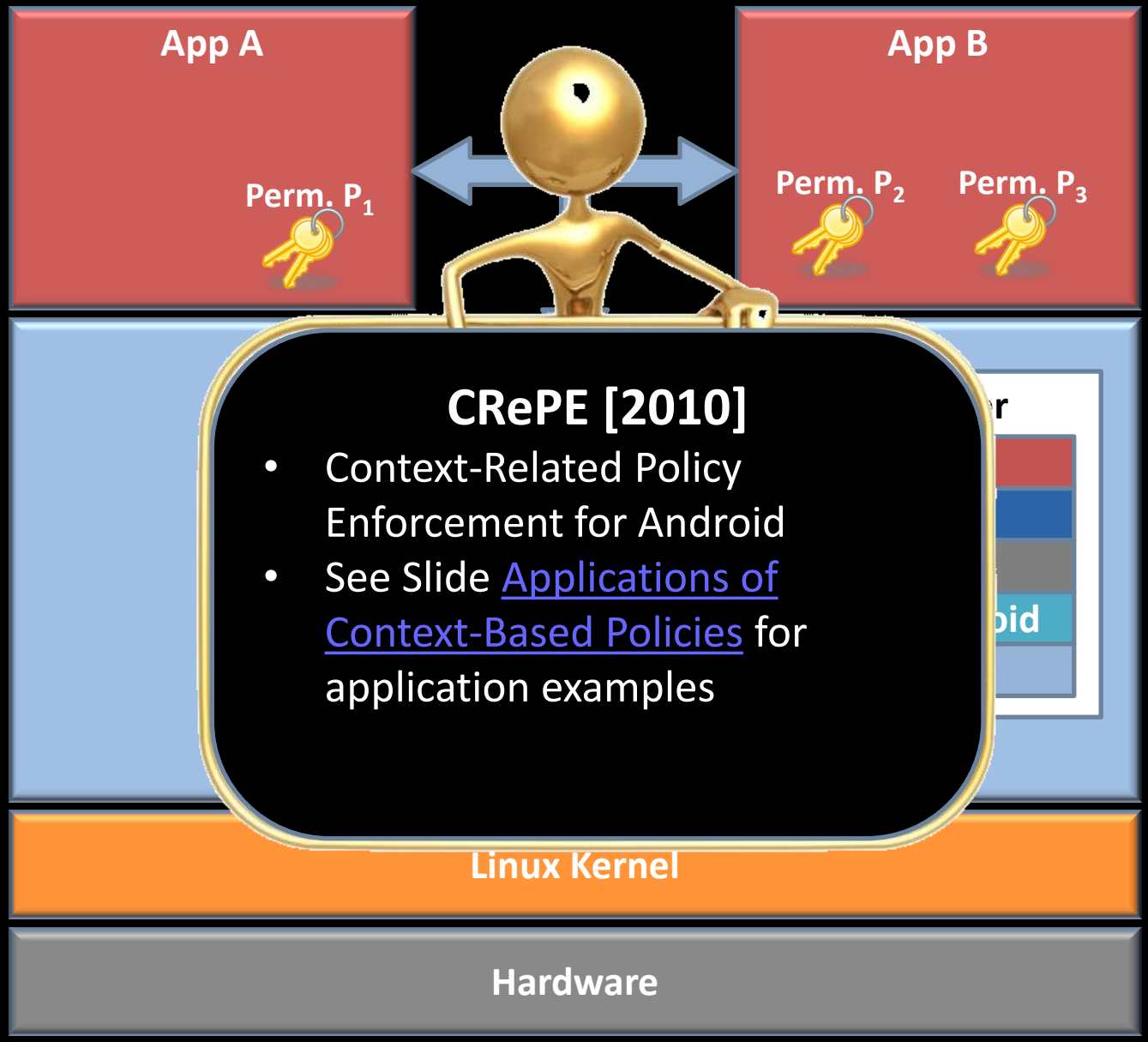
Security Extensions for Android



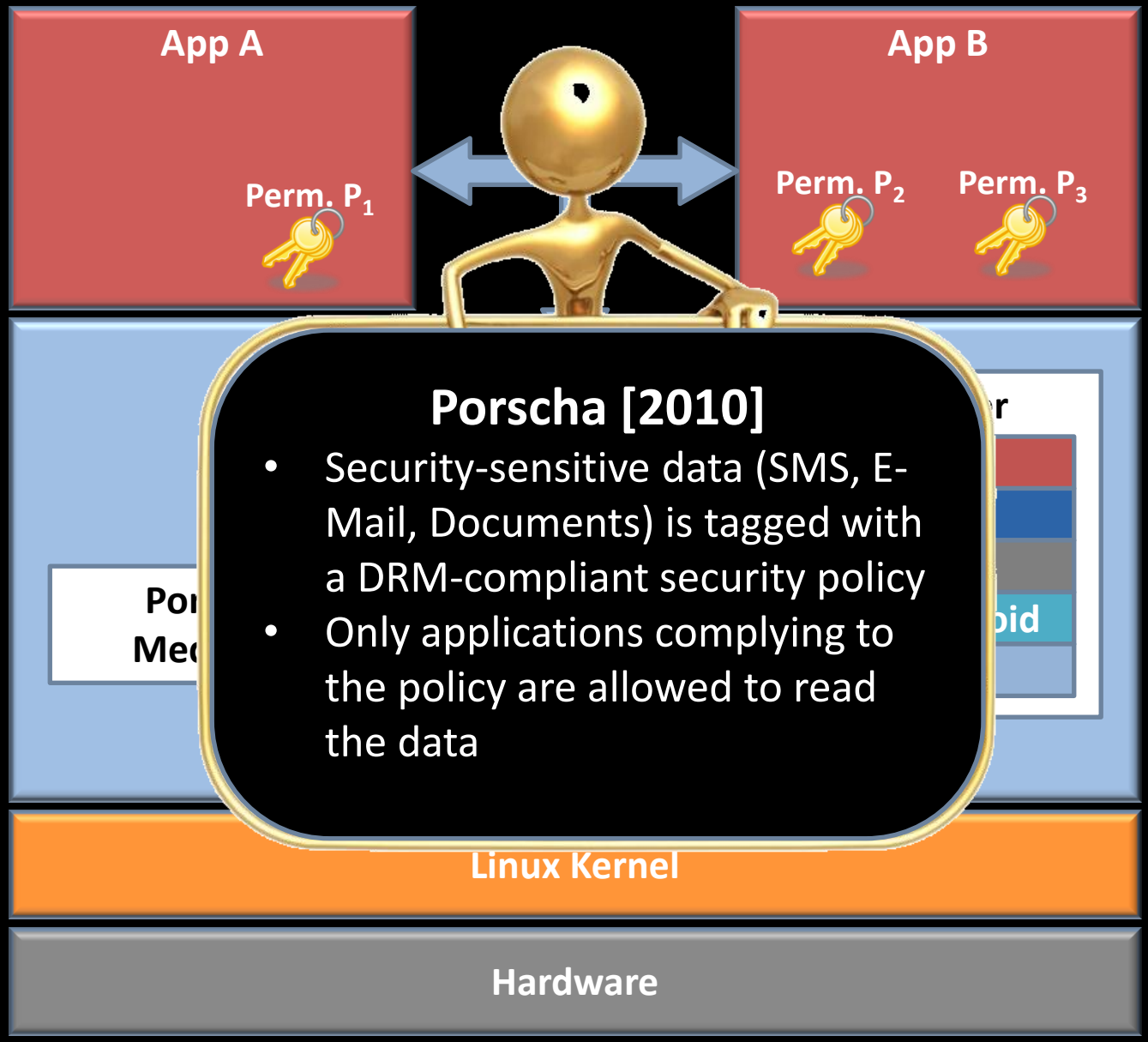
Security Extensions for Android



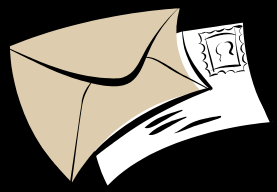
Security Extensions for Android



Security Extensions for Android



To: App A

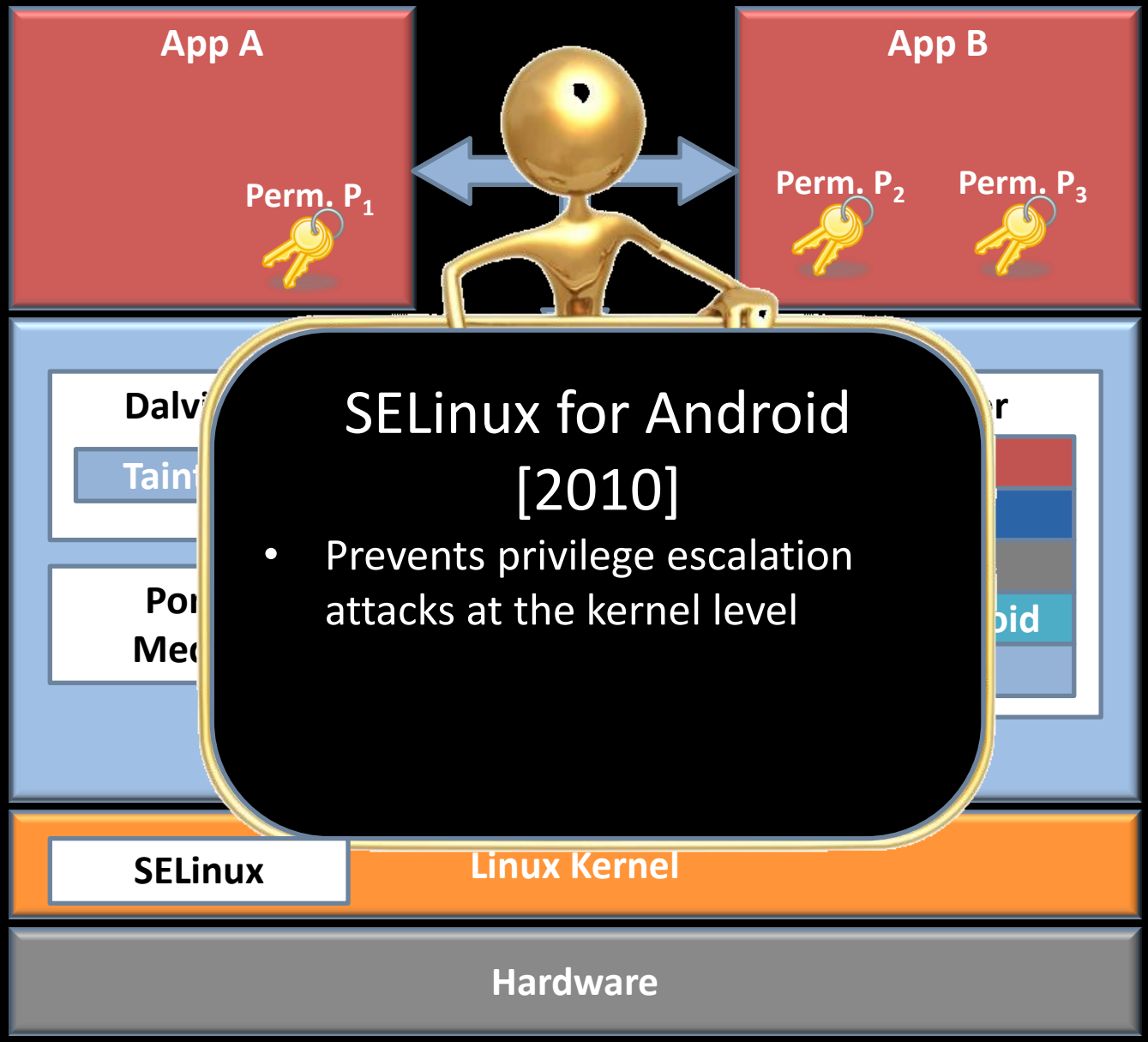


Security Extensions for Android

TaintDroid [2010]

- Deploys dynamic taint analysis in order to detect unauthorized leakage of sensitive data
- Applied to real apps in Android Market, showed many of them leak sensitive data

Security Extensions for Android



Android‘s Kernel Security

November 2010

Serious security bugs found in Android kernel. An analysis of Google Android Froyo's open source kernel has uncovered 88 flaws that could expose users' data

http://www.eweekeurope.co.uk/news/serious-security-bugs-found-in-android-kernel-11040

Mobile Trusted Platform Module: More Security Functions in Hardware

Need for Security Hardware

- **Even secure software cannot verify its own integrity**
  - Integrity metrics, reporting and verification requires trusted third party/component
- **Malicious software can access and tamper data of other software**
  - Hardware-based secure storage required
  - Hardware-enforced isolation of security-critical programs required
- **True random numbers fundamental to cryptography**
  - Hardware-based random number generation required

Trends and Future…..

- **Trusted Execution Environment**
  - Provides assurance about trustworthiness of security critical operations
- **Security and crypto functions in common hardware**
  - Intel TXT, AMD Presideo, ARM TrustZone, M-Shield (Nokia platforms)
  - Trusted Platform Modules (TPM) embedded in nearly every platform

Trusted Execution Environment

Trusted Execution Environment (TrEE) Based on M-Shield

Supported in hardware (i.e., M-Shield from Texas Instruments)

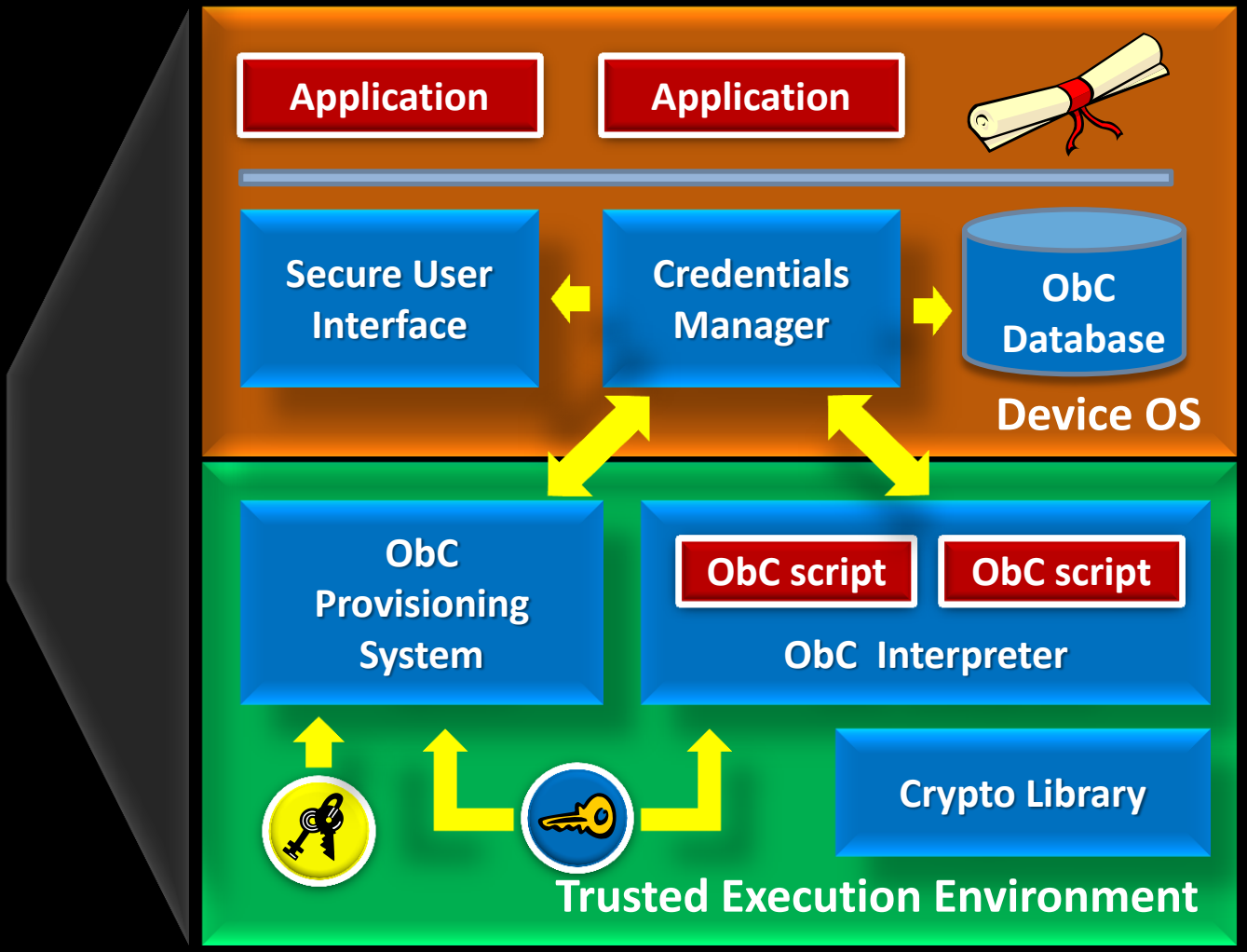
Provides isolated execution environment for trusted code

TrEEs are available on off-the-shelf devices (i.e., Nokia N900)

Untrusted Execution Environment

Trusted Execution Environment

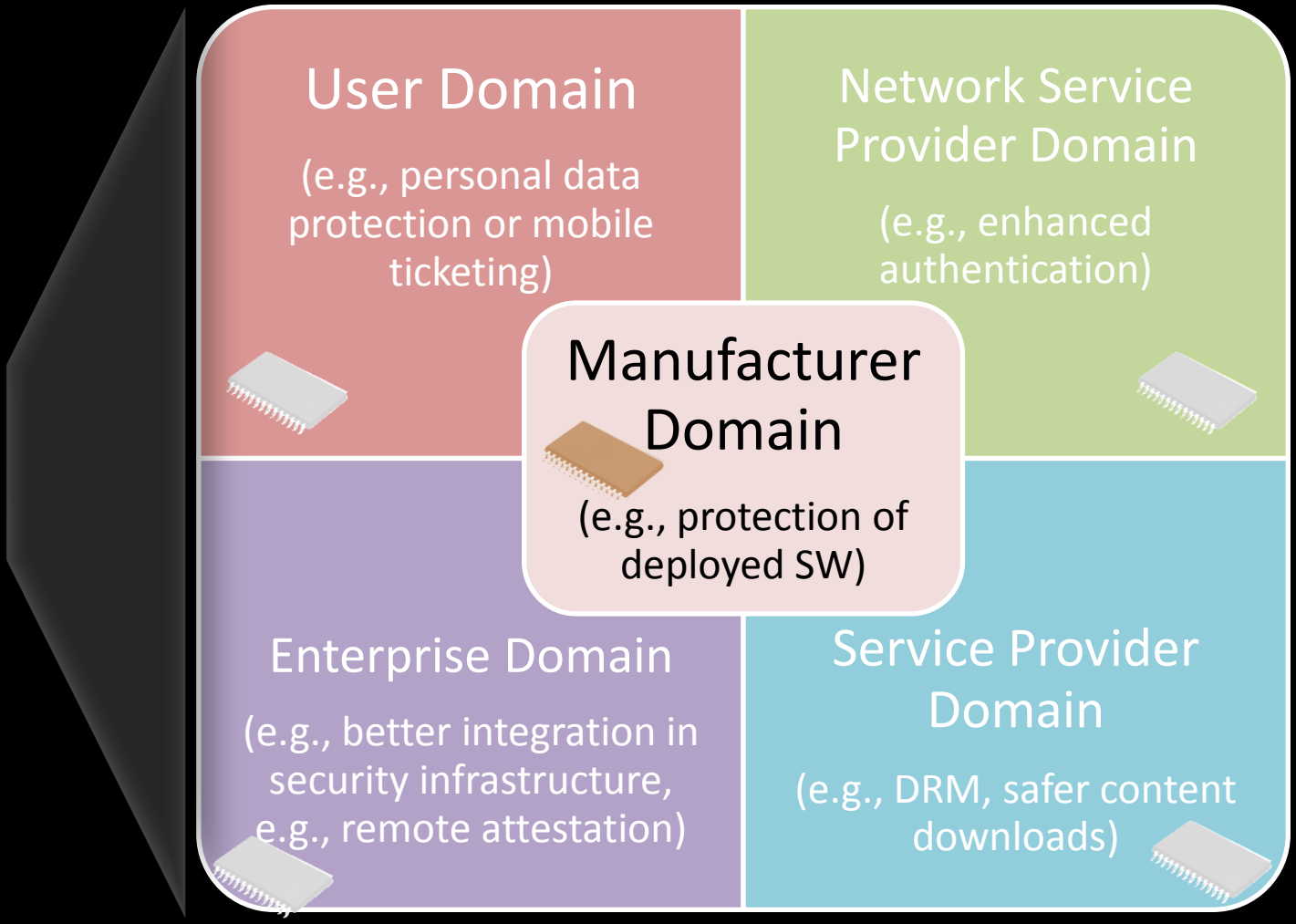
Nokia's On-board Credentials: Architecture



TCG Mobile Trusted Module: MTM Concept

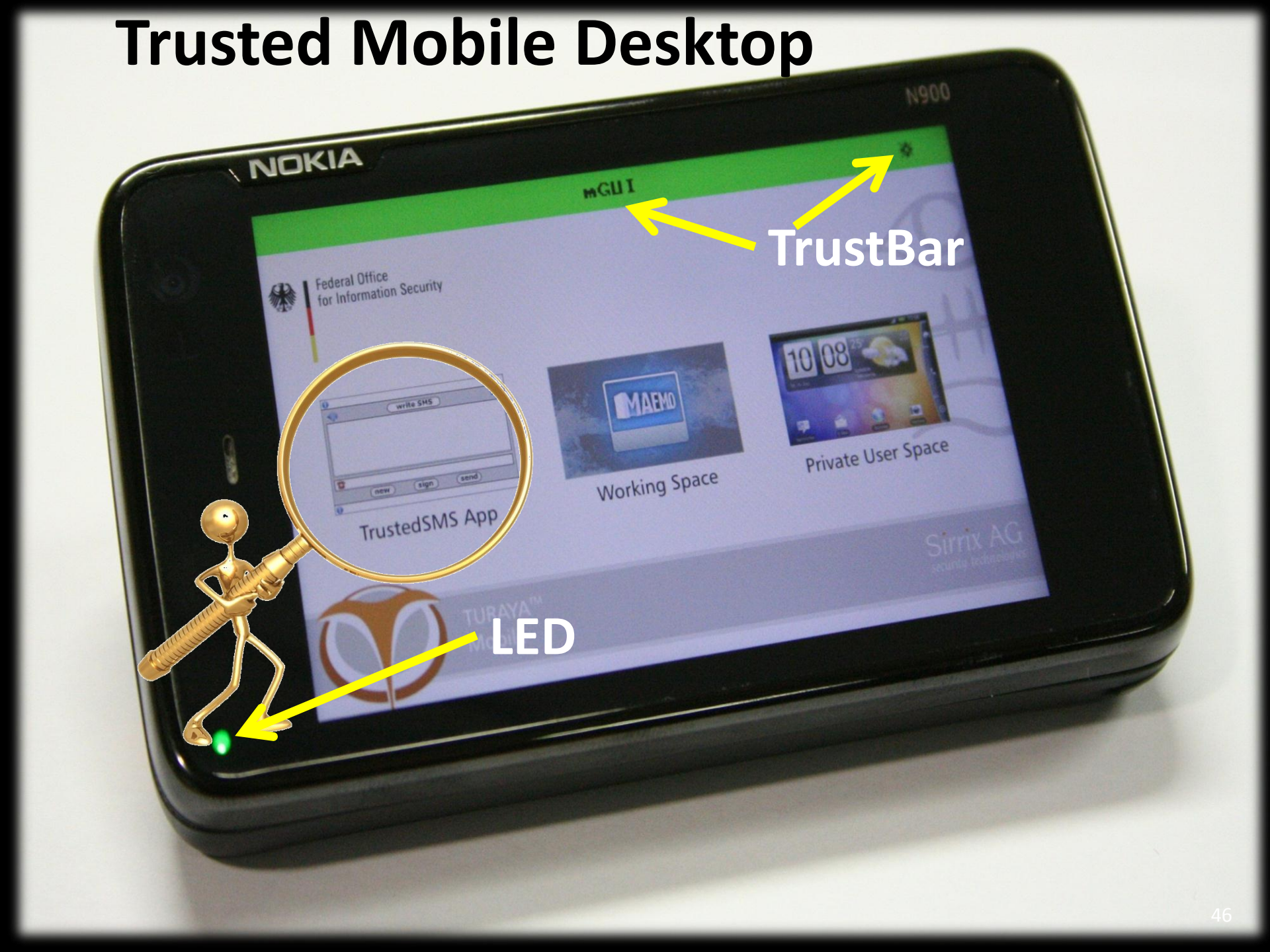
- Conceptually TPM v1.2
- Tailored for mobile use-cases
- Two types of owners for remote and local stakeholders
- Multiple parallel MTM instances with different owner each
- New Roots-of-Trust in terms of isolation for a software-based implementation
- Adapted command set from TPM specifications
- Remote Integrity Metrics (Certificates)
- Secure Boot

MTM Stakeholder Engines



Minimizing Trusted Computing Base by Security Kernel

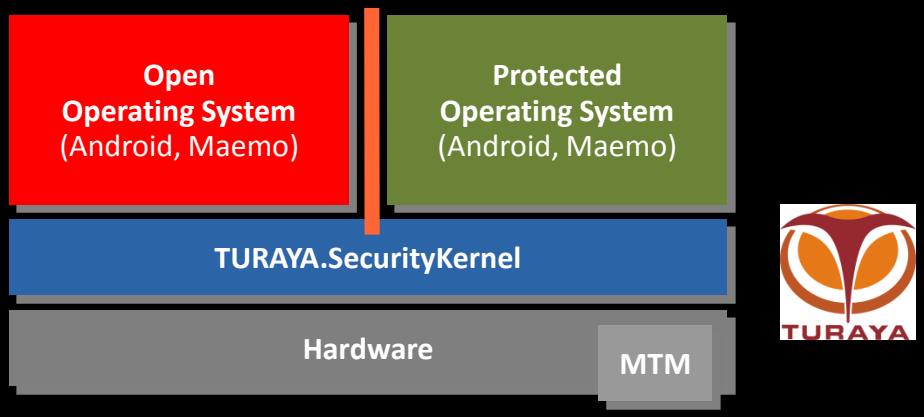
Trusted Mobile Desktop



Trusted Mobile Desktop

- **Goal**
  - Protecting sensitive data from malware and mis-configurations
  - Deploying existing modern hardware and software components
  - Strictly separated simultaneous working environments
- **Applications**
  - Voice encryption for GSM/UMTS/VoIP
  - Trustworthy client to access intranet
  - Class-3 Reader for secure ePA, smartcards, etc.

Architecture and Components



- **Hardware**
  - Support of hardware anchors such as the mobile trusted module (MTM) or smardcards
- **TURAYA.SecurityKernel**
  - Isolation of the operating systems to protect against viruses and Trojans
  - Secure user interface (GUI) to protect against trojans
  - Encryption of all user data to protect against offline attacks
- **Operating System**
  - Private under full control of the end-user
  - Corporate part under full control of the organization/company

Conclusion, Current and Future Work

- **Security of smartphones becomes crucial in future**
  - Particularly, other embedded devices interface smartphones
  - Security and privacy protection by design (are we too late again)
  - Security as enabler for new business models
- **For smartphones much of current research is devoted to Android OS**
  - Efficient and usable security extensions
- **Control Flow Integrity (CFI) on ARM**
  - Defeat run-time attacks

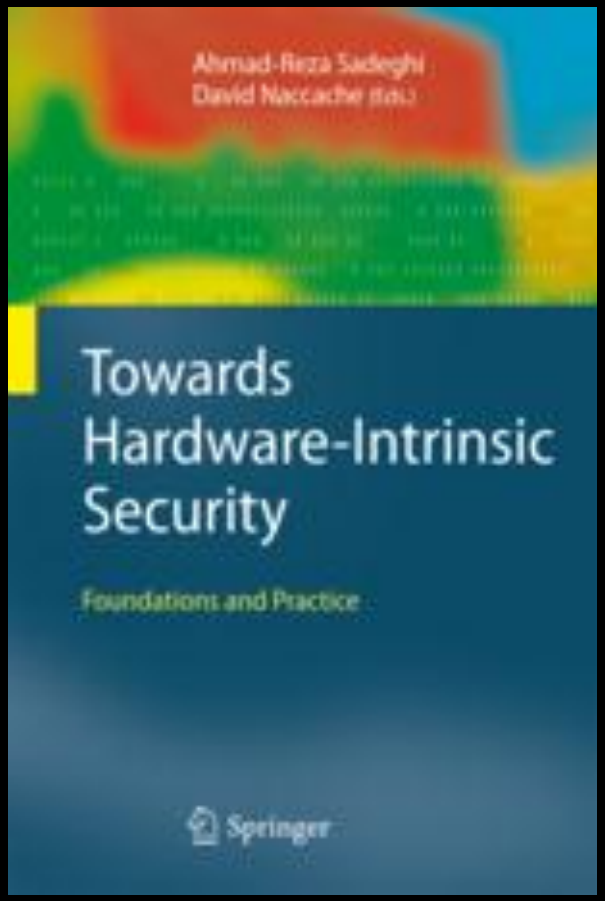
TRUST Conference at CMU/Pittsburg, USA

4th International Conference on Trust and Trustworthy Computing

22-24 June 2011, Pittsburgh, PA USA

www.trust2011.org

Thank You for Your Attention



Towards Hardware-Intrinsic Security
Foundations and Practice
Series: Information Security and Cryptography
Ahmad-Reza Sadeghi;
David Naccache (Eds.)