BizzTrust for Android

Moderne und vertrauenswürdige IT-Sicherheitsarchitekturen für mobile Endgeräte

Michael Gröne, Sirrix AG

Internet-Sicherheits-Konferenz
2. Juni 2015, Gelsenkirchen

SONY

Sirrix AG
security technologies

SecurITy
made in Germany

Sirrix AG

Founded in 2005 as a technology spin-off from the Institute for Cryptography and Security at the German Research Center for Artificial Intelligence.

Mission:

Providing proactive, trustworthy IT solutions, based on cutting-edge technology and know-how in the domain of cryptography, and the security of information and communication.

“Building Trustworthy Solutions for standard governmental and enterprise workflows.”

Sirrix AG is today one of the worldwide technology leader in „Trusted Infrastructures“ and
one of the main IT-security and crypto providers in Germany

HQ in Saarbrücken

- EMV-isolated development areas
  Clearance for Classified development
  up to TOP SECRET

Branches in Bochum and Darmstadt

- High-Security Building with radiation-shielded infrastructure

HQ in Saarbrücken

NL in Bochum

ROHDE&SCHWARZ

Sirrix AG
security technologies

SecurITy
made in Germany

Product Lines

- VOICE ENCRYPTION SYSTEMS
  - ISDN/VoIP/GSM
  - TETRA/BOS-D/SNS VS-NfD
  - NATO-SCIP VS-NfD
- Fax Encryption Systems
- Radio Encryption Systems
  - Modules for VHF/UHF Radios
  - Handsets for HF-Radios VS-NfD

- TURAYA ™ TrustedInfrastructure
  - TrustedVPN
  - TrustedDesktop
  - TrustedServer
  - TURAYA ™ Embedded
  - TURAYA ™ Mobile

- BitBox Secure Browsing
- TrustedDisk Volume und USB-Encryption VS-NfD
- PanBox
- Mobile Device Security
  - TrustedMobile iOS
  - BizzTrust™

TrustedObjects Manager Freigegeben für VS-NfD
Management for
Appliances, Policies, Users, Identities, Trusted Domains, …

Several Products are approved for Classified Use (VS-NfD or NR).

Challenges & Risks

What do we want?

- Make calls…
- Read & write messages
- Railway info, book a hotel…
- Twitter
- Make & share photos
- Games?

- Use smartphone for business
- Have contacts available
- Synchronize events
- Read & write mails
- Read & edit documents
- Enterprise-specific apps

SecurITy made in Germany

Users do not want

- Give IT access to personal information
- Restrict the functionality of the device

Enterprises do not want

- Manage personal information
- Unauthorized access to enterprise data

SecurITy made in Germany

Vulnerabilities of Smartphones (1/2)

Smartphones get lost or are stolen

- *Risk: Disclosure of stored information (mails, contacts, documents, …)*

Passphrases are not secure and will be broken

- *Risk: Disclosure of stored data, unauthorized access to enterprise resources (Intranet, Mails, …)*

Eavesdropping of the communication

- *Risk: Disclosure of transmitted information (passphrases, PINs, credentials, …), eavesdropped telephone calls*

Information collecting ("Datensauger") Apps

- *Risk: Disclosure of confidential information (contacts, calendar, location, …)*

Vulnerabilities of Smartphones (2/2)

Exploits of Vulnerabilities of Apps

- Direct access to app data
- Indirect access to data of other apps

➲ *Risk: Disclosure of confidential information*

Exploits of Vulnerabilities of Android

- Access to cryptographic keys
- Bypassing of isolation and encryption mechanisms

➲ *Risk: Disclosure of confidential information, unauthorized access to enterprise resources (intranet, mail, …)*

SecurITy made in Germany

BizzTrust for Android

BizzTrust: Secure isolation of apps and data

- Separation into two (or more) security domains
  - Enterprises have full control over business domain
  - Internet access and social media apps are restricted to personal domain
- Strong isolation
  - Isolation of apps and user data
  - Apps of one domain have no access to the other domain.
  - Business apps do not have direct access to the Internet

SecurITy made in Germany

BizzTrust Security Level

- **Hardened Operating System**
- **Protection against Exploits**
- **Strong Isolation**

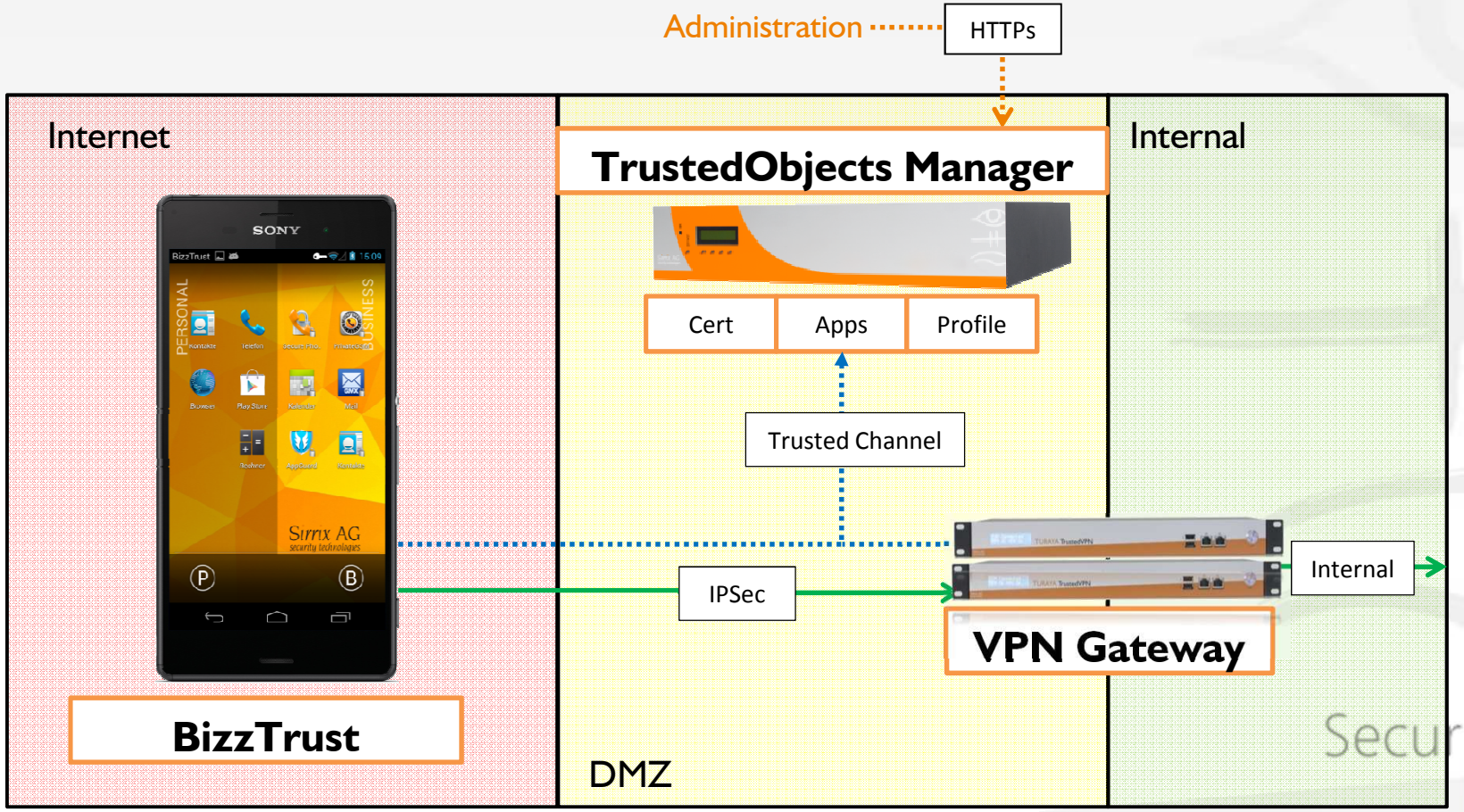
- **Control of interfaces**
- **Data encryption**

- **Policy management**
- **VPN**

Good
Samsung Knox
divide by enterproid
TouchDown™ With Exchange ActiveSync®
MobileIron
SYBASE AFARIA
SAFE SAMSUNG FOR ENTERPRISE
Symantec.
airwatch mobile device management
McAfee

made in Germany

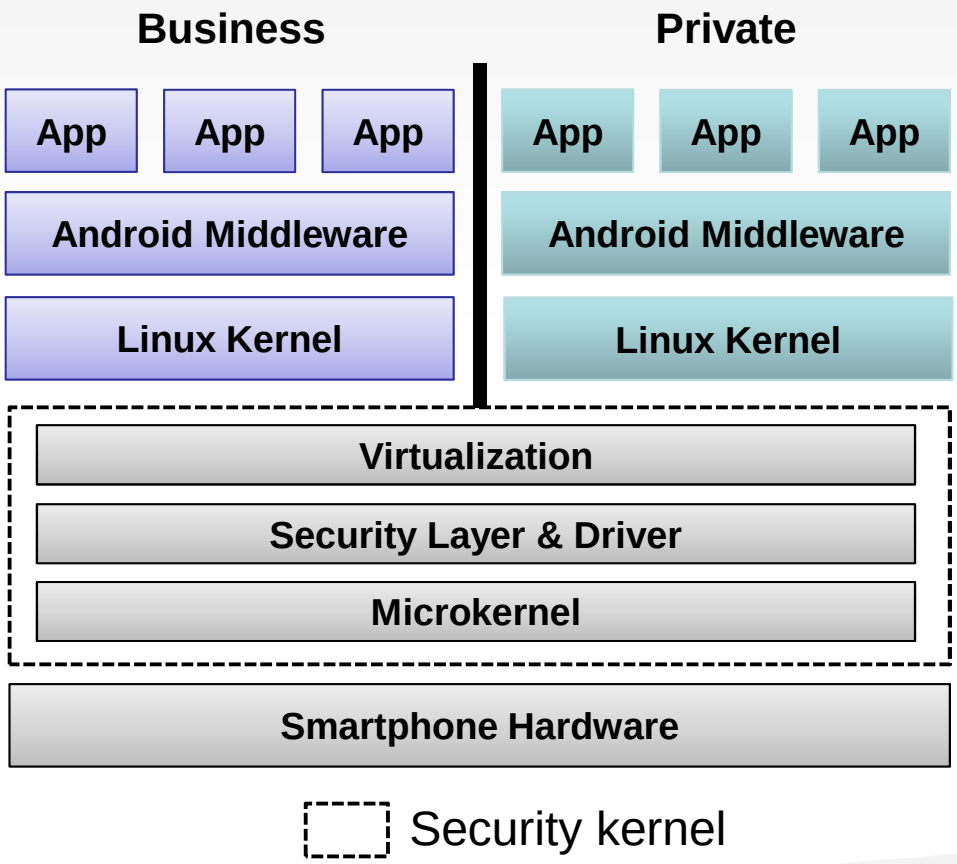
General IT Infrastructure



SecurITy made in Germany

Security Architecture

1. Microkernel-based Security Architecture



Advantages

- Small TCB

Disadvantages

- Porting costly
- Driver development
- Power consumption

Examples

- SimKo III (Telekom)
- MoTrust (Sirrix)

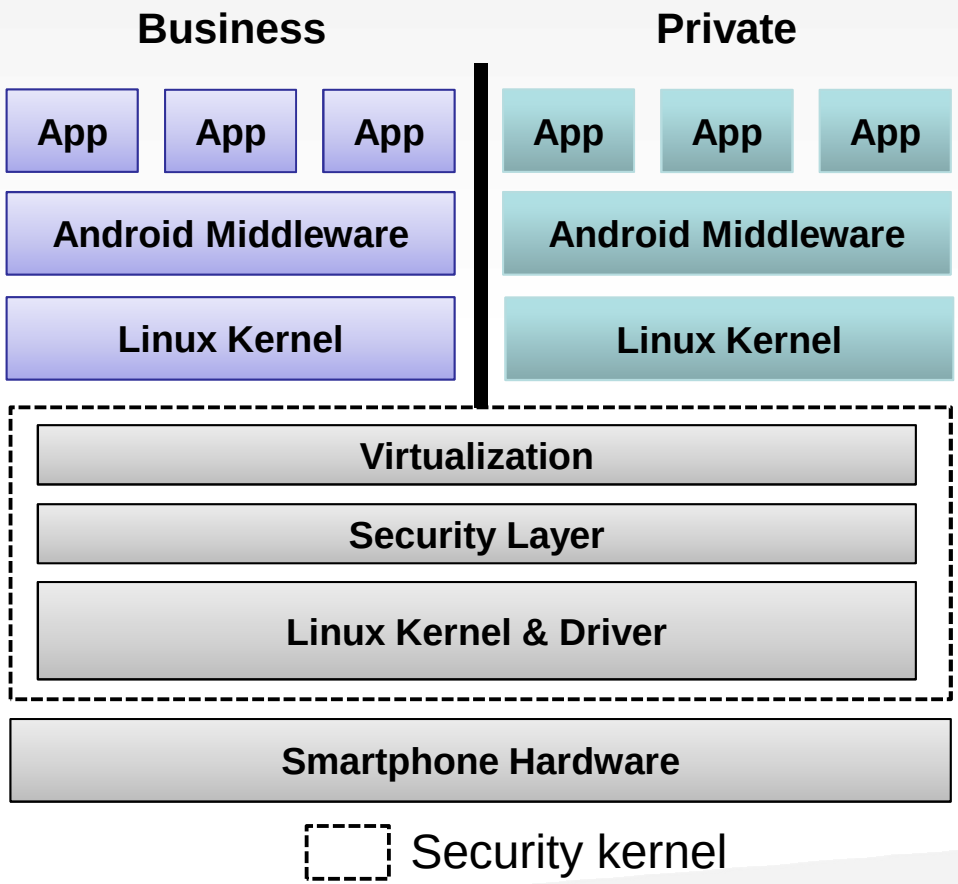
SecurITy made in Germany

MoTrust Prototype (Sirrix AG & BSI, 2009-2010)

- OKl4 Microkernel
- TURAYA SecurityKernel
- SecureGUI + TrustBar
- TPM/MTM Support
- 3 Android Instances
- Native Secure SMS-App
- Nokia N900

SecurITy made in Germany

2. Security Architecture based on Linux Containers



Advantages

- Porting easier

Disadvantages

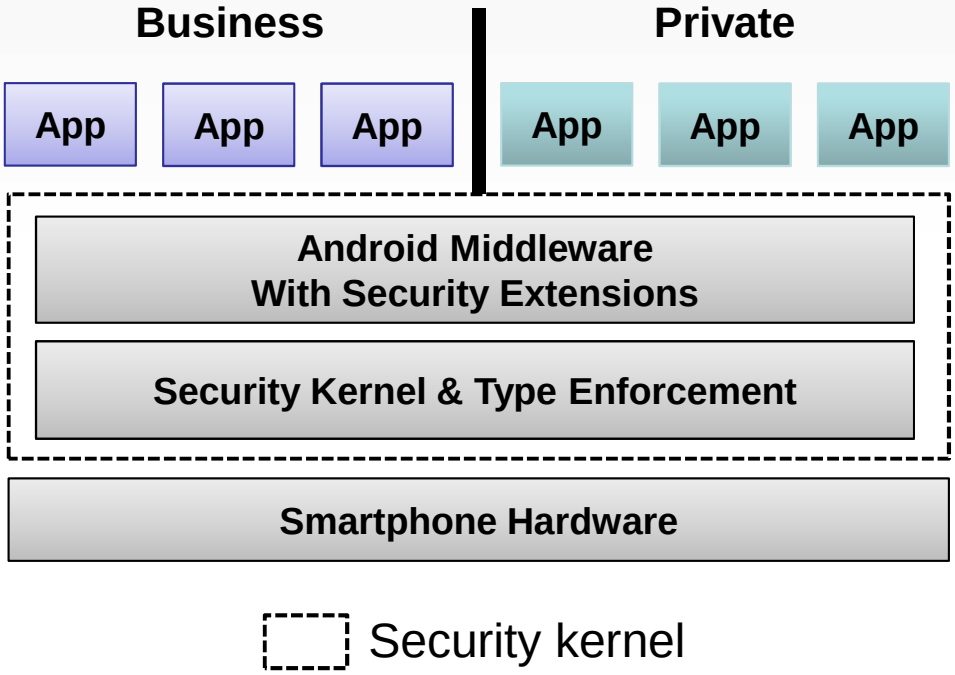
- Power consumption

Examples

- trust | me (Fraunhofer AISEC)
- RUBTrust (RUB/Sirrix)

SecurITy made in Germany

3. Security Architecture with Type Enforcement



Advantages

- Porting easier
- Low energy consumption

Disadvantages

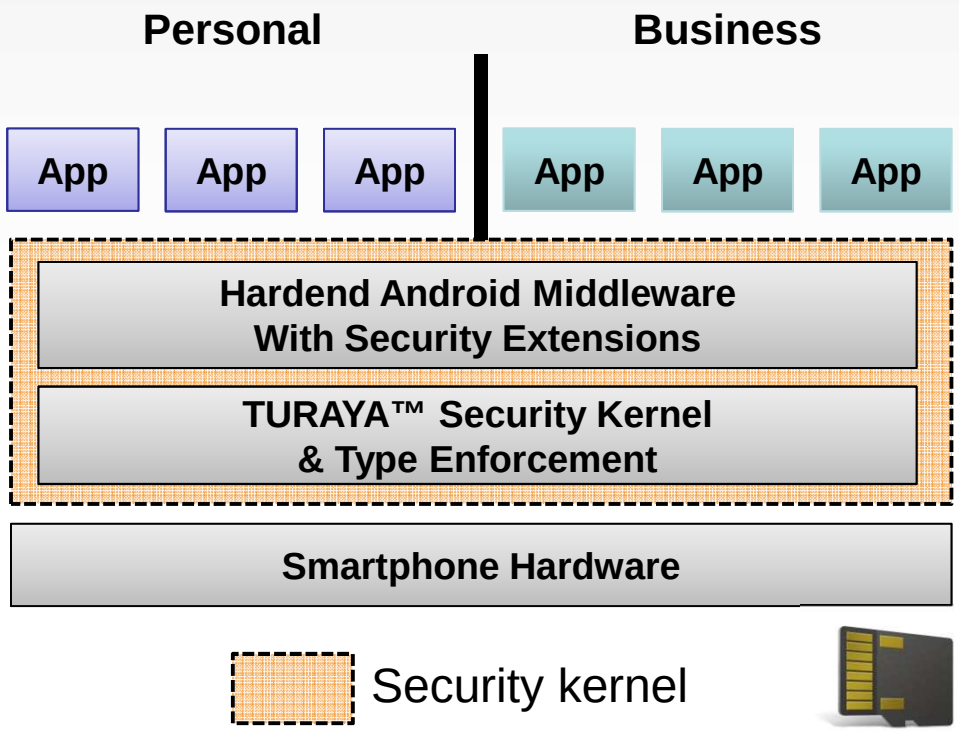
- TCB more complex

Examples

- BizzTrust (Sirrix/Fraunhofer SIT)
- KNOX

SecurITy made in Germany

BizzTrust Security Architecture with Type Enforcement



SecurITy made in Germany

BizzTrust Security Features (1)

Data at Rest

- Encryption of apps & user data on the device
- Isolation between critical and uncritical apps
  (e.g., „Personal“ vs. „Business“)
  - No access through standard Android interfaces
    (e.g., access to contacts by other apps)
  - No access through exploits of the Android middleware
  - No access through exploits of the underlying Linux system
- Type enforcement applied to all apps (protection against malware)

BizzTrust Security Features (2)

Data at Move

- Encrypted communication with enterprise resources using IPsec
  - Mails, contacts, calendar
  - Access to the Intranet
  - Enterprise-specific applications
  - Internet access through the enterprise firewall

Central Management (BSI approved for VS-NfD)

- Management of users, devices & policies
- MDM-Functions
- Secure App-Store for business domain
  - Based on TOM-generated certificates

SecurITy made in Germany

THANK YOU!

Sirrix AG
Im Stadtwald, Geb. D3 2
66123 Saarbrücken
GERMANY

Tel +49 (0)681/95986-0
Fax +49 (0)681/95986-500

Email info@sirrix.com
Web www.sirrix.com

Referenzen:

Alkassar, Heuser, Stüble:
Vertrauenswürdige Smartphones: Technologien und Lösungen,
13. Deutscher IT-Sicherheitskongress, Bad Godesberg Mai 2013.

Alkassar, Schulz, Stüble:
Sicherheitskern(e) für Smartphones: Ansätze und Lösungen,
Datenschutz und Datensicherheit (DuD) 3/2012.