Sirrix AG
security technologies

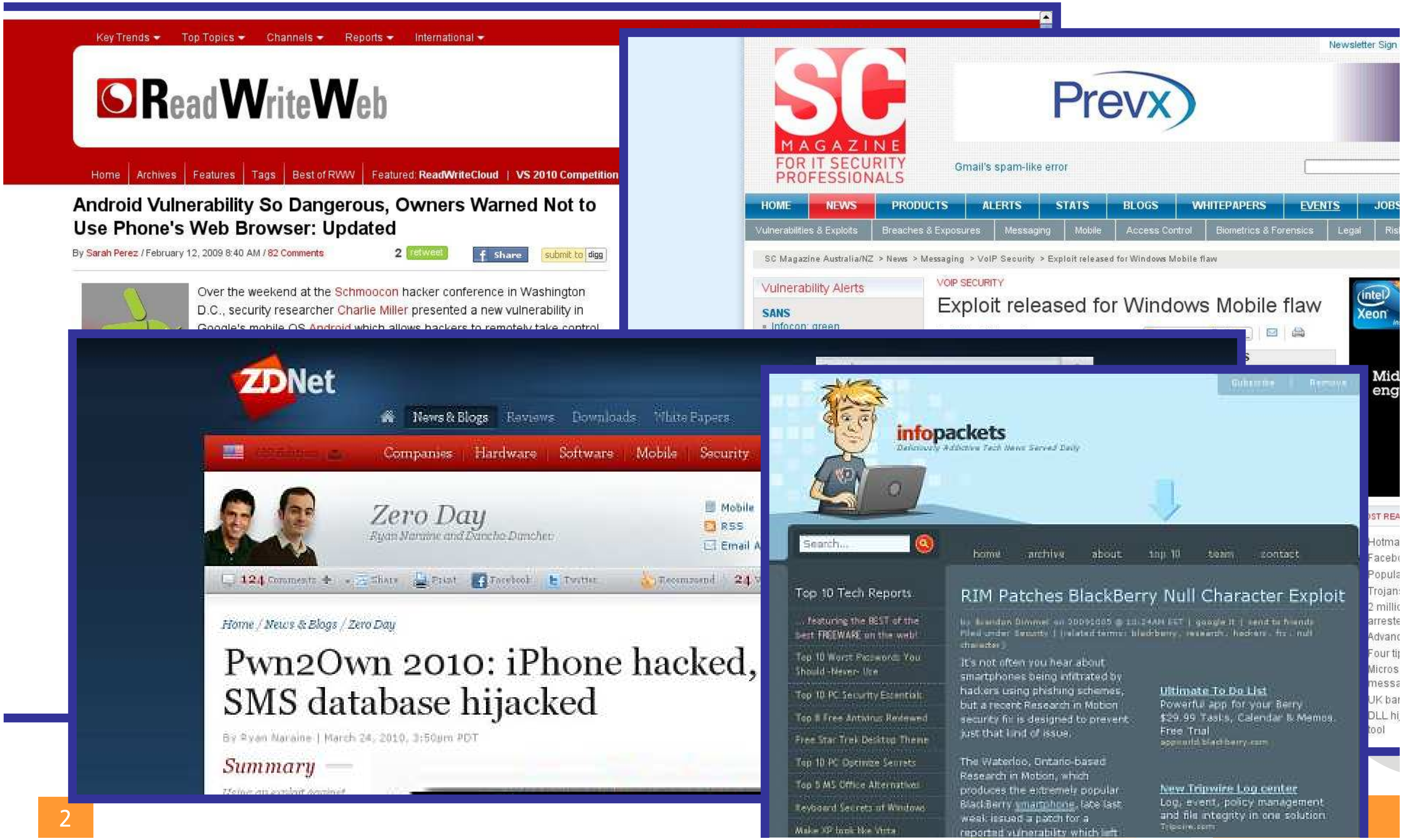
Short presentation: Practical Realization of Smartphone Security

Since Successful Business
needs Trustworthy Solutions.

Christian Stüble, Marcel Selhorst

Round Table at RSA Conference 2011
February, 14th 2011 | San Francisco

Increasing Number of Security Flaws



Android Vulnerability So Dangerous, Owners Warned Not to Use Phone's Web Browser: Updated

By Sarah Perez / February 12, 2009 8:40 AM / 82 Comments

Over the weekend at the Shmoocon hacker conference in Washington D.C., security researcher Charlie Miller presented a new vulnerability in Google's mobile OS Android which allows hackers to remotely take control

VOIP SECURITY

Exploit released for Windows Mobile flaw

Pwn2Own 2010: iPhone hacked, SMS database hijacked

By Ryan Naraine | March 24, 2010, 3:50pm PDT

Summary

Using an exploit against

Top 10 Tech Reports

... featuring the BEST of the best FREEWARE on the web!

Top 10 Worst Passwords You Should -Never- Use

Top 10 PC Security Essentials

Top 8 Free Antivirus Reviewed

Free Star Trek Desktop Theme

Top 10 PC Optimize Secrets

Top 5 MS Office Alternatives

Keyboard Secrets of Windows

Make XP look like Vista

RIM Patches BlackBerry Null Character Exploit

by Brandon Dimmel on 20091005 @ 11:24AM EST | google it | send to friends
Filed under Security | (related terms: blackberry, research, hackers, fix, null character)

It's not often you hear about smartphones being infiltrated by hackers using phishing schemes, but a recent Research in Motion security fix is designed to prevent just that kind of issue.

The Waterloo, Ontario-based Research in Motion, which produces the extremely popular BlackBerry smartphone, late last week issued a patch for a reported vulnerability which left

Ultimate To Do List
Powerful app for your Berry
$29.99 Tasks, Calendar & Memos.
Free Trial
appworld.blackberry.com

New Tripwire Log center
Log, event, policy management and file integrity in one solution.
Tripwire.com

Some Usecases, Multiple Security Requirements

Enterprise Applications

- Access to Corporate Networks (corporate apps)
- Corporate Communications (E-Mail/voice/messaging)
- Secure Storage (contacts, E-Mails, documents)
- Single-Device for work/private use
- Security Requirements: Strong Isolation

Payment

- Allowing payments, (e.g., Mobile Wallet located on the Smart Phone or NFC payment)
- Security Requirements: Strong Isolation and protection from the user

Identification

- Tool for strong authentication (e.g., nPA)
- Allowing high value transaction on the Smart Phone (e.g., QES)
- Security Requirement: Strong isolation, trust in the content displayed to the end-user, certified prove of own integrity

Developments

Gemalto/TrustedLogic: Trusted Foundations Software

- Based on ARM TrustTone

Giesecke&Devrient: MobiCore

- Based on ARM TrustTone and Qualcomm Snapdragon

Sirrix AG: TURAYA MobileDesktop

- Based on Security Kernel
- First to run on a COTS mobile device

Trusted Mobile Desktop

Federal Office
for Information Security

Developed on behalf of BSI

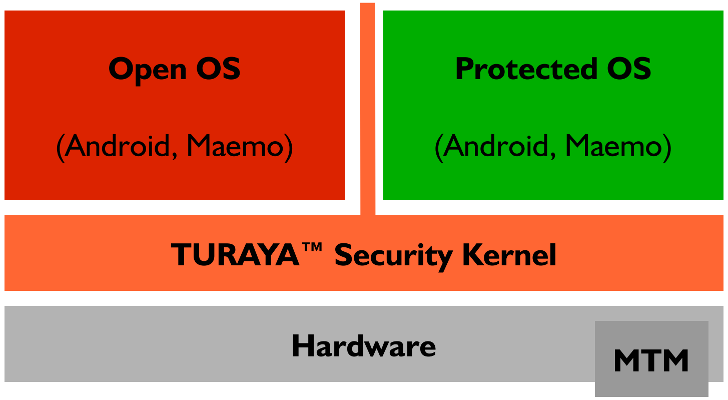
Goals

- Protection of sensitive data against malware and failure
- Using commercial off-the-shelf (COTS) mobile devices
- Providing two (or more) isolated working environments, executed in parallel
- Integrity Proof of envirponments

Example Apps

- Trusted Mobile Signature, Voice Encryption
- Trusworthy Client for corporate access and communication
- Class-3 Reader, running on mobile phone

Architecture and Components



Hardware

- Support von Hardware-Anchor as Mobile Trusted Module (MTM) or SD-Cards

TURAYA SecurityKernel

- Isolation of OS to protect against malware
- Secure GUI to protect against malware
- Remote Attestation to protect against user fraud
- Encryption of persistant data to protect against offline-attackts

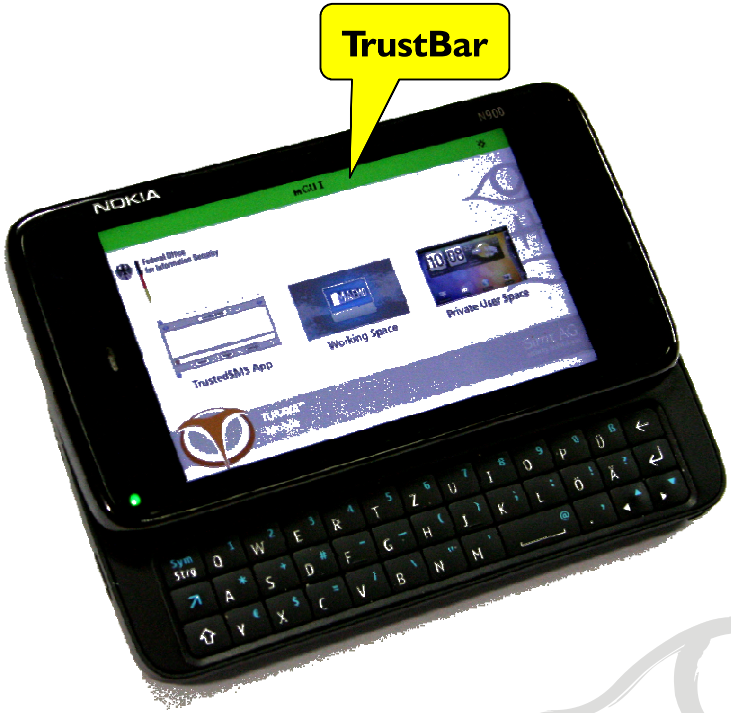
Operation Systems

- Open OS under full control of user
- Protected OS under control of user‘s organization/enterprise

Implementation

Current state

- Implemented on Nokia N900 Smartphone in collaboration with BSI
- Three working environments
  - **TrustedSMS**: Secure Messaging App
  - **Attestation**: protected OS
  - **Userlinux/Meego**: open OS



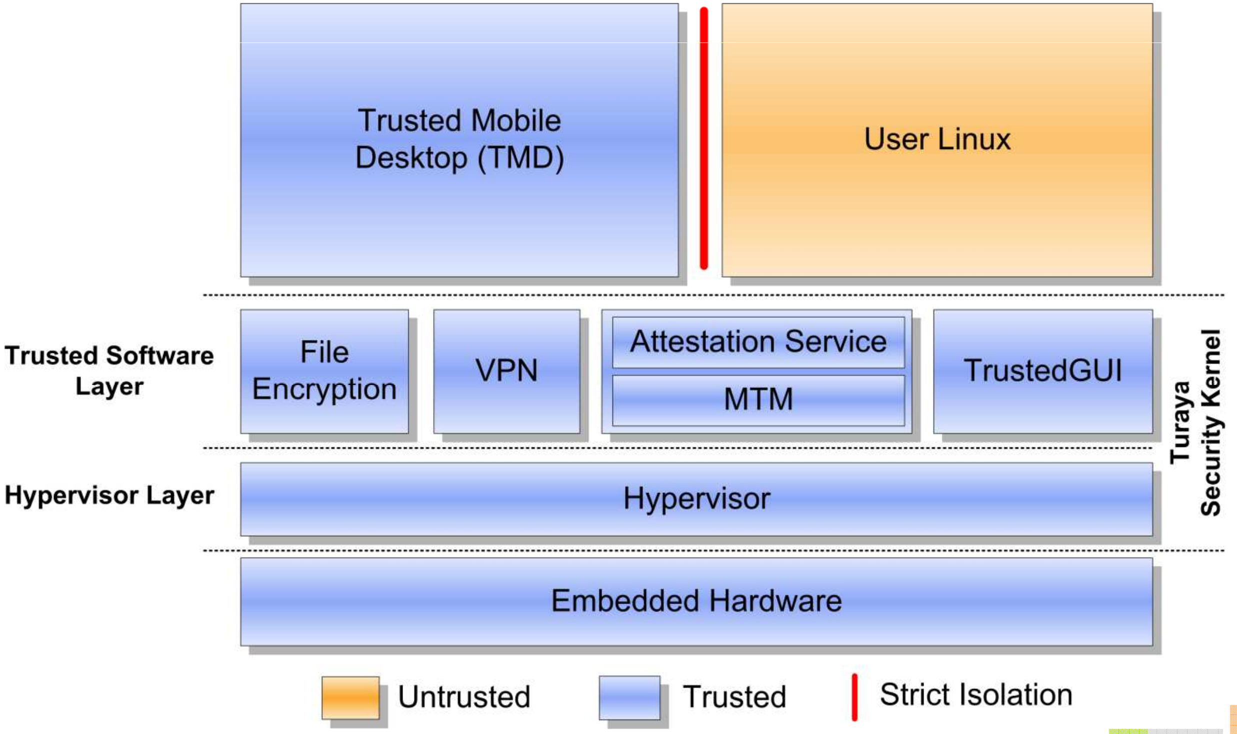
Security Features

- TrustBar for App Identification
- Switching between work environments
- Protection of user inputs (touchpad, keyboard, audio)
- Protection of user data (Isolation, encrypted storage, VPN)

Towards a Trusted Mobile Desktop (i)

Architecture

- Microkernel based security kernel providing security services
- Trusted Computing: Mobile Trusted Module (MTM)
- Strict isolation of compartments



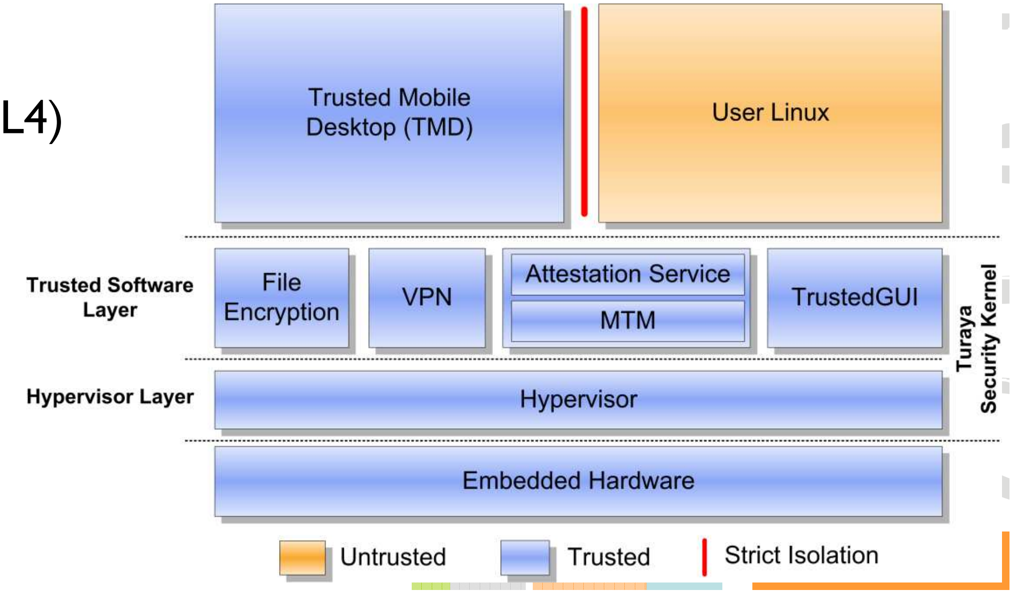
Turaya Security Kernel

Hypervisor Layer

- Traditional Virtual Machine Monitor (VMM)
- Management of
  - hardware resources (memory, IRQs)
  - processes
  - compartments / partitions / cells
- Enforcement of communication policies between isolated compartments
- Usage of different Microkernels possible (e.g., PikeOS P4 / OKL4 /L4)

Trusted Software Layer

- Provides high-level security services



Trusted Software Layer (ii)

Mobile Trusted Module (MTM)

- Software-based „TPM“ implementation
- Compliant to Trusted Computing Group (TCG) MTM spec.
- Based on MicroTSS
- Running within isolated compartment
- Verifies „Reference Integrity Measurement“ (RIM) certificates

→ necessary for secure boot

- Attests compartment configuration to external entities

Sirrix AG
security technologies

Trusted Software Layer (iv)

File Encryption

- Acts as virtual file system
- Interface for persistent storage to the TMD
- Transparently encrypts files
- Files are bound to compartment configuration
- Stored within untrusted OS

→ efficient usage of available (limited) storage (e.g., MMC)

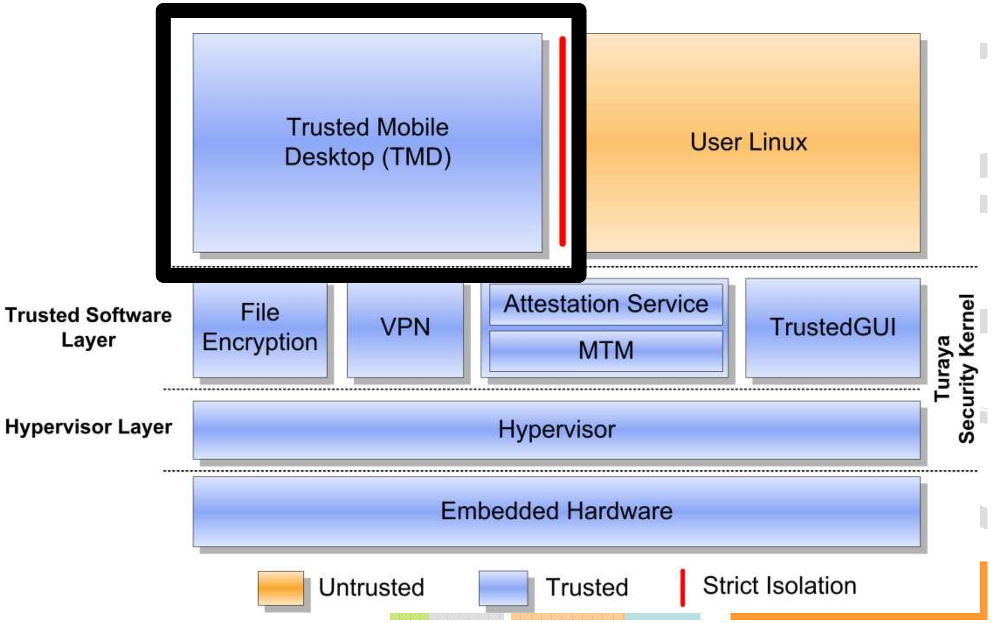
→ allows TMD compartment to be read-only

→ in context of security domains, users
can send / backup encrypted files

Application Layer (i)

Trusted Mobile Desktop Compartment

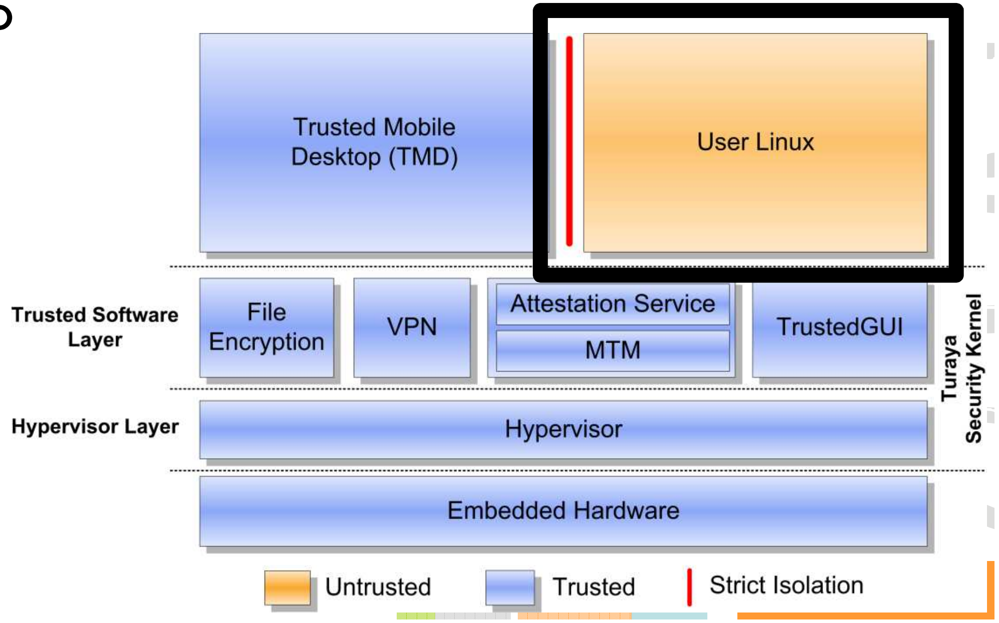
- Office working environment
- Can be under control of the company
- Read only (using File Encryption service)
- Includes business software:
  - E-Mail client
  - VoIP
  - SMS messenger
- Compartment is measured



Application Layer (ii)

User Linux Compartment

- Known / familar working environment of user
- Based on Android / Maemo / MeeGo
- User is allowed to install apps
- Due to strict isolation and security services
  - Malware doesn't affect sensitive data of TMD
  - Data theft prevented due to encryption / binding of files
  - No overlay attacks due to TrustedGUI
  - No password theft due to TrustedPath



Other Application Areas in Embedded Security

Machine2Machine Communications

- Wireless Sensors and Actors Networks (WSAN4CIP, VERIFSOFT)
- Smart-Grid, Smart-Meter (TECOM)
- Internet of Things

Car Entertainment Apps

Software Defined Radio (SDR)

- Protection of Baseband and Waveforms
- Multi-national crypto suites

…

It’s your turn now . . .

Sirrix AG
Ammar Alkassar
Building D3²
66123 Saarbrücken, Germany

Phone +49-681-95986-0
Fax +49-681-95986-500

a.alkassar@sirrix.com
http://www.sirrix.com

Sirrix AG
security technologies