

## *Practical Exercise 3*

### Technology II

**Mobile Business I (WS 2010/11)**

Prof. Dr. Kai Rannenber

T-Mobile Chair of Mobile Business & Multilateral Security  
Johann Wolfgang Goethe University Frankfurt a. M.



**Master of Science in Management**  
*-Prüfungstermine Wintersemester 2010/11-*

	<b>11:30 Uhr</b> MSM - Grundlagenmodule	<b>15:00 Uhr</b> MSM - Modul aus Finance	<b>15:00 Uhr</b> MSM - Modul aus Accounting	<b>15:00 Uhr</b> MSM - Modul aus Inf. Management	<b>15:00 Uhr</b> MSM - Modul aus Freier Bereich
21. Feb. 11	-----	CFIN	IFRS	-----	CFIN
22. Feb. 11	JAAN	-----	-----	ITRE	<b>FECO</b> <b>11:30 Uhr</b>
23. Feb. 11	ADMA	-----	-----	-----	ETAX
24. Feb. 11	<b>MABP</b> <b>15:00 Uhr</b>	MPMA	-----	MABP	MABP   MPMA
25. Feb. 11	-----	EMFI	-----	-----	EMFI
28. Feb. 11	<b>INKO</b> <b>15:00 Uhr</b>	-----	-----	INKO	INKO
1. Mrz. 11	-----	UBUF	UBUF	-----	SMOM
2. Mrz. 11	SMMA	MEAC	-----	-----	MEAC
3. Mrz. 11	-----	-----	PCGU	-----	PCGU   SCFE
4. Mrz. 11	CMAP	-----	IAEE	-----	<b>FINE</b> <b>11:30 Uhr</b>
7. Mrz. 11	-----	RIMI	-----	ISMA	ISMA   RIMI
8. Mrz. 11	CFVA	PEVC	DARE	DARE	SCCO
9. Mrz. 11	<b>EFN1</b> <b>15:00 Uhr</b>	EFN1	-----	EFN1	-----
10. Mrz. 11	-----	-----	-----	SESI	SESI
<b>11. Mrz. 11</b>	<b>MOB1</b> <b>15:00 Uhr</b>	ETIF	-----	MOB1	MOB1   ETIF

## *Lecture 8*

Smartcards and Related  
Application Infrastructures

**Mobile Business I (WS 2010/11)**

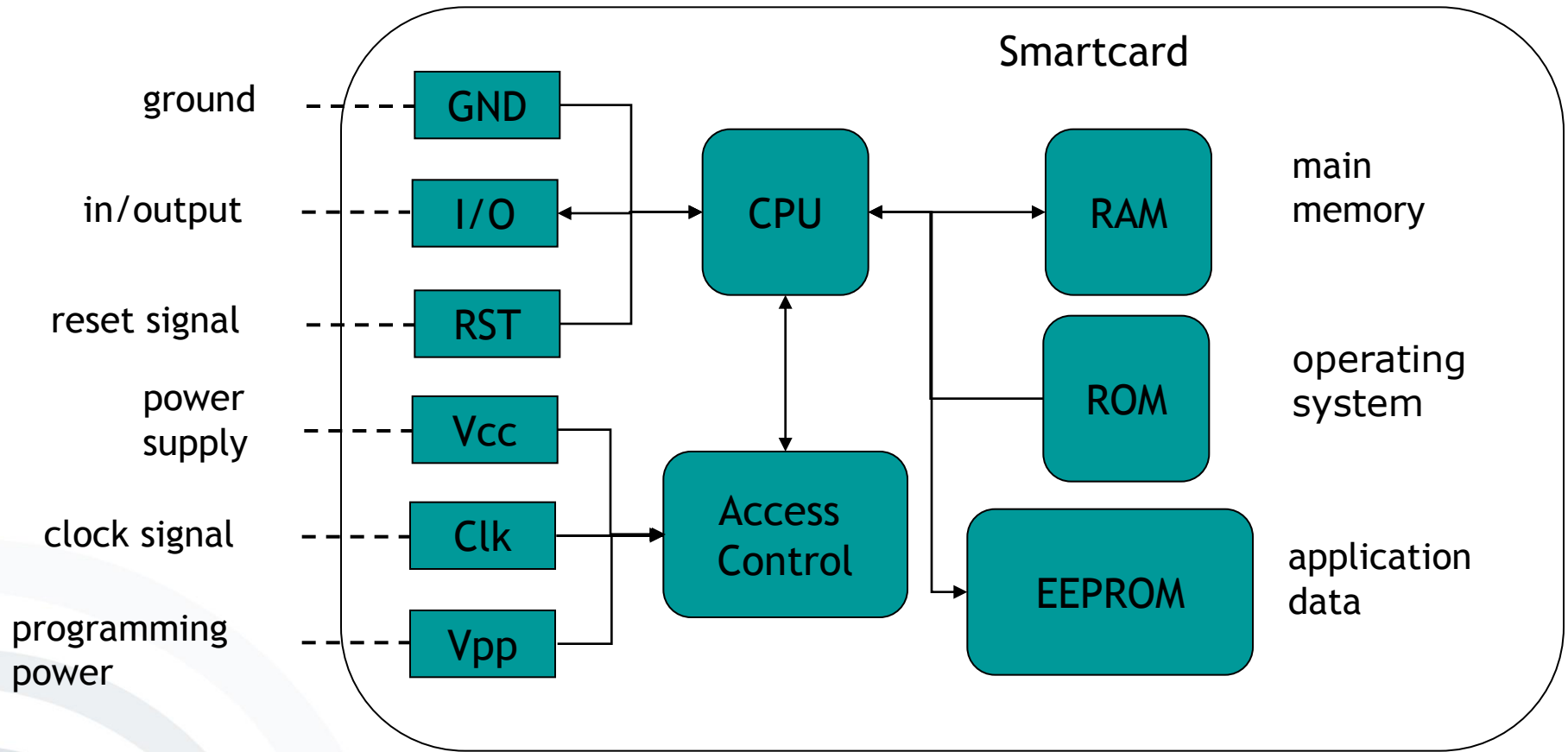
Prof. Dr. Kai Rannenber

T-Mobile Chair of Mobile Business & Multilateral Security  
Johann Wolfgang Goethe University Frankfurt a. M.



- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- Universal SIM (USIM)

- Small computers with **memory, operating system, software, processor, I/O and access control**
- **Chip protected against manipulation**
- After being **initialised with keys** and other data smartcards are distributed to their users.



[Source: SecCommerce2002]

- Used when **security** of data (e.g. for keys, signatures, physical access control, payment) is needed in **insecure environments**
- **Examples:**
  - Phone cards of Deutsche Telekom
  - Signature cards according to German Signature Law
  - Smartcard applications for PC
  - Smartcards for mobile communication (SIMs)

# Smartcards – Examples



## Protection needed against:

- Unauthorised usage of services through forged user data
- Duplication of a user's credentials
- „Cracking“ of credentials
- Billing fraud

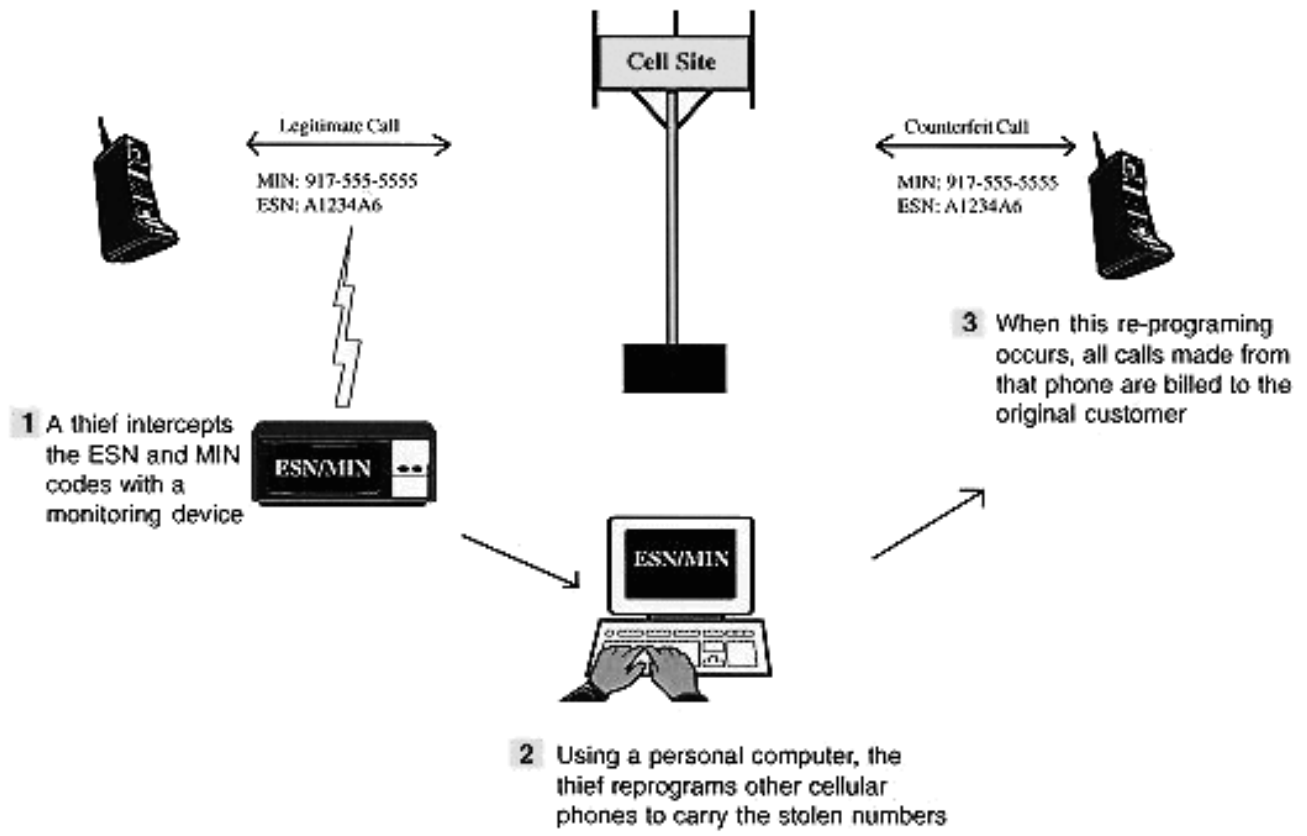
## CELLULAR COUNTERFEITING/CLONING FRAUD

### Cellular Phone Counterfeiting

With each call made, a cellular phone transmits an Electronic Serial Number (ESN) and a Mobile Identification Number (MIN) identifying the caller. Possession of these numbers is the key to the counterfeiting.

Example for faulty system design (CDMA)

Duplication of intercepted user IDs



- Smartcards – Introduction
- Subscriber Identity Module (SIM)
  - Functionality
  - Technology
  - SIM Application Toolkit (SAT)
- Universal SIM (USIM)

- In GSM and UMTS since 1991, upcoming for WLAN
- Represents contract between subscriber & network operator
- Authorises a “phone” to use the network by linking it to a **subscription**
- **3450 Mio** GSM subscriptions [GSM2009]
- **More** countries with **SIM** infrastructure (219, 2010-Q4) than with **McDonald’s** (125, 2010-Q4) and **more than UN** member states (192, 2010-Q4)

[GSM2010, McDonalds2007, Wiki2010, UN2006]



- **SIMs are Smartcards:**
  - SIM cards serve as security medium.
  - Tamper-resistance prevents counterfeiting.
  - robust design
- Contain **International Mobile Subscriber Identity (IMSI)** for subscriber identification and the key  $K_i$  provided by the mobile operator
- Reliably execute computational functions for the mobile device

- SIM serves as „**identity card**“ for GSM cellular phone subscribers.
- SIM identifies the **issuer of the card** – important for the **billing of roaming subscribers** by roaming partner.
- SIM allows for **secure billing of roaming subscribers** through SIM-cryptography – important for card issuer.
- SIM contains additional **configuration data** of the GSM system.

- Protected data:
  - IMSI, PIN, PUK
  - A3, A8 crypto algorithms
  - List of subscribed services
  - Language used by the subscriber
- Dynamic data:
  - Cell information
  - Frequency information
  - Dynamically generated (session) keys
  - Attributes of GSM login
  - User data (address book, telephone list, SMS memory)

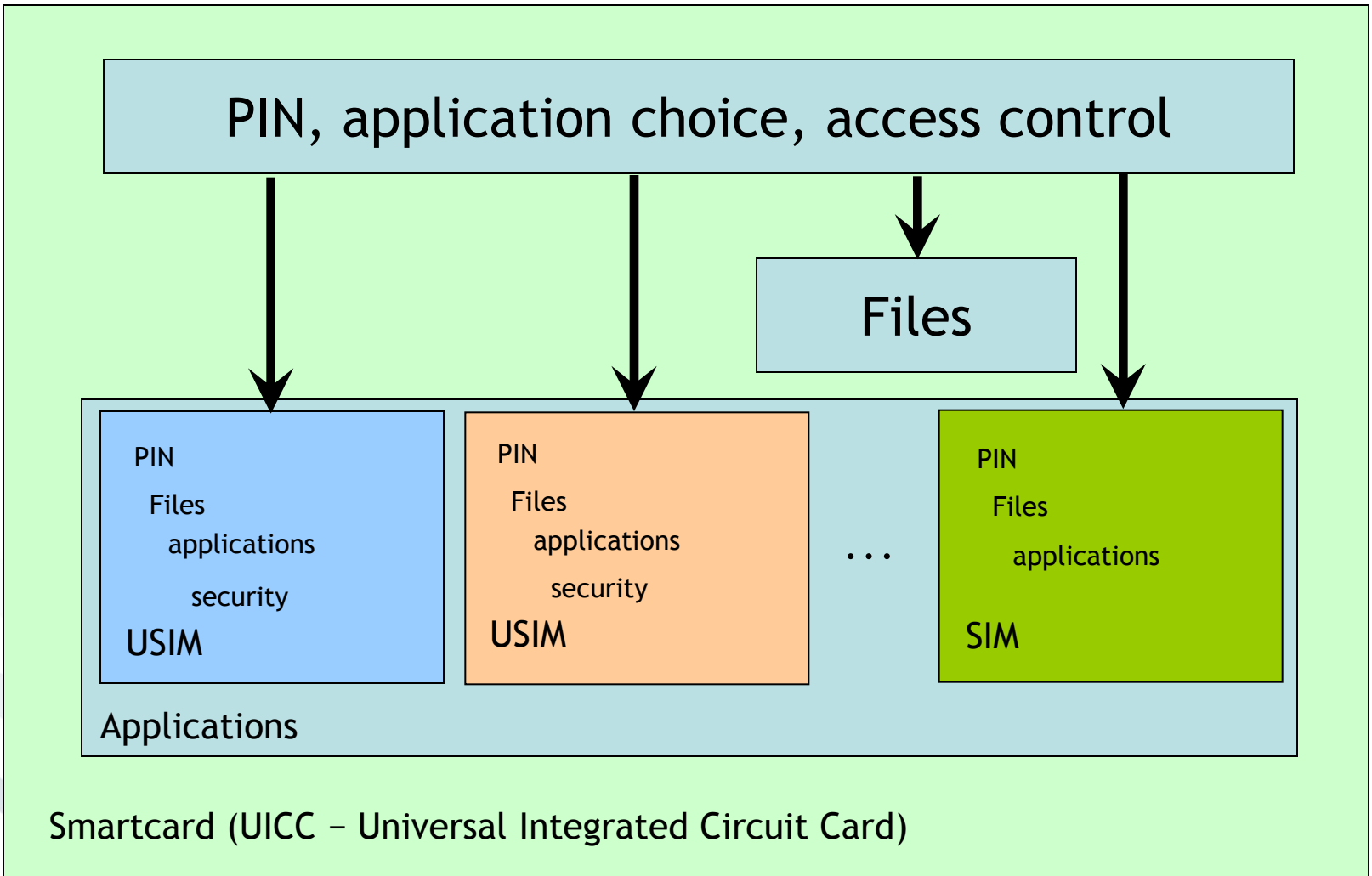
- **ETSI GSM 11.11** [GSM2006] specifies electrical as well as software interfaces between SIM and device.
- A **serial interface** is used for accessing the card.
- Communication through **SIM commands**
- Device can access **files** or execute **actions** through SIM commands.
- „SIM Application Toolkit“ allows for implementing of **additional applications** on a SIM.

- Provides an interface for **Value Added Services** implemented on **programmable SIMs** for interacting with mobile devices
- **Standardised 1996** as ETSI GSM 11.14, extended 1999 [GSM2006]
- **Controls I/O, Telephony, Download**
- Allows for **security functionality**
- „Living standard“

- **Mobile Banking and Brokerage**
  - T-Mobile and T-Online SMS banking
- **Secure payment** via cellular phone
- **Authentication** of users trying to access servers
- **Location-based services**
  - ATM search, navigation
- **Security applications in general**
  - Mobile signatures

- Smartcards – Introduction
- Subscriber Identity Module (SIM)
- Universal SIM (USIM)

- **Standardised** in 3GPP TS 21.111 and 3GPP TS 31.102 [GSM2006]
- **Successor** of SIM in 3G networks (but 3G networks are downward compatible to many SIMs)
- Supports different „virtual“ **USIMs** and **SIMs** on one cards – i.e. multifunctional smartcard
- Specified as „**UMTS-SIM**“, to support authentication, authorisation and computation of future services



Smartcard (UICC – Universal Integrated Circuit Card)

- **Support for multiple applications**
- **End-to-end security** from the USIM to the application
- **Authentication of the network towards the USIM via cryptography**
  - ➔ **Multilateral Security** is possible!
- **Downward compatible to SIM**
- **Extended phone book on card:**
  - Email addresses
  - Multiple names & numbers for each entry
  - More memory
  - Standardised entries

## Visions of new Opportunities

- **Market entry of USIM „disguised“ as SIM**
  - ➔ UMTS activated by operator
- **Multiple USIMs – possibly from competing providers – can technically coexist on one card. Selection via menu on mobile device**
  - ➔ Reduction of operator switching cost
- **Switching to anonymous prepaid USIM as a privacy option when using privacy sensitive services?**

## Lecture 9

### Mobile Devices

### Mobile Business I (WS 2010/11)

Prof. Dr. Kai Rannenber

T-Mobile Chair of Mobile Business & Multilateral Security  
Johann Wolfgang Goethe University Frankfurt a. M.



[Source: HTC]

- **Categorisation of Mobile Terminals**
- **Components of Mobile Terminals**
  - Accumulators
  - Processors, Memory, and Storage
  - Display Technologies
  - I/O Technologies

- Categorisation is possible by:
  - Technical characteristics
  - Application aspects
    - Functional completeness (Is the functionality comparable to a desktop PC/Laptop?)
    - Size of the terminal/device
    - Security features

- Hardware independence
  - Independent terminals
  - Terminals with external communication
  - Terminals with external security modules
  - Terminals with external memory
- Operating system – Characteristics
  - Memory security, file security, access control
  - Security module support, secure I/O, program and system integrity

- Lifespan of an application
  - Battery consumption, amount of data, and size of memory
  - Data integrity, amount of communication, and costs
- Completeness of the functionality for the end-user
  - Information / Reaction
  - Limitations due to device size
  - Feature Sets

- Device size
  - Small / integrated devices
  - „Pocket-sized“
  - „Laptop-sized“
- Access to the security module
  - Data integrity, encryption
  - Digital signatures
  - Access control, authentication

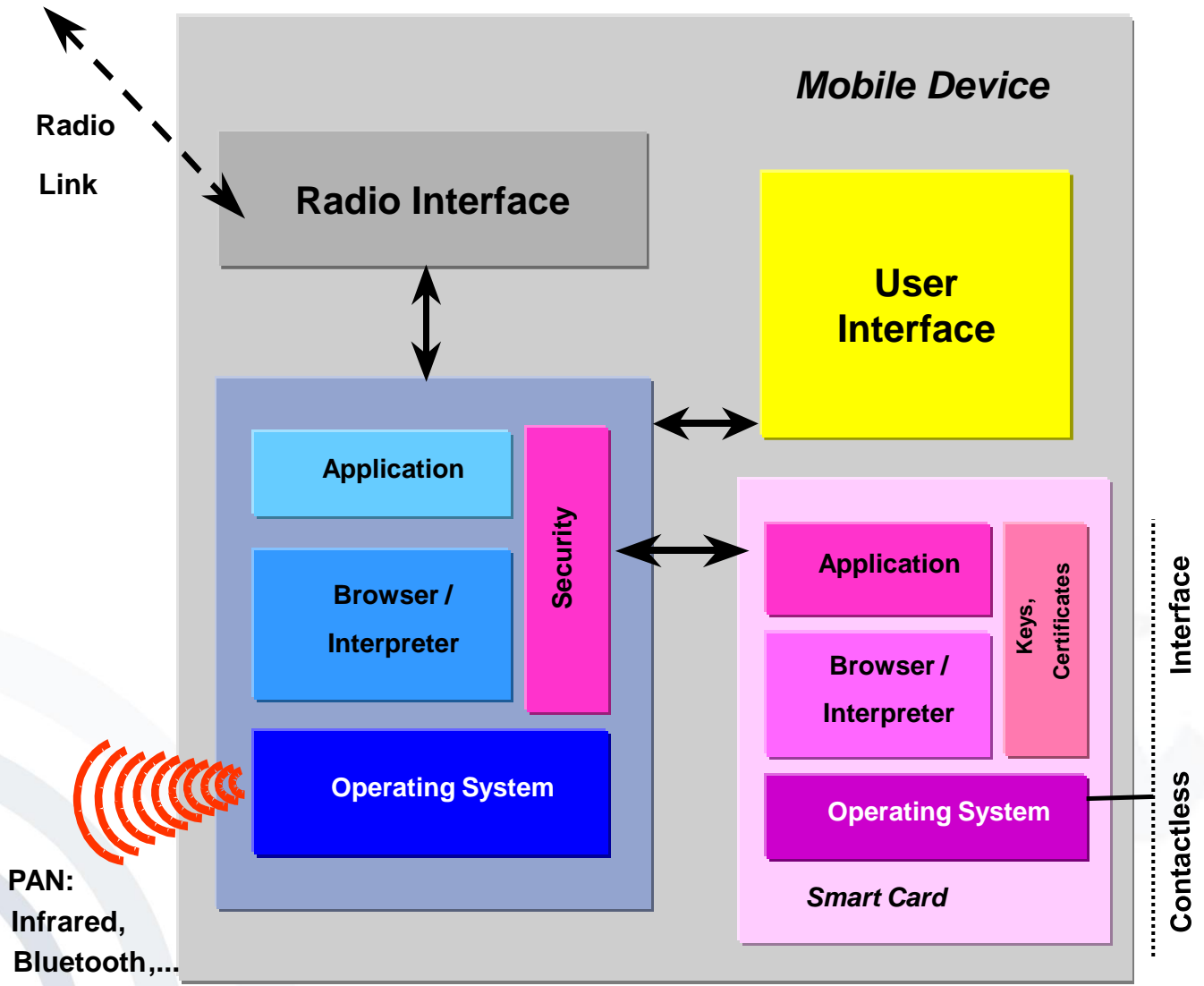
- Different requirements for different kinds of devices:

	Mobile Phone	PDA	Laptop
<i>Number of „Switch-ons“ per day</i>	Low	?	?
<i>Duration of usage per task</i>	?	Low	High

Based on [Burckhardt2001]

- Categorisation of Mobile Terminals
- Components of Mobile Terminals
  - Accumulators
  - Processors, Memory, and Storage
  - Display Technologies
  - I/O Technologies

# Functional Architecture



[Posegga2001]

- The size of a mobile terminal is considerably determined by its:
  - Input Facilities (e.g. keyboard)
  - Output Facilities (e.g. display)
- ➔ Separation of components (e.g. display in the watch, head-mounted-displays)

- Categorisation of Mobile Terminals
- Components of Mobile Terminals
  - Accumulators
  - Processors, Memory, and Storage
  - Display Technologies
  - I/O Technologies
    - Device Input
    - Personal Area Networks (PAN)

- Personal environment, short range
- **Purpose:** Connection of devices in short range, for example PDA and printers.
- Replaces cable-connections:
  - Infrared Data Association (IrDA)
  - Bluetooth



- IrDA: Infrared Data Association (1993):
- Standardized infrared-protocols
- IrDA Version 1: asynchronous, serial connection up to 115 kbps
- Point-to-Point
- Protocol-family for various purposes
- New specification: up to 4 Mbit/s
  
- Exemplary applications:
  - Transmission of mobile business cards
  - Sales data extraction from cigarette vending machines
  - Connection between mobile and laptop
  - Wireless printing

- Attributes:
  - Wireless
  - Range of up to 10 meters
  - Illumination-angle  $15^{\circ}$  -  $30^{\circ}$
- Disadvantages:
  - **Sounding:** If the infrared-ray misses the target
  - Optical connection required
  - Short interruptions of the optical connection, e.g. between laptop and mobile phone in trains, lead to complete network-interruption.

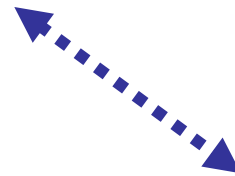
- Frequency range of 2.4 GHz
- Simple and cheap possibility to set up ad-hoc networks of limited range (up to 10 meters)
- No official standard, but de-facto-standard
- Consortium: Ericsson, Intel, IBM, Nokia, Toshiba, etc.
- Broadly supported by the industry



# Personal Area Network (PAN)

Popular Bluetooth Applications

Picture transmission  
between devices



Wireless communications between devices  
(Bluetooth-Headset)



- Connection of periphery-devices (headsets, keyboards, mice, etc.)
- Setting up of ad-hoc networks for spontaneous data exchange
- Ad-hoc connection of different networks (e.g. laptop ↔ mobile or phone ↔ GSM ↔ net)
- Applications similar to applications based on infrared technology
- Weaknesses of infrared technology were overcome
  - Increased bandwidth (up to 865.2KBit/s)
  - No optical connection between devices necessary
  - Expanded range (up to 10m)
  - Allows setting up of ad-hoc networks instead of point-to-point connections

## *Lecture 10*

# Market Overview of Mobile Operating Systems and Security Aspects

**Mobile Business I (WS 2010/11)**

Prof. Dr. Kai Rannenber

T-Mobile Chair of Mobile Business & Multilateral Security  
Johann Wolfgang Goethe University Frankfurt a. M.



- Mobile OS unavailable to other device manufacturers
  - Overview
- Manufacturer-independent mobile OS
  - Overview
  - Symbian platform (by Symbian Foundation)
  - Embedded Linux
  - Android (by Open Handset Alliance)
  - Microsoft Windows CE, Pocket PC, Pocket PC Phone Edition, Mobile
  - Microsoft Windows Phone 7
- Security features of selected mobile OS

# Mobile OS unavailable to other device manufacturers

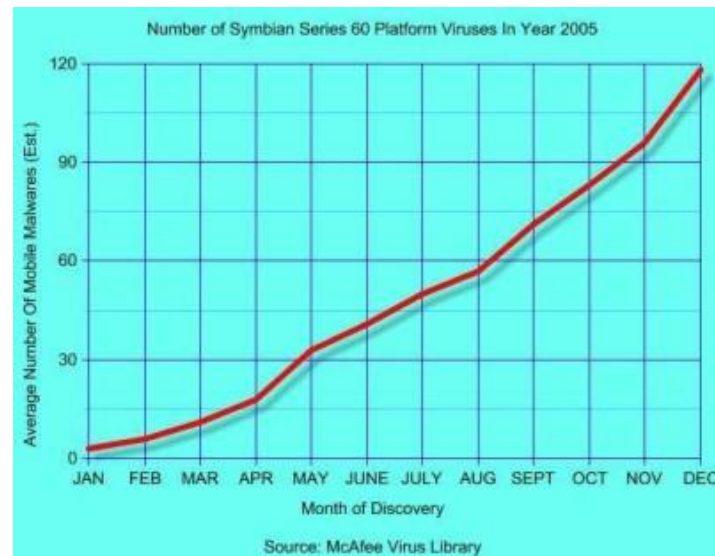
- In the past, most mobile phone manufacturers used their own “closed” operating systems for their mobile devices.
- Today, more and more platforms switch to more open and interoperable operating systems (e.g. Windows CE, Symbian OS).
- Some manufacturers (still) rely on own OS, e.g. RIM Blackberry OS, Apple iOS.
- **Advantage:** Tend to be not as much affected by malware than “open” operating systems
- **Disadvantage:** Less flexible, as 3<sup>rd</sup>-party software cannot be easily installed and executed

- Palm OS (Garnet OS)
  - Latest release: Most devices equipped with Palm OS 5.4
- Apple iOS (Unix-based)
  - Latest release: iOS 4.2.1
- RIM BlackBerry OS
  - Latest release: BlackBerry OS 6.0
- HP webOS (initially developed by Palm)
  - Latest release: webOS 2.0
  - Not to be confused with Palm OS (now: Garnet OS) that was also initially developed by Palm
- Samsung bada
  - Latest release: 1.2 (Samsung S8530 Wave II phone)

- Mobile OS unavailable to other device manufacturers
  - Overview
- Manufacturer-independent mobile OS
  - Overview
  - Symbian platform (by Symbian Foundation)
  - Embedded Linux
  - Android (by Open Handset Alliance)
  - Microsoft Windows CE, Pocket PC, Pocket PC Phone Edition, Mobile
  - Microsoft Windows Phone 7
- Security features of selected mobile OS

- Today, mobile operating systems allow the execution of 3<sup>rd</sup>-party software
  - As a result, malware can also be executed on mobile operating systems, either intentionally or by security leaks inside the mobile operating system (exploits).
- Possible threats for the user are:
  - Device malfunction
  - Loss of data (malware erasing data)
  - Loss of money (e.g. malware sending SMS to premium services )
  - Shorter battery runtime (more processing/resource usage)

- **09/2000:** Liberty Horse Trojan
- **12/2000:** Telefonica SMS Mailer
- **08/2001:** Flooder sends unwanted SMS
- **09/2001:** Phage erases data on Palm devices
- **02/2003:** Nokia V-Card exploit
- **09/2004:** First Symbian OS malware
- ...



- Memory protection
  - Processes are not able to access the memory of other processes.
- File protection
  - Encryption
  - Access control
- Access controls
  - Definition of access rights and monitoring of their enforcement.
- Support for security modules
- Secure I/O
- Code integrity management: Integrity of programs is checked before they are started by e.g.
  - Checking certificates
  - Proof Carrying Code
- Additional Security Software may be needed, e.g.
  - Virus scanners
  - Firewalls

- Every user has certain assigned access rights, e.g.
  - Reading a file
  - Writing a file
  - Accessing a peripheral device
- The OS controls that users or the processes started by a user, can only execute those actions, which they are allowed to.

<i>Object</i> <i>User</i>	<i>F1</i>	<i>F2</i>	<i>F3</i>	<i>Device's Periphery</i>
<b>U1</b>	Read		Read	
<b>U2</b>				Print
<b>U3</b>		Read	Execute	
<b>U4</b>	Read Write		Read Write	

# Security of Operating Systems

Operating System	Memory Protection	File Protection	Access Control	Support for Security Modules	Secure I/O	Code Integrity Mgt.
Symbian 9.x	✓	✓	✓	(✓)	x	✓
PalmOS 5.x	x	x	x	(✓)	x	x
Windows CE 6.2 Windows Mobile 6.5	✓	✓	✓	(✓)	x	✓
PocketPC 2003 Phone Edition	x	x	✓	(✓)	x	x
Embedded Linux	✓	(✓)	✓	(✓)	x	x
Android	✓	✓	✓	(✓)	x	x
J2ME	✓	x	x	(✓)	x	✓

(✓) → Feature is available, depending on the available hardware (e.g. availability of a card reader).

## *Lecture 11*

Concepts of Mobile  
Operating Systems

**Mobile Business I (WS 2010/11)**

Prof. Dr. Kai Rannenber

T-Mobile Chair of Mobile Business and Multilateral Security  
Johann Wolfgang Goethe-University Frankfurt a. M.



- Functions
- Processes
  - States and elements

- Virtual Machines



## What is an operating system (OS)?

- An OS is a program that serves as a mediator between the user and the hardware.
- It enables the users to execute programs
- *Other properties:* Multi-user, multi-thread, high availability, real-time, ...

- ***Primary goal of an OS:*** Easy usage of the actual hardware
- ***Secondary goal of an OS:*** Efficient usage of the hardware

- Operating System (OS) features:
  - Memory protection, file protection, access controls
  - Security module support, secure input and output, protection of applications and the system's integrity
  - Resource sharing:
    - Memory (RAM, storage)
    - Central Processing Unit (CPU)
    - Input / Output devices (I/O)



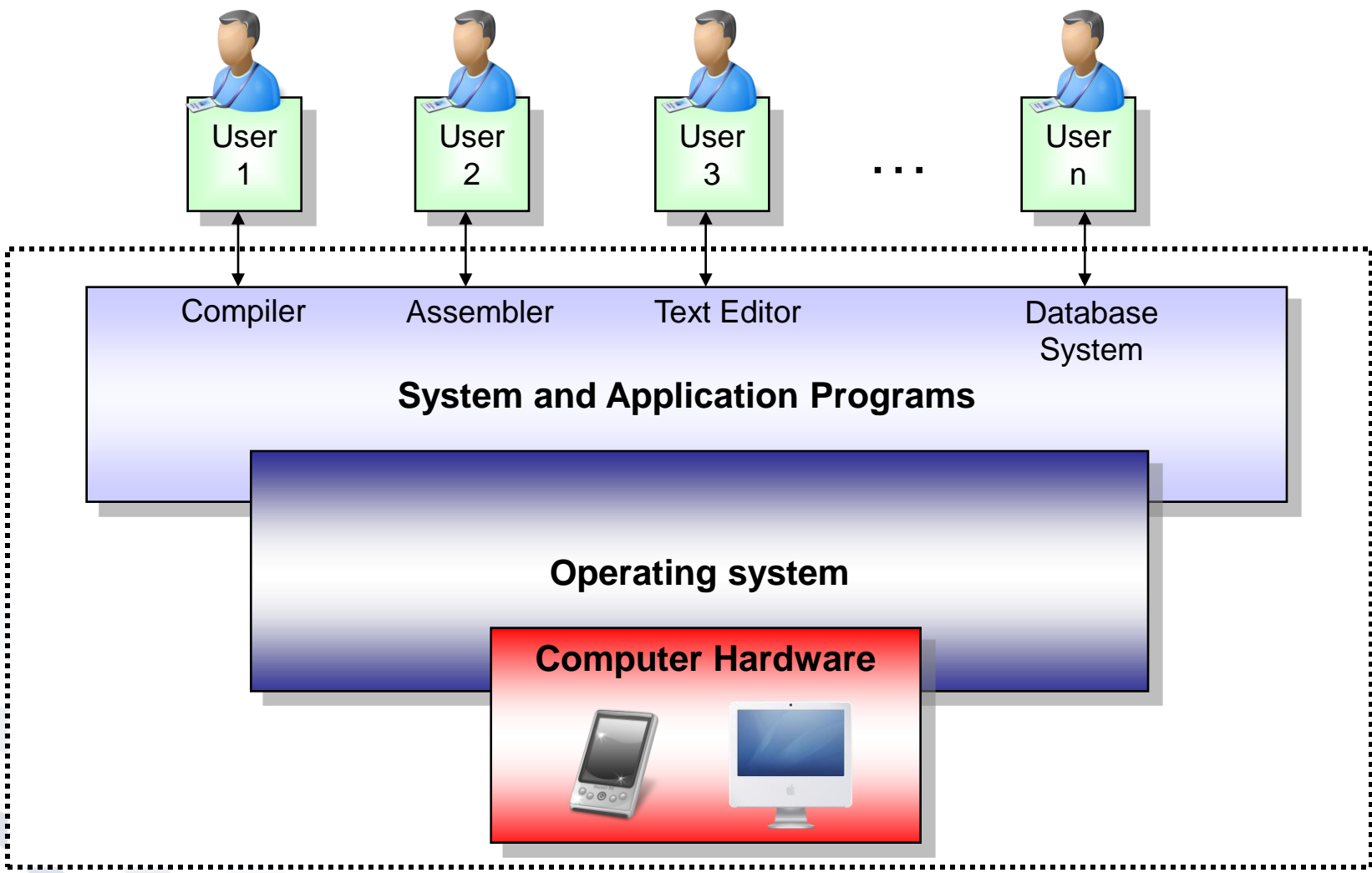
- **Controlling of the resources:**
  - Computation time, real-time processing:  
“Who is computing how much? How long does it take?”
  - Memory (RAM, Disk):  
“Who gets which part of the memory?”



- **Security functions:**
  - Protection of the data (memory, hard disk):  
“Who is allowed to access resources?”
  - Process protection (computation time, code, isolation):  
“Who is allowed to compute?”




- **Communication:**
  - Allocation of I/O-Resources
  - Processing of the communication
  - User interface (UI)



- Functions
- Processes
  - States and elements

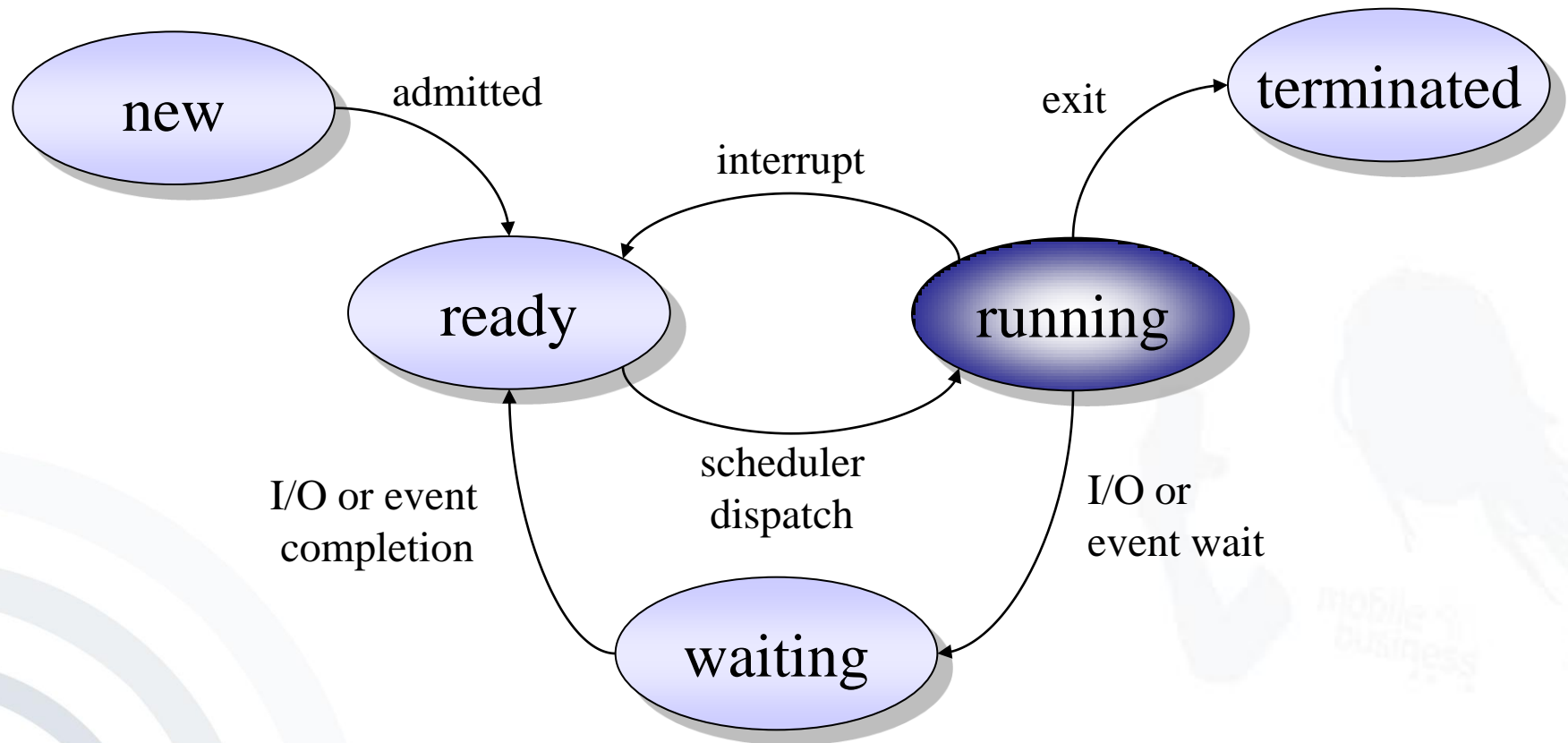
- Virtual Machines

- Several programs (processes) can run simultaneously & concurrently on an OS: 
- *How are processes managed in a system with regard to processing time, memory, etc?*
- *Which process is allowed to access resources when?*
- *How are resources (I/O) shared among processes?*
- *How do processes exchange data among each other?*

- A process is a program “in operation”.
- A process uses resources, such as CPU time, memory, files, and I/O devices.
- The resources of a process are allocated while it is created or when it is running.
- The operating system has to manage the process (creation, resource distribution, etc.).

- More than simple code!
- Program counter: Indicates on which point in the code the process resides.
- Contents of the process registers:
  - **Stack**: Contains temporary data, such as subroutine parameters or return addresses, etc.
  - **Data section**: Contains the global variables
  - **Heap**: Dynamically allocated memory

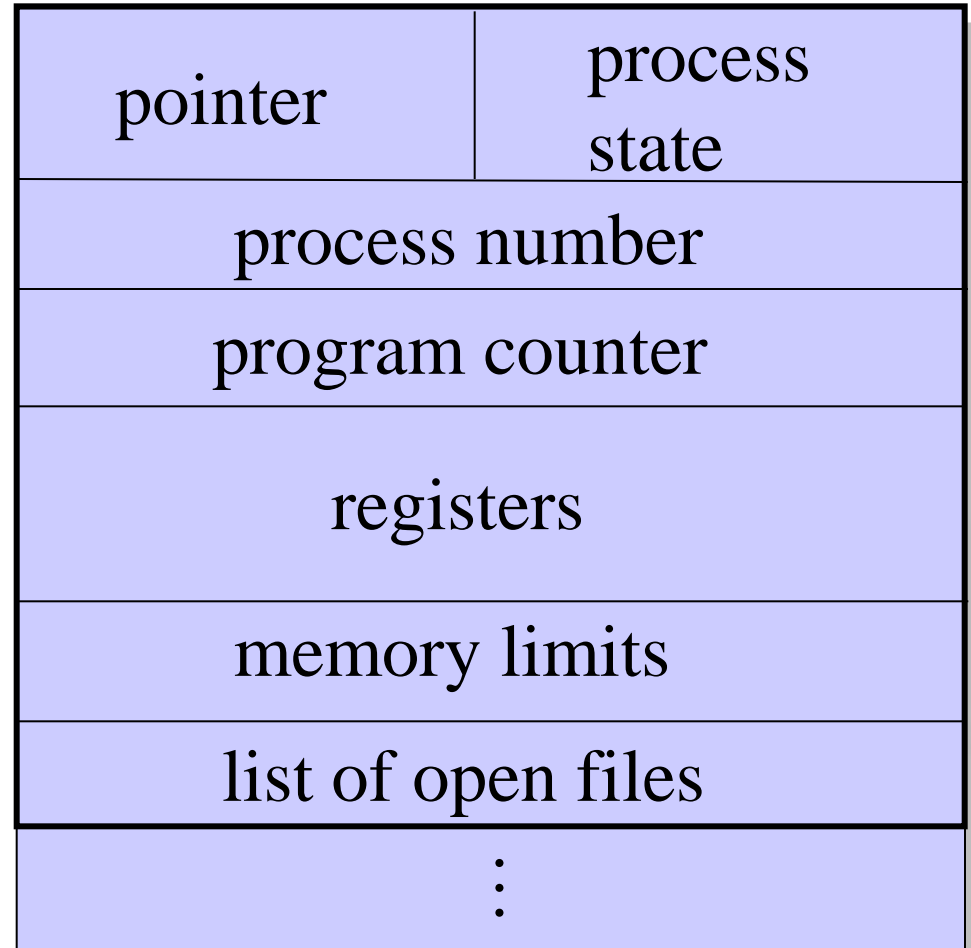
# States of a Process



- **New:** Process is created.
- **Ready:** Process is waiting for being executed.
- **Running:** Process is running.
- **Waiting:** Process is waiting for results:
  - Completion of an I/O-operation
  - An event
- **Terminated:** Process is terminated.

## Abstracted View on a Process: Process Control Block (PCB)

- Abstracted representation of the contents of a process control block (PCB), needed by an operating system.



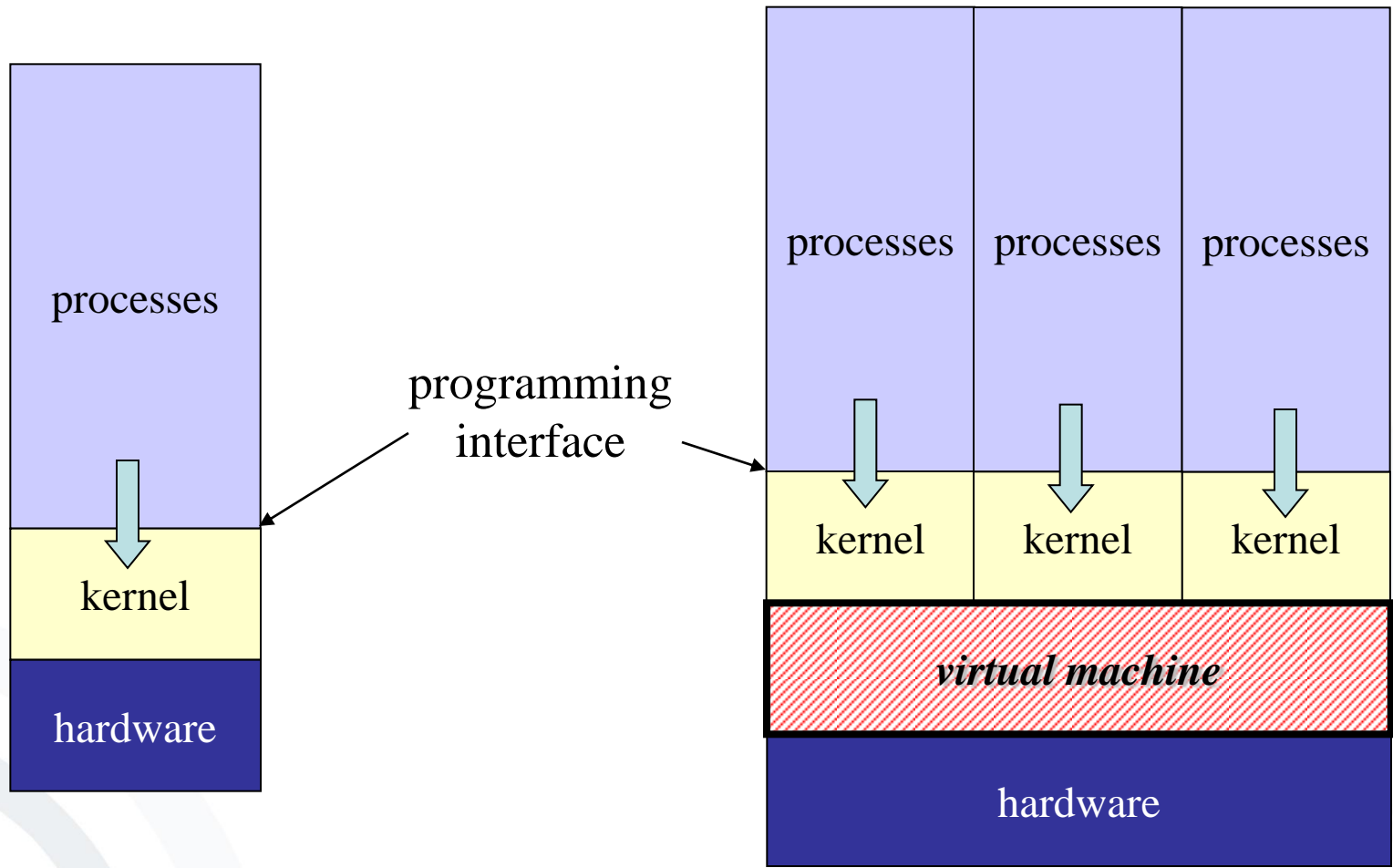
- **Process State:** *new, ready, running, waiting, ...*
- **Program Counter:** Address of the next command to be executed
- **CPU Registers:** Accumulator, Index Register, Stack Pointer and general registers
- **Information for:**
  - CPU-Scheduling
  - Memory-Management
  - Accounting
  - I/O Status

- Functions
- Processes
  - States and elements

- Virtual Machines

- Intermediate layer between an operating system and a software application.
- The system creates the impression that every process has its own machine, having a separate CPU and its own memory.
- Protection of the resources (sandboxing)
- Complete isolation between the different virtual machines running on the host system.
- **Examples:**
  - Java Virtual Machine
  - VMWare
  - Virtual PC 2004
  - IBM z/VM
  - Emulators (e.g. ScummVM or PocketPC Emulator  
➔ exercise course)

# Virtual Machines



[SilberGalvin1999]