mobile business

Exercise 3

Technology Basics II

Mobile Business I (WS 2017/18)

Peter Hamm, M.Sc.

Deutsche Telekom Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.

Literature

- This set of slides is based upon the following lectures:
  - ***Lecture 8:*** Smart cards and Related Application Infrastructures
  - ***Lecture 9:*** Mobile Devices
  - ***Lecture 10:*** Concepts of Mobile Operating Systems
  - ***Lecture 11:*** Market Overview of Mobile Operating Systems and Security Aspects

mobile business

Exercise 1: Smartcards

a) What are smart cards and what components do they consist of (=what do they contain)?

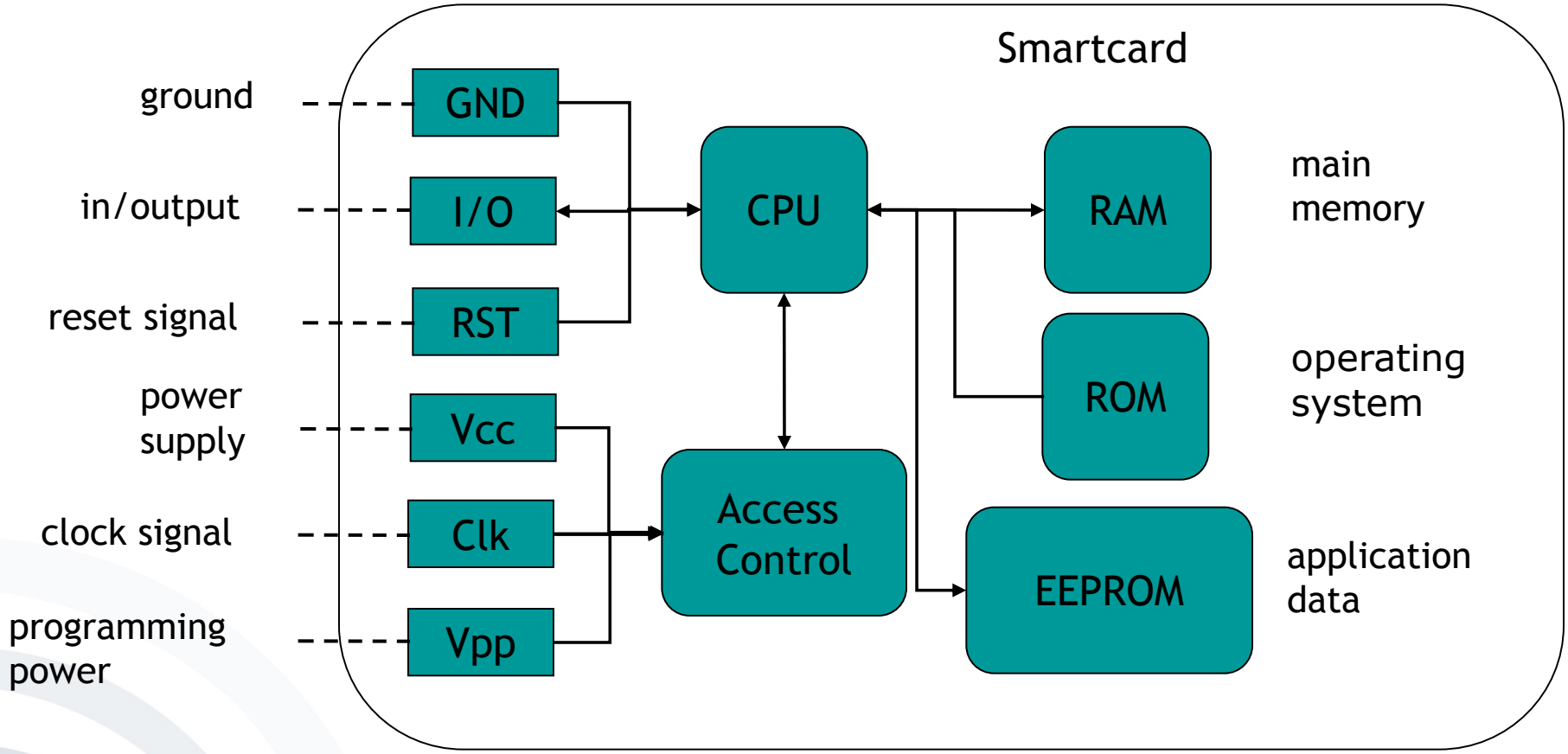
1

Smartcards

- 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.

1a

Smartcards



1a

[Source: SecCommerce2002]

Exercise 1: Smartcards

b) Why are they used and what role do smartcards play with respect to
(i) security
(ii) applications?

1

Smartcards

- 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)

mobile business

Smartcards – Examples

1b

Why Smartcards?

Protection needed against:

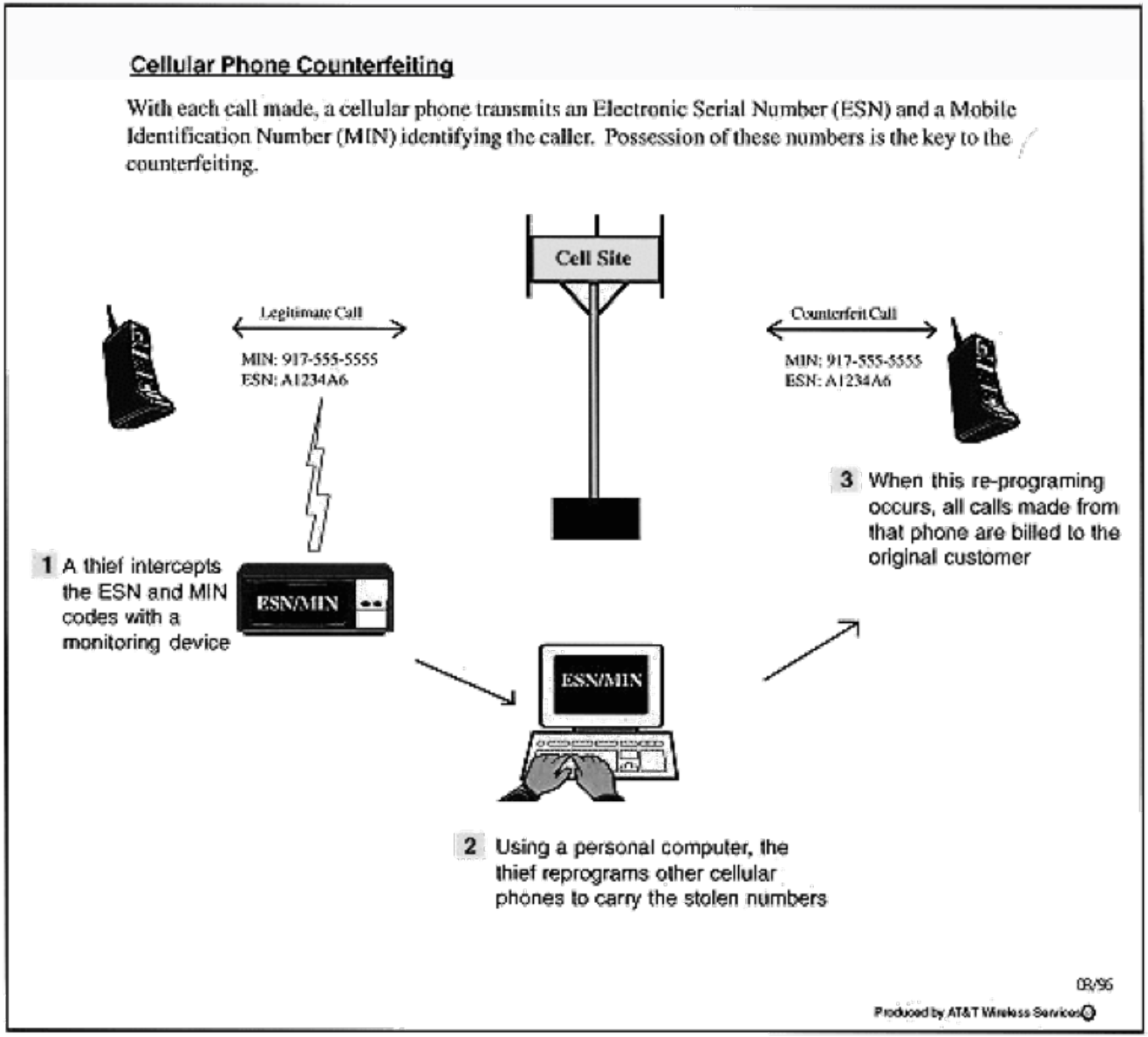
- Unauthorised usage of services through forged user data
- Duplication of a user's credentials
- „Cracking" of credentials
- Billing fraud

1b

CELLULAR COUNTERFEITING/CLONING FRAUD

Example for faulty system design (CDMA)

Duplication of intercepted user IDs



1b

Exercise 2: Subscriber Identity Module (SIM)

a) Name the most important function of the Subscriber Identity Module (SIM) in GSM and UMTS networks.

2

Smartcards for Mobile Communication

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 encryption key $\mathbf{K_i}$ provided by the mobile operator

Reliably execute computational functions for the mobile device

2a

cf. [EffingRankl2008]

The Subscriber Identity Module (SIM)

- In GSM and UMTS since 1991, upcoming for WLAN
- **Represents** contract **between subscriber & network operator**
- Authenticates and authorizes **a "phone"** to **use** the network by linking it to a **subscription (authentication)**
- More and more called "Subscriber **Identification** Module" to reflect progress in the general field of **Identity Management (identification)**

2a

Exercise 4: Subscriber Identity Module (SIM)

b) What does the Subscriber Identity Module contain? Which of these contents are protected, which are not and why?

2

SIM Card Content (Extract)

- Protected data:
  - IMSI, PIN, PUK
  - A3, A8 crypto algorithms for signing and encryption
  - 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)

2b

Exercise 2: Subscriber Identity Module (SIM)

c) Name other functionalities of the Subscriber Identity Module.

2

SIM: Functionality

- 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.

2c

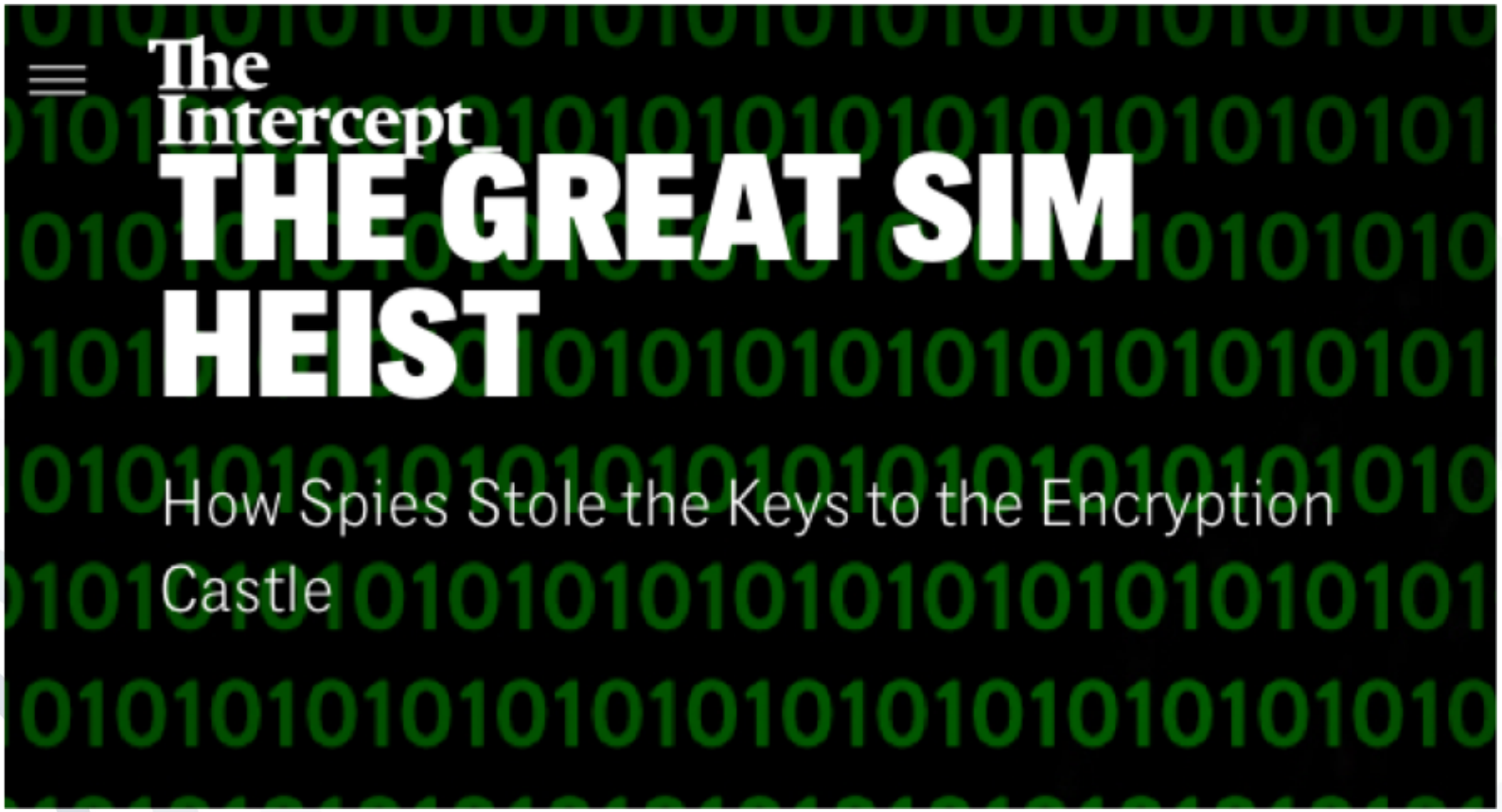
Smartcards for Mobile Communication

- **SIM**s 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

2c

cf. [EffingRankl2002]

- **Have you heard about the Gemalto SIM card hack?**



A the internal computer network of the largest manufacturer of SIM cards in the world, stealing encryption keys used to protect the privacy of cellphone communications across the globe, according to top-secret documents provided to *The Intercept* by National Security Agency whistleblower Edward Snowden.

The hack was perpetrated by a joint unit consisting of operatives from the NSA and its British counterpart Government Communications Headquarters, or GCHQ. The breach, detailed in a secret 2010 GCHQ document, gave the surveillance agencies the potential to secretly monitor a large portion of the world's cellular communications, including both voice and data.

The company targeted by the intelligence agencies, Gemalto, is a multinational firm incorporated in the Netherlands that makes the chips used in mobile phones and next-generation credit cards. Among its clients are AT&T, T-Mobile, Verizon, Sprint and some 450 wireless network

https://theintercept.com/2015/02/19/great-sim-heist/

Exercise 2: Subscriber Identity Module (SIM)

d) What is SIM Application Toolkit?
   (i) What does it do?
   (ii) Name application examples for SIM Application Toolkit.

2

SIM: Integration into Mobile Phones

- **ETSI GSM 11.11** [GSM2006] standard - 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“ (STK) allows for implementing **additional applications** on a SIM.

2d

SIM Application Toolkit – SAT

- 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“

2d

SAT – Application Examples

- **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

2d

Exercise 2e: Secure Element

e) Describe the role and functionality of the UICC as a secure element.

mobile business

Exercise 2e: Secure Element

- In today's smartphones, a Secure Element can be found as a chip embedded directly into the phone's hardware, or in a SIM/UICC card provided by your network operator.
- It provides secure storage and execution environment.
  - Important functionality for e.g. secure mobile payment
  - Can provide software to "emulate" a normal bank card to process payment information

2e

Exercise 3: Universal SIM/USIM

a) What is a USIM?

3

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

3a

Exercise 3: Universal SIM/USIM

b) Name the innovations introduced with the USIM.

3

USIM – Visions of new Opportunities

- Tiny computer - several mini applications
- A 3G (UMTS) handset equipped with a USIM card can be used to make video calls, assuming the calling area is covered by a 3G network
- Better security (new encryption algorithm) for calls, data, and storage
- Larger, richer phonebook
  - thousands of contacts instead of a maximum of 255 in a SIM
  - can contain email addresses, a second or third phone number, etc;

3b

Exercise 3: Universal SIM/USIM

c) What is a UICC and how do USIMs relate to a UICC?

3

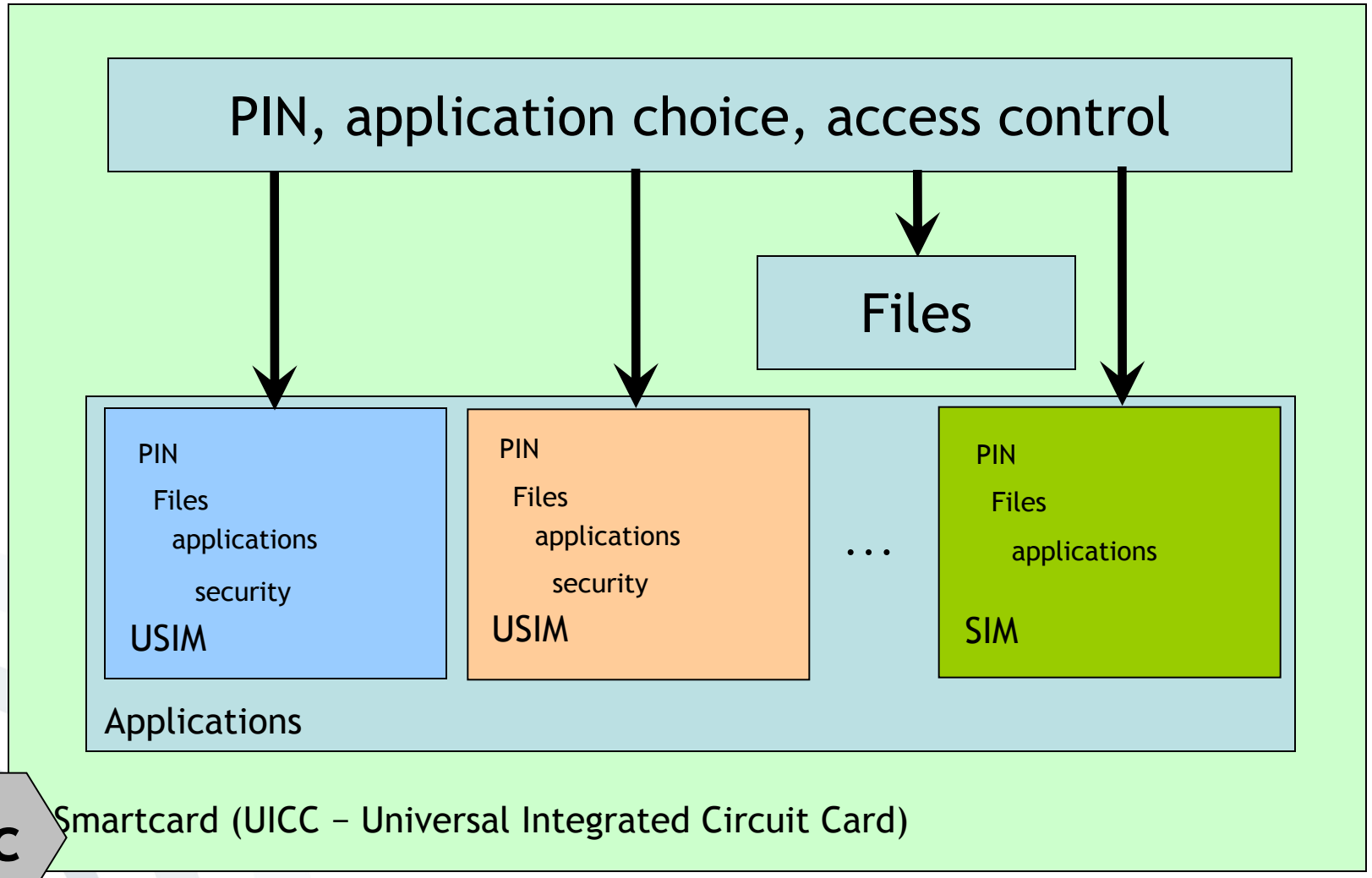
Exercise 3: Universal SIM/USIM

c) What is a UICC and how do USIMs relate to a UICC?

- The Universal Integrated Circuit Card (UICC) is the smart card used in mobile terminals in GSM and UMTS networks.
- In a GSM network, the UICC contains a SIM application and in a UMTS network it is the USIM application.

3

USIM on UICC – Structure



3c

Exercise 3: Universal SIM/USIM

d) Describe market opportunities and effects of competing USIMs.

3

USIM – Innovations

- **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

3d

USIM – Visions of new Opportunities

Market entry of USIM „disguised“ **as SIM**

➲ UMTS activated by operator

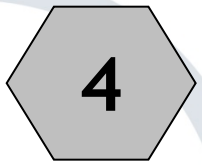
Multiple USIMs – possibly **from competing providers** – can technically coexist on one card. Selection via menu on mobile device

➲ Reduction of operator switching cost

Switching to anonymous prepaid USIM as a privacy option when using privacy sensitive services?

Exercise 4: Mobile Devices

a) How can mobile devices be categorized?
   (i) Technical characteristics
   (ii) Application Aspects



- 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

4a

Categorisation of Mobile Devices

Technical Characteristics

- 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

4a

Categorisation of Mobile Devices

Application Aspects 1

- 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

4a

Categorisation of Mobile Devices

Application Aspects 2

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

4a

Use Cases

- Different requirements for different kinds of devices:

	Mobile Phone	Tablet	Laptop
Number of „Switch-ons“ per day	low	low	variable
Frequency of use cases	very high	rather low	low
Duration of usage per task	?	short/ medium	high

Based on [Burckhardt2001]

4a

Exercise 4: Mobile Devices

b) Name four components of mobile devices. Which two of these components do considerably determine the size of a mobile terminal?

4

Components
Mobile Devices

- Main physical components of Mobile Devices
  - Accumulators
  - Processors, Memory, and Storage
  - Display
  - Means for I/O

Size of a mobile Device

- The size of a mobile terminal is considerably determined by its:
  - Input Facilities (e.g. keyboard)
  - Output Facilities (e.g. display)

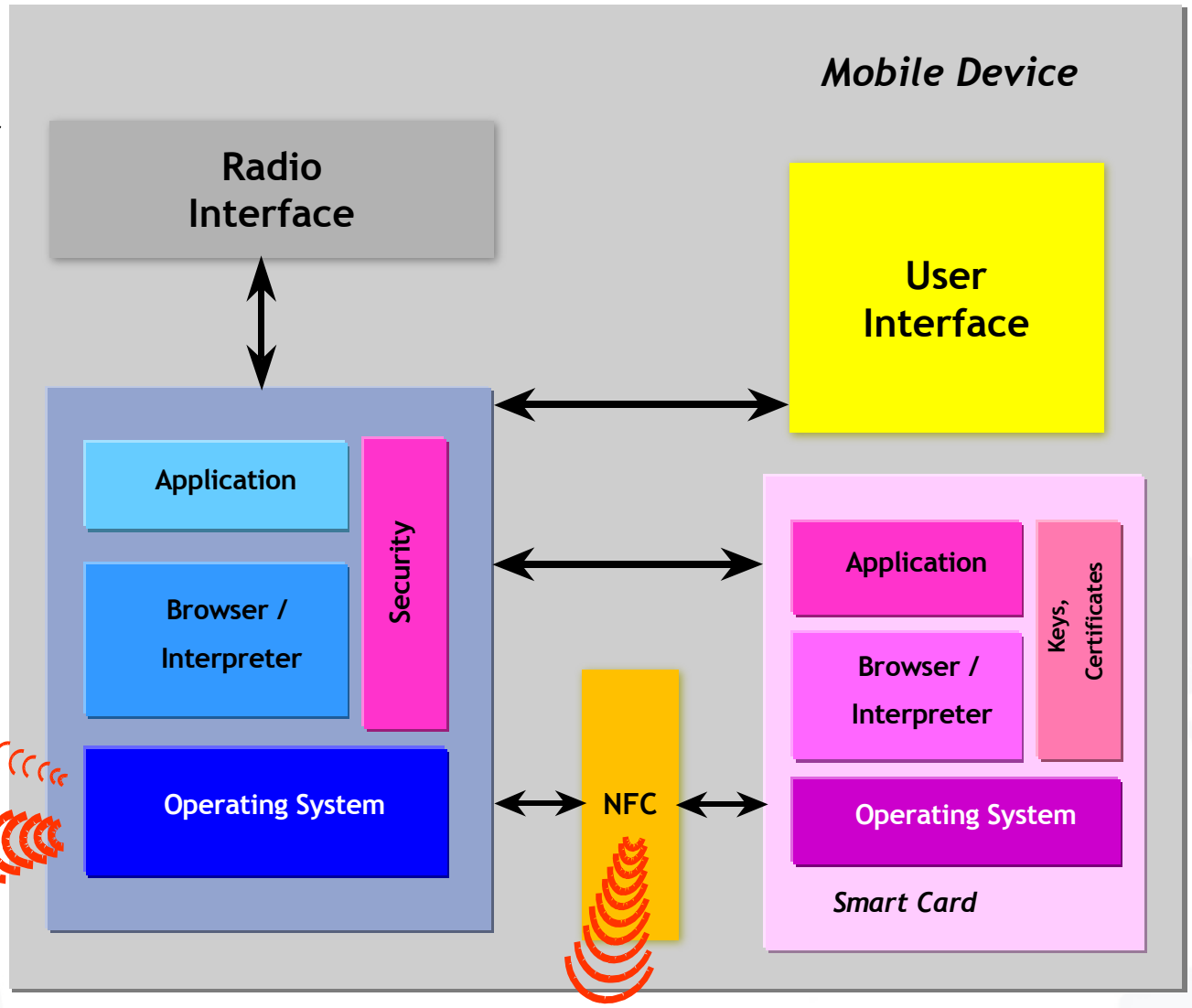
➲ Separation of components (e.g. display in the watch, head-mounted-displays)

Exercise 4: Mobile Devices

c) Describe the functional architecture of a mobile device.

4

OS – Functional Architecture



Based on [Posegga2001]

Exercise 5: Personal Area Networks (PAN)

a) Personal Area Networks (PAN) – what are they good for, what do they do?

5

Personal Area Network (PAN)

- Personal environment, short range
- ***Purpose***: Connection of devices in short range, for example mobile device and printer.
- Replaces cable-connections:
  - **I**nfra**r**ed **D**ata **A**ssociation (IrDA)
  - Bluetooth
  - Near Field Communication (NFC)

5a

Exercise 5: Personal Area Networks (PAN)

b) Please do briefly describe the related technologies IRDA and Bluetooth. Name the advantages and disadvantages of both IRDA and Bluetooth.

5

Personal Area Network (PAN)
Infrared

- IrDA: Infrared Data Association (1993):
- Standardized infrared-protocols
- Asynchronous, serial connections up to 115 kbit/s (Serial Infrared) or 4 Mbit/s (Fast Infrared)
- Point-to-Point
- Protocol-family for various purposes

- Exemplary applications:
  - Transmission of mobile business cards
  - Sales data extraction from cigarette vending machines
  - Connection between mobile and laptop
  - Wireless printing
  - Remote control for consumer electronics, e.g. TVs

5b

Personal Area Network (PAN)

Infrared-Transmission

- Attributes:
  - Wireless
  - Range of up to 10 meters
  - Illumination-angle 15° -30°
- 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.

5b

Personal Area Network (PAN)

Bluetooth

- 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
- v4.2 (2014) improved speed, privacy, and connectivity (support for the Internet of Things)
- Broadly supported by related industries:
  - Computer hardware
  - Software
  - Consumer electronics
  - …

5b

Bluetooth™

Personal Area Network (PAN)

Popular Bluetooth Applications

Sound transmission
(to earphones, headphones
or Hi-Fi equipment)

Wireless communications between devices
(Bluetooth-Headset)

5b

Personal Area Network (PAN)

Bluetooth Applications

- Connection of periphery-devices (headsets, keyboards, mice, etc.)
- Setting up of ad-hoc networks for spontaneous data exchange
- Applications similar to those 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

5b

a) What are the advantages and disadvantages of mobile operating systems unavailable to other device manufacturers?

6

Mobile OS unavailable to other device manufacturers

- Originally, most mobile phone manufacturers used their own “closed” operating systems for their mobile devices.
- Later, more and more platforms switched to more open and interoperable operating systems (e.g. Windows CE, Symbian OS, Android).
- 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***: Interoperability - Less flexible, as 3rd-party software cannot be easily installed and executed

b) Name two mobile operating systems unavailable to other device manufacturers and two manufacturer-independent mobile operating systems.

6

Mobile OS unavailable to other device manufacturers

- Palm OS (Garnet OS)
  - Latest release: Most devices equipped with Palm OS 5.4
- Apple iOS (Unix-based)
  - Latest release: iOS 8
- BlackBerry OS
  - Latest release: BlackBerry OS 10.3
- Nokia Series 40, Asha
  - Latest release: Asha 1.4
- Samsung bada
  - Latest release: 2.0

6b

Manufacturer-independent mobile OS

- Linux: LiMo (Linux Mobile), Openmoko Linux, Qt Extended (Qtopia) 
- Symbian platform
  - Latest release: “Nokia Belle Feature Pack 2“ for Symbian^3 devices
- Android (by Open Handset Alliance) 
  - Latest release: 5.0 (Lollipop)
- Windows Mobile
  - Latest release: Windows Mobile 6.5.5
- Windows Phone
  - Latest release: Windows Phone 8.1
- Maemo (by Nokia) → MeeGo (by Nokia, Intel) → Sailfish OS (by Jolla) 
  - Latest release: Sailfish OS v1.1.0.39 (October 2014)
- Tizen (by Samsung, Intel, Linux Foundation) 
  - Latest release: 2.3 (November 2014)
- Firefox OS (by non-profit organisation Mozilla) 
  - Latest release: 1.4 (August 2014)
- China-Focused Mobile OS
  - Currently under development by Taiwan-based HTC

[WSJ2013]

 = Linux-based

c) When mobile operating systems allow the execution of 3rd-party software, what are the threats resulting from this for the user?

6

Current Threats from Malware on Mobile OS

- Many mobile operating systems allow the execution of 3rd-party software:
  - Malware can 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)

6c

Beginnings of Mobile Malware

- ***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
- …

Strong growth of Mobile Malware

- The number of malware programs masquerading as legitimate mobile apps grew by more than 600 percent in 2012
- Most popular target: Android

[ATD2013]

6c

mobile business

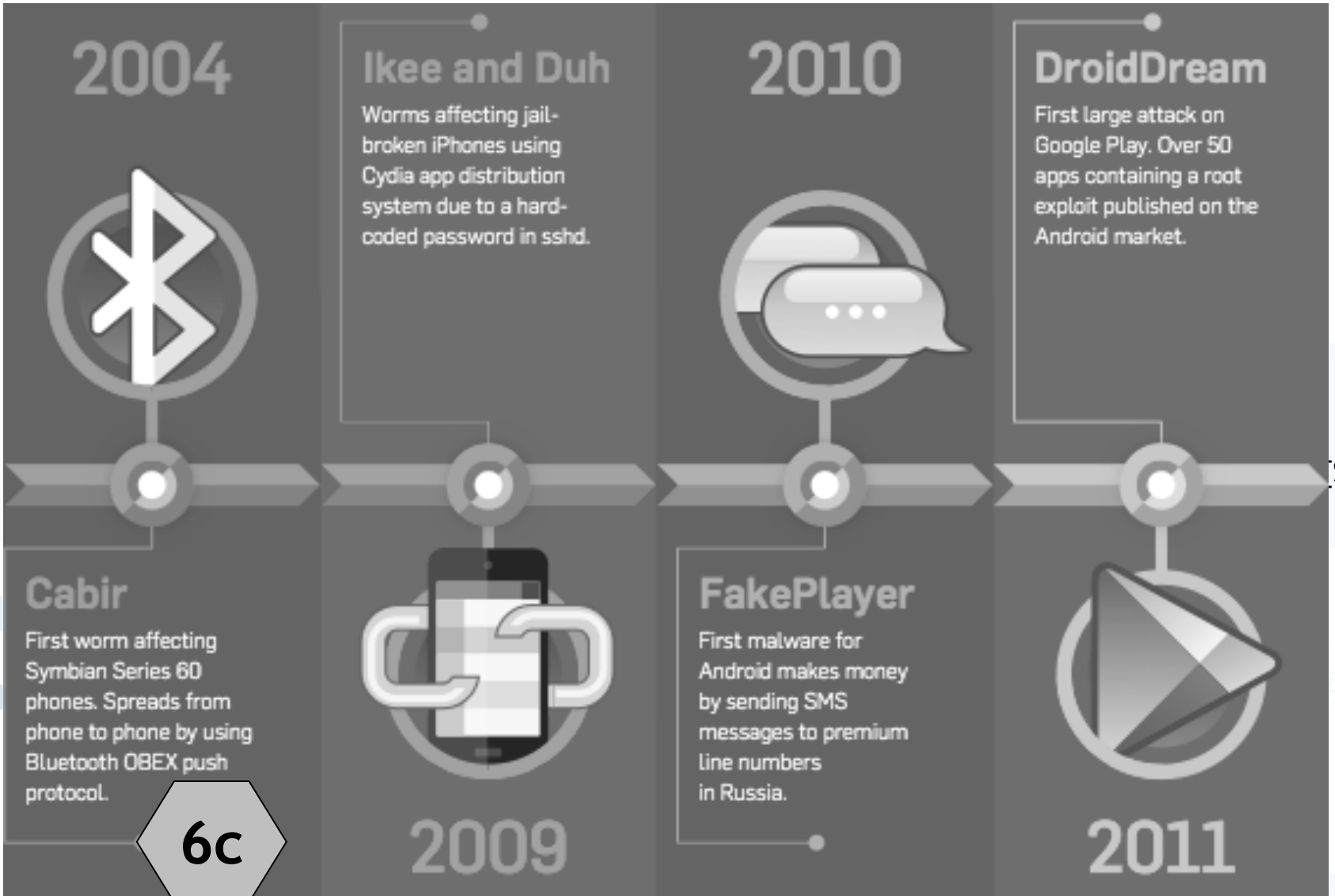
Timeline PDA/Mobile Threats 2004-2015

6c

[Sophos2015]

mobile business

Timeline PDA/Mobile Threats 2004-2011



[Sophos2015]

6c

mobile business

Timeline PDA/Mobile Threats 2011-2015

[Sophos2015]

d) What are the security precautions and countermeasures available in mobile operating systems?

6

Security Precautions and Countermeasures

- 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 the are started by e.g.
  - Checking certificates
  - Proof Carrying Code
- Additional Security Software may be needed, e.g.
  - Virus scanners
  - Firewalls

6d

Security of Mobile Operating Systems

Security measures	Apple iOS	Google Android	BlackBerry	Windows Phone
Access-control options	PIN, passcode, fingerprint	PIN, passcode, swipe, FaceLock	PIN, smartcard	PIN, passcode
MDM-configurable PIN/passcode policy	Yes	Yes	Yes	Yes
Full-device encryption	iPhone 3GS+ every iPad	Selected tablets (Android 3+) Selected phones (Android 4+)	All BlackBerry phones	Windows Mobile 6.5 Windows Phone 8
SD card encryption	No SD cards	OEM proprietary	Yes	No
Remote wipe	Removes encryption keys	Resets to factory defaults	Removes encryption keys Optionally scrubs memory	Varies by OEM/OS version

6d

[SM14]

Exercise 7: Concepts of Mobile Operating Systems

a) What is an OS and what are its main goals?

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

7a

[SilberGalvin1999]

Exercise 7:
Concepts of Mobile Operating Systems

b) Name three functions of the operating system and state two examples (exemplifications) for each of these functions.

7

OS Functions

- Controlling and sharing of 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?”
  - Security module support

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

c) What is a process? What does it do, what does it use and how is the mobile operating system involved?

Process

- 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.).

Components of a Process

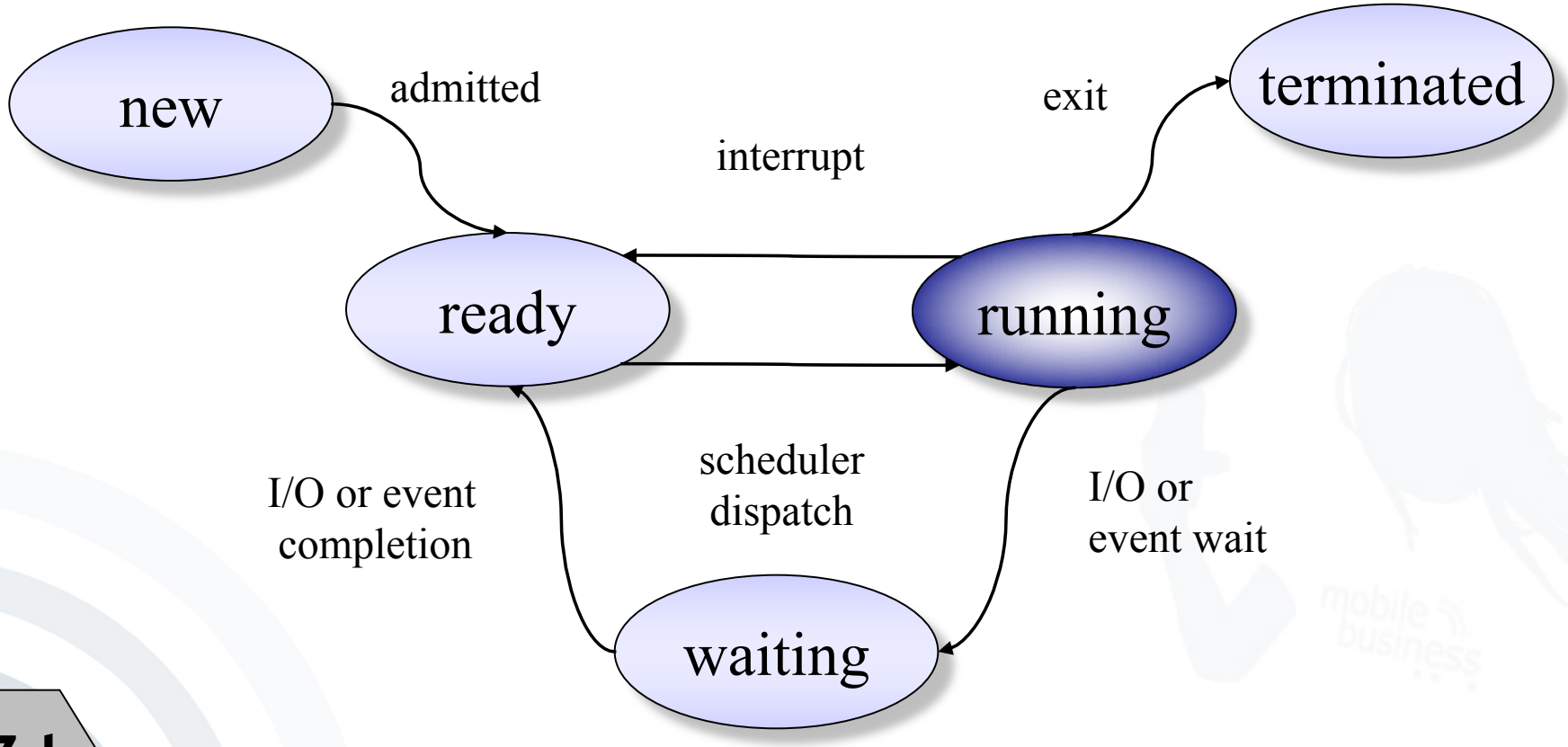
- More than simple code!
- Program counter: Indicates on which point in the code the process resides.
- Contents of the process registers:
  - ***Stack:*** Contains temporary data, such as subroutine parameters or return addresses, etc.
  - ***Data section:*** Contains the global variables
  - ***Heap:***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

Exercise 7: Concepts of Mobile Operating Systems

d) Which are the states of a process?

7

States of a Process



7d

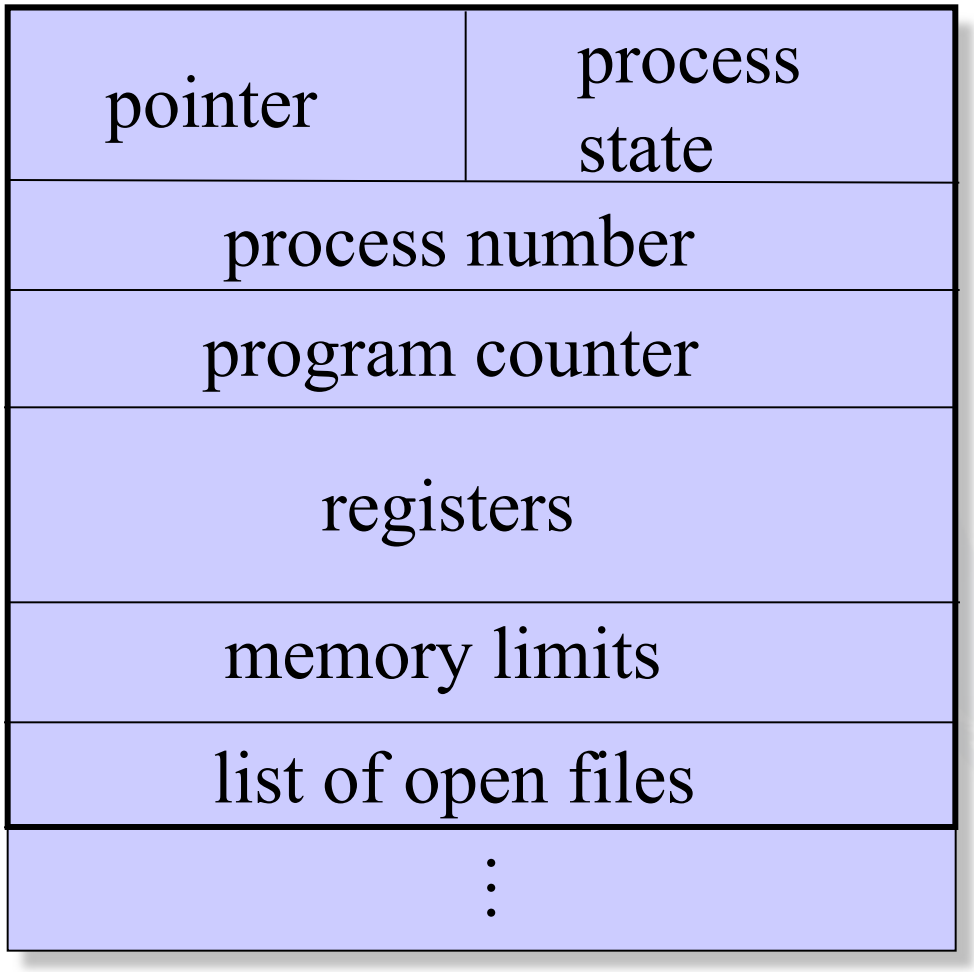
[SilberGalvin1999]

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.



[SilberGalvin1999]

7d

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

- **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

7d

Literature

- This set of slides is based upon the following lectures:
  - ***Lecture 8:*** Smartcards and Related Application Infrastructures
  - ***Lecture 9:*** Mobile Devices
  - ***Lecture 10:*** Concepts of Mobile Operating Systems
  - ***Lecture 11:*** Market Overview of Mobile Operating Systems and Security Aspects

Thank you!

Contact: mob1@m-chair.de