Security of embedded Systems

Peter Langendörfer

telefon: 0335 5625 350
fax: 0335 5625 671

e-mail: langendoerfer [at] ihp-microelectronics.com
web: http://www.tu-cottbus.de/fakultaet1/de/sicherheit-in-pervasiven-systemen/

Organizational issues

Dates for written exam:

- 22.02.: 12.30 – 13.00 Uhr: ZHG/SR 2
- or

Type of questions

- Forget about „What is written on slide 36 in part 4“
- Questions will be of the following style:
  - Why do I need MMUs
  - What are limitations of MMUs
  - How can I prevent buffer overflows
  - Name 3 approaches to improve securrity of embeded systems and explain one in detail including pros and cons
- How to prepare
  - Meet in small groups and excersie to talk about the topic
  - Play Q&A
  - Think about what could the silly guy ask when preparing examples follow

Introduction: Design Principles

Core Principle that guarantee design/building of a secure system

- ***Small interface***
- ***Access-control contracts***
- ***Tunneling***
- ***Secure booting***
- ***Effective resource control***

Questions to ask:

- Which of the techniques explained can be used to implement/realize the feature (may be more than one)
- What are pros/cons
- How to circumvent the technique

Introduction: Design Principles

Core Principle that guarantee design/building of a secure system

- ***Small interface*** approach can be built by using two alternative approaches:
  - The µ-kernel approach separates the system in small pieces,
  - extensible systems use safe languages or transaction-like mechanisms

- ***Access-control contracts*** an object or a group of objects declare their needs and the specific functions that they provide
  - role-based access control (RBAC).

Introduction: Design Principles

Core Principle that guarantee design/building of a secure system

- ***Tunneling*** adding a required property to a software component by using an additional layer.
  - This may include an insecure communication channel that is used to transfer data. Hence, the provided security level of the software component that implements the additional layer can be ignored.

- ***Effective resource control*** providing an effective defense against denial-of-service attacks
  - Becoming key in the field of embedded system

Introduction: Design Principles

Core Principle that guarantee design/building of a secure system

- ***Virtual machines*** provide a high level separation of software components by an emulation of a hardware architecture.
  - the costs of emulating the hardware architecture are an issue
  - Currently considered to be acceptable for powerful devices only
- ***Separation of mechanisms and policies*** is important
  - Mechanisms are a collection of functions and facilities that are necessary to enforce policies.
  - system designer is in control of complex decisions and operations
- Here we consider ***protection*** as a mechanism to ensure the integrity of an operation implemented in a device
- The know how ***how to build a secure system***
  - Is well-established in traditional OSs.
  - these technologies are more or less applicable for embedded systems as well, or need to be properly adapted.

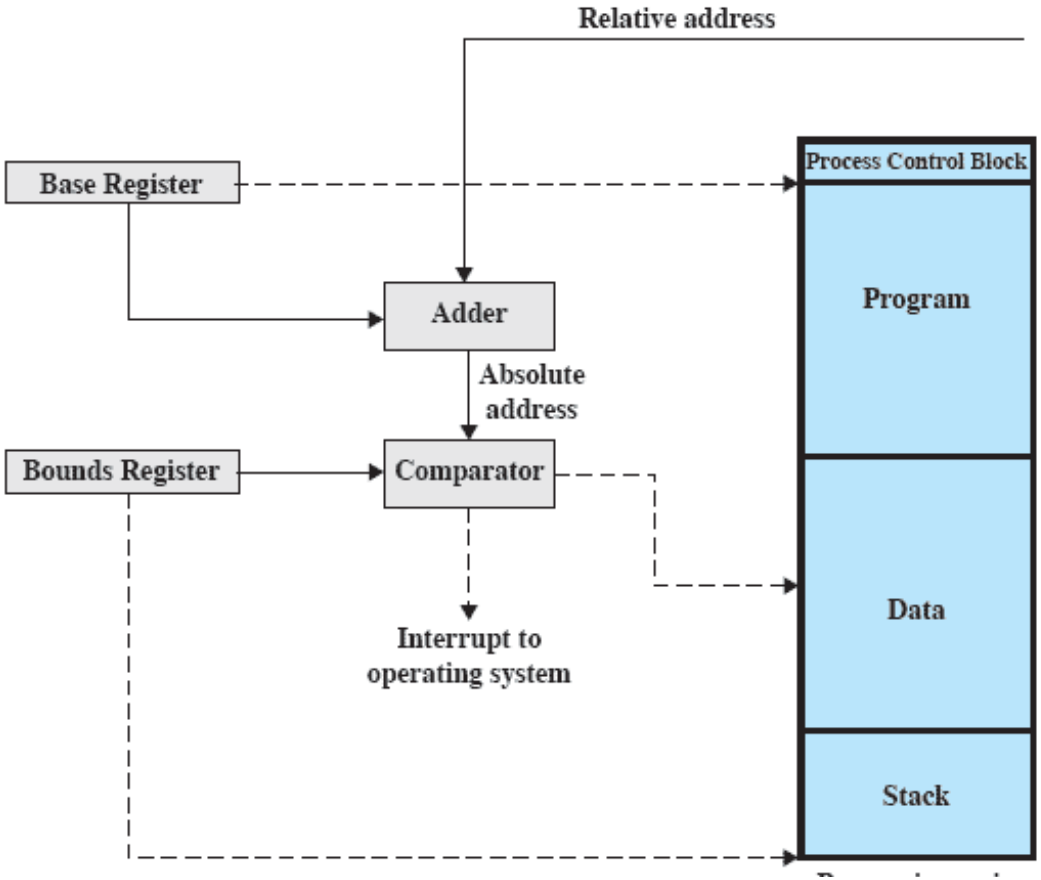
Other Protection Means

What can be done in case proper design was not successful

- Code integrity/attestation
- Verification of system behaviour
- Modification of the hardware

Questions to ask:
- What are pros/cons
- How to circumvent the technique

Relocation



Questions to ask:

- Explain how and why relocation can be used to improve the security of a system
- Compare it with similar approaches

Access Matrix

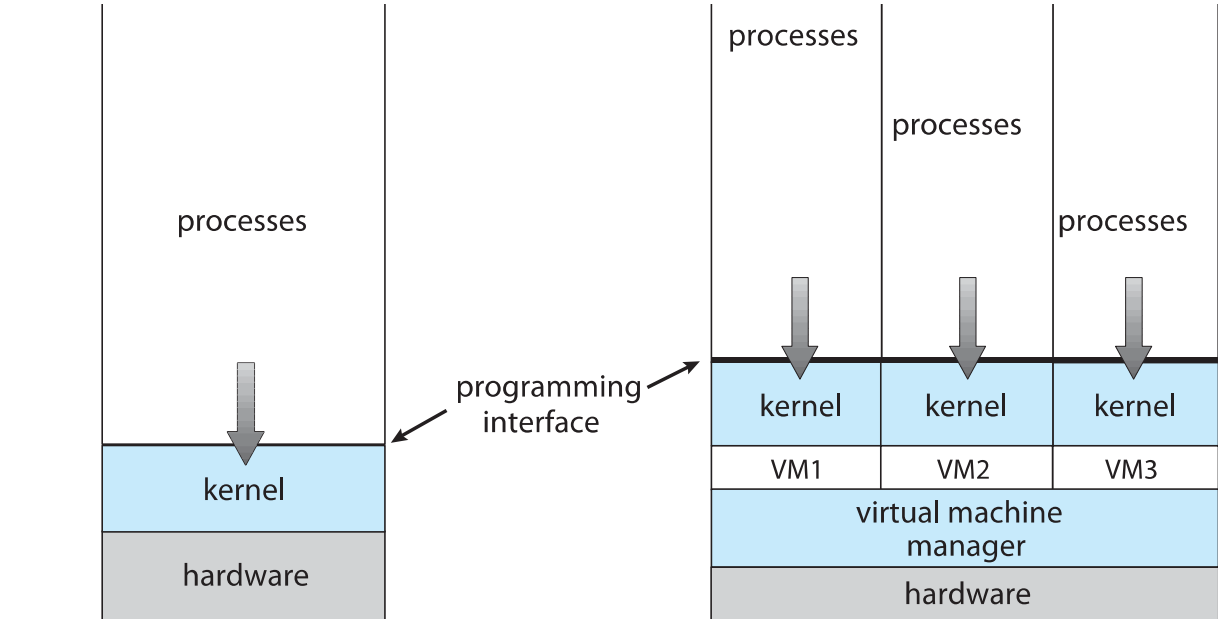
- View protection as a matrix (**access matrix**)

Questions to ask:

- Who may update the matrix and why
- What are limitations of the accwss matrix

object / domain	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	

System Models



Non-virtual machine

Virtual machine

Questions to ask:

- What type(s) of protection can be realized using VMM
- Why aren‘t they standard in embedded systems