Physikalisch-Technische Bundesanstalt
Braunschweig and Berlin
National Metrology Institute

Different Operating Systems, different securing Methods

Experience report

Patrick Scholz, 8.52

Overview

- I would like to show you how to make your operating system **Windows** or **Linux** more **secure** in the **legal metrology** with relatively simple and already existing **mechanism**.

- For this purpose, we dealt with the **tools** and **mechanisms** of these **operating systems** in department 8.5 and came up with **solutions** and **possibilities** that I now want to give you.

- These have already been **published** and presented at **conferences**:
  - **IMEKO** (6-7 June 2017): „**Security Concepts for Software in Measuring Instruments**“
  - **SPI** (7-10 May 2017): „**Software Security Frameworks and Rules for Measuring Instruments under Legal Control**“

Introduction

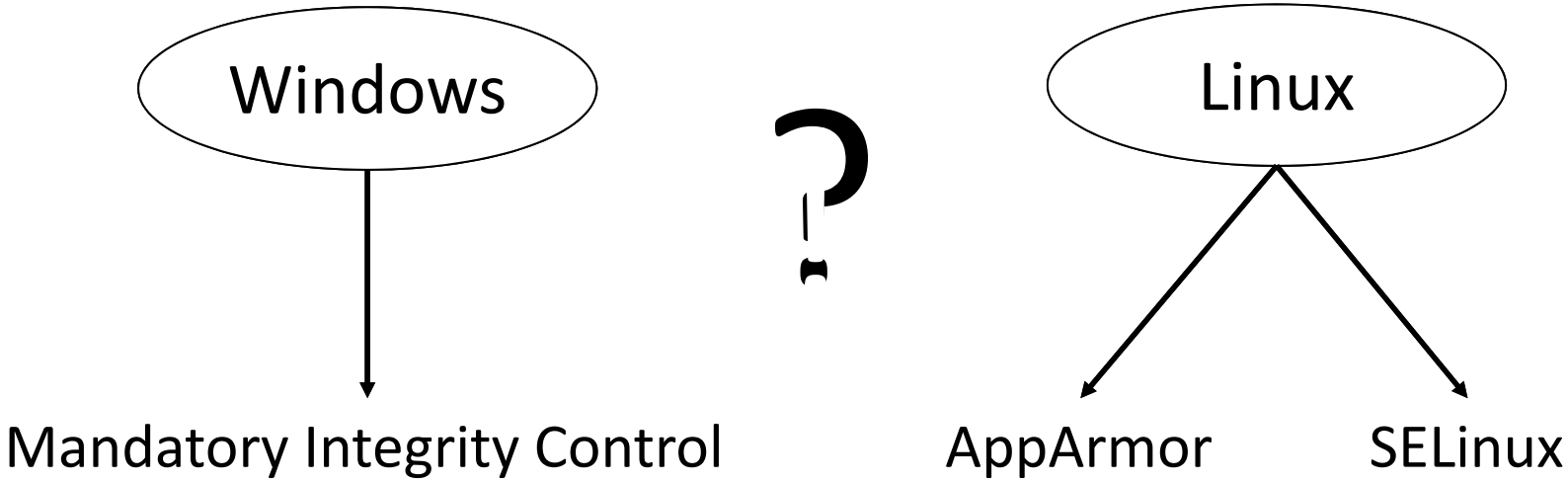
- In **legal metrology**, there are **three general objectives** with regard to the IT security of measuring devices:
  - **data confidentially**
  - **data integrity**
  - **system availability**

[1]

- Current measuring devices have more and more functionalities and use **General Purpose Operating Systems**, such as **Windows** or **Linux**, which have **several million source lines of code**.

- Studies have shown that on average, a **software error** is to be applied to approximately **2300 source lines of code** [2].

How to secure?



I will show you how

Windows – What´s MIC?

- **Windows** and **Linux** use **Discretionary Access Control** (**DAC**), according to which **access rights** are determined by the identity of a subject (for example a user).

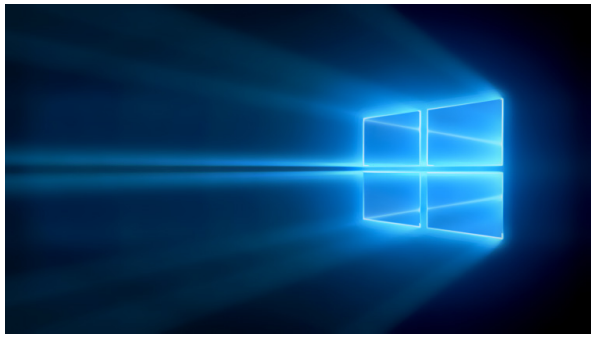
- **Windows** has also been using a so-called **Mandatory Integrity Control** (**MIC**) since Vista, a **Mandatory Access Control** (**MAC**), which is superior to the DAC.

- MIC uses **Integrity Level** (**IL**) and Mandatory Policies (a system-wide **No-Up Policy**):

Integrity Level	Security-ID
untrusted	S-1-16-0
low	S-1-16-4096
medium	S-1-16-8192
high	S-1-16-12288
system	S-1-16-16384

Policy:

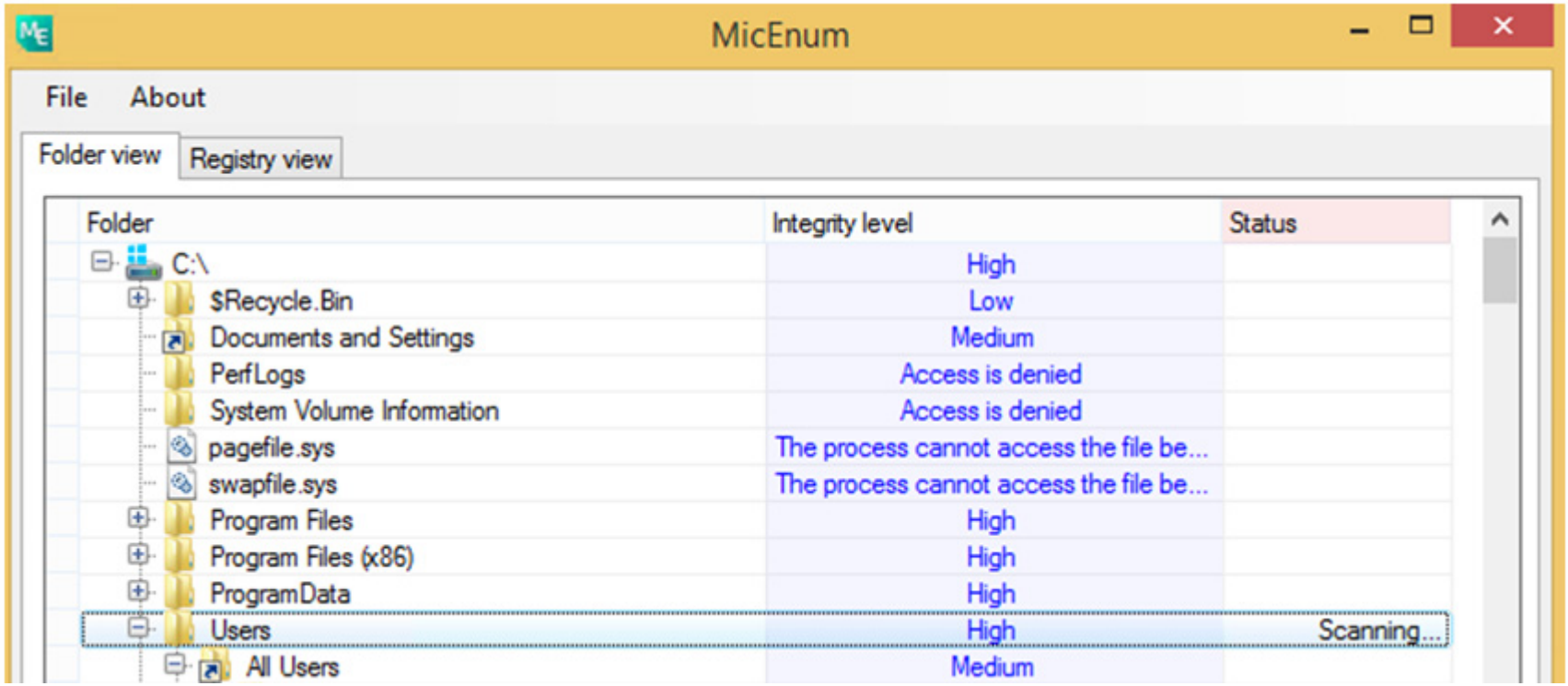
- **No Write Up**
- **No Read Up**
- **No Execute Up**



[3]

Windows – How to use MIC?

- To display the **IL of objects**, it takes an additional **tool**, for example, "**MicEnum**“:



[4]

Windows – Example for legal metrology

Measuring Instrument

[5]

Linux – What´s AppArmor?

- The **ApplicationArmor** is a kernel extension in **Linux** with which a **MAC** can be used in addition to **DAC**.
- Each **object** can have a so-called **profile**.
- **Default deny** is valid.

[6]

- A profile only **allows** what is set in the profile by a **rule**.
- AppArmor does **not** provide **complete monitoring** of the entire system.
- It **monitors only** what a **profile** has and only **after restarting** the system.

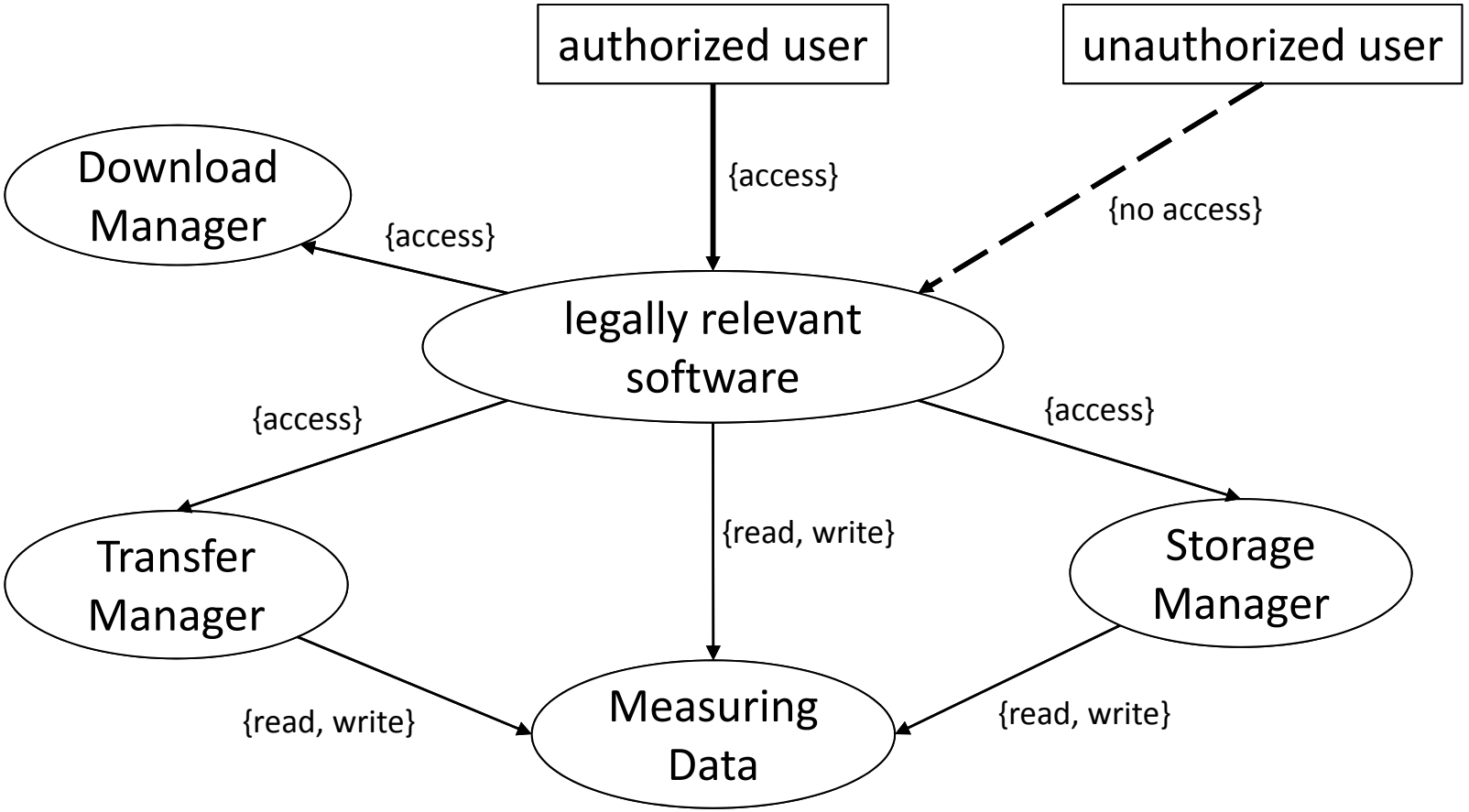
Linux – What´s AppArmor?

- **AppArmor** and **SELinux** offer different **operating modes**:
  - **enforce mode**
  - **audit mode**
  - **complain mode**

- AppArmor **logs all violations** of loaded profiles.

- **AppArmor** can be installed next to **SELinux** in the Linux kernel, but both kernel extensions can **not** be **used simultaneously**.

Linux – Example for legal metrology



Linux – What´s SELinux?

- Like AppArmor, the **Security-Enhanced Linux** (SELinux) is an extension of the Linux kernel.

- In contrast to AppArmor, SELinux basically **monitors the entire system** and also does not allow access that is not granted by a rule (**default deny**).

- Each subject and each object is obtained by an additional **SELinux security label**, the so-called **security context**:
  - **user**
  - **role**
  - **domain** (or **type**)

[7]

- This makes it possible to use a **Mandatory Access Control** (MAC) and an **Role Based Access Control** (RBAC) in addition to the **Discretionary Access Control** (DAC) in Linux.

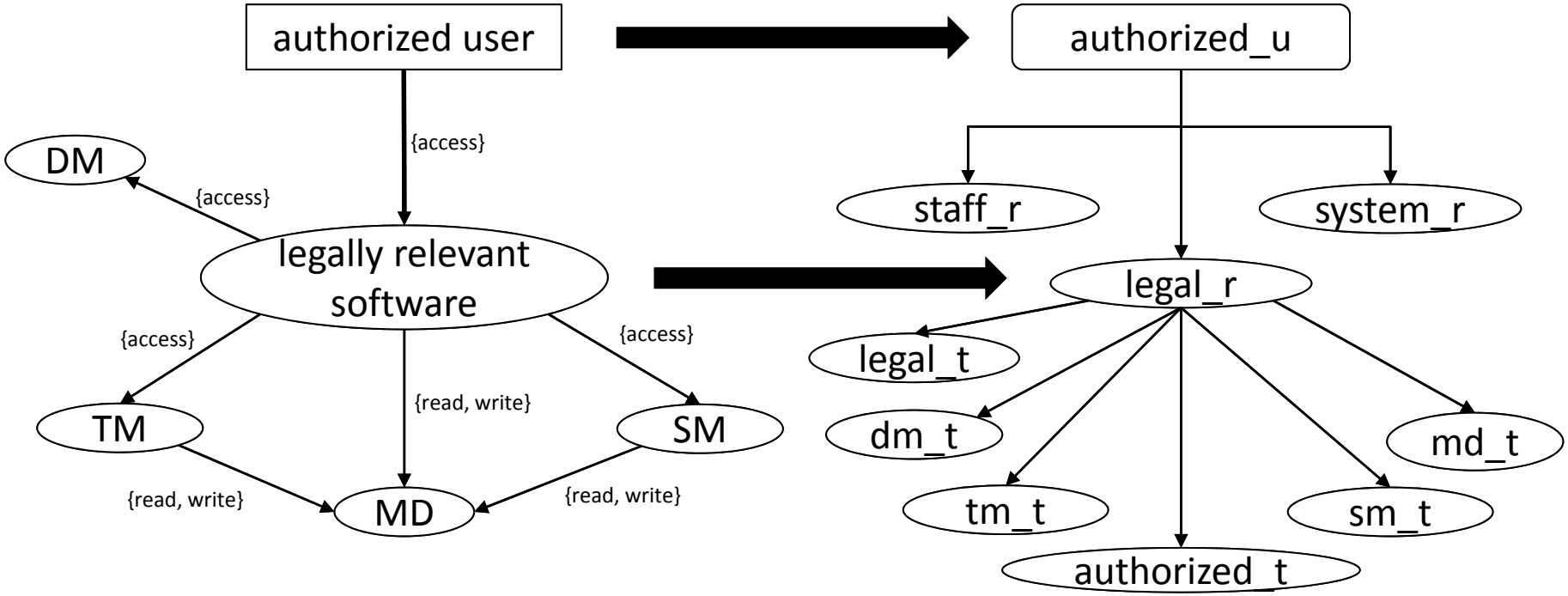
Linux – What´s SELinux?

- SELinux offers the possibility to **create** its own **type enforcement rules** and to combine them to a policy.

- However, several **thousands** of such **rules** are needed to **secure** the most important network services.

- SELinux therefore offers ready-made **policies** with different objectives:
  - **Targeted-Policy**
  - **Strict-Policy**
  - **Reference-Policy**

Linux – Example for legal metrology



Legend:
DM: Download Manager
TM: Transfer Manager
MD: Measuring Data
SM: Storage Manager

Summary

- In **Windows**, you can use **Mandatory Integrity Control** to give each subject and object an **integrity level** between untrusted and system. With this and the **system-wide no-up policy**, you can make the system more secure.

- In **Linux**, you can use **AppArmor** to assign a **profile** to each object and store access decisions in it. **Logs** allow you to keep control.

- As an alternative to AppArmor, you can also use **SELinux** in **Linux**, which gives each subject and object a **security label** consisting of **user**, **role** and **type** (or **domain**), providing a high degree of security through **Type Enforcement rules** and **Role Based Access Control**.

- Now it is up to you to choose which is the right mechanism for you.

Thank you for your attention

References

References:

[1] „http://www.3s-erp.de/3s-erp/3s-produkte-was-macht-3s/“; last: 06.06.2017

[2] Chelf, B. Measuring software quality – A Study of Open Source Software. Chief Technology Officer, Coverity. 2011.

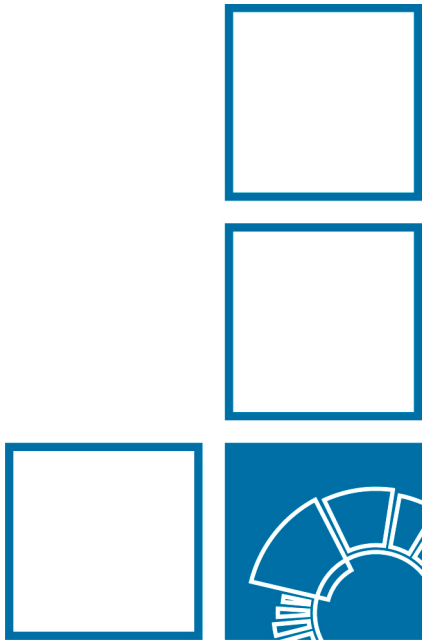
[3] “https://windowsunited.de/2015/07/29/windows-10-iso-jetzt-downloaden/”; last: 14.06.2017

[4] „https://www.elevenpaths.com/labstools/micenum/index.html“; last: 07.06.2017

[5] „https://www.pinterest.de/austintc68/“; last: 07.06.2017

[6] „https://sharewiz.net/secure_server_apparmor_security.html“; last: 07.06.2017

[7] „https://lintut.com/how-to-disable-selinux-on-centos-6-5/“; last: 08.06.2017



Physikalisch-Technische Bundesanstalt
Braunschweig and Berlin
Abbestraße 2 - 12
10587 Berlin

Patrick Scholz
Telefon: 030 3481 7021
E-Mail: patrick.scholz@ptb.de
www.ptb.de