



Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences



17th SIG e-Assessment workshop

Improving BYOD exam security by combining SEB with Lernstick

Ronny Standke (BFH) and Thore Sommer (Kiel University)

Intro Lernstick

<https://lernstick.ch>



Live system for BYOD (no installation, USB boot)



open
personal
huge collection of software
free



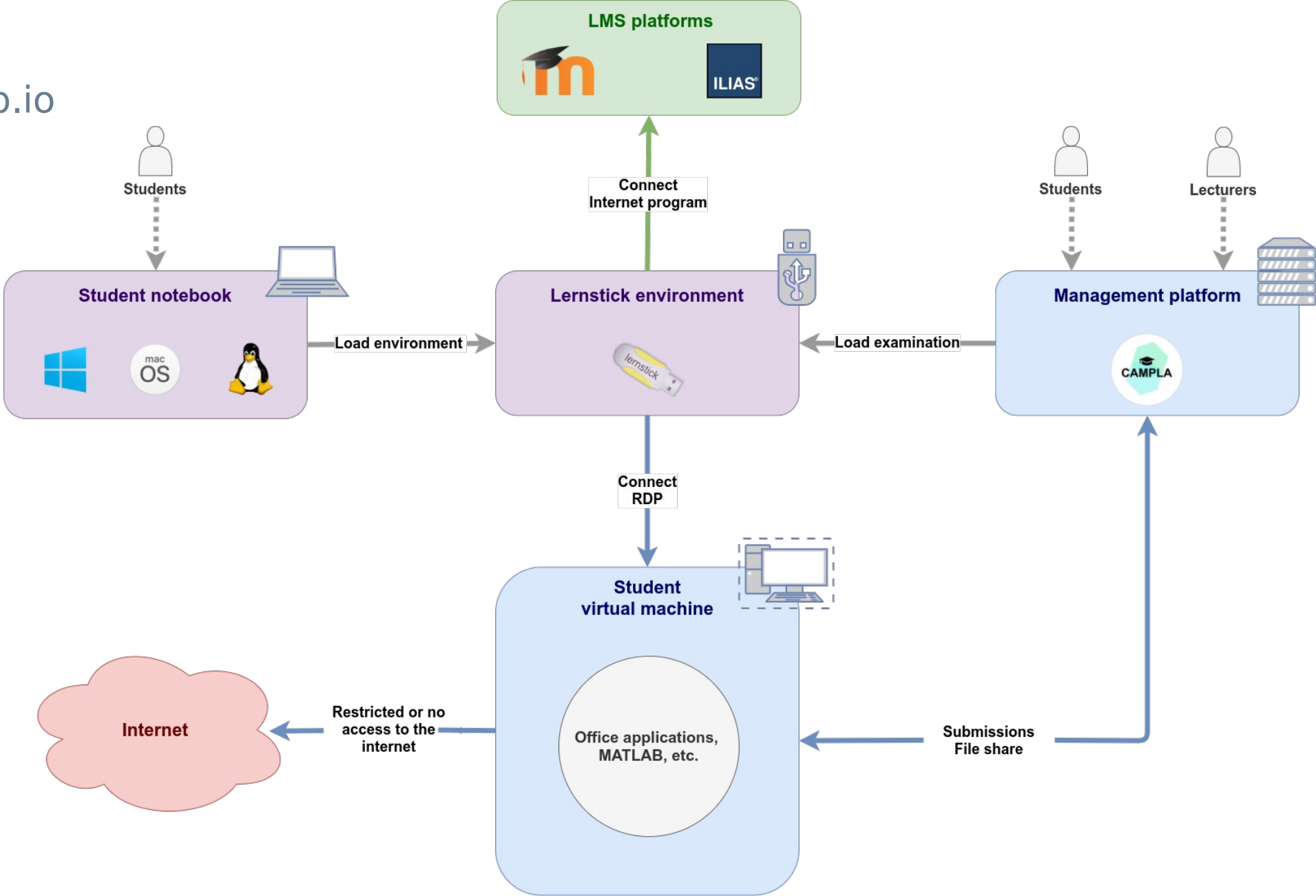
closed
institutional
reduced software set
free



customer specific
commercial

CAMPLA

<https://campla.github.io>



Typical exam environment problems

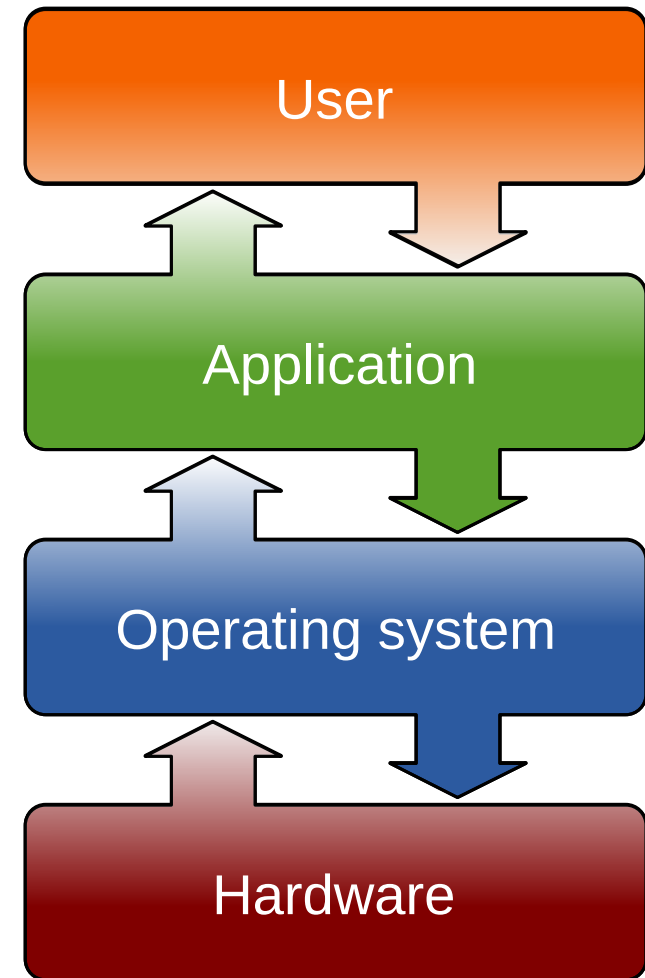
Attackers only need:

- Criminal energy
- Knowledge
- **Opportunities & time**



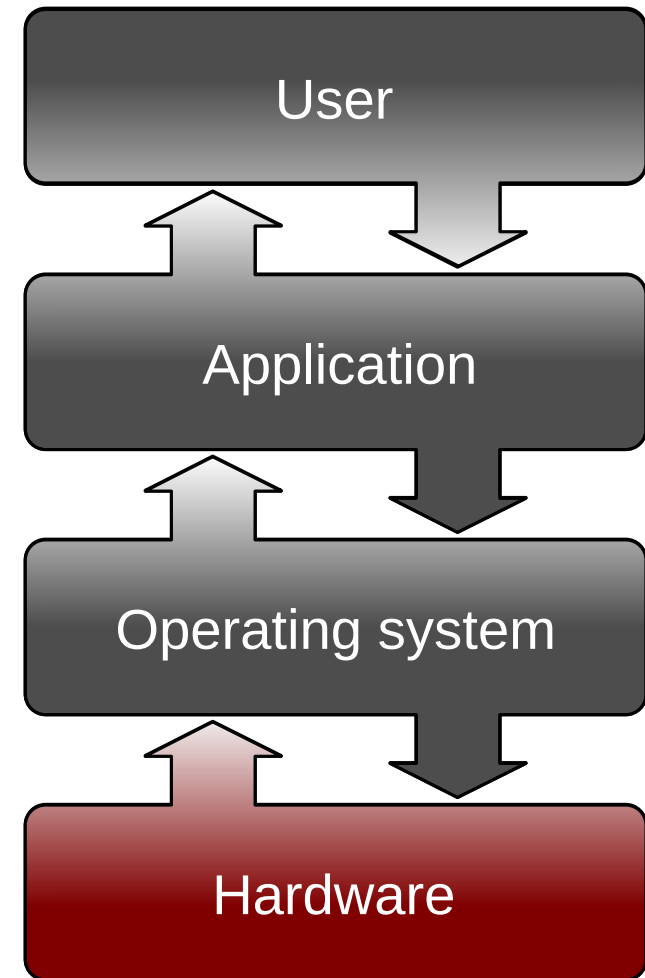
BYOOS?

- "Bring your own Operating System"?
- Subsequent installation of "exam software"?
- Security can NOT be guaranteed!



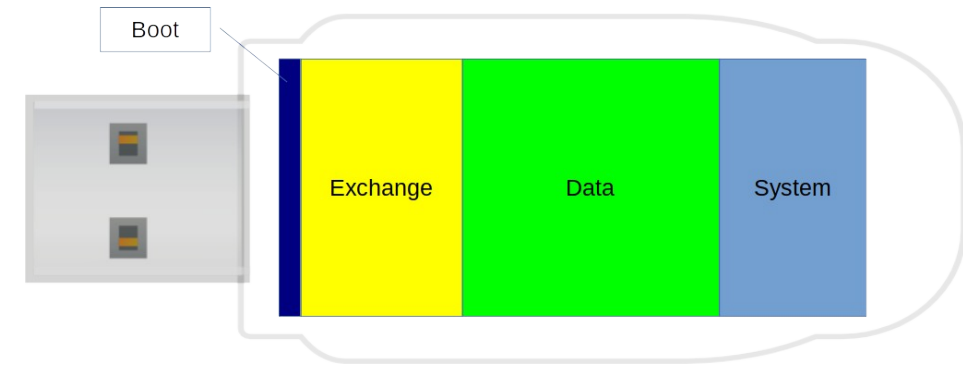
BYOH

- "Bring your own Hardware"
- Much higher level of security possible
- Operating system and applications are provided by the educational institution



Security problems of Lernstick EXAM

- Exam system is stored on off-the-shelf commodity USB flash drives
- No protection against manipulation!
- PIN locked flash drives?
 - expensive
 - still no protection against "fake environments"
 - still no protection against temporary unauthorized reboots during exam



Improving security in BYOD exams

How can we trust the system if we cannot trust the user?

→ Trusted Platform Module (TPM)

- Remote system state verification

→ TPM based Remote Attestation

- Verification of the system boot

→ Secure Boot

- Verification of file integrity

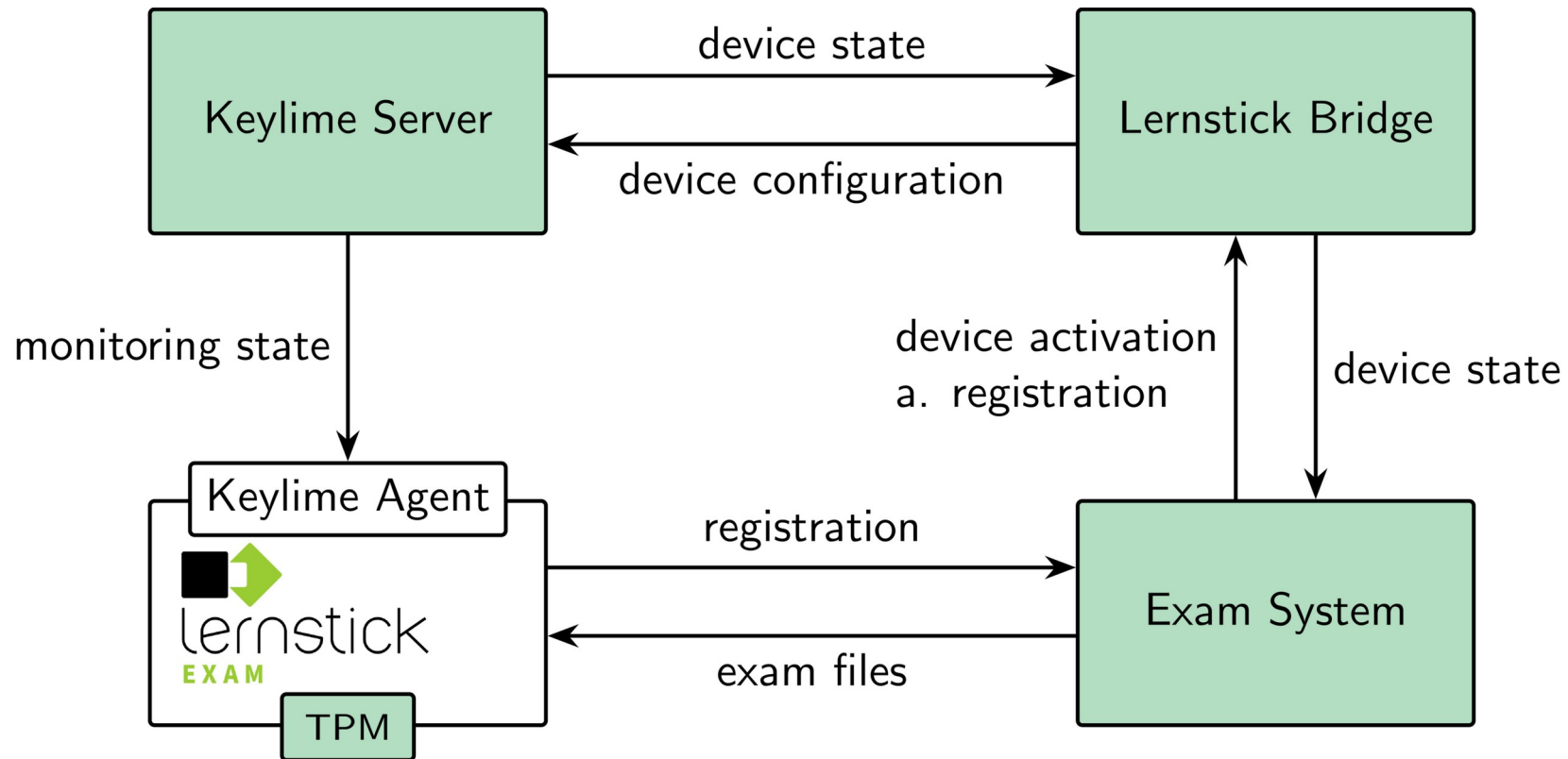
→ dm-verity (Android/Chrome OS)



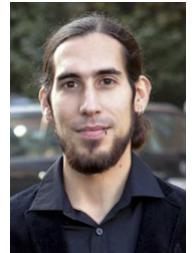
Credit: https://www.infineon.com/export/sites/default/_images/product/security-smart-card-solutions/SLI9670.jpg_1006886318.jpg

Required technologies are widely adopted

Cooperation with Kiel University (Remote Attestation for Lernstick EXAM)



Dr.-Ing. Sandro Esquivel



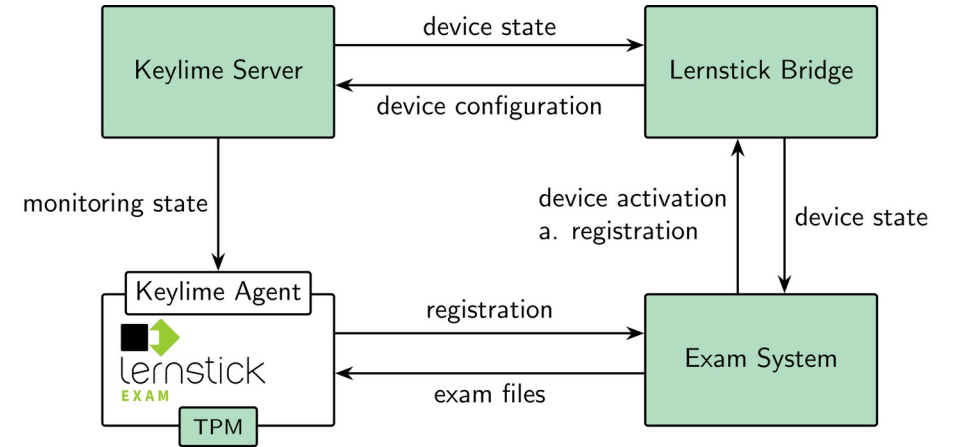
Thore Sommer



Security vs. Simplicity

Do we REALLY have to do all this?

There is SEB, right?...



TPM

PCR values

UEFI

Linux

dm-verity

Secure Boot

Firmware

Keylime

BYOD exam security issues are very real!

1000 and 1 way to bypass Safe Exam Browser - Prog.World - Mozilla Firefox

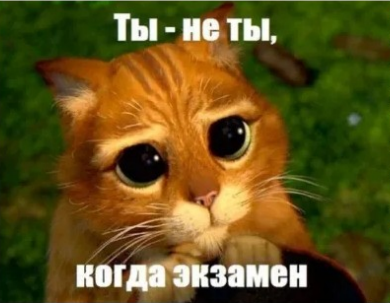
1000 and 1 way to bypass

https://prog.world/1000-and-1-way-to-bypass-safe-exam-browser/

Suchen

Prog.World

1000 and 1 way to bypass Safe Exam Browser



Okay, not 1000 and 1 way, but there are quite a few of them! What are we talking about? The fact that the COVID-19 pandemic has made many changes in our lives, including in education – both school and university. Lessons, lectures and seminars have moved to the online format, but the question of how to deal with the control of progress remains. How can teachers make sure that the student taking the exam has not opened the cheat sheets in the next tab?

In Russia, this problem was solved using an open-source program. [Safe Exam Browser \(SEB\)](#)... It would seem that now not a single freebie seeker will be able to cheat, but is this “fortress” really so inaccessible? Come under the cut, today we will tell and show you a bunch of ways to cheat SEB!

SEB Support - 2021-02-05

Btw. SEB and an exam system/LMS like Moodle can also check the integrity of the SEB binary, when using the Browser Exam Key. But of course the SEB binary could be manipulated as mentioned in the article you referred, to still send the correct Browser Exam Key even though being hacked. On infrastructure which isn't managed and protected by the institution (like their own, properly secured computers), you can never be 100% sure about the integrity of the software on it. Obviously when doing BYOD remote exams, you can never provide perfect security by technological means (if any proctoring company promises that, that's marketing nonsense).

SEB Security Demo

SEB issues

- Security can not be enforced on the users OS
- Exploits needs to be written only once

```
public bool IsVirtualMachine()  
{  
    ... many checks ...  
  
    return isVirtualMachine;  
}
```



```
public bool IsVirtualMachine()  
{  
    ... many checks ...  
  
    return false;  
}
```

Proposal



- **Application layer**
- Sophisticated exam management
- LMS integration (e.g. Moodle)
- Much simpler version than today
(BYOD security is solved by operating system layer)



- **Operating system layer**
- Secure base for BYOD exams with laptops
- Minimal environment
- Exam system agnostic