

# An Architecture for Producing Trustworthy Linux Programs

Michael Neises  
ITTC and EECS Department, University of Kansas

August 22, 2021

## **Part I**

# **Introduction**

## **1 Research Statement**

- 1.1 The seL4 Microkernel can be leveraged to create trustworthy systems.**
- 1.2 An architecture can be developed to facilitate the creation of trustworthy systems.**

## **2 Motivation**

- 2.1 Trustworthy systems are desirable.**

## **3 Contribution**

- 3.1 I will provide an architecture to facilitate the creation of trustworthy systems.**
- 3.2 Using my architecture, I will generate some non-trivial trustworthy system from simple source files.**

## **4 Overview of Proposal**

- 4.1 I will implement a single trustworthy system.**
- 4.2 I will argue that the systems are trustworthy.**
- 4.3 I will implemented an architecture for generation of trustworthy systems.**
- 4.4 I will re-implement the first system using the architecture.**

## **Part II**

# **Related Work**

## **5 Background Work**

- 5.1 I paved the way for kernel module development as part of the seL4 build-system.**

## **6 Related Work**

- 6.1 Paul Rowe's paper "Confining"**

## **Part III**

2

# **Methodology**

## **7 Building the Solution**

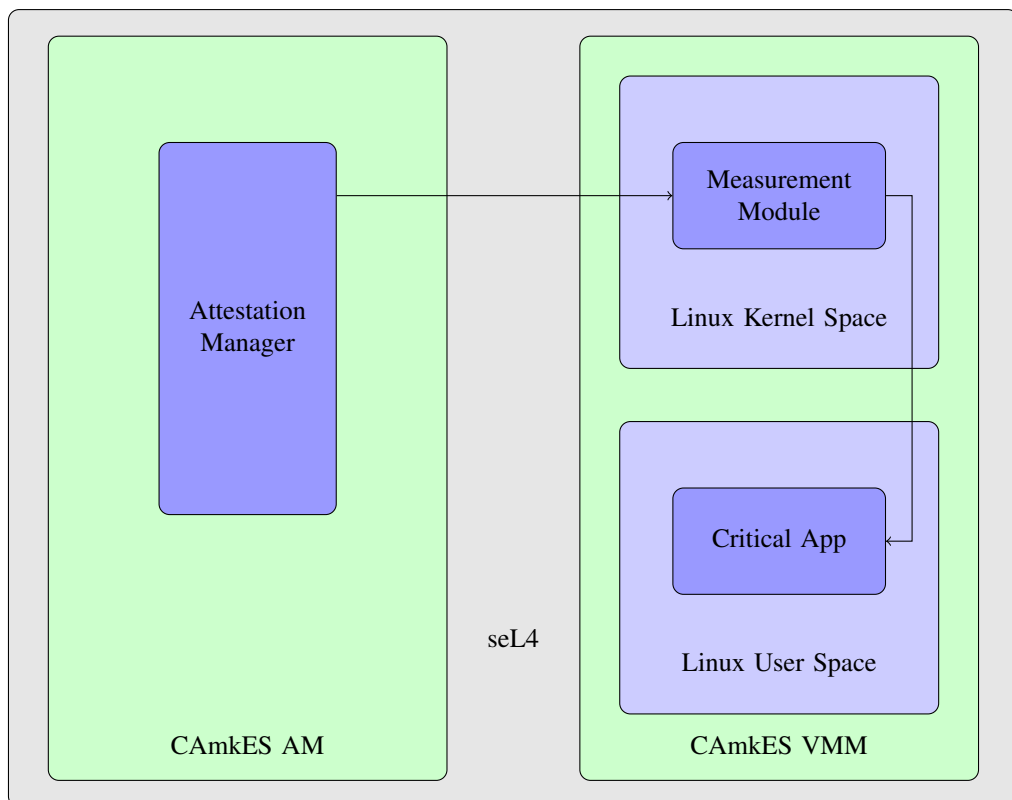
**7.1 It's a lot of system programming in C.**

**7.2 It's also a lot of CMake.**

**7.3 There are architectural camkes files.**

## **8 Describing the Solution**

**8.1 Show the picture.**



- 8.2** Paint a picture of the simple, trustworthy kernel hosting the feature-rich, vulnerable kernel as a guest.

## **9 Evaluating the Solution**

- 9.1** This architecture should be resilient against kernel module attacks.
- 9.2** This architecture should be trivial to use.

## **Part IV**

# **Research Plan**

## **10 Work So Far**

- 10.1** The simple kernel has already measured and judged the modules of the vulnerable kernel.

## **11 Work To Do**

- 11.1** I must implement measurement and subsequent execution of binaries present in the Linux system.
- 11.2** The architecture must prove resilient to meaningful attacks.
- 11.3** The architecture must include automation tools.
- 11.4** The architecture would like to support many languages at the highest level.

## **Part V**

# **Conclusions and Future Work**

## **12 Summarize the Proposal**

test

- 12.1 I will provide a foundation for trustworthy systems.**
- 12.2 I will implement a trustworthy system on my foundation.**

### **13 Identify What Needs Done**

- 13.1 The architecture must be completed.**
- 13.2 The argument must be completed.**
- 13.3 The architecture must be automated.**

### **14 Outline Research Plan**

- 14.1 I must finish implementing.**
- 14.2 I must read to connect with the literature.**
- 14.3 I must write to explain what I've done.**