Thesis: Outline

Oberon Swings

April 20, 2022

Contents

Chapter 1

Introduction

- Smartphones everywhere
  - Everyone has one
  - Interchangeable with PC
- Sensitive data
  - Lots of traffic
  - Personal data stored
- Comparable to IoT
  - Hardware similarities
  - Security features (lot less than PC)

1.1 Problem statement

- IoT security
  - Minimize overhead
- PC functionality
  - Banking, e-Health and mails
- Missmatch
  - Sensitive data requires good security
  - Functionality is pushed but security lags behind

1.2 Contributions

- Reproduction of paper
  - Replicated solution as closely as possible
  - Evaluation about results compared to original
- Open source code (proof of concept)
  - Enable easier reproduction/verification in the future
- Extra experiment measurements
  - Comparable experiments (to be able to compare)
  - More elaborate experiments (to allow better decision making)
- Comparison with similar solutions
  - Overview of comparable papers (pros and cons)
  - Weak points and strenghts of the reproduced paper compared to the others

1.3 Outline

In the next chapter more background information about among other things ARM TrustZone and Remote Attestation will be given. In the third chapter the methods secure applications will be explained. In the fourth chapter the goal and outcome of the experiments will be made clear. The final chapter will conclude this thesis informing the reader about limitations of this work and possible future directions of research.

Chapter 2

Background

2.1 Remote Attestation

- Goal
  - Verify integrity
- How it works
  - Verifier
  - Prover
  - Proof
- Assumptions
  - Trusted third party
  - Secure keys

2.2 Trusted Execution Environment

- Execution
  - Isolation
  - Authentic code
  - Runtime integrity
  - Strict interfaces
- Trust
  - Static
  - Dynamic

- Security
  - Data separation
  - Sanitization
  - Control of information flow
  - Fault isolation

2.3 ARM TrustZone

- Normal World
  - Rich OS
- Secure World
  - Trusted Kernel
  - NS-bit
  - Secure Configuration Register
- Peripherals
  - TZ Address Space Controller
  - TZ Protection Controller (interrupts)

2.4 PinePhone

- Open source
  -
- Linux
  -
- ARM TrustZone
  -

2.5 Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes

- Solution
  - Overview

- Trusted Boot
  - Trusted load phase
  - Attestation during boot
- Remote attestation
  - Trusted execution time
  - Pagebased approach

Chapter 3

Method

3.1 Detailed Problem

- Lots of functionality
  - Sensitive data
  - Mobile computing
- Performance driven
  - All resources to functionality
  - Little room for security
  - Extensive security measures needed
- Hardware security solution
  - Security embedded in hardware
  - Better for performance
  - Correct implementation required

3.2 System Model

- Open platform
  - Multiple software providers
  - Platform owned by user
- Secure software execution
  - Software isolation
  - Secure data storage

3.3 Attacker Model

- Physical access
  - Threats
  - Vulnerabilities
- OS/Firmware attacks
  - Threats
  - Vulnerabilities
- Software attacks
  - Threats
  - Vulnerabilities

3.4 Solution

- Secure boot
  - Root of Trust
  - Chain of Trust
  - Secure starting point
- User attestation
  - Integrity (control flow, data structures, ...)
  - Authenticity (code, ...)
- Trust
  - Execution
  - Data protection

Chapter 4

Implementation

4.1 Attestation TA

- Trusted Application
  - Hash NW memory pages
  - Store reference values in secure memory
  - Make comparison and notify user
- NW OS interaction
  - Retrieve address of memory page
  - Translate into physical address
  - Provide datastructures to TA
- Extensions
  - Notify user using trusted IO
  - Decrease dependency on NW OS
  - Attest more than just code pages (data structures, invariants,...)

Chapter 5

Experiments

5.1 Performance

5.2 Performance Evaluation

5.3 Security Properties

5.4 Security Evaluation

Chapter 6

Conclusion

6.1 Related work

- Secure boot, Trusted boot and remote attestation for ARM TrustZone-based IoT Nodes
- DAA-TZ: An Efficient DAA Scheme for Mobile Devices Using ARM TrustZone
- SecTEE: A Software-based Approach to Secure Enclave Architecture Using TEE
- TZ-MRAS: A Remote Attestation Scheme for the Mobile Terminal Based on ARM TrustZone
- TrustShadow: Secure Execution of Unmodified Applications with ARM TrustZone

6.2 Comparison of Approaches

- Effectiveness
  - Reached goal
  - Defends most variety of attacks
  - Stronges security guarantees
- Assumptions
  - Least assumptions
  - Most realistic

6.3 Future Improvements

- Best approach
  - Overview
  - Reasoning
- Weaknesses
- Possible improvements
  - inspiration from Lightweight and Flexible Trust Assessment Modules for the Internet of Things
- Different solutions

Chapter 7

Discussion

- Solution overview
  - Reproduction
  - Thorough understanding paper solution
  - Extensions
- Shortcomings
  - Unaccounted for attacker possibilities
  - Unaccomplished desired guarantees
- Positives
  - Open source code
  - Thorough comparison