Safety and Security of Embedded Device OS

1 Theme: Operation System

2 Subject: Security Testing

List of Abbreviations

IOT	Internet of Things

3 Background

IoT (Internet of Things) have emerged as the universal platform that combines IT (information technology) and OT (operation technology), revolutionizing manufacturing, transportation, health care, and many other industry sectors. However, the rapid developments in IoT pose a series of unique security challenges. Especially, at the core of every IoT platform, the operating systems (OS) that drive IoT devices are at high risk, partly due to the lack of tools that can automatically analyze and detect security vulnerabilities in those OS. Although such tools exist for conventional computers, they are not applicable to IoT OS because of “peripheral dependencies”---the wide range of peripherals for IoT devices makes virtualization/emulation impossible, and thus the existing tools useless.

4 Scope

We propose to solve the fundamental problem that prevents the application of security testing tools to IoT OS. We will follow a novel approach named peripheral-agnostic emulation. Our goal is to allow IoT OS and security testing tools to run in a specially emulated environment that does not require pre-knowledge or specific models for dependent peripherals, thus making existing and new dynamic OS testing methods possible. As a result, all kinds of IoT OS can be comprehensively tested using intended device/SoC specifications without requiring real hardware or expensive models. Furthermore, thanks to the fully emulated environment, dynamic tests, such as fuzzing and stress testing, can be done in a scalable fashion, which will greatly facilitate vulnerability and flaw discovery for IoT OS.

5 Expected Outcome and Deliverables

We expect the outcome and deliverables as following:

- A new method for generically modeling IoT peripheral devices
- A new emulation technology for IoT OS, capable of supporting a wide range of peripherals and SoC specifications
- A new platform for performing dynamic security tests on IoT OS at scale

6 Acceptance Criteria

- All the existing IOT peripherals will be modeled in this project.
- Given an new ARM-M based peripheral-agnostic IOT device, the peripherals could be automatically dectected, and vulnerabilities and flaws in the driver could be effectively found.
- This platform could be ported to Huawei IOT OS.

7 Phased Project Plan

Phase No.	Phase description	Time(months)	Main task content	Output Standard that should achieve
1	**Understanding IoT/embedded peripheral I/O characteristics**	4	a. Survey of existing IoT peripherals b. Parsing peripheral datasheets and documentations c. Taxonomy of devices and OS d. Generating per-category models summarizing peripheral external behaviors	Investigation Report Design documents of proposal.

			.	
2	**Designing Peripheral-agnostic Emulation for IoT OS**	8	a. Design functional emulator for ARM Cortex-M b. HAL layer simulation c. Peripheral model integration d. Peripheral detection and inference e. Experiments and evaluation Result collection and paper writing	The implementation, the validation and test reports.

Trademarks and Permissions

Confidentiality

All information in this document (including, but not limited to interface protocols, parameters, flowchart and formula) is the confidential information of Huawei Technologies Co., Ltd and its affiliates. Any and all recipient shall keep this document in confidence with the same degree of care as used for its own confidential information and shall not publish or disclose wholly or in part to any other party without Huawei Technologies Co., Ltd's prior written consent.

Notice

Unless otherwise agreed by Huawei Technologies Co., Ltd, all the information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Distribution

Without the written consent of Huawei Technologies Co., Ltd, this document cannot be distributed except for the purpose of Huawei Innovation R&D Projects and within those who have participated in Huawei Innovation R&D Projects.