ARIA Applied Research in Action

Tizen OS Support for SOTI MobiControl Interoperability

Qi Zhao, Yin-Hung Chen

SOTI Inc.

Introduction of SOTI® MobiControl

Brief Intro

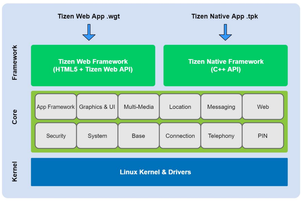
SOTI MobiControl is an enterprise mobility management (EMM) solution that secures and manages Google Android™, Apple® iOS, Linux®, macOS® and Microsoft Windows® devices (after our project, it will support Tizen™ devices as well), throughout their entire lifecycle, from deployment to retirement. It removes the complexity from managing a multi-OS, multi-vendor and multi-purpose business mobility program.

Key Supports

- Keep worker working by using Kiosk Mode or Remote Controlling
- Manage mobile content and applications via over-the-air installation, removal and configuration
- Get mobile devices deployed quickly and correctly through varies of enrollment methods and multi-layer protection
- Reduce device downtime with the help of build-in SOTI Assist Diagnostic Function

Quick Hack of Tizen™ Operating System

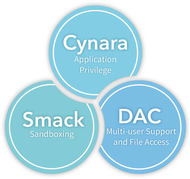
- Tizen is an open and flexible operating system that is widely used by Samsung IoT devices
- Tizen comes in multiple profiles to serve different industry requirements. The current Tizen profiles are Tizen IVI (in-vehicle infotainment), Tizen Mobile, Tizen TV, and Tizen Wearable
- Tizen is built on top of the Linux kernel and is supported by The Linux Foundation
- Tizen OS has put a lot of efforts in creating a highly efficient Security Model/ Architecture compared to other similar lightweight operating systems
- Tizen brings up the concept of Internet of Things (IoT) and is buzzed as The OS of Everything.

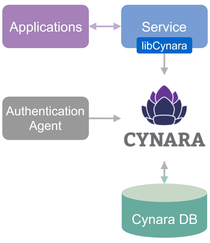


Porting Difficulties

Tizen Security Model

- All the 3rd-party apps are required to obtain the author and distributor signatures. Apps are only available on Tizen Store. For testing purpose sideloads, developers must create the keys with the device ID of the testing machine.



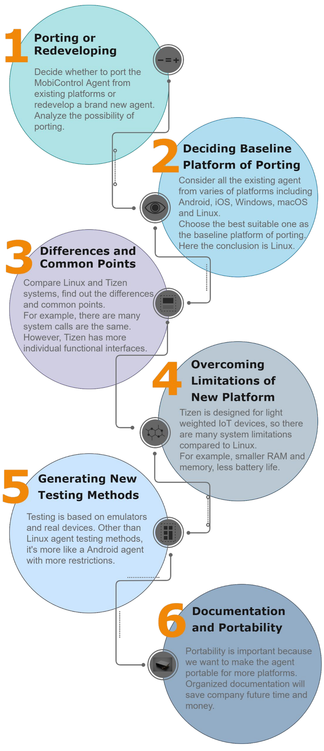


- DAC maintains the UID and GID as in Linux, which provides the multi-user support and file access.
- SMACK performs the sandbox mechanisms. Apps are only allowed to access specific resources in their app directories.
- Cynara maintains a database of privilege rules. Apps must predefine privileges to perform protected functionalities. Privilege rules are stored in the Cynara database and checked while the apps are executed.

Tizen Hardware Constraints

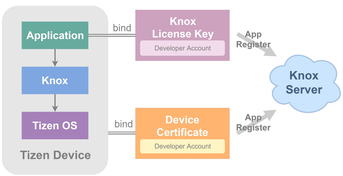
Tizen usually runs on mobile or IoT machines that have no access to sufficient power, memory and storage space, so it sets specific constraints to preserve resources. For instance, the devices will lose the ability to get notifications and even the network connections after standing still for a while, which causes significant problems to the agent functionalities.

Porting Process



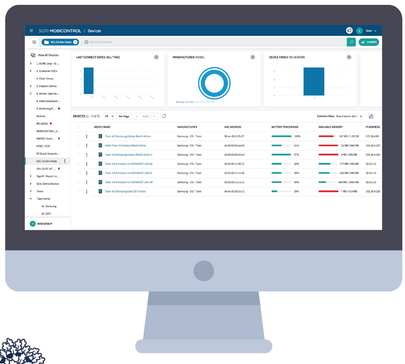
Challenges and Solutions

- Due to the sandbox mechanism, the agent cannot run as the administrator and perform operations in other app directories.
- We must use Knox MDM APIs to access security-sensitive information and actions, which requires a complicated registration process to get the authentications.
- The incompatibility of various versions of firmware makes our porting unscalable for all devices.
- On account of the security and efficacy considerations, Tizen removes or replaces some Linux functionalities. For instance, it uses Wayland as its window system instead of x11, and there is no ssh server in Tizen, which makes the remote control even more difficult.



Reference

- Mooney, James D. "Bringing portability to the software process." Dept. of Statistics and Comp. Sci., West Virginia Univ., Morgantown WV (1997)
- https://www.pebblebay.com/embedded-software-porting/
- Ajin Abraham. "Hacking Tizen: The OS of Everything" (2015)
- Icon made by Freepik from www.flaticon.com



Computer Science
UNIVERSITY OF TORONTO