SeCloak:
ARM TrustZone-based Mobile Peripheral Control

Matthew Lentz, Rijurekha Sen,
Peter Druschel, Bobby Bhattacharjee

MAX PLANCK INSTITUTE
FOR SOFTWARE SYSTEMS

Control Over Your Devices

Powerful sensing and communication capabilities

- But can be misused by malicious software!

Consider important scenarios:

- Journalists use airplane mode while meeting with source
- Turn off microphone to prevent snooping

Sensing

Camera
Microphone
Location
Motion
Orientation
…

Communication

NFC
Bluetooth
WiFi
Cellular
…

Users Have Limited Control

There are two fundamental issues:

- Incomplete settings
  - e.g., Motion sensors on Android
- No assurance that settings are enforced
  - Platform shown to be hard to secure as a whole

engadget

Your phone's motion sens
give away PINs and passw

Apparently, hackers can decipher your passwords by the phone moves as you type.

...

But because mobile apps and websites don't need to ask permission to access most of them, malicious programs can covertly 'listen in' on your sensor data and use it to discover a wide range of sensitive information about you such as phone call timing, physical activities and even your touch actions, PINs and passwords.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Cyber Threats to Mobile Phones

Paul Ruggiero and

Mobile Thre

Smartphones, or m
(PCs), are appearin
and relatively lax s

Against the Law: Countering Lawful Abuses of Digital Surveillance

Andrew 'bunnie' Huang Edward Snowden

Front-line journalists are high-value targets, and their enemies will spare no expense to silence them. Unfortunately, journalists can be betrayed by their own tools. Their smartphones are also the perfect tracking device. Because of the precedent set by the US's "third-party doctrine," which holds that metadata on such signals enjoys no meaningful legal protection, governments and powerful political institutions are gaining access to comprehensive records of phone emissions unwittingly broadcast by device owners.

Forbes

Security
JUL 27, 2015 @ 06:00 AM 145,228

Stagefright: It Only Takes One Text To Hack 950 Million Android Phones

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

critical vulnerabilities have left 95 per
nt of Google GOOGL -0.12% Android phones
en to an attack delivered by a simple
ultimedia text, a mobile security expert
rned today. In some cases, where phones
rse the attack code prior to the message
ing opened, the exploits are silent and the
er would have little chance of defending
eir data. The vulnerabilities are said to be
worst Android flaws ever uncovered.

Problem Statement

What is minimally required to give users **secure** control over their devices?

Without

- affecting usability or stability
- changes to existing software

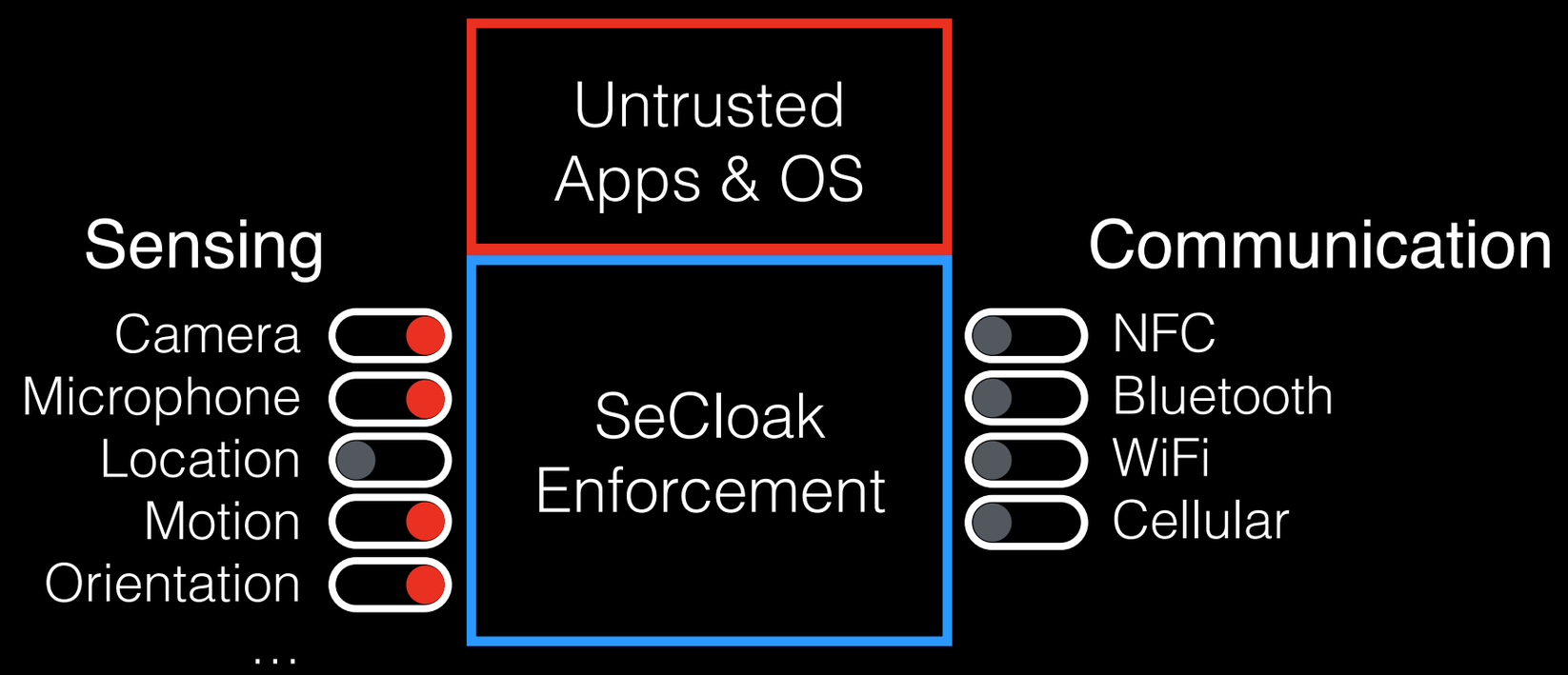
SeCloak - “Secure Cloak”

What is minimally required to give users **secure** control over their devices?

SeCloak provides secure “virtual” switches to users

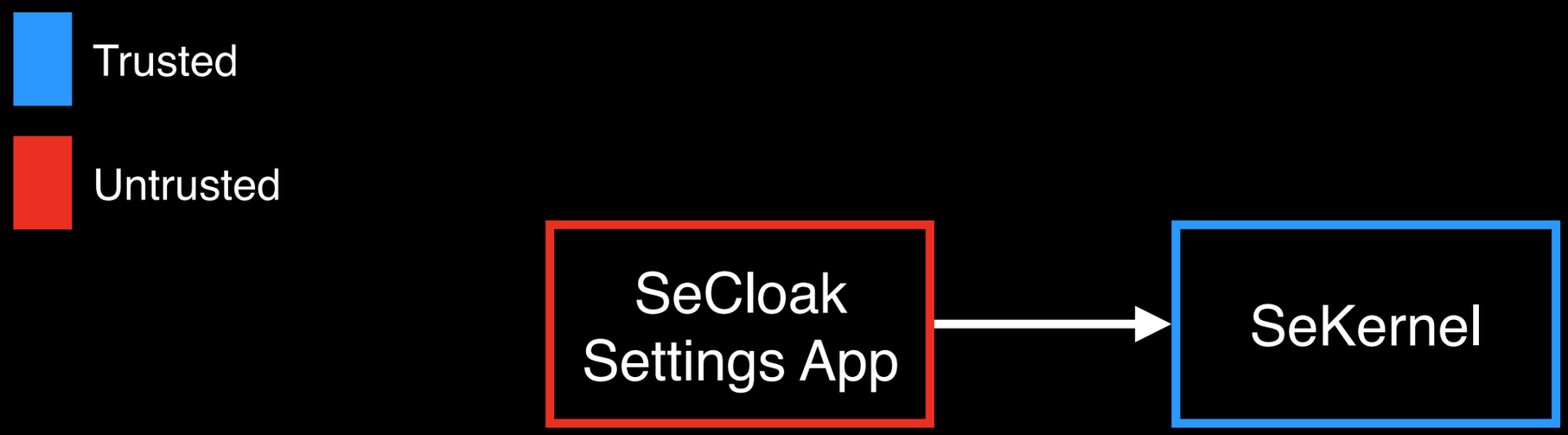
SeCloak - “Secure Cloak”

What is minimally required to give users **secure** control over their devices?

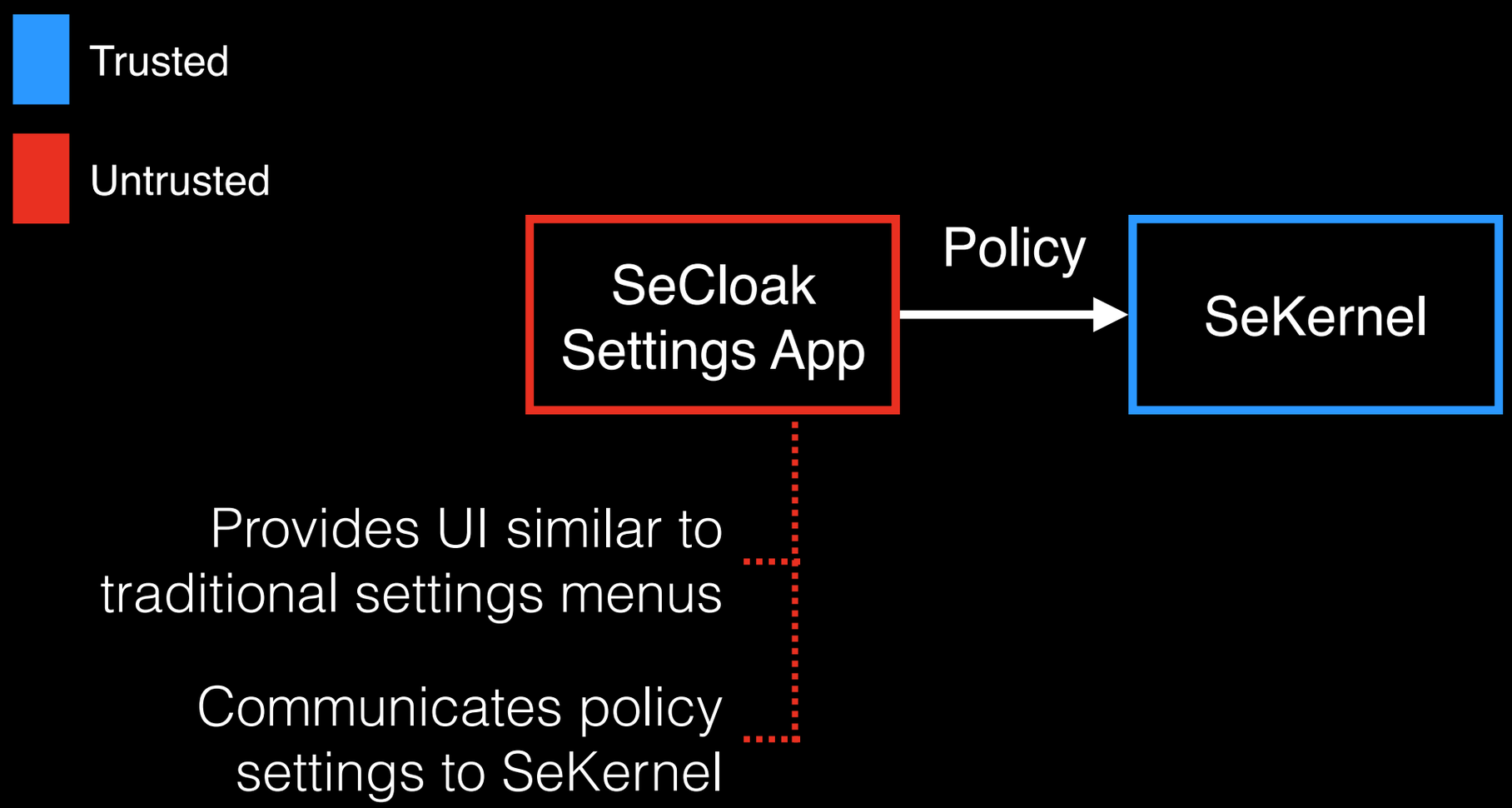


SeCloak provides secure “virtual” switches to users

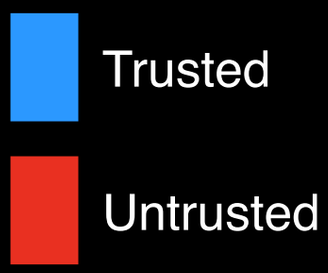
SeCloak Design

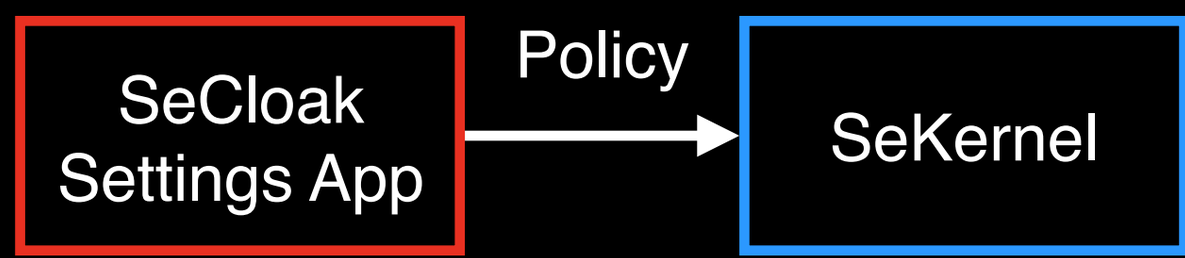


SeCloak Design



SeCloak Design





Provides UI similar to traditional settings menus

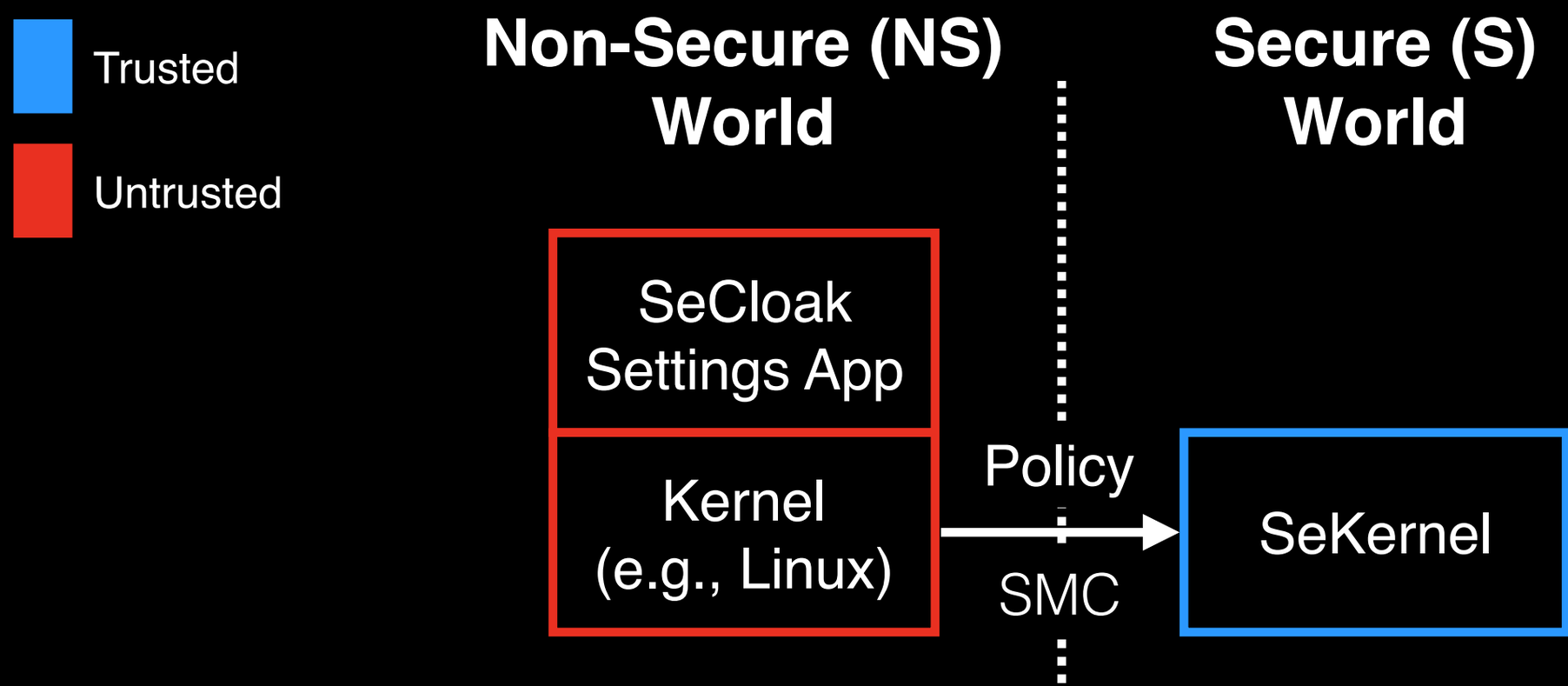
Communicates policy settings to SeKernel

Secure (re)display and user confirmation of policy

Configure HW protections to disable untrusted access

Handle access faults to enforce user policy

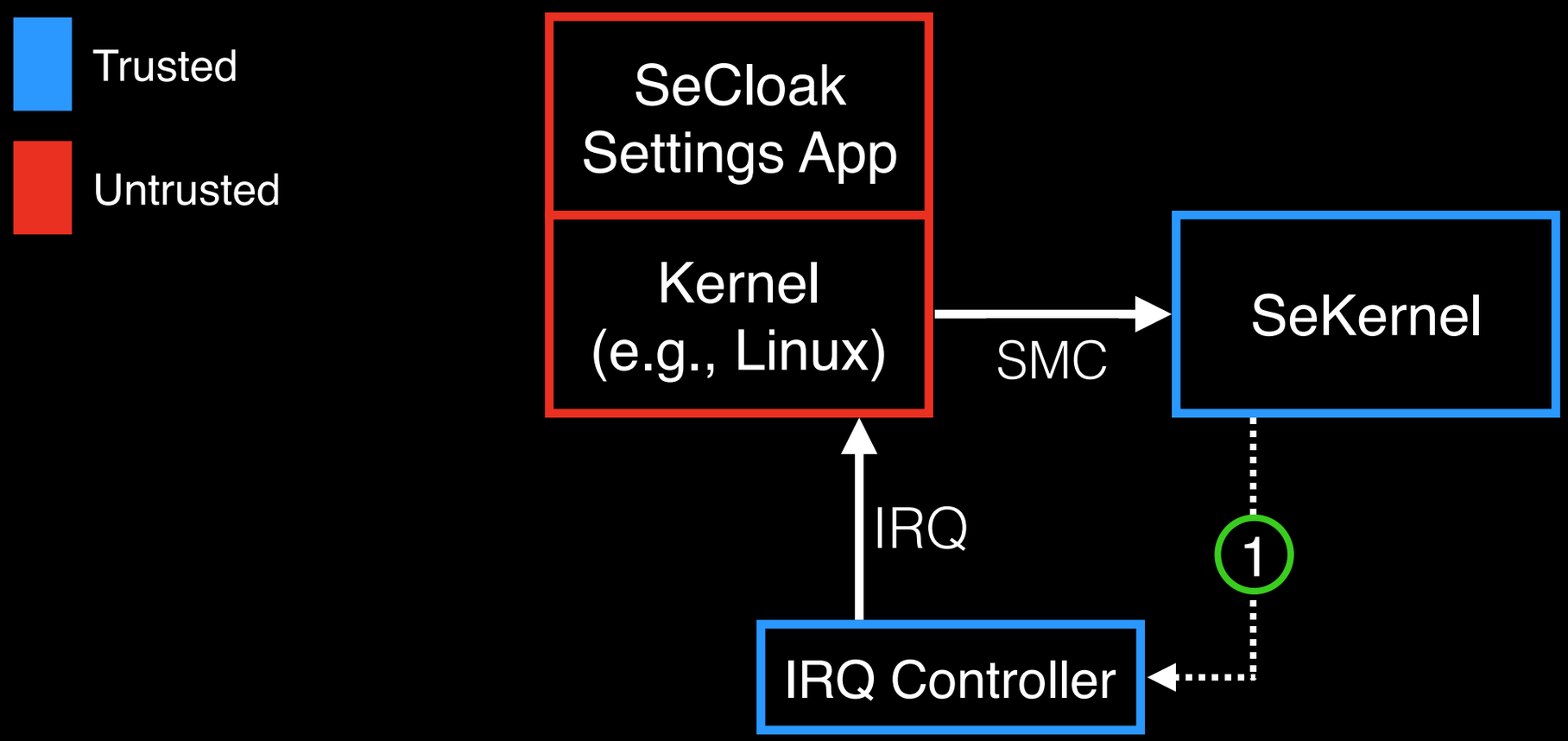
SeCloak on ARM TrustZone



ARM TrustZone supports two “worlds”

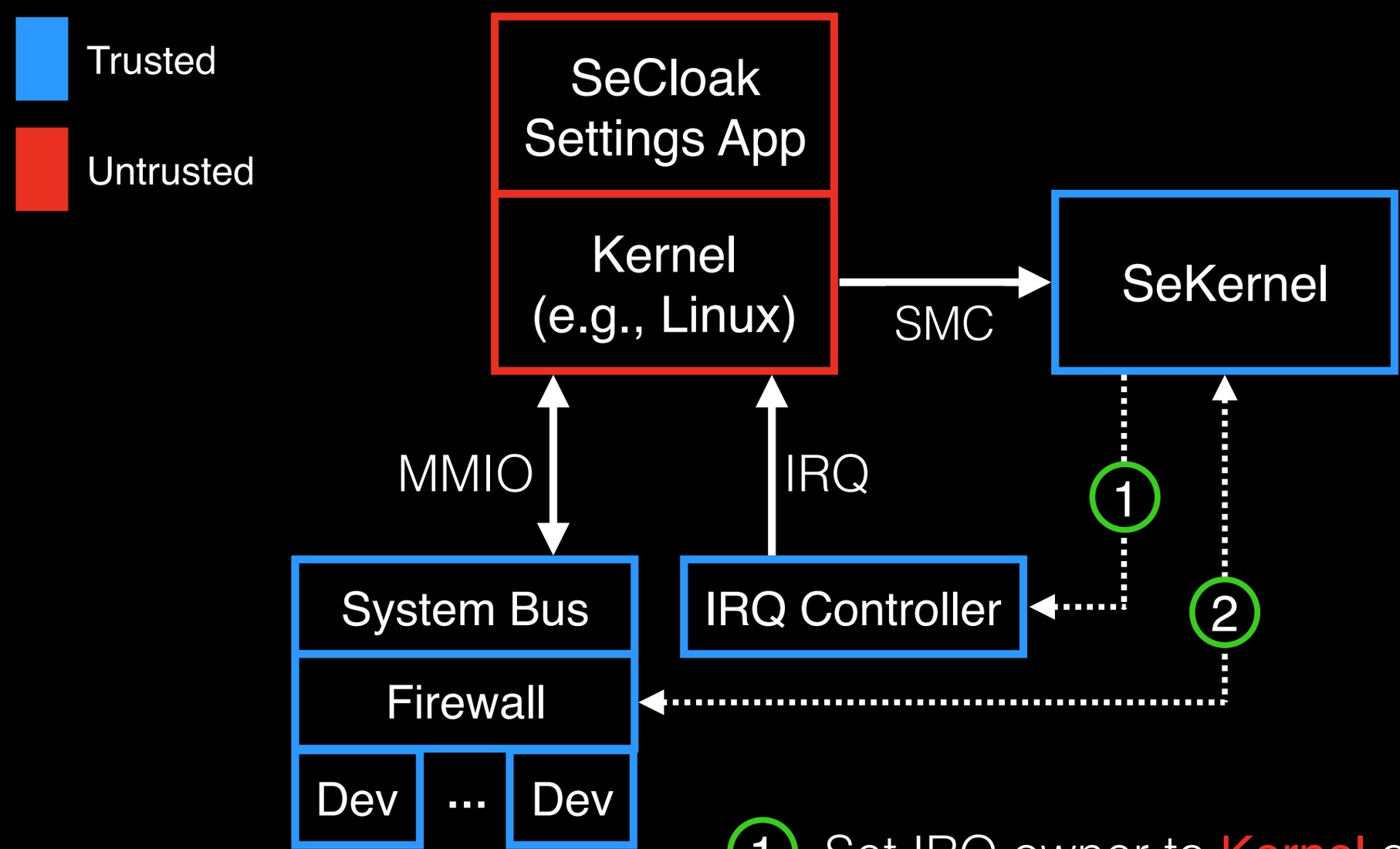
- Isolates SeKernel from untrusted kernel and apps
- Allows SeKernel to configure hardware protections

Hardware Protections



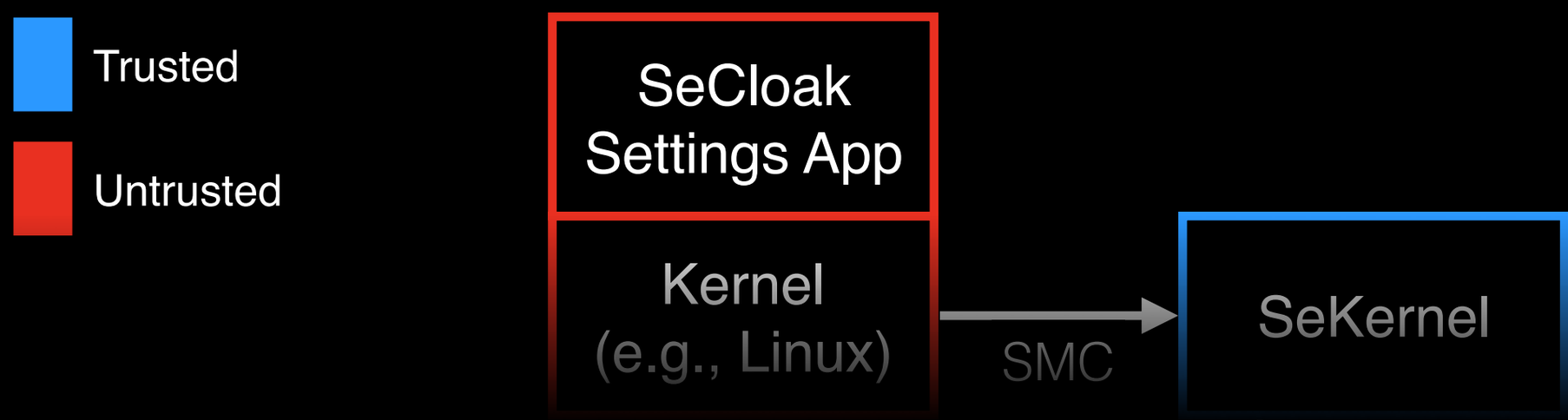
1 Set IRQ owner to Kernel or SeKernel

Hardware Protections



1. Set IRQ owner to Kernel or SeKernel
2. Configure to deny accesses made by Kernel
   Reports access faults to SeKernel

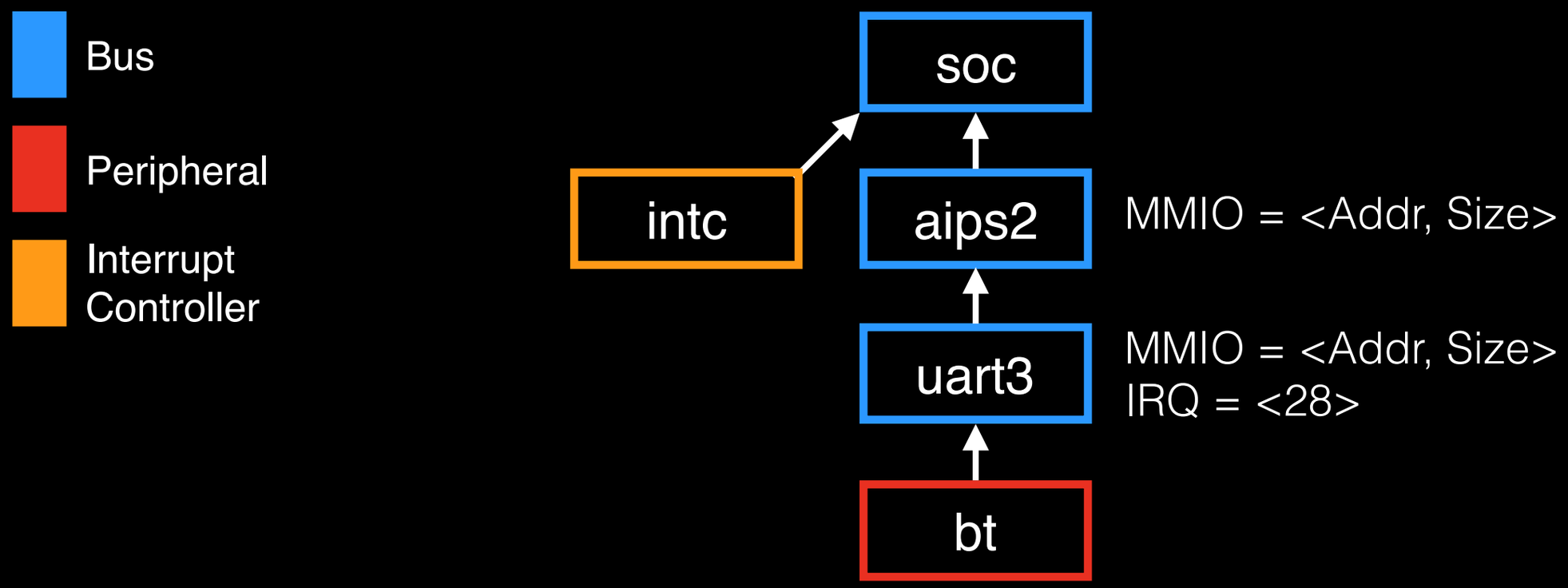
Hardware Protections



How do we securely identify these protection domains for devices?

1. Set IRQ owner to Kernel or SeKernel
2. Configure to deny accesses made by Kernel
   Reports access faults to SeKernel

Device Tree (DT)

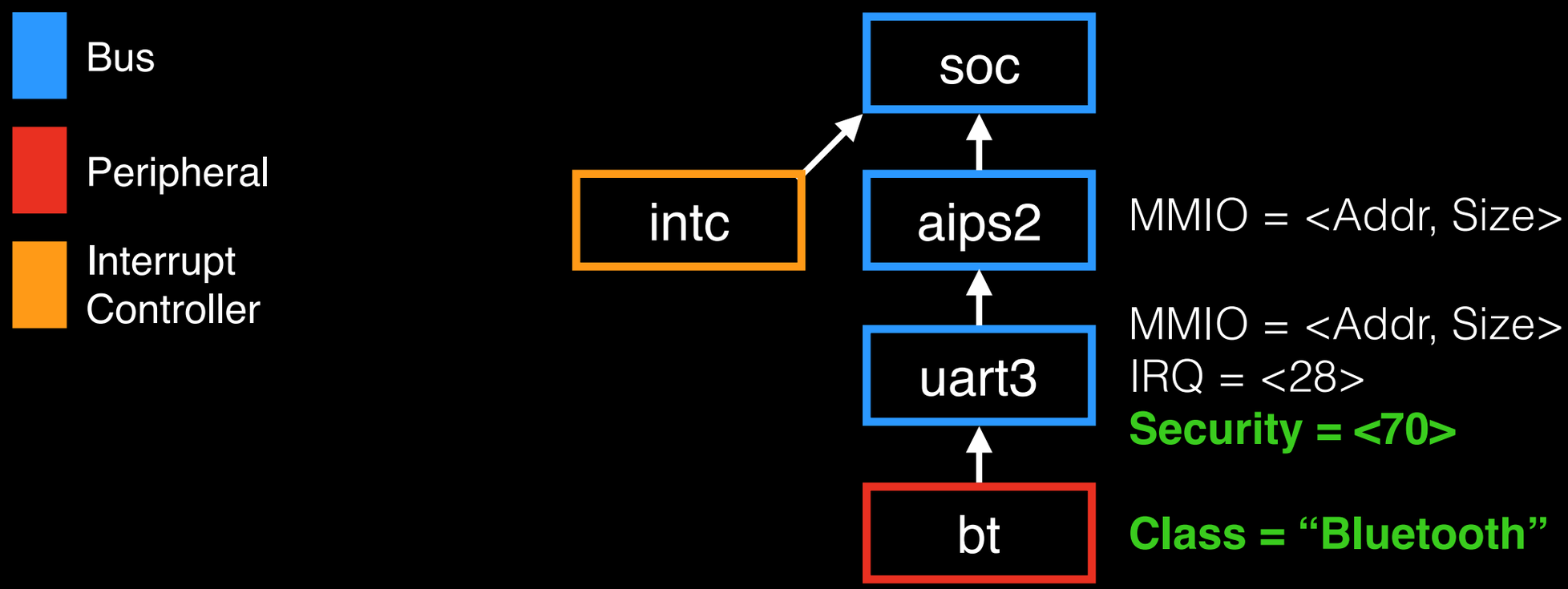


Device Tree specifies embedded hardware

- Each node represents a device

Nodes contain configuration properties

DT with SeCloak Properties

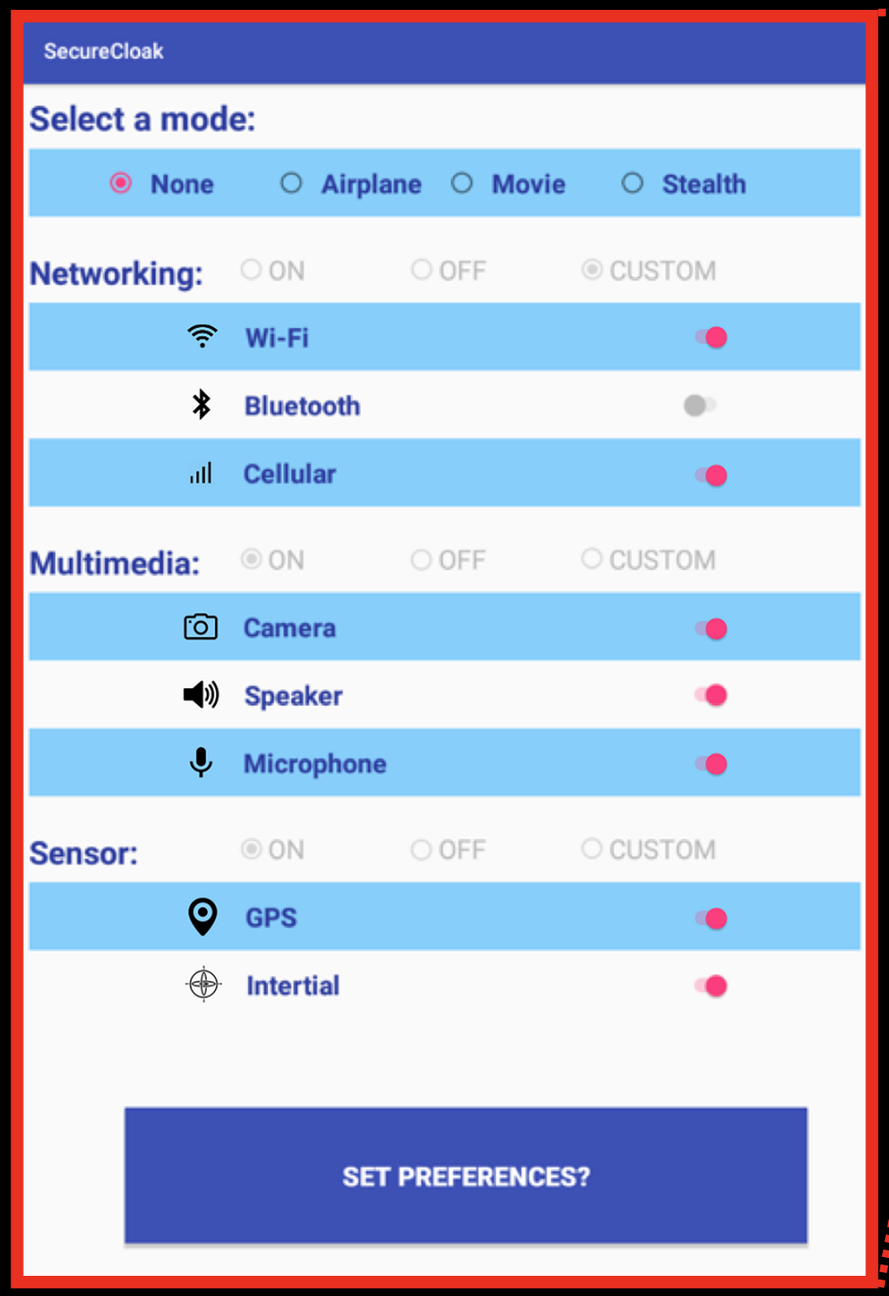


Added **Security** and **Class** properties

- Security corresponds to HW firewall configuration
- Class associates a known setting name with a device

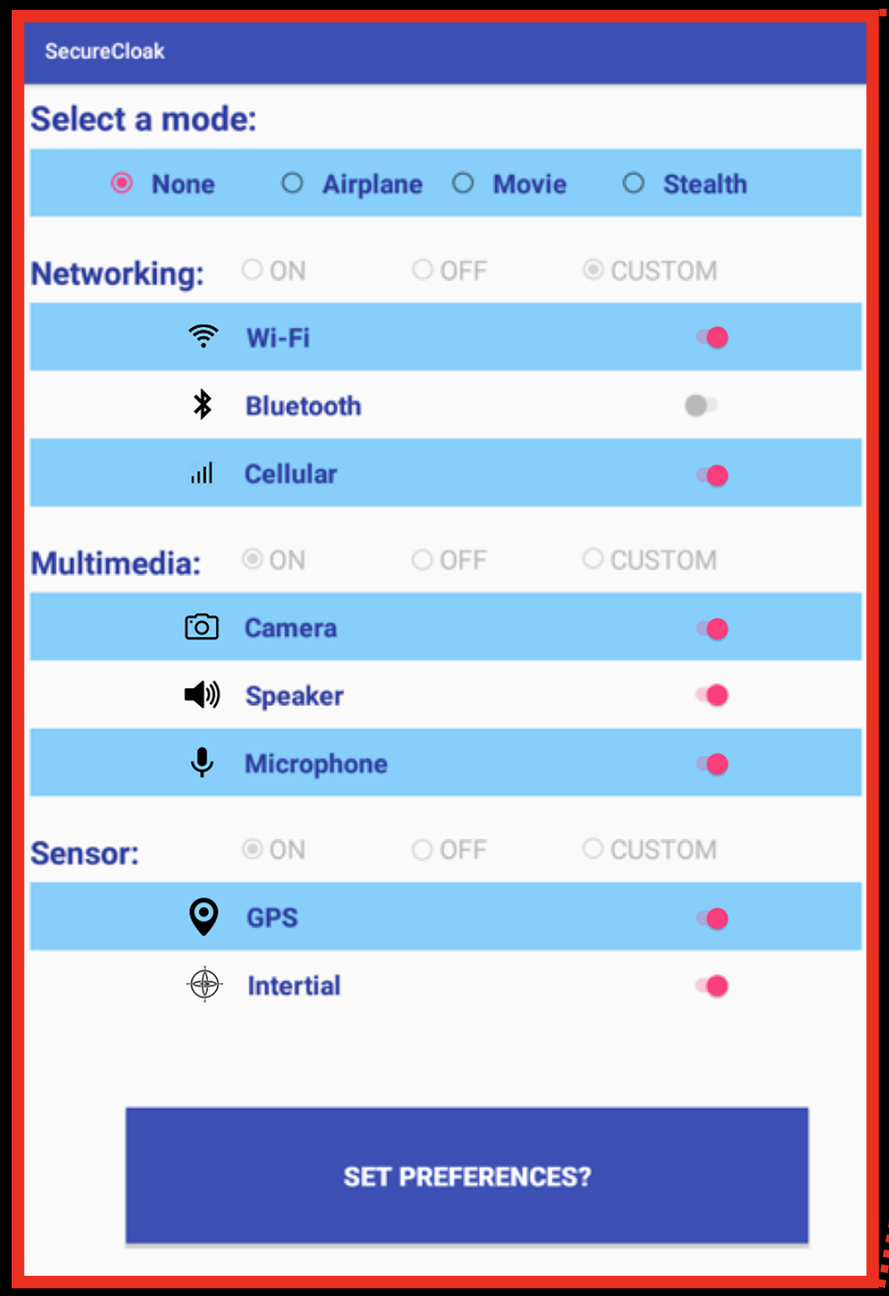
SeKernel verifies and parses a signed DT

Application Functionality



SeCloak Settings App

Example: Disabling Bluetooth



SeCloak Settings App

Kernel (e.g., Linux)

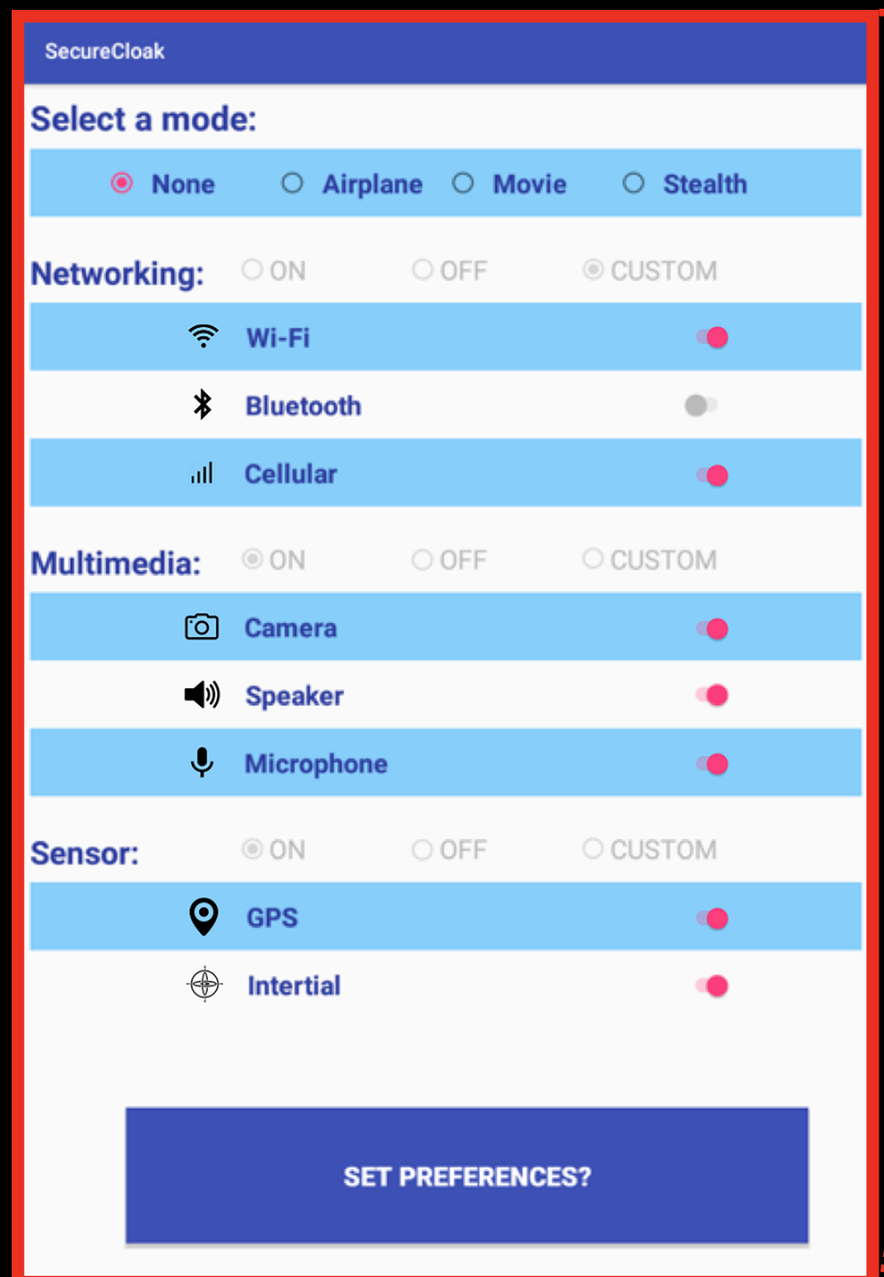
SMC

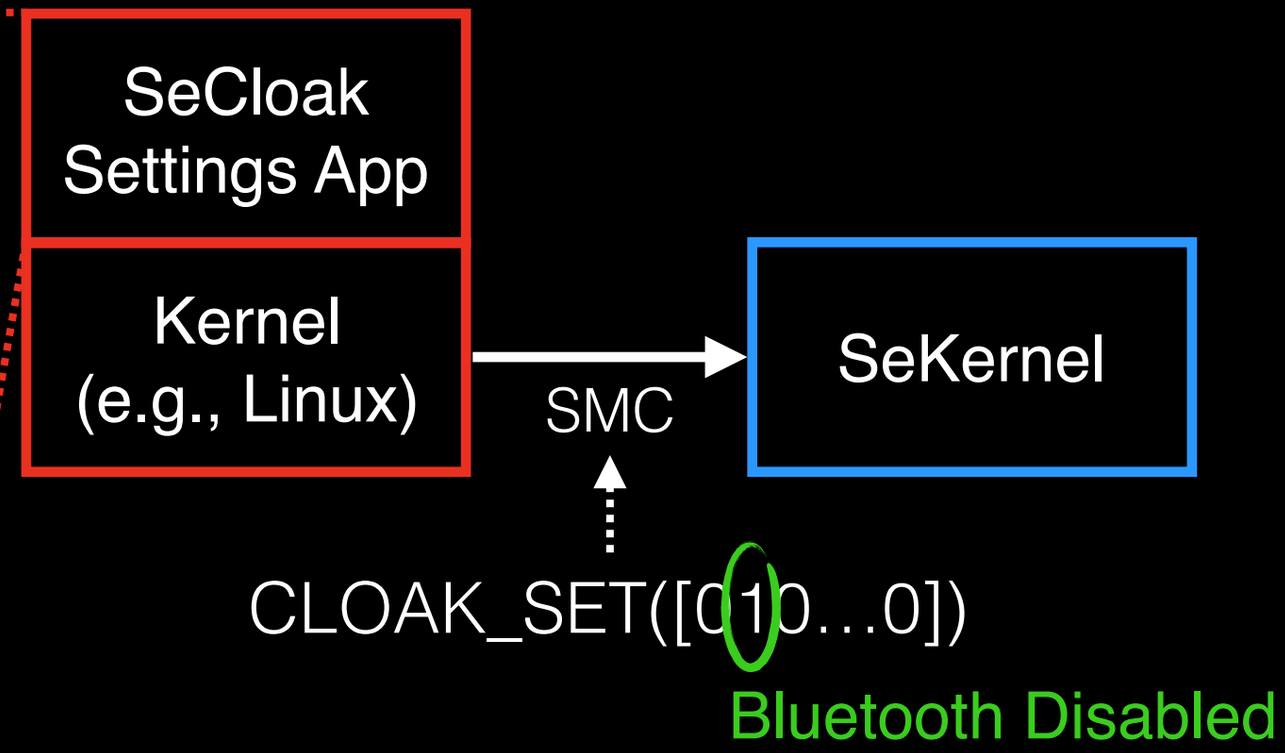
SeKernel

CLOAK_SET([010…0])

Bluetooth Disabled

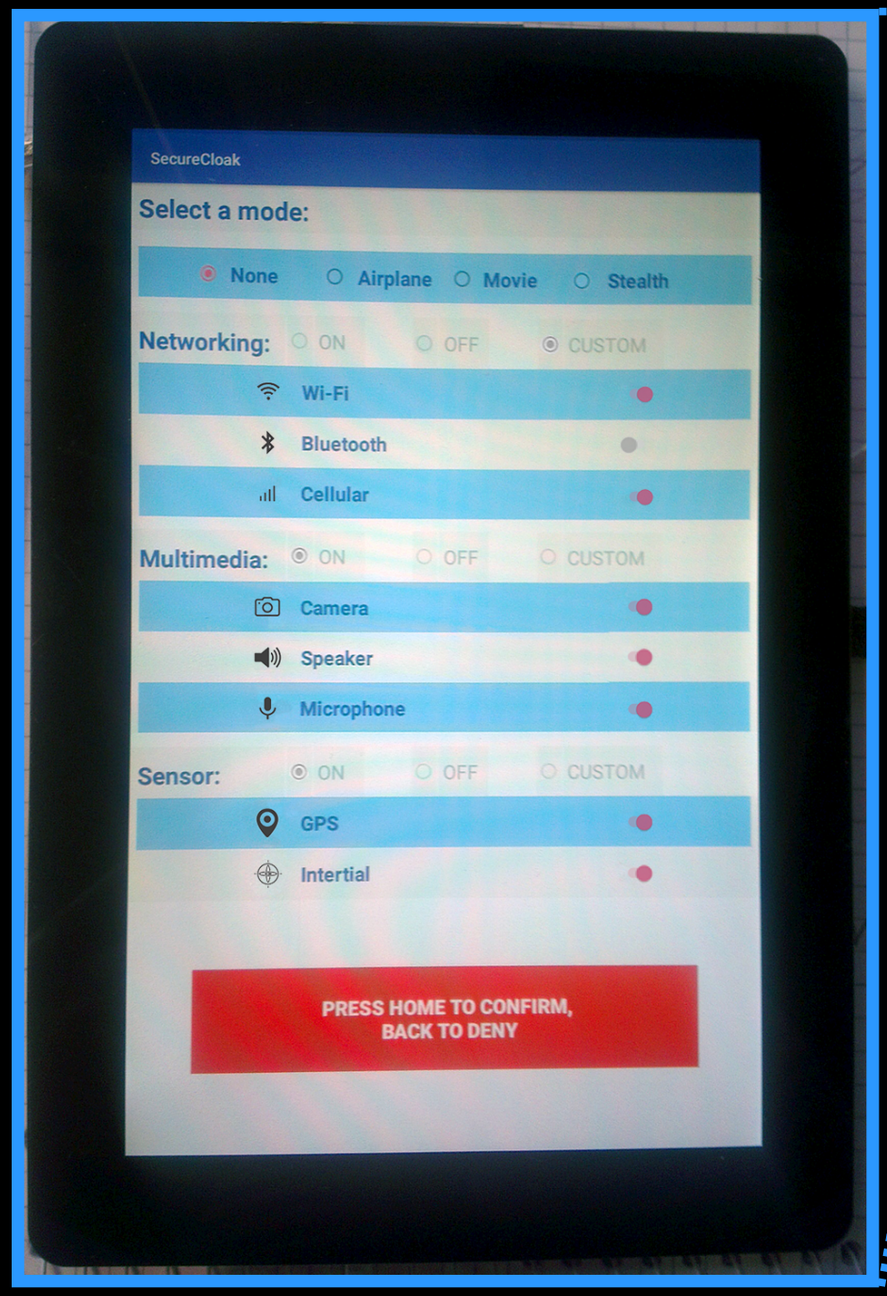
Example: Disabling Bluetooth





Policy could be modified by malicious software!

SeKernel: Confirming Policy

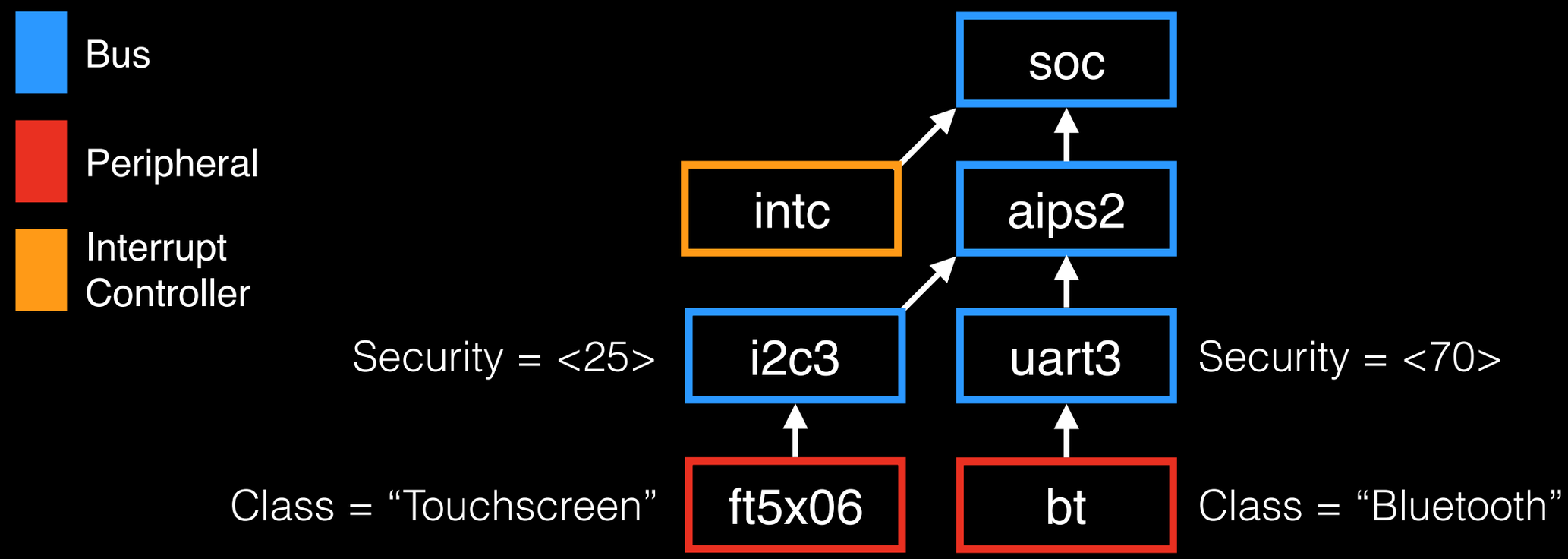


SeKernel

CLOAK_SET([010…0])

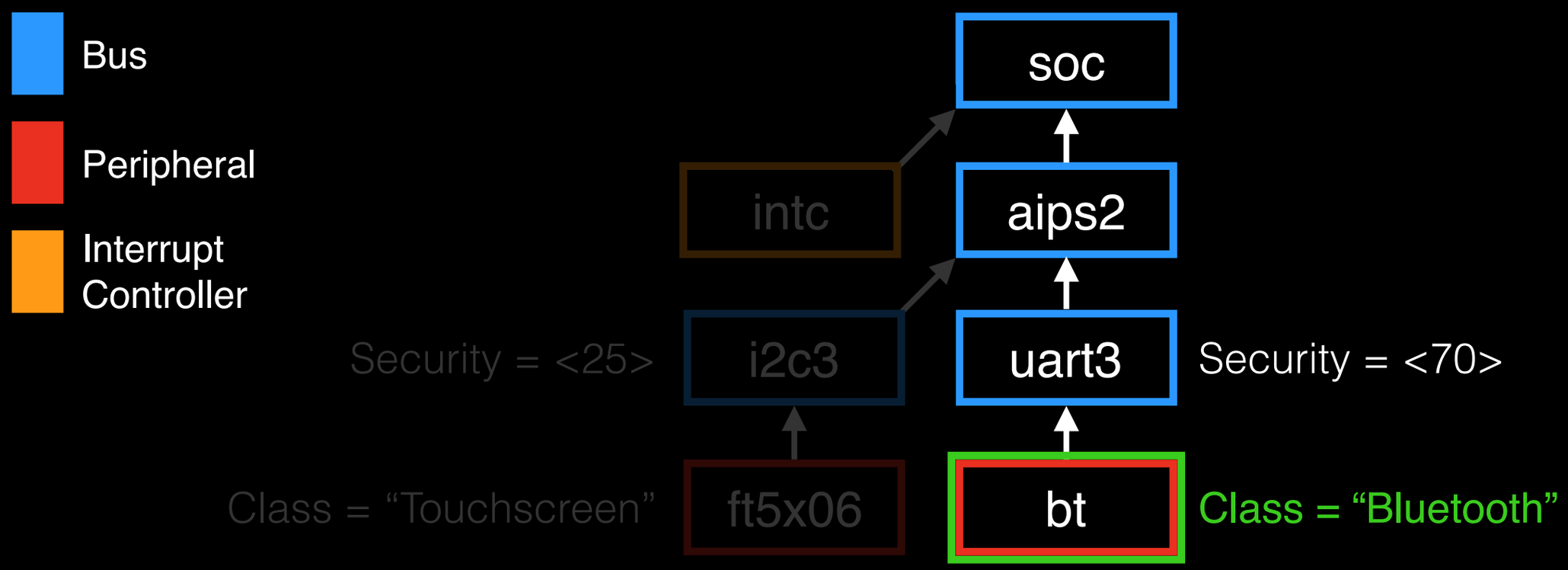
1. Acquire the display and input devices
2. Turn on the LED to notify user that SeKernel is active
3. (Re)Display settings to user
4. Wait for user confirmation for whether to apply settings…

SeKernel: Applying Policy



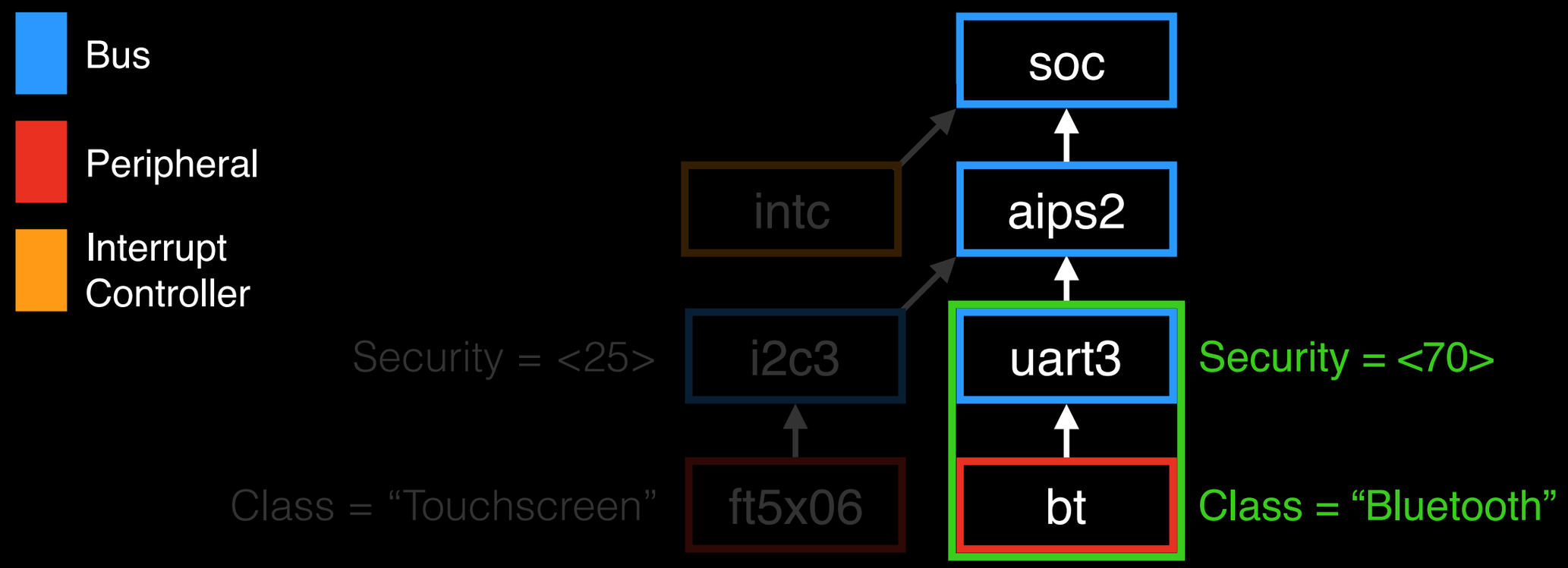
CLOAK_SET([010…0])

SeKernel: Applying Policy



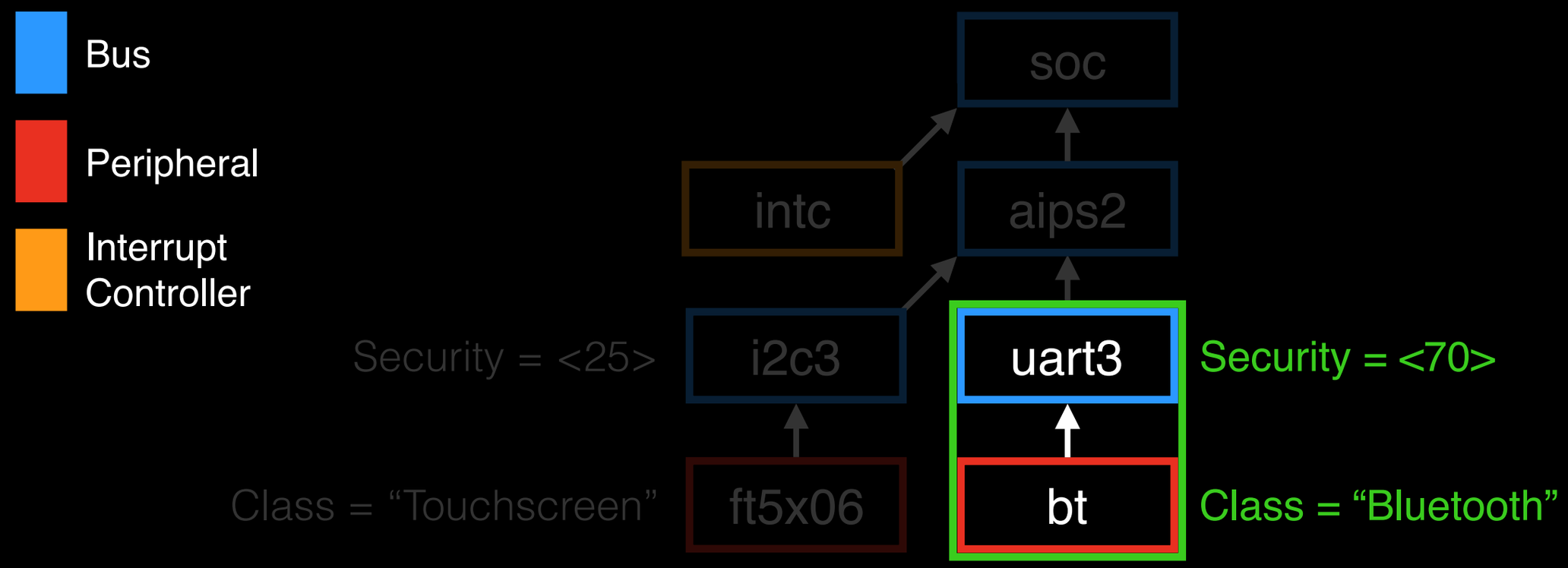
CLOAK_SET([010…0])

SeKernel: Applying Policy



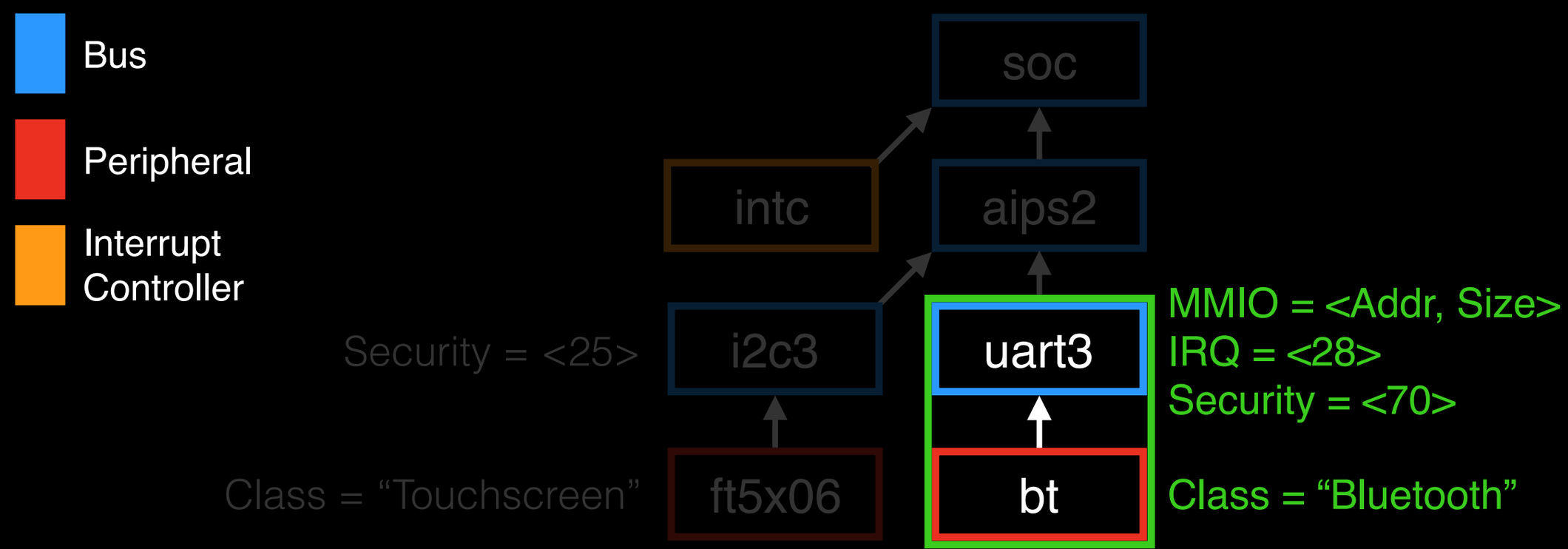
CLOAK_SET([010…0])

SeKernel: Applying Policy



CLOAK_SET([010…0])

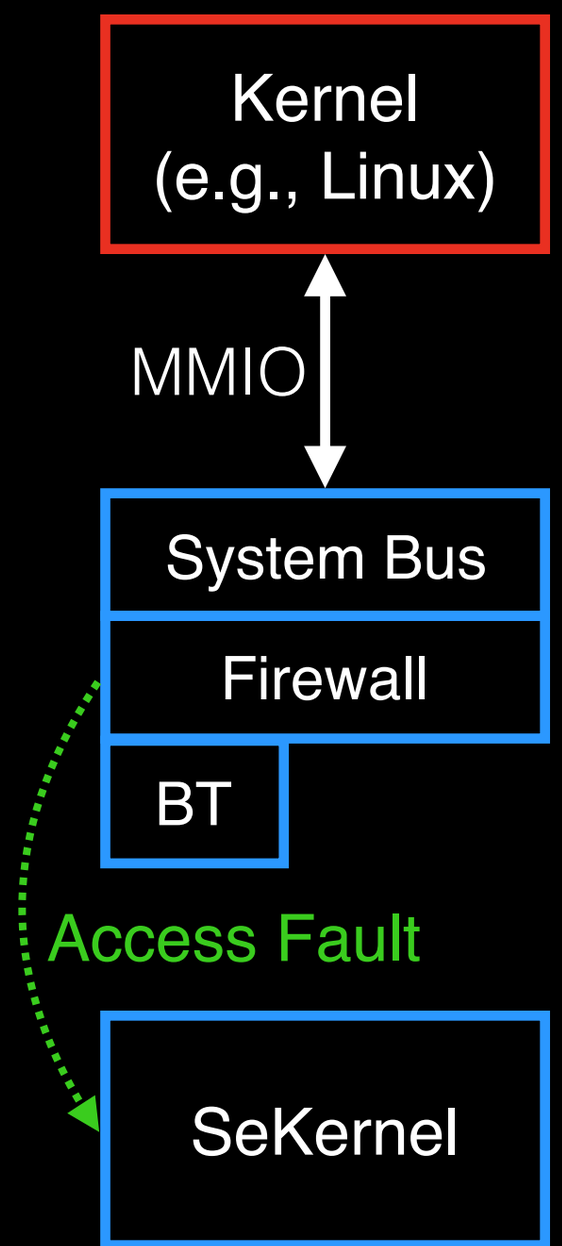
SeKernel: Applying Policy



For all devices in the subtree:

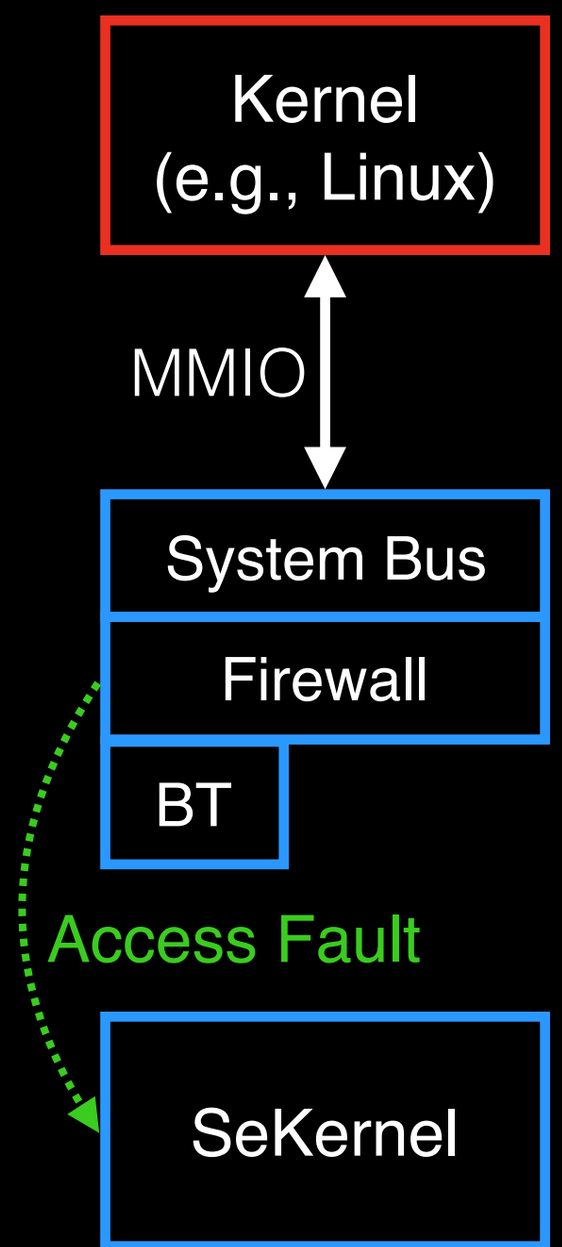
- Secure and disable IRQs
- Configure firewall protections
- Setup fault handler for MMIO accesses

SeKernel: Fault Handling



What happens if the Kernel accesses a protected device?

SeKernel: Fault Handling



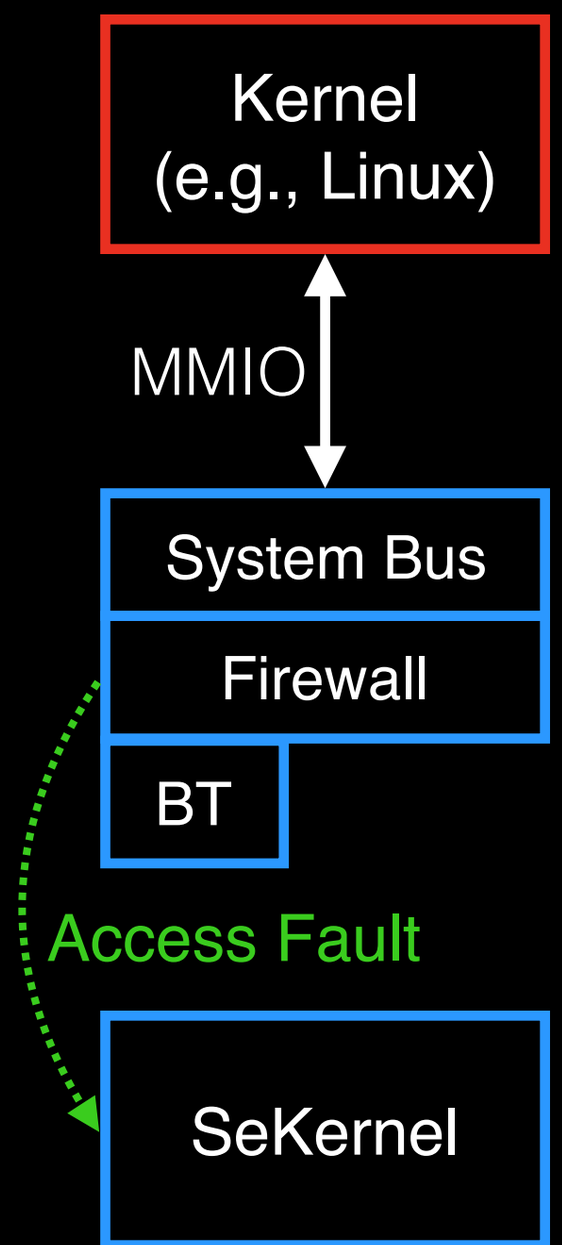
1 Determine instruction and data address

`(LDR|STR) Reg, [Address]`

From disassembling the instruction

From CPU fault information

SeKernel: Fault Handling



1 Determine instruction and data address

`(LDR|STR) Reg, [Address]`

From disassembling the instruction

From CPU fault information

2 Lookup and enforce policy for address

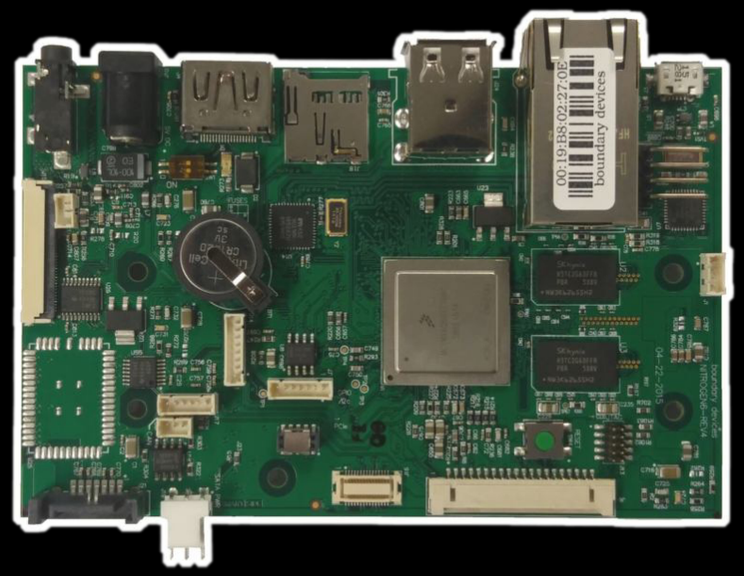
Deny Discard STR / Return 0 for LDR

Allow Issue LDR/STR & Optionally modify value

Set of devices with common security group *(or)*
Device shared between NS/S worlds

Evaluation

Prototype for Nitrogen6X board



i.MX6 SoC with ARM Cortex A9 (1GHz)

SeKernel implemented in <15k LoC

Based on pared-down OP-TEE OS

Includes drivers for CSU, Framebuffer, GPIO, and Keypad

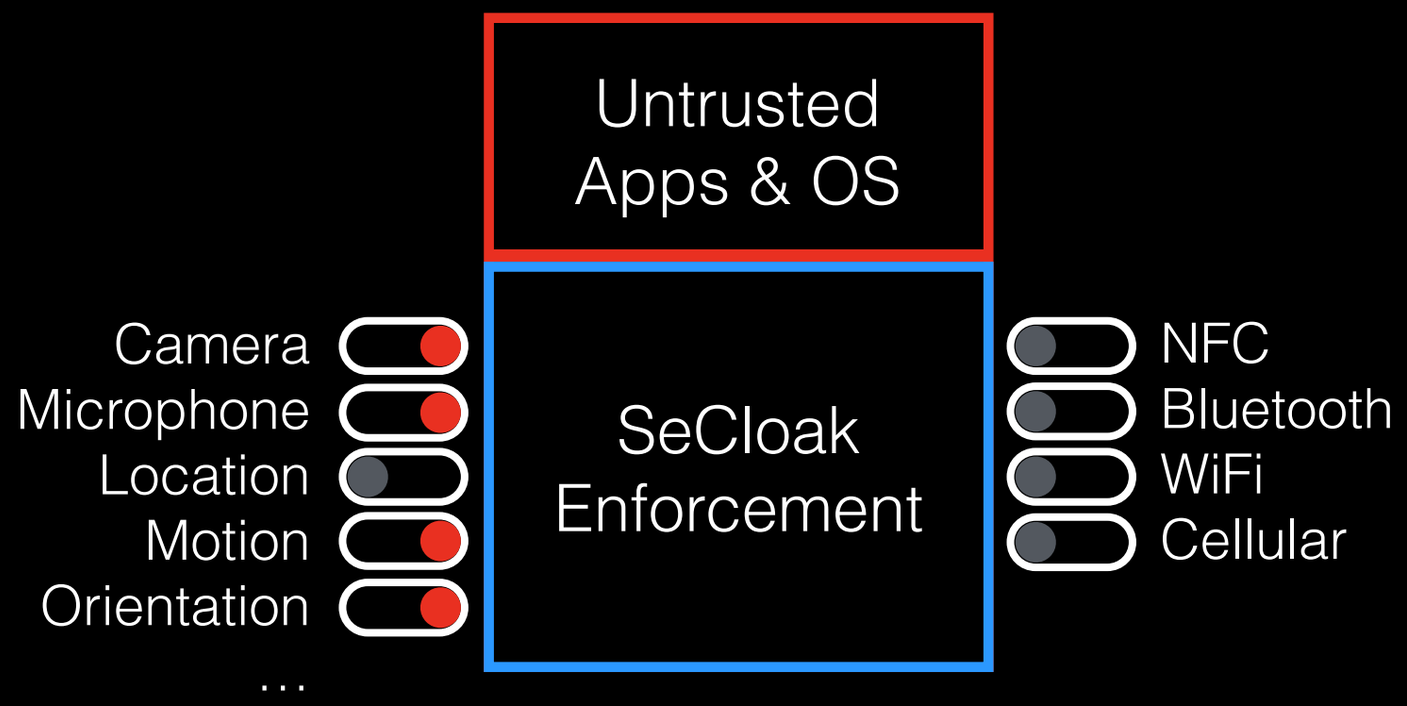
Benchmarks demonstrate reasonable overhead:

	Instruction Time (μs)	
Execution	**Load (LDR)**	**Store (STR)**
Baseline	0.11	0.29
Emulated	1.14	1.19

Repeated accesses to WiFi controller register

Summary

SeCloak enforces user-specified on/off control policies
small enforcement kernel runs alongside any OS



Source code is available at:
www.cs.umd.edu/projects/secureio

MAX PLANCK INSTITUTE
FOR SOFTWARE SYSTEMS

Backup Slides

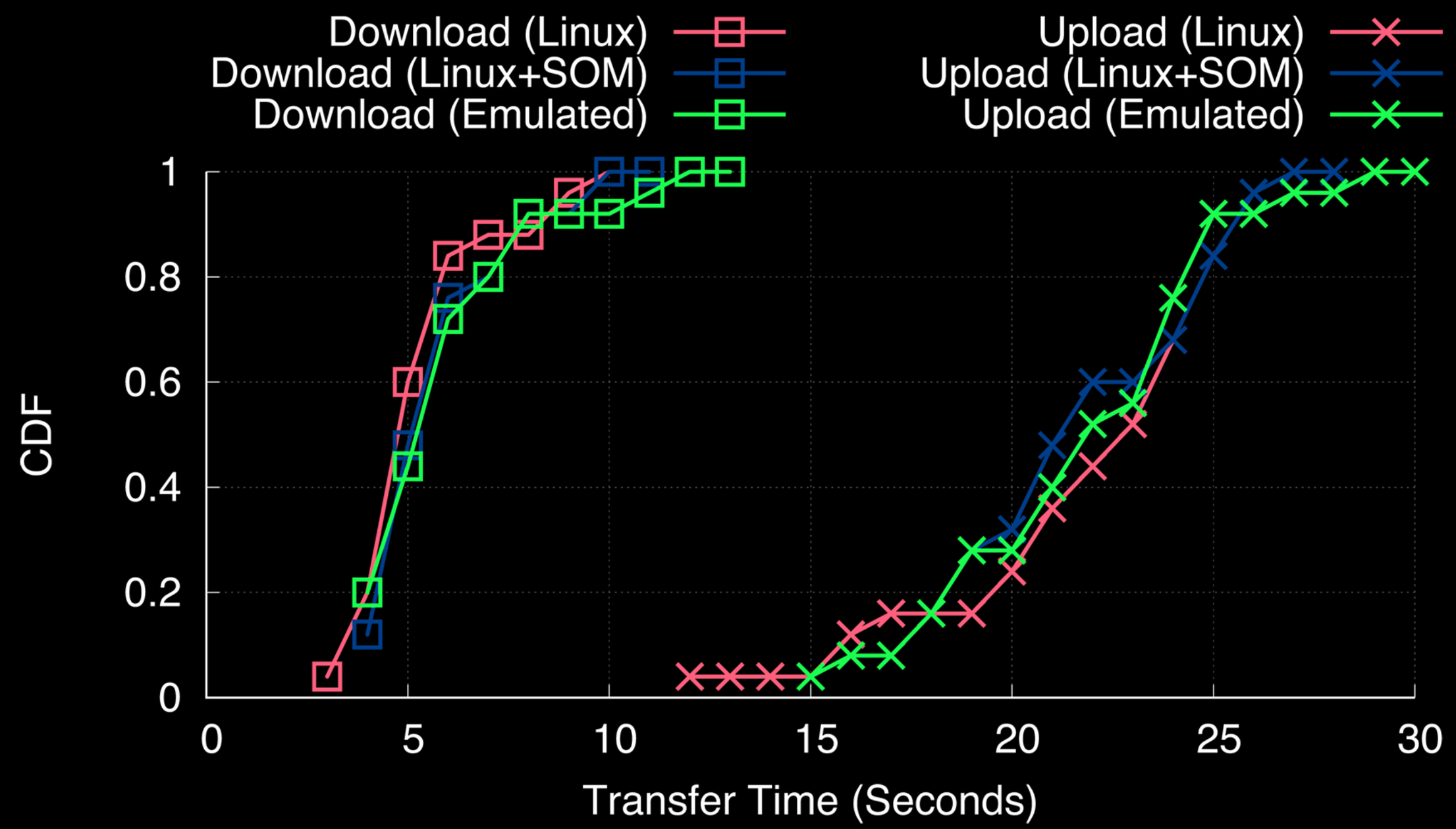
SeKernel: LoC Breakdown

	LOC Breakdown				
Type	**C Src**	**C Hdr**	**ASM**	**Total**	**Stmt**
Core	3233	2357	1391	6981	3781
Drivers					
CSU	45	9	0	54	29
Device Tree	401	57	0	458	261
Frame Buffer	146	29	0	175	113
GPIO	562	15	0	577	284
GPIO Keypad	169	14	0	183	89
<Other>	579	167	0	746	265
Drivers Total	1902	291	0	2193	1041
Libraries					
libfdt	1220	350	0	1570	840
bget/malloc	1421	68	0	1489	797
<Other>	1479	1182	81	2742	1212
Libraries Total	4120	1600	81	5801	2849
Total	9255	4248	1472	14975	7671

Micro: Emulated LDR/STRs

	Instruction Time (μs)	
Execution	**Load** (`ldr`)	**Store** (`str`)
Linux	0.11	0.29
Linux+SOM	0.27	0.33
Emulated	1.14	1.19

Macro: Emulated Wi-Fi



SeKernel: Emulation Details