



It's TEEtime: Bringing User  
Sovereignty to Smartphones

Shweta Shinde

# Is the chat app on your smartphone secure?



Malware  
Permission Abuse  
Security Vulnerabilities

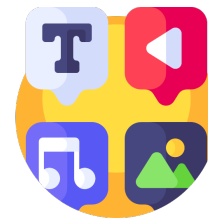
Credit: WhatsApp, Signal Messenger, iStock.com/FilippoBacci, Icon made by Freepik from www.flaticon.com



# Is the chat app on your smartphone secure?



Malware  
Permission Abuse  
Security Vulnerabilities



Credit: WhatsApp, Signal Messenger, iStock.com/FilippoBacci, Icon made by Freepik from www.flaticon.com

So... is there a problem?

**A security expert found that Apple's latest iPhone can still track your location data, even if you toggle it off for every app**

**Google tracks your movements, like it or not**

So... is there a problem?

***Fortnite Creator Sues Apple and Google  
After Ban From App Stores***

So... is there a problem?

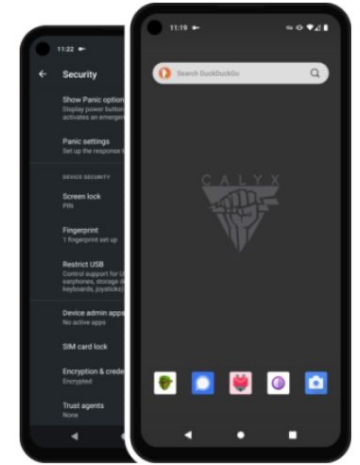
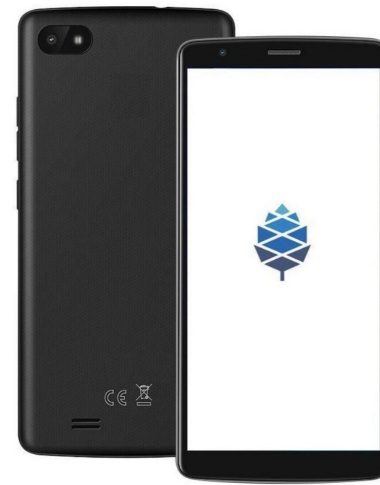
## **Germany at odds with Apple on smartphone coronavirus contact tracing**

**NHS in standoff with Apple and Google over coronavirus tracing**

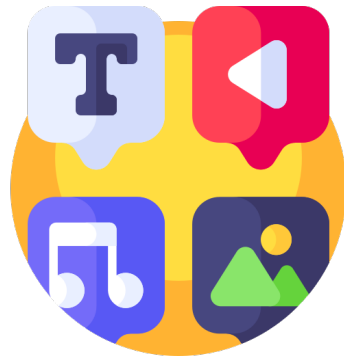
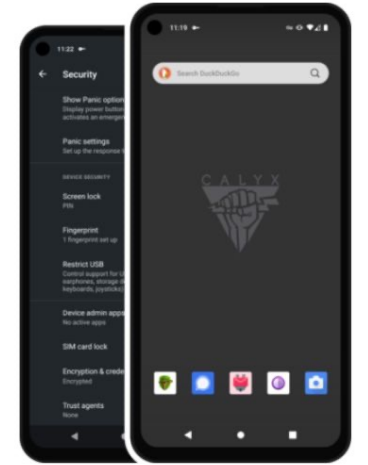
**Tech firms place limitations on how tracing apps may work in effort to protect users' privacy**

## **France urges Apple and Google to ease privacy rules on contact tracing**

# Why don't users switch to another ecosystem?



# Why don't users switch to another ecosystem?



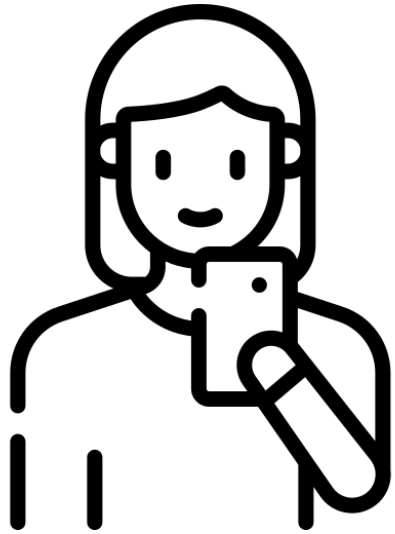


# Ideally: Sovereignty in the existing ecosystem



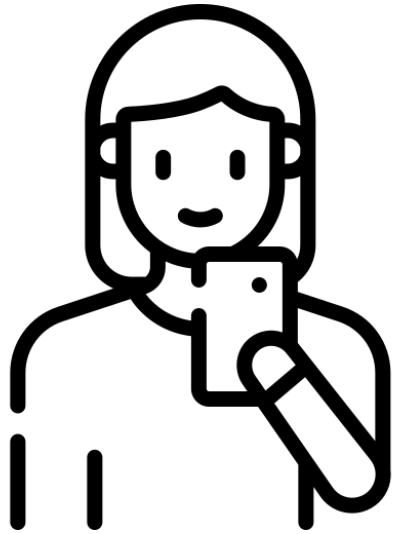
Credit: rawpixel.com

# 3 stakeholders in smartphone's sovereignty

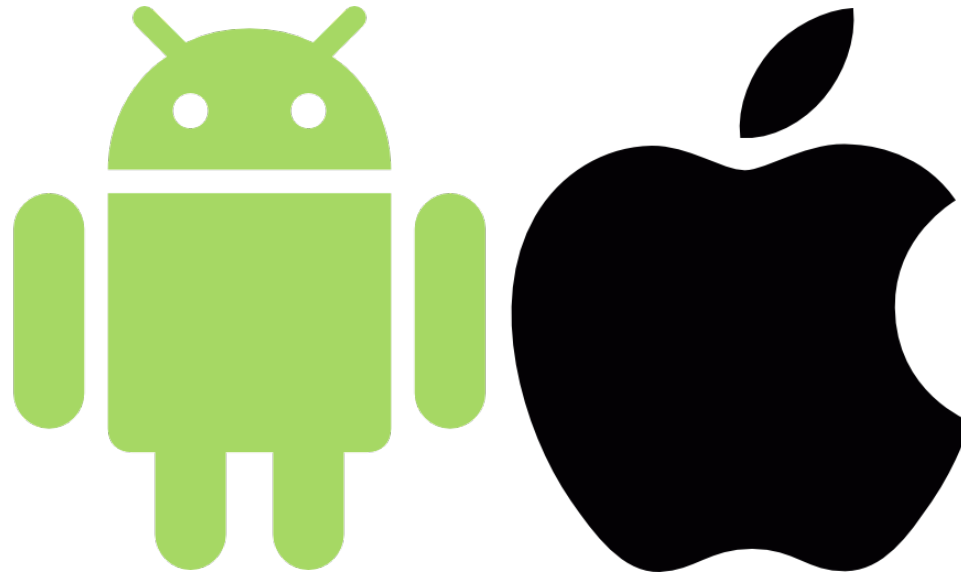


e.g., Secure Chat  
Contact Tracing

# 3 stakeholders in smartphone's sovereignty

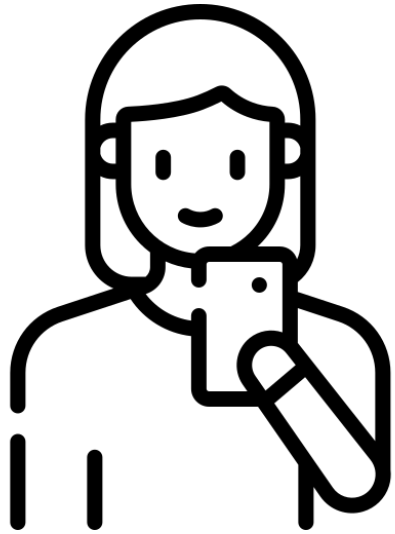


e.g., Secure Chat  
Contact Tracing

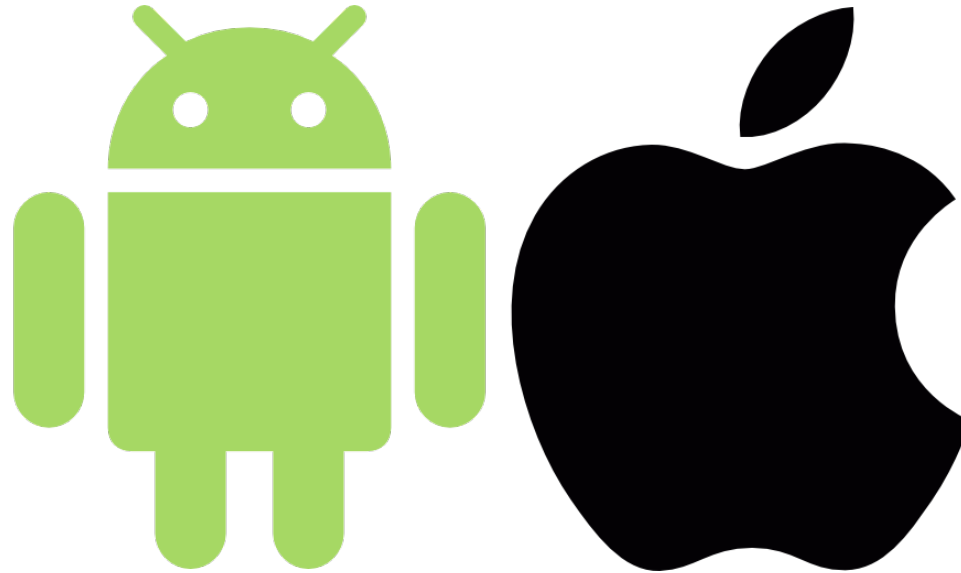


e.g., Mail client,  
Photo gallery

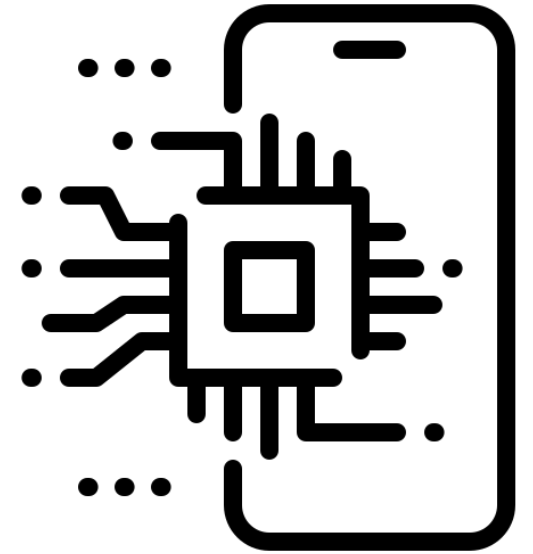
# 3 stakeholders in smartphone's sovereignty



e.g., Secure Chat  
Contact Tracing



e.g., Mail client,  
Photo gallery



e.g., Biometric Auth  
Secure Updates

Icon made by Freepik from [www.flaticon.com](http://www.flaticon.com)

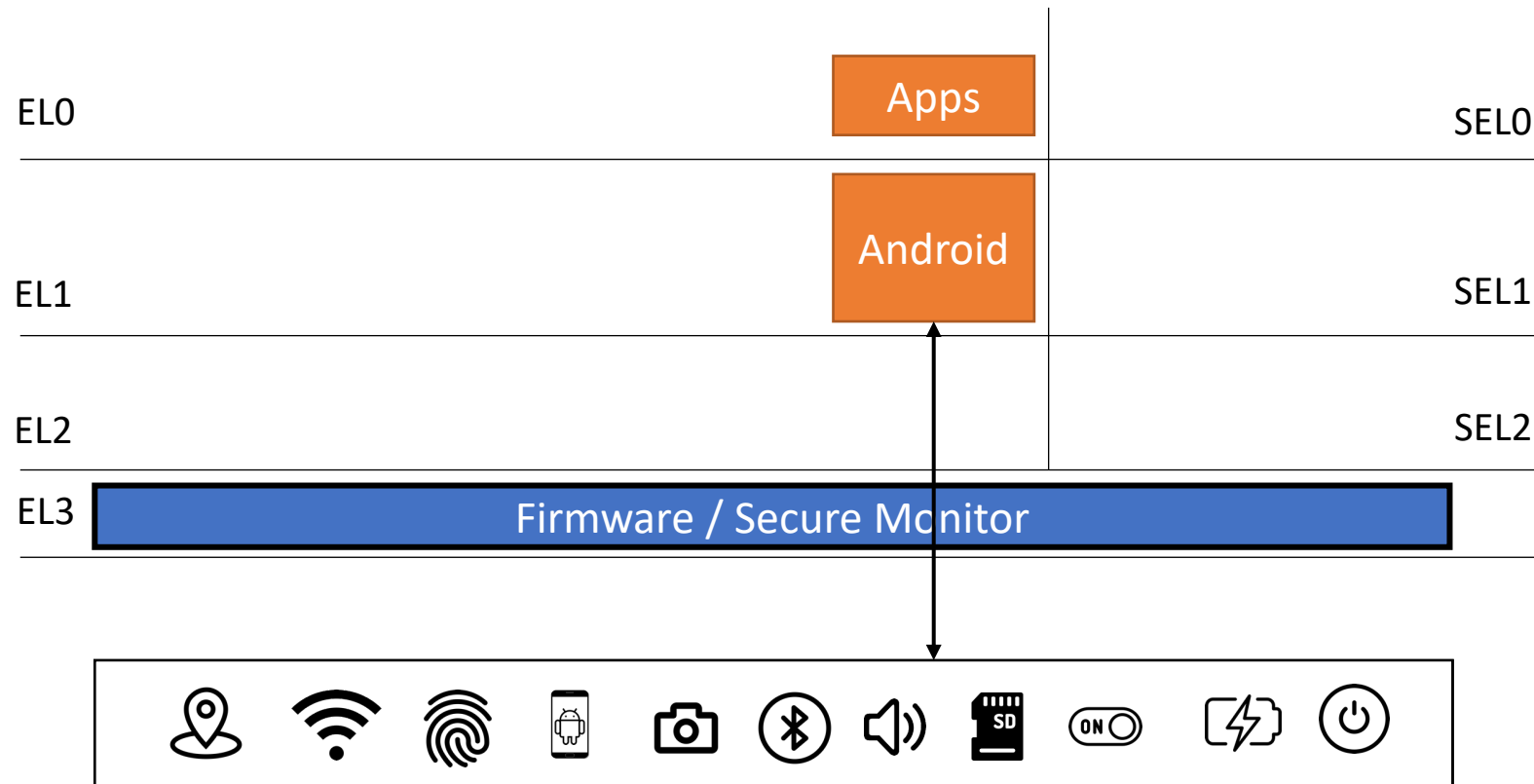


# Current Ecosystem

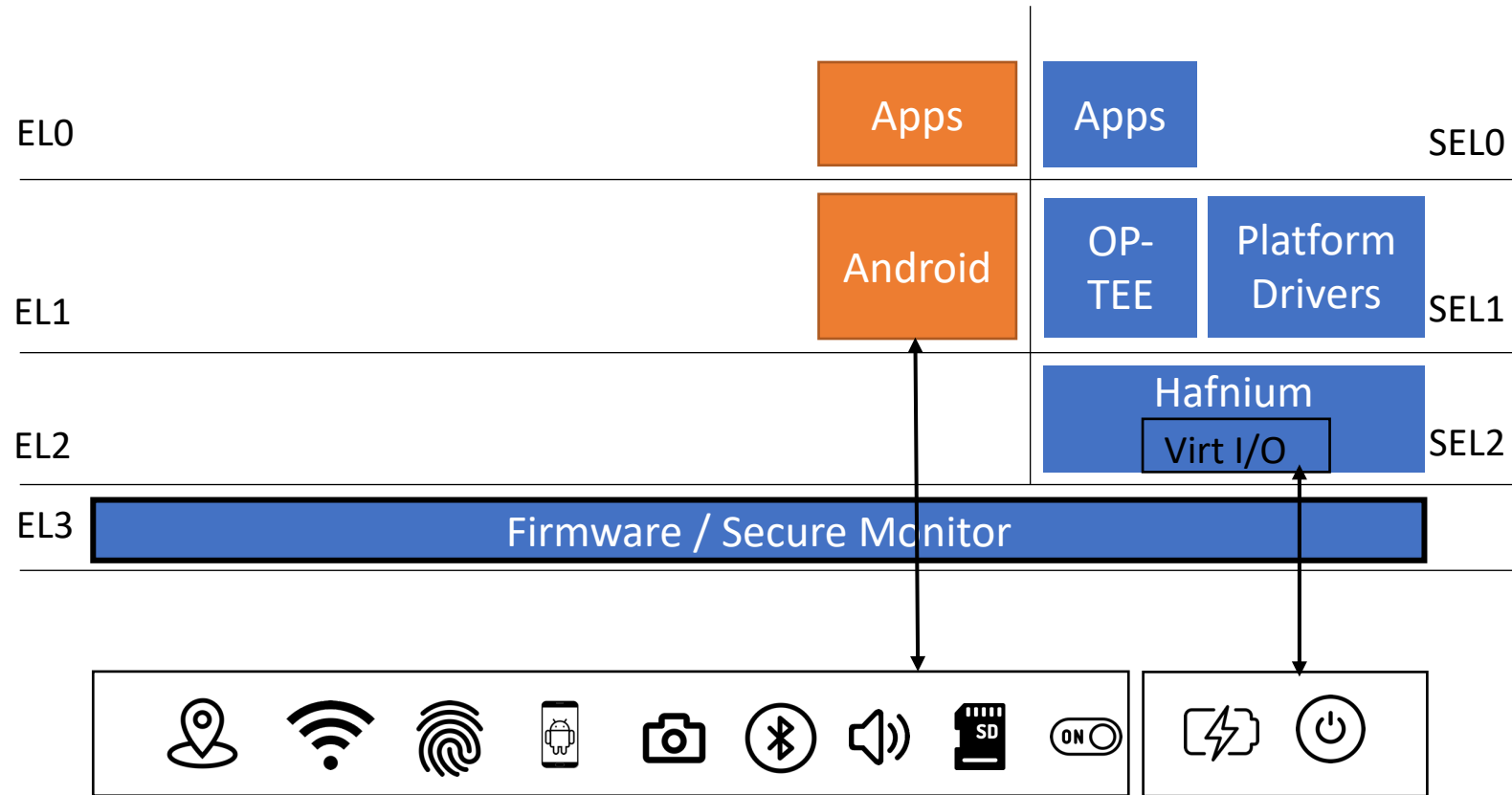
EL0	SELO
EL1	SEL1
EL2	SEL2
EL3	



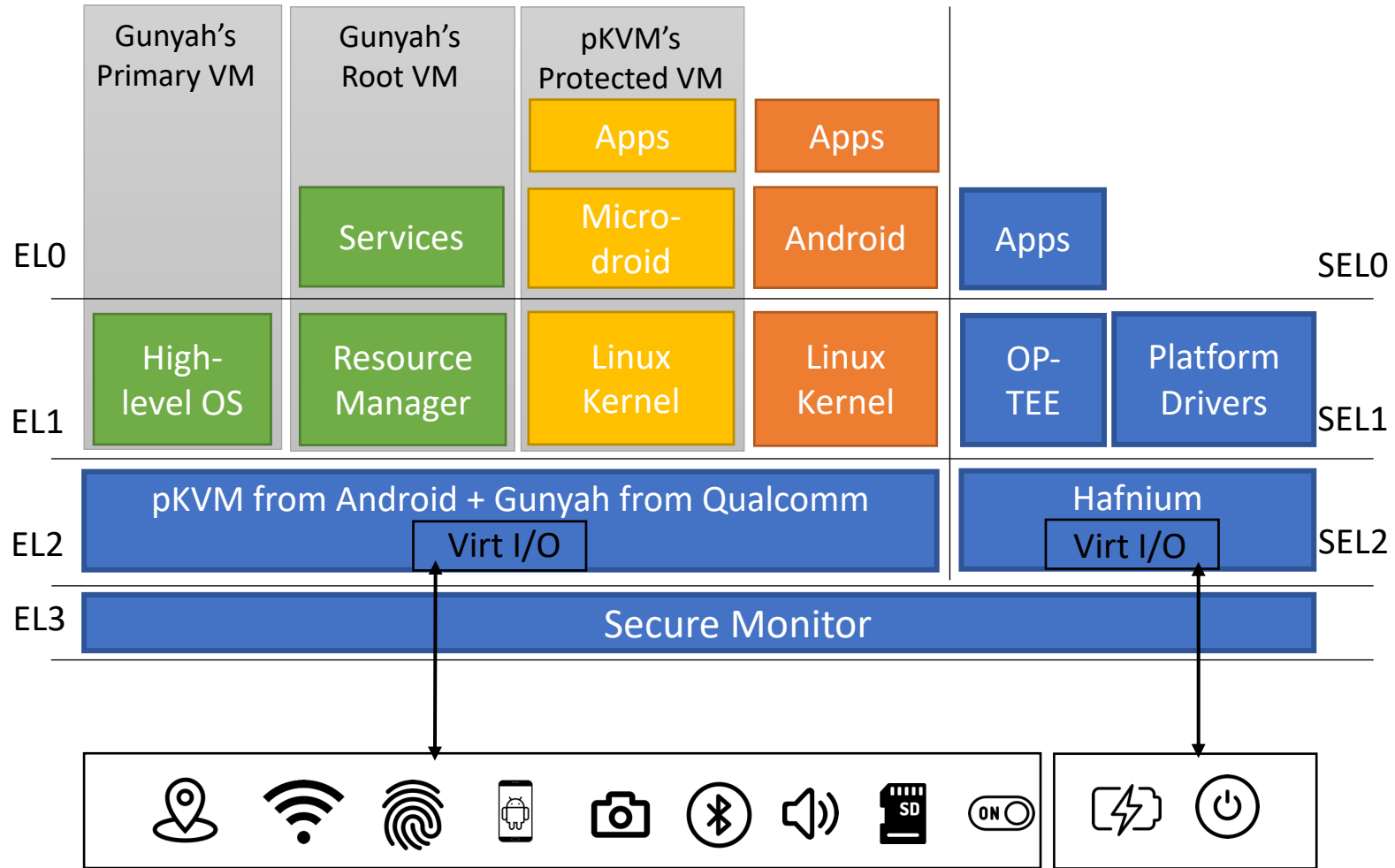
# Current Ecosystem: User View



# Current Ecosystem: Manufacturer & OS View

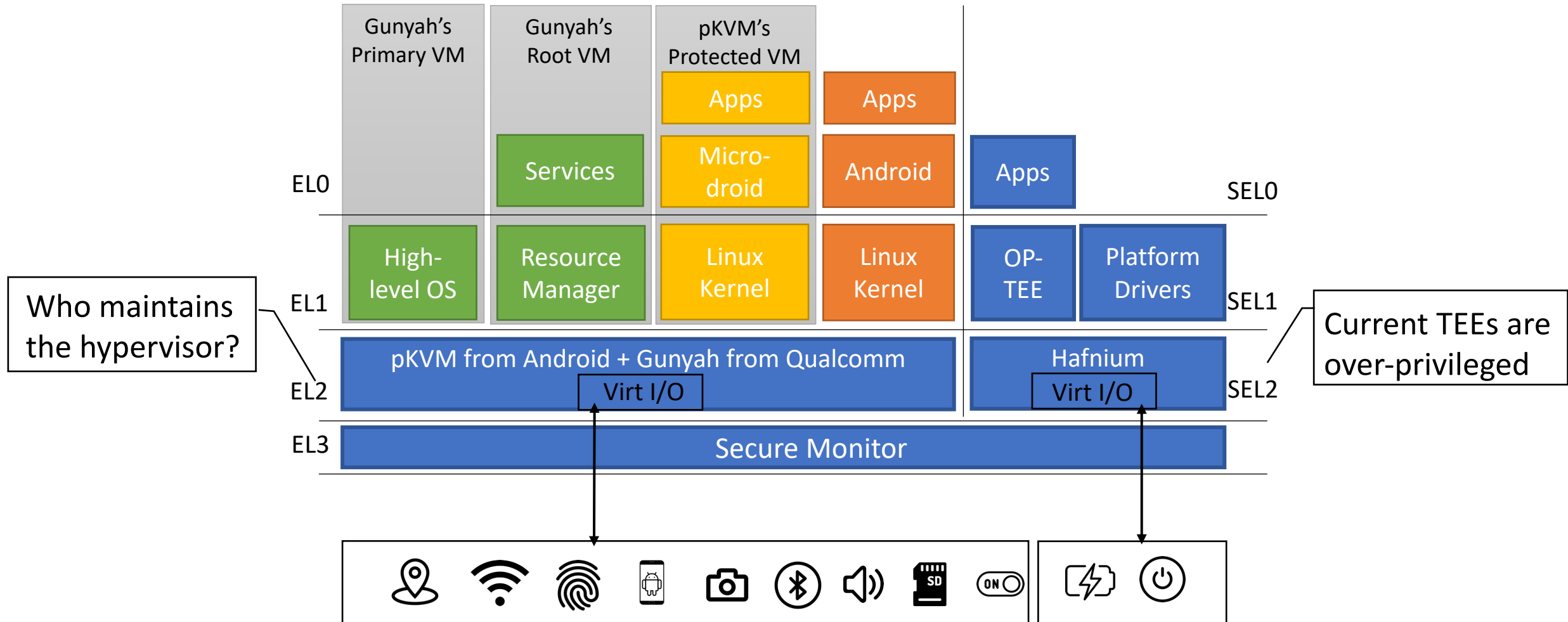


# Current Ecosystem: Manufacturer & OS View

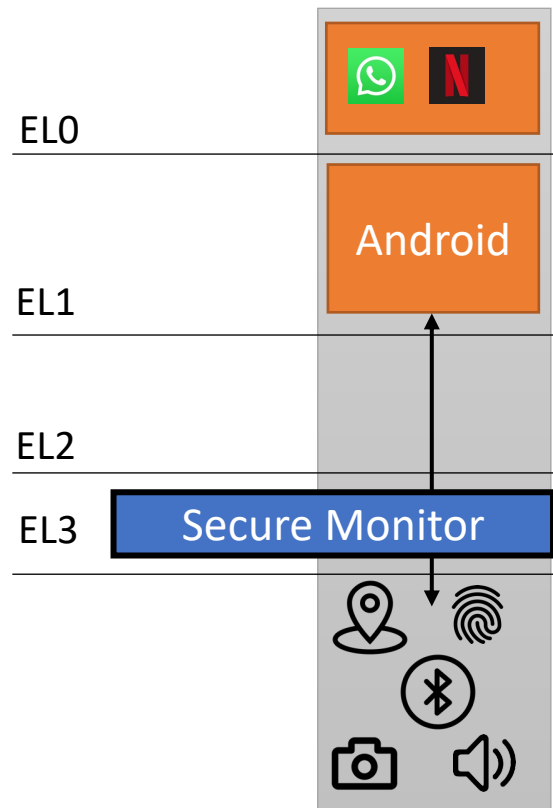




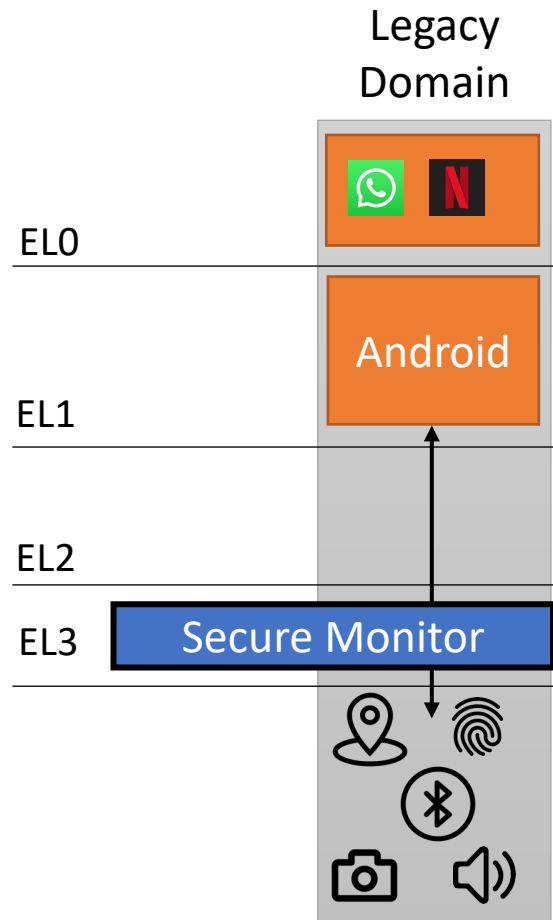
# Current ecosystem is unsuitable



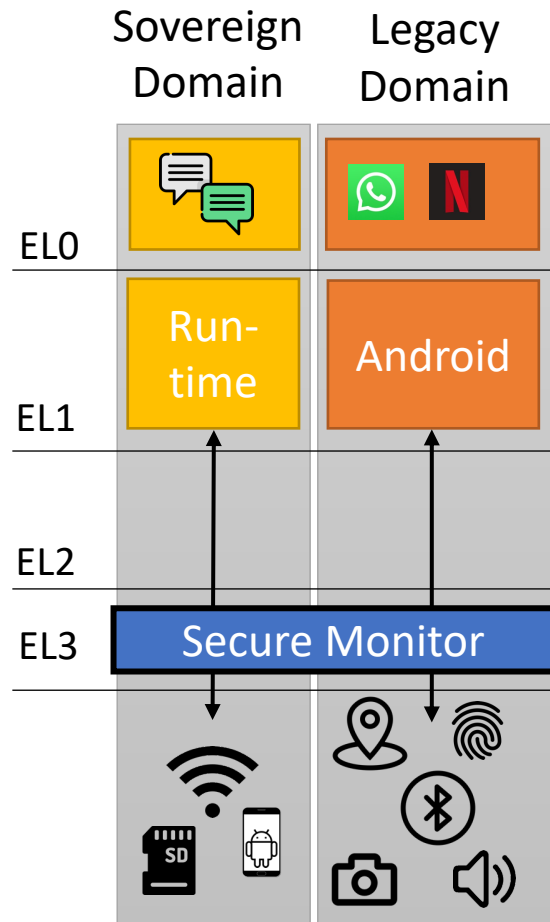
# Our Proposal: TEEtime



# Our Proposal: TEEtime

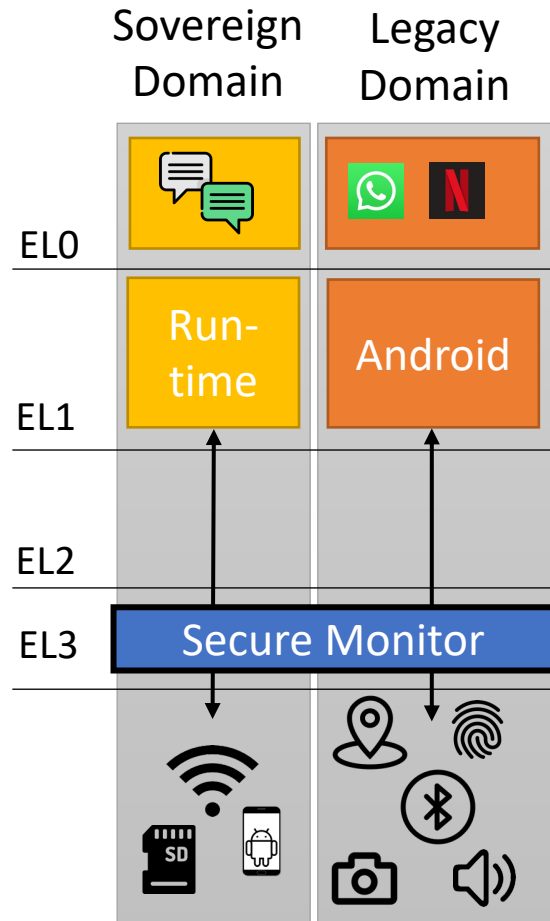


# Our Proposal: TEEtime



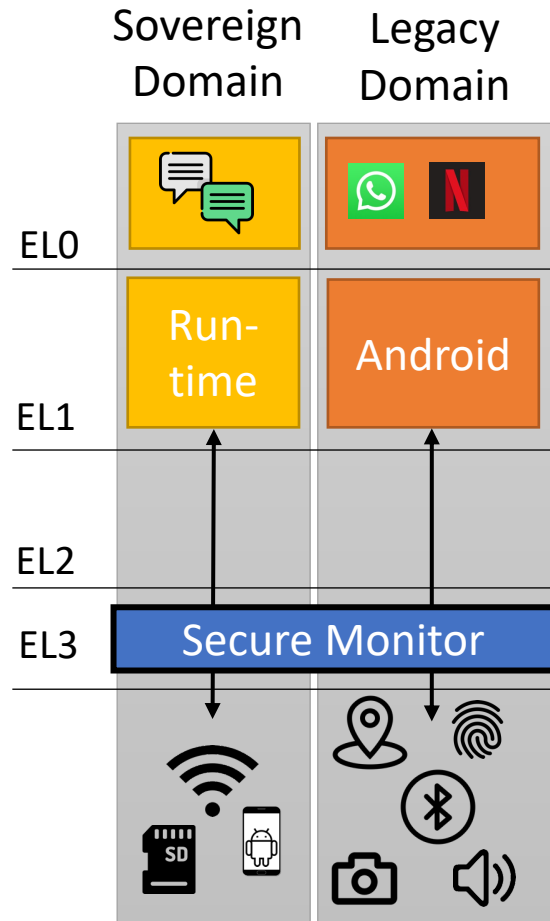


# Our Proposal: TEEtime



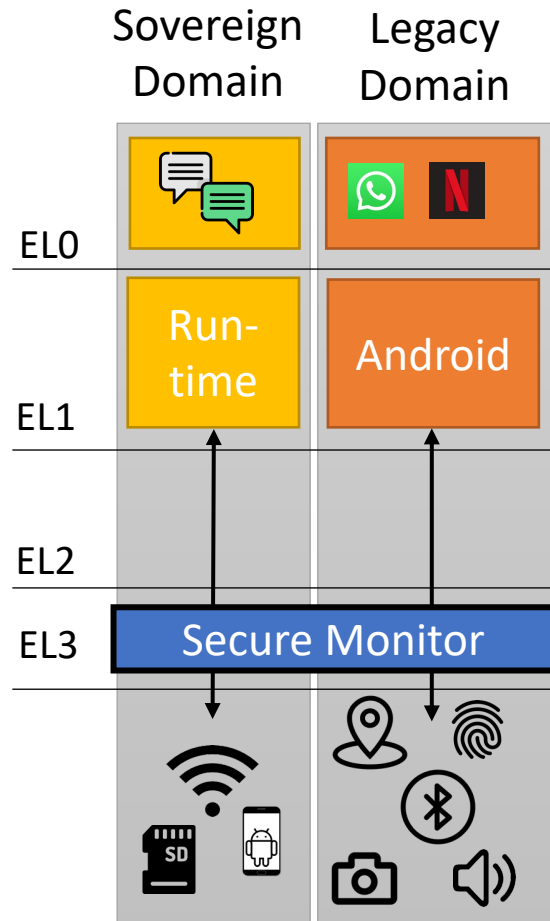
- Simple and pragmatic for sovereignty
- Doesn't disrupt existing OSES and apps

# Our Proposal: TEEtime



- Simple and pragmatic for sovereignty
- Doesn't disrupt existing OSeS and apps
- Hypervisor is not in the TCB
- Only firmware modifications

# Our Proposal: TEEtime



- Simple and pragmatic for sovereignty
- Doesn't disrupt existing OSe and apps
- Hypervisor is not in the TCB
- Only firmware modifications
- Peripherals directly assigned to domains
- Isolation enforced by existing hardware

# Example Use-case: Secure Chat App

- Deploy chat app in sovereign domain, Android in the legacy domain



Sovereign domain needs

Execution time

Isolated memory

Access to touchscreen

Access to network

Access to storage



# Example Use-case: Secure Chat App

- Deploy chat app in sovereign domain, Android in the legacy domain



Sovereign domain needs

Execution time

Isolated memory

Access to touchscreen

Access to network

Access to storage

Legacy domain continues to

Perform scheduling

Manage memory

Access other peripherals

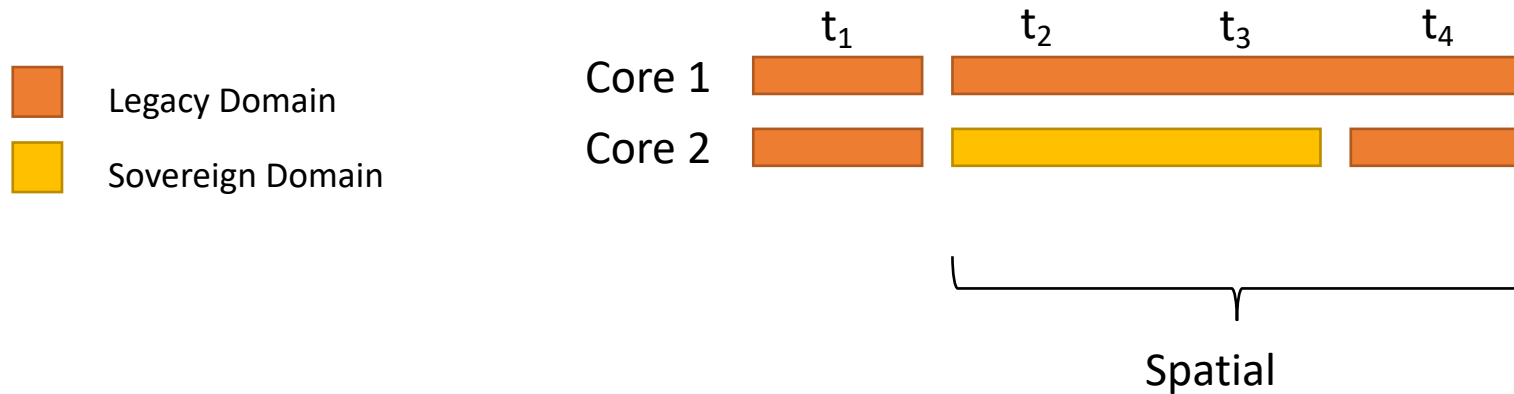


# Challenge 1: Execution and Memory Isolation

- Secure monitor configures isolation, hardware mechanisms enforce it

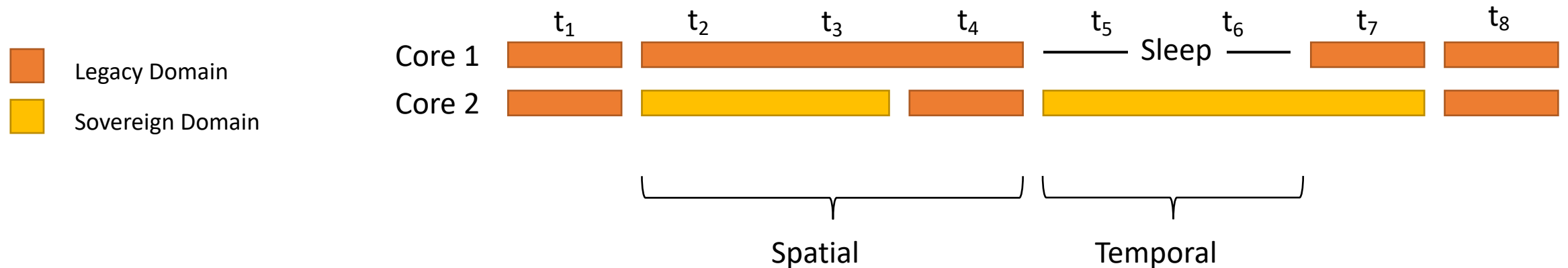
# Challenge 1: Execution and Memory Isolation

- Secure monitor configures isolation, hardware mechanisms enforce it  
Domains are isolated by executing
  - On different cores



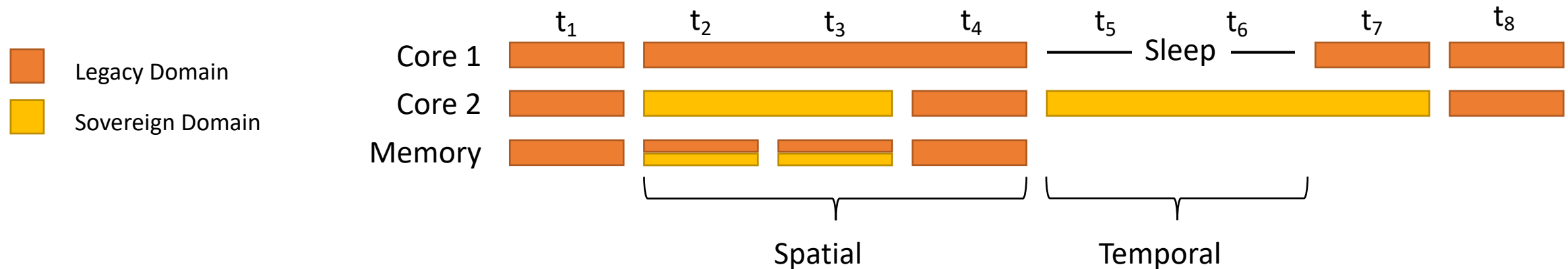
# Challenge 1: Execution and Memory Isolation

- Secure monitor configures isolation, hardware mechanisms enforce it  
Domains are isolated by executing
  - On different cores and/or
  - At different times



# Challenge 1: Execution and Memory Isolation

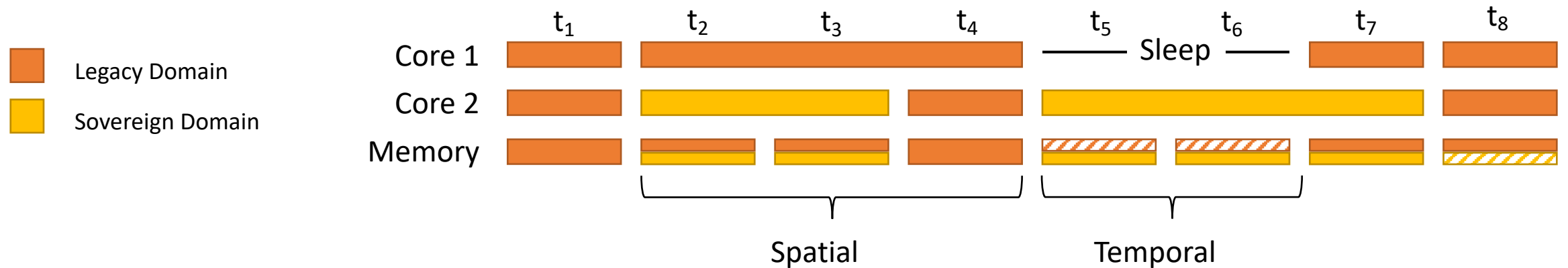
- Secure monitor configures isolation, hardware mechanisms enforce it  
Domains are isolated by executing
  - On different cores and/or
  - At different times



- Memory accesses are isolated by
  - Allowing accesses based on core ID

# Challenge 1: Execution and Memory Isolation

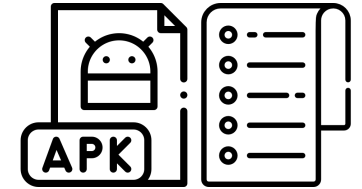
- Secure monitor configures isolation, hardware mechanisms enforce it
  - Domains are isolated by executing
    - On different cores and/or
    - At different times



- Memory accesses are isolated by
  - Allowing accesses based on core ID and/or
  - Blocking access to the memory of currently inactive domain

## Challenge 2: Peripheral Assignment

- When to attach and detach a peripheral to a domain?
- If and how to share a peripheral between domains?
- How to transfer a peripheral between domains?

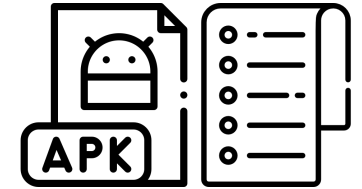


App + Manifest



## Challenge 2: Peripheral Assignment

- When to attach and detach a peripheral to a domain?
- If and how to share a peripheral between domains?
- How to transfer a peripheral between domains?



App + Manifest

Sovereign domain needs:

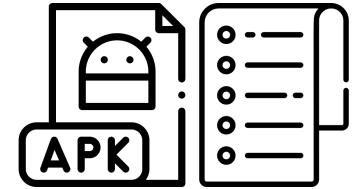


Access to **touchscreen**

**Exclusive:** Always auto-assigned to the Sovereign domain when it executes, taken away from Legacy domain, handed-over at the end

# Challenge 2: Peripheral Assignment

- When to attach and detach a peripheral to a domain?
- If and how to share a peripheral between domains?
- How to transfer a peripheral between domains?



App + Manifest

Sovereign domain needs:



Access to **touchscreen**

**Exclusive:** Always auto-assigned to the Sovereign domain when it executes, taken away from Legacy domain, handed-over at the end

Access to **storage and network**

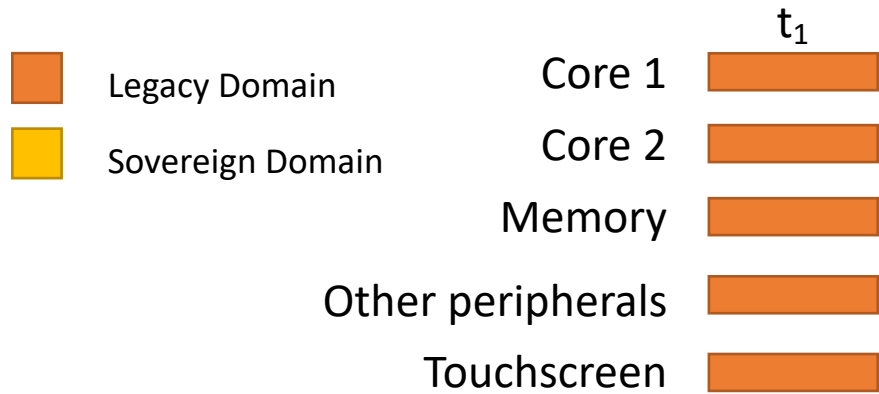
**Proxy:** Always owned by Legacy domain

Allows Sovereign domain to access via secure channel

# Challenge 3: Peripheral Isolation

**Peripheral Access:** Read from and write to the memory-mapped peripheral address regions

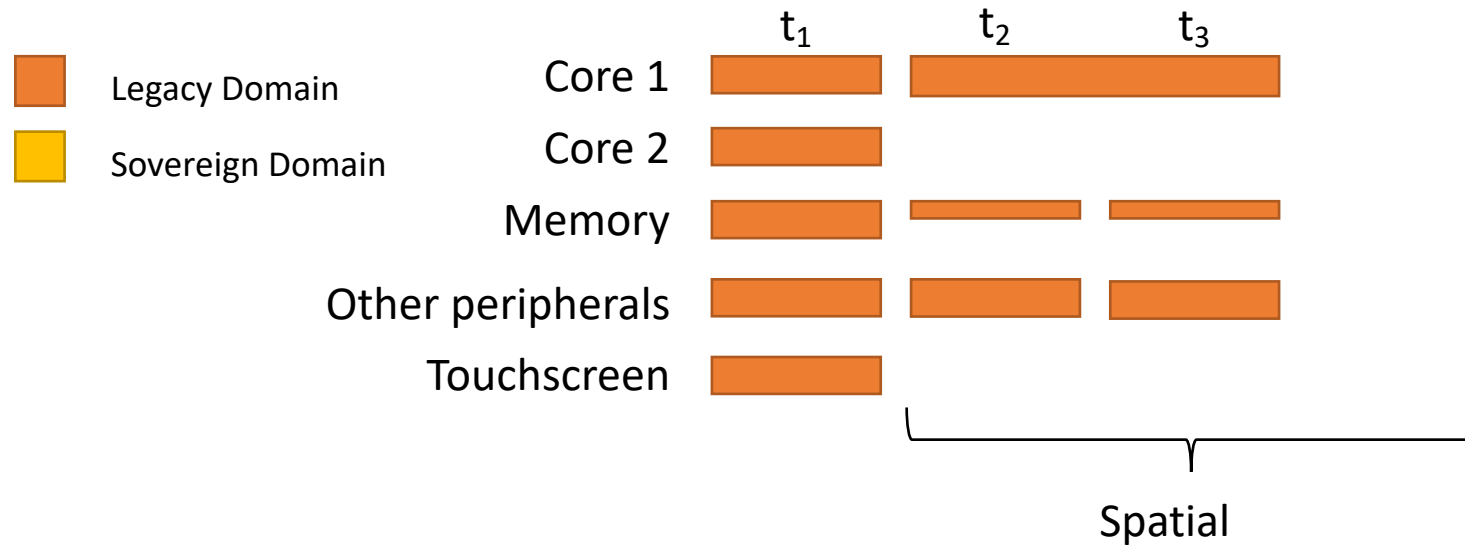
Apply isolation at address-space level



# Challenge 3: Peripheral Isolation

**Peripheral Access:** Read from and write to the memory-mapped peripheral address regions

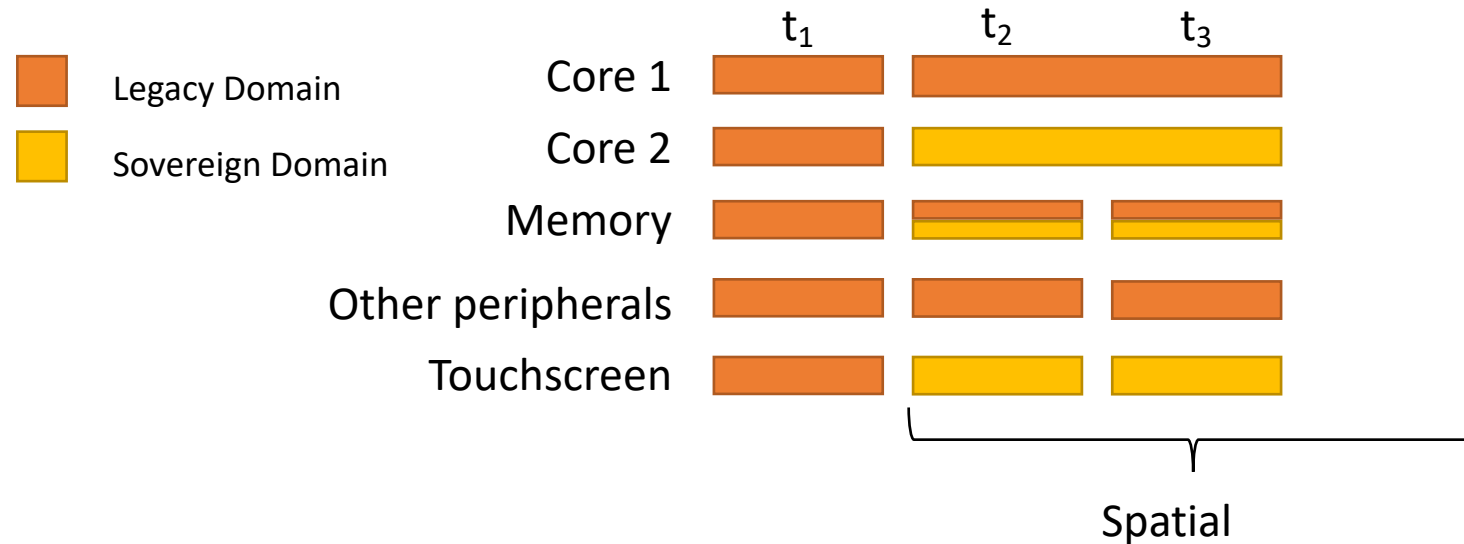
Apply isolation at address-space level



# Challenge 3: Peripheral Isolation

**Peripheral Access:** Read from and write to the memory-mapped peripheral address regions

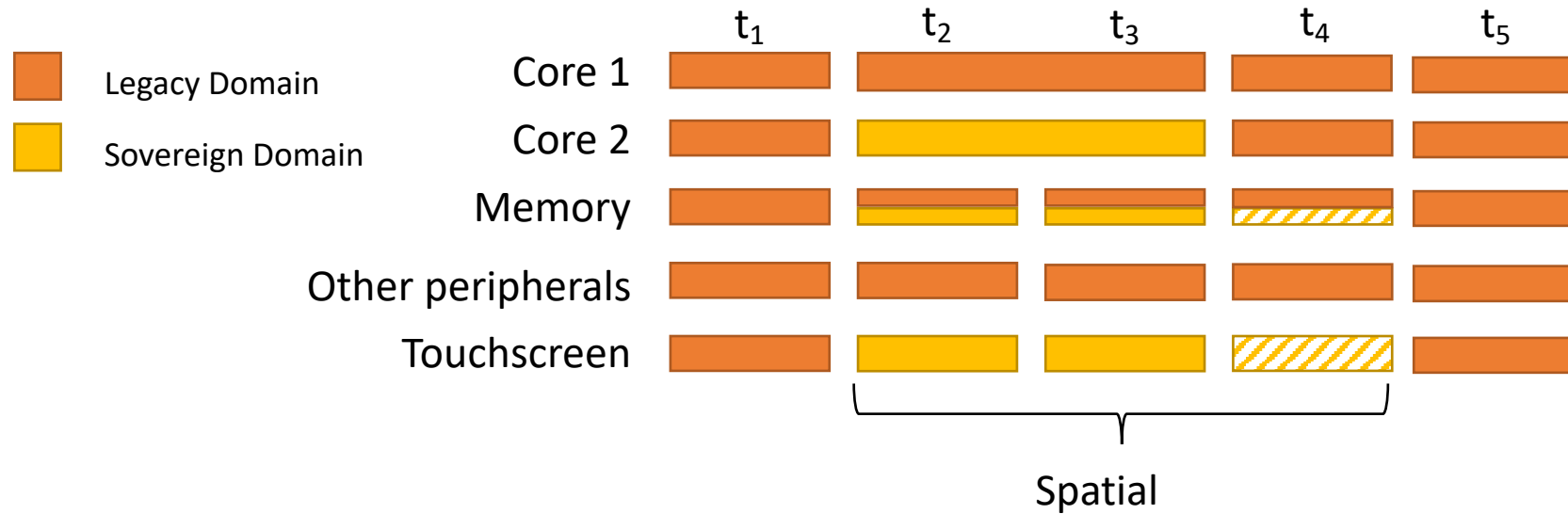
Apply isolation at address-space level



# Challenge 3: Peripheral Isolation

**Peripheral Access:** Read from and write to the memory-mapped peripheral address regions

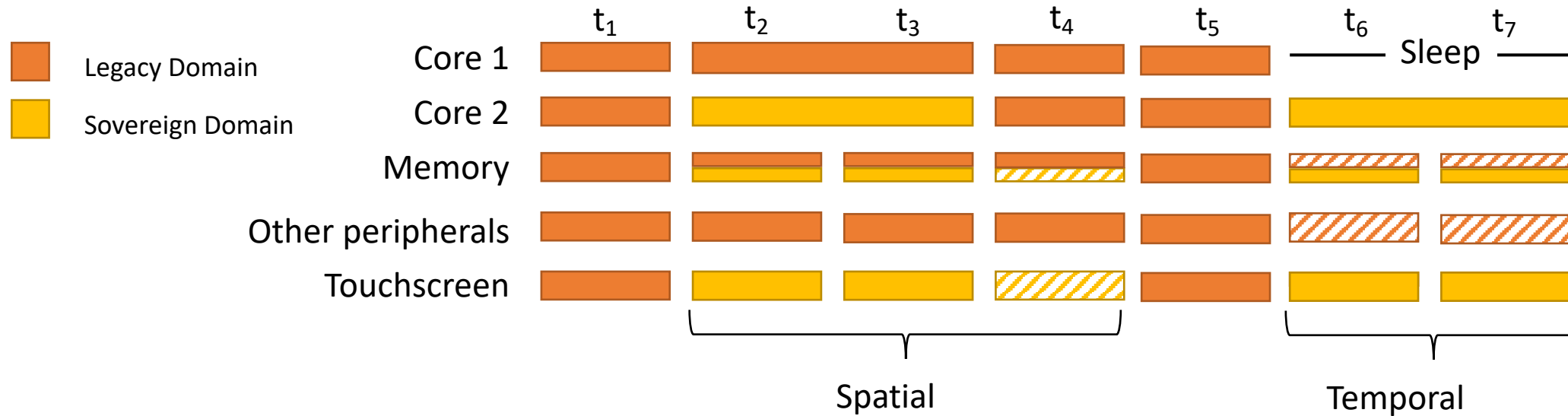
Apply isolation at address-space level



# Challenge 3: Peripheral Isolation

**Peripheral Access:** Read from and write to the memory-mapped peripheral address regions

Apply isolation at address-space level

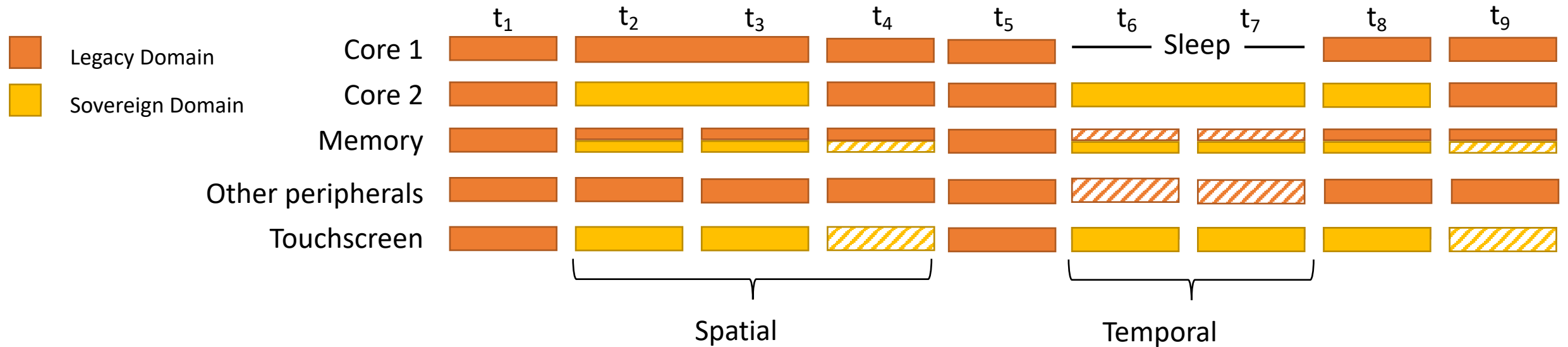




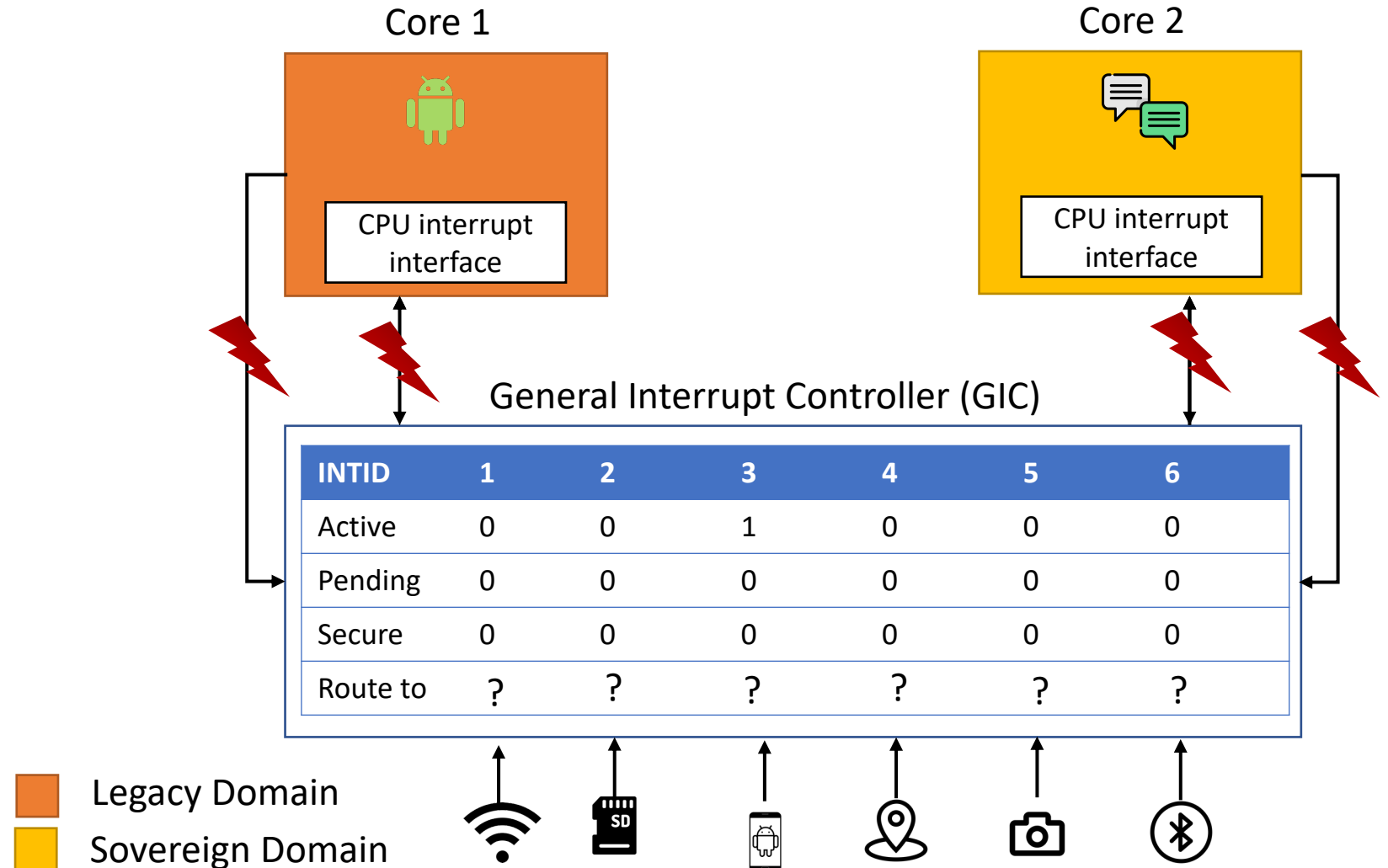
# Challenge 3: Peripheral Isolation

**Peripheral Access:** Read from and write to the memory-mapped peripheral address regions

Apply isolation at address-space level

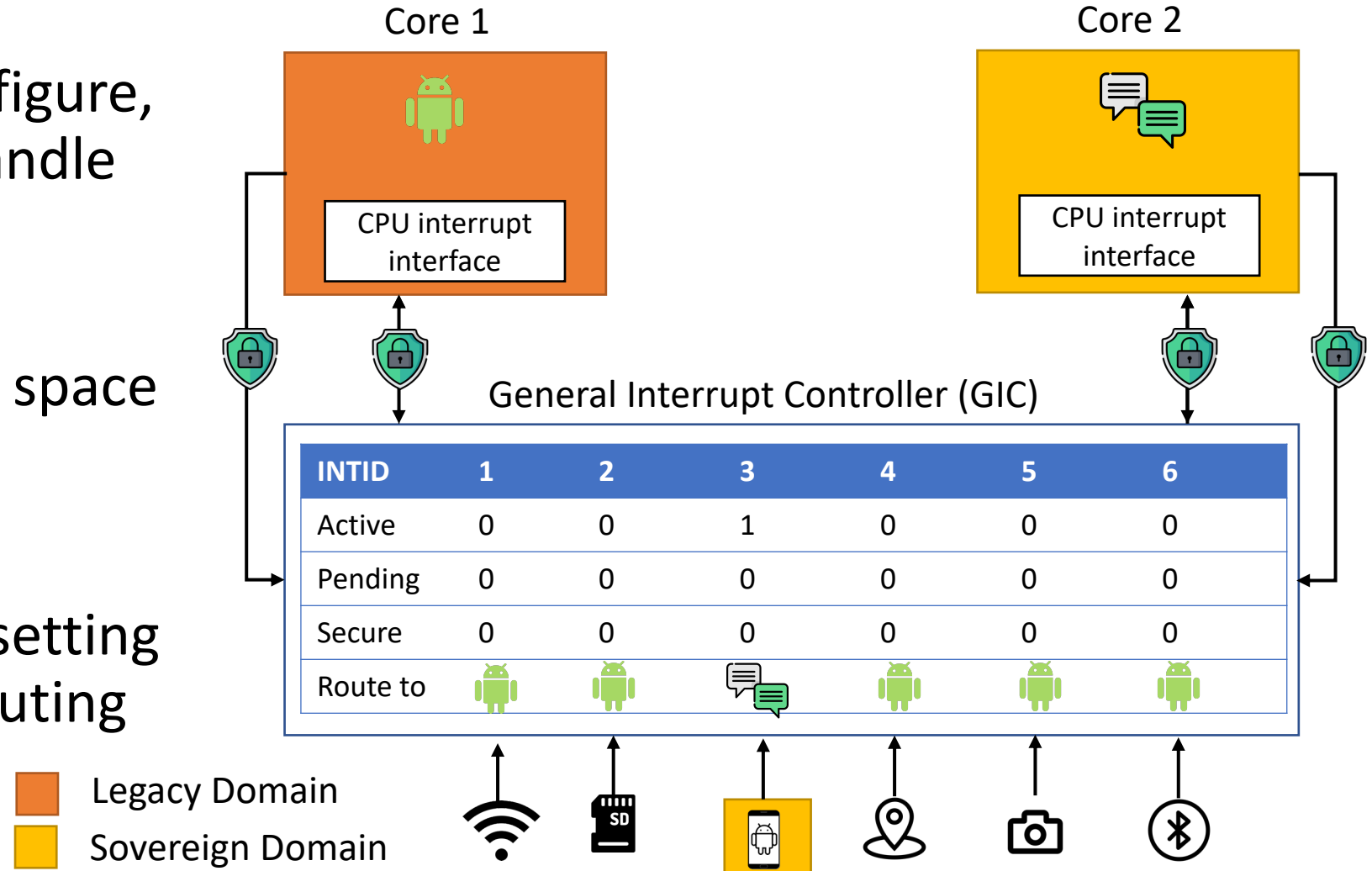


# Challenge 4: Interrupt Management

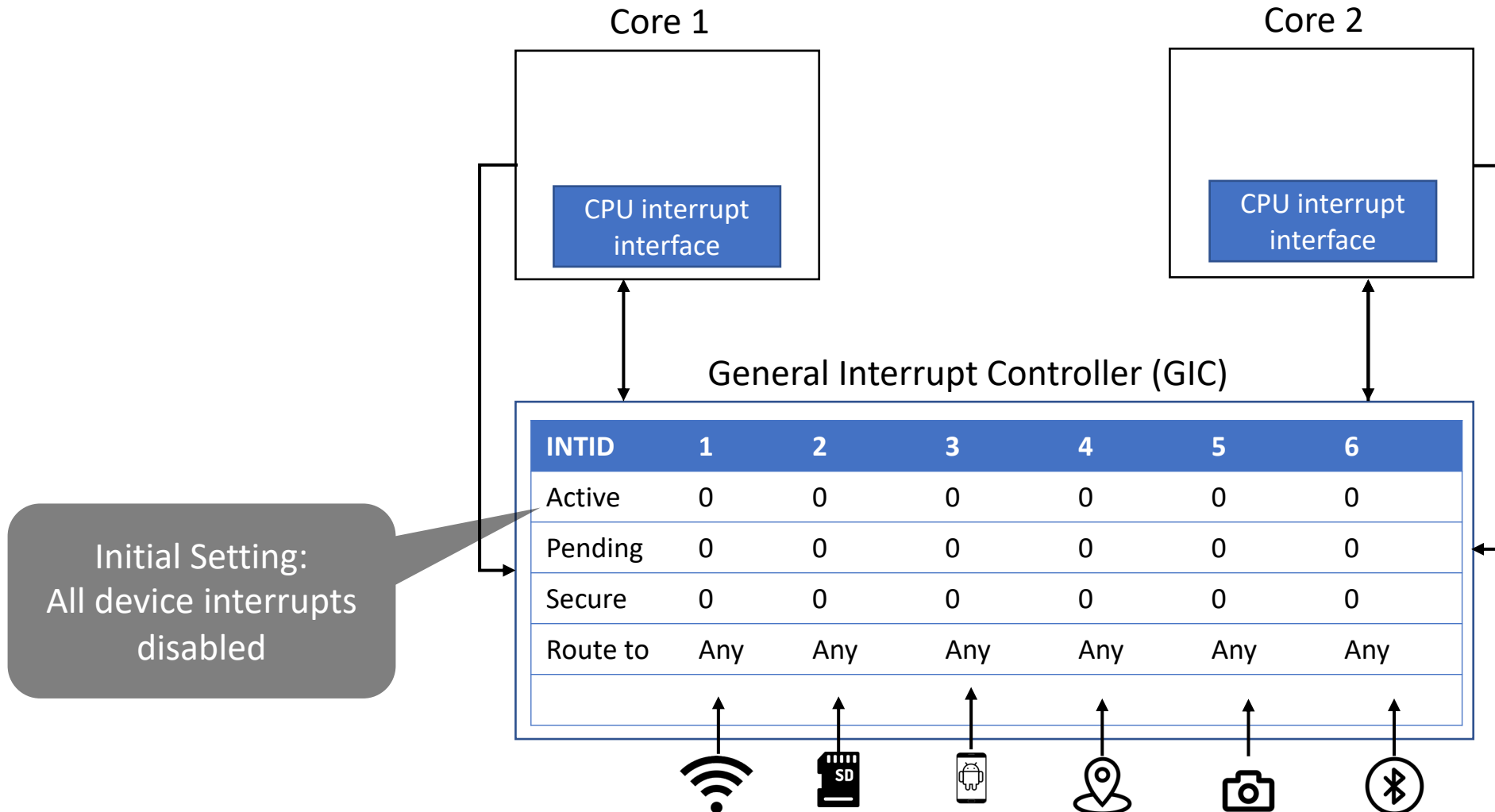


# Challenge 4: Interrupt Management

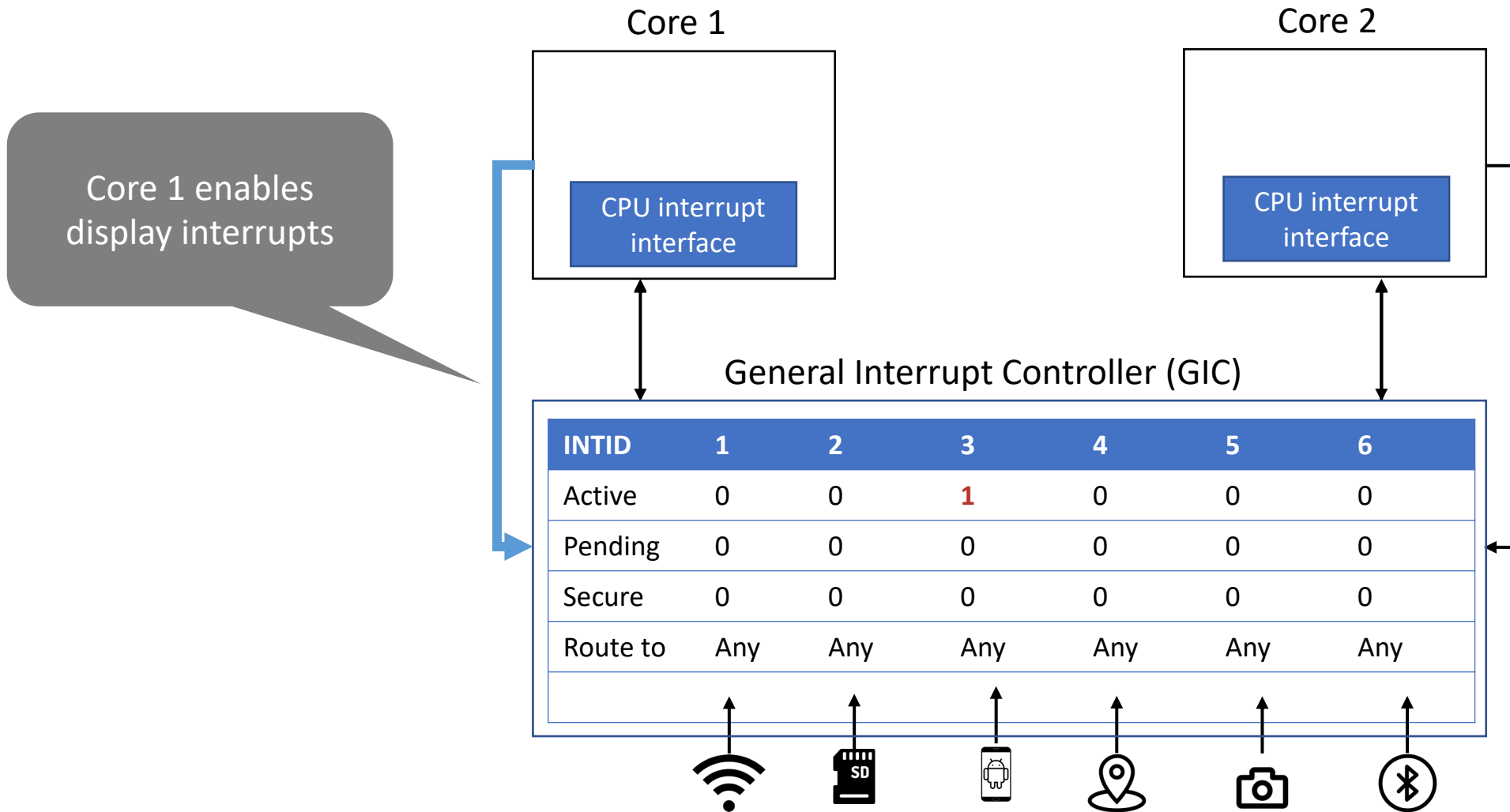
- Domain needs to configure, route, receive, and handle peripheral interrupts
- Cannot apply address space based isolation here
- Isolate configuration setting and enable correct routing



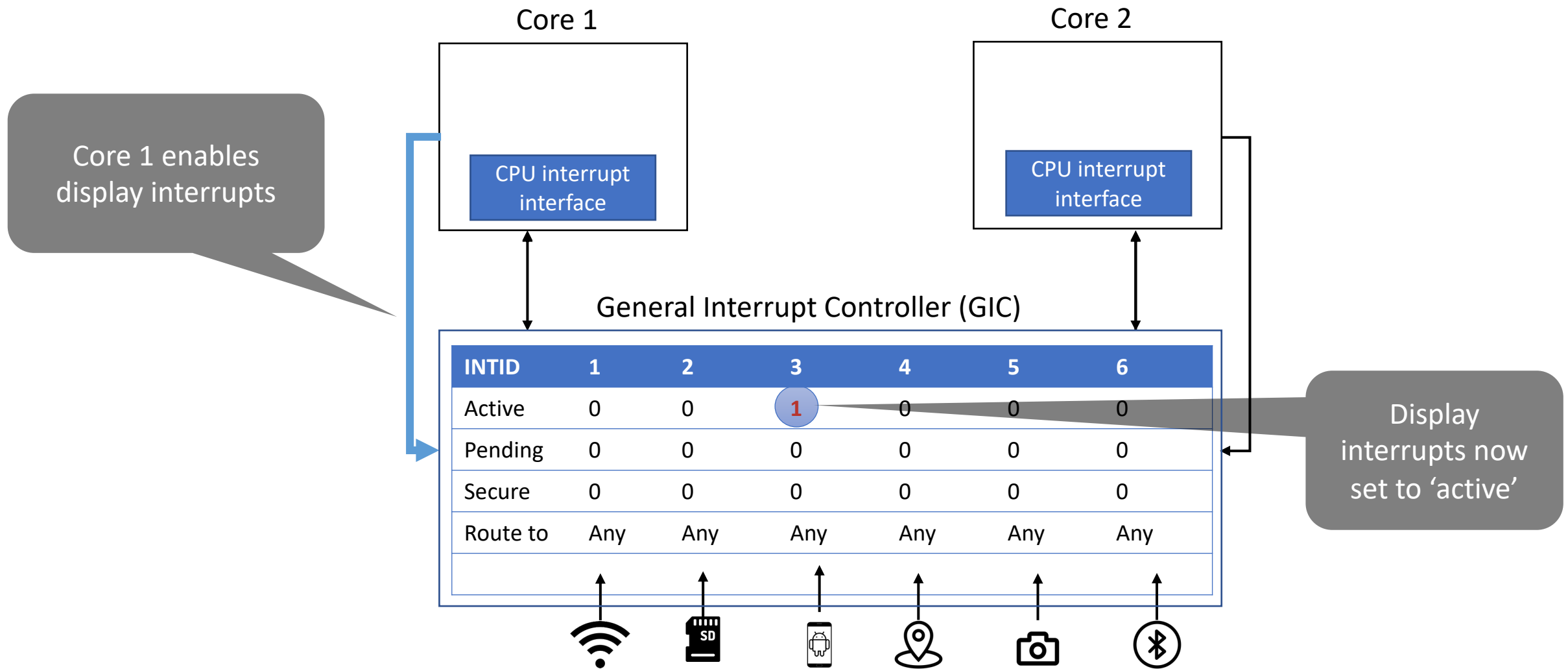
# Typical Interrupt Handling on Arm



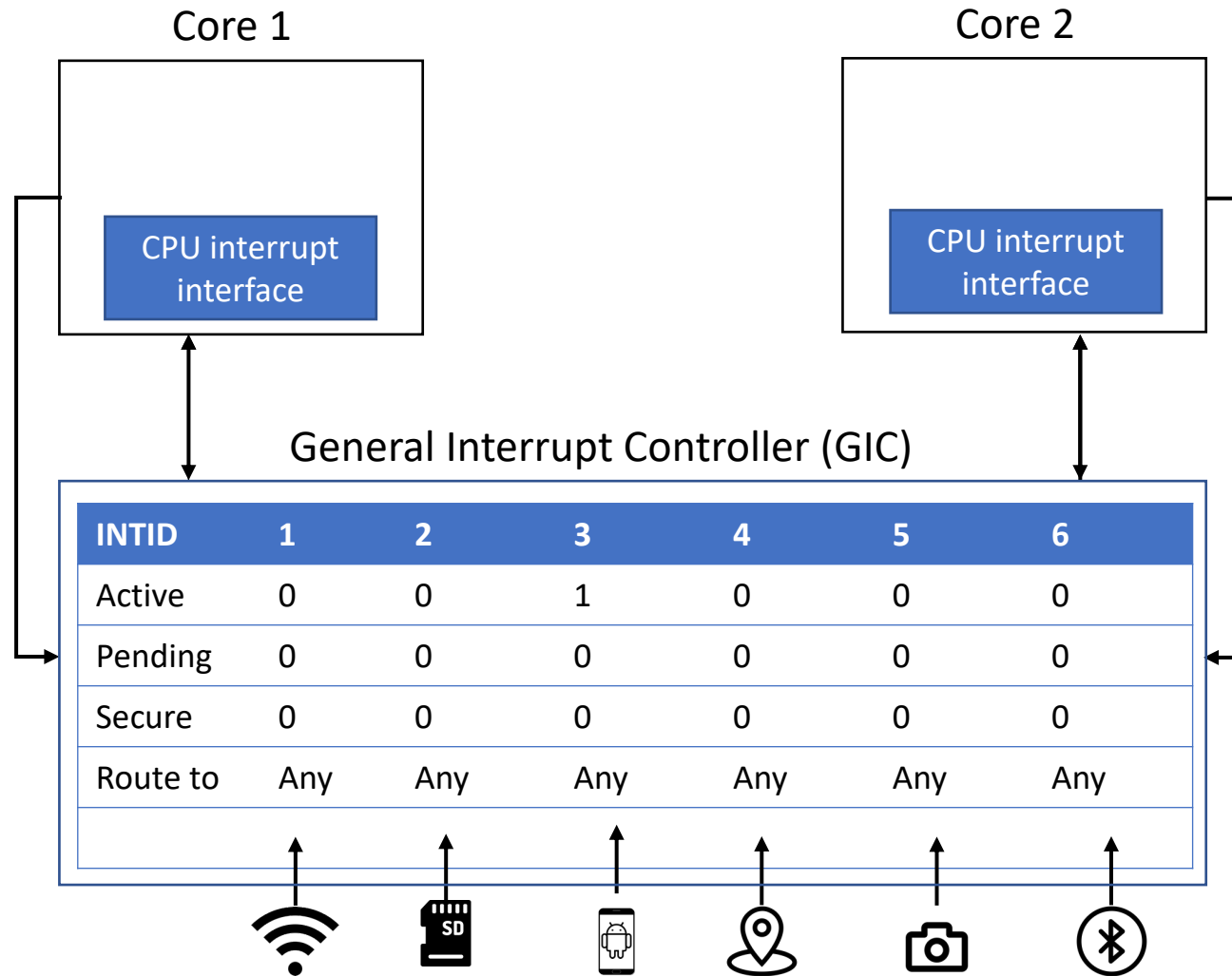
# Typical Interrupt Handling on Arm



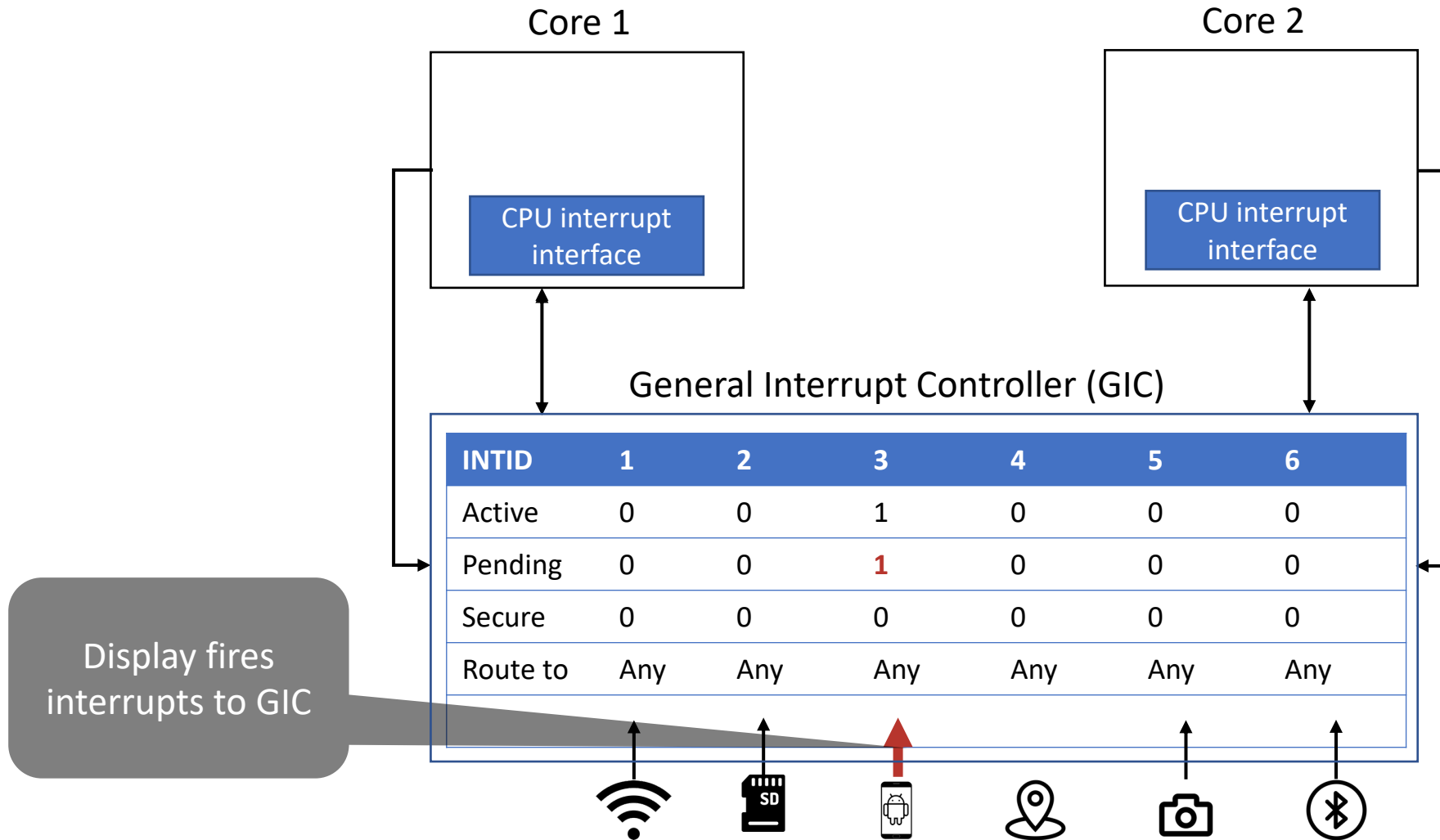
# Typical Interrupt Handling on Arm



# Typical Interrupt Handling on Arm

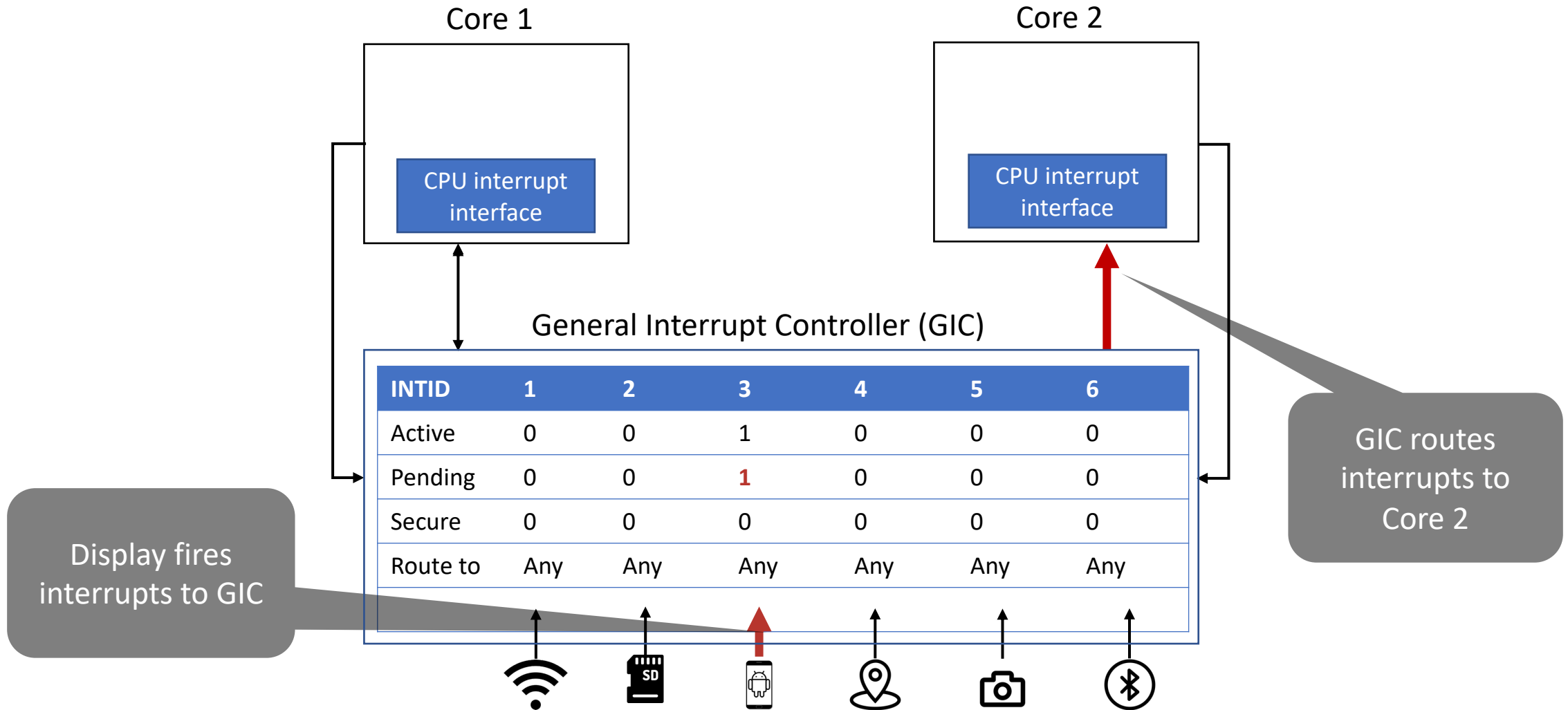


# Typical Interrupt Handling on Arm

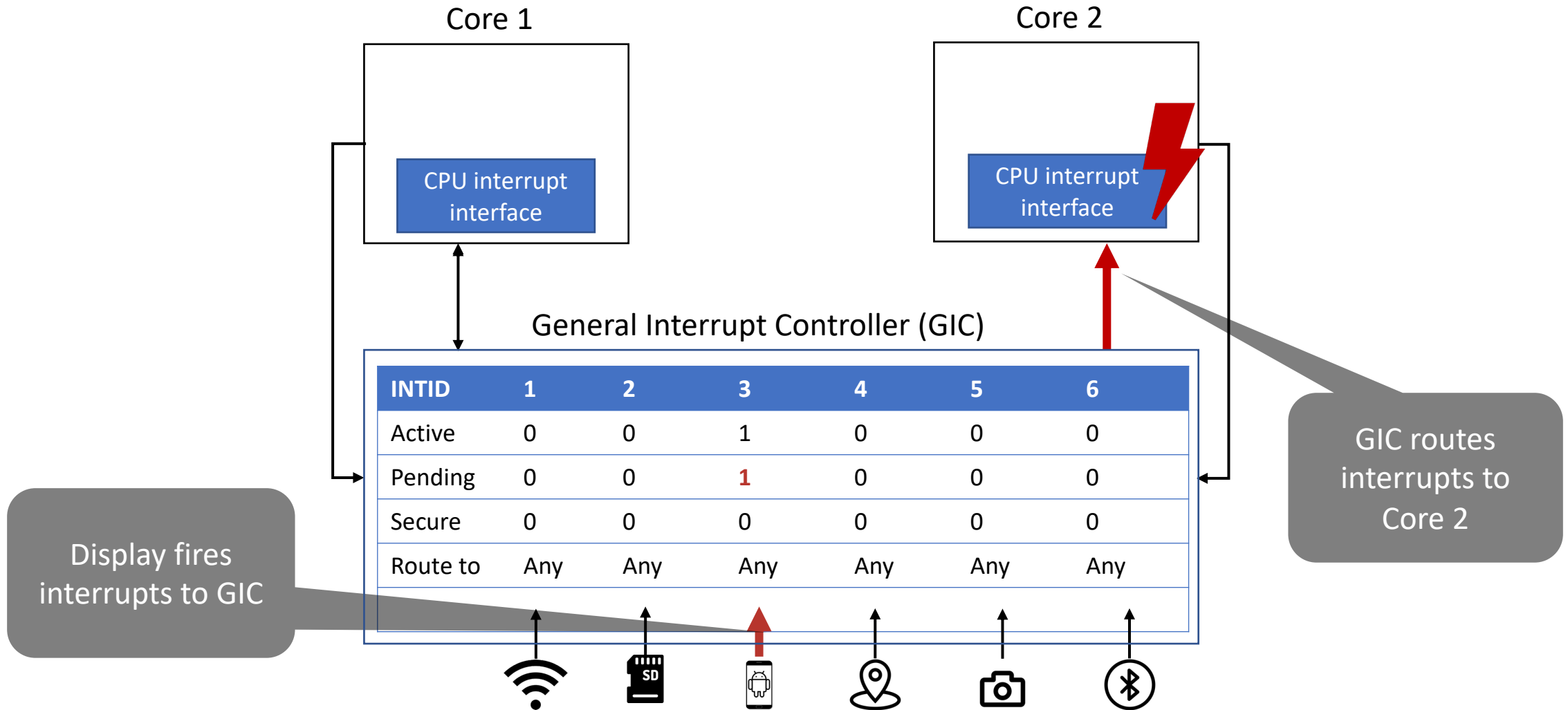




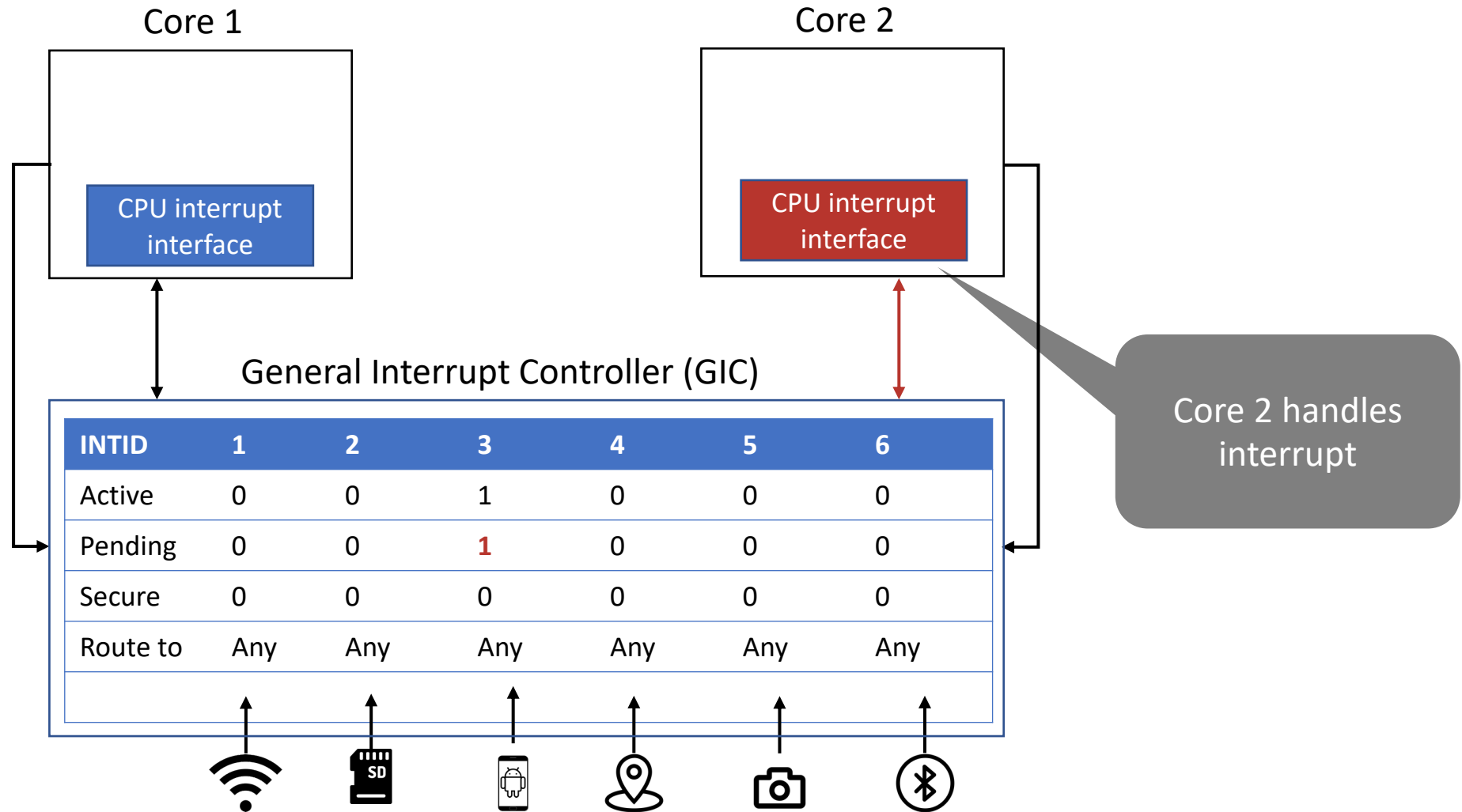
# Typical Interrupt Handling on Arm



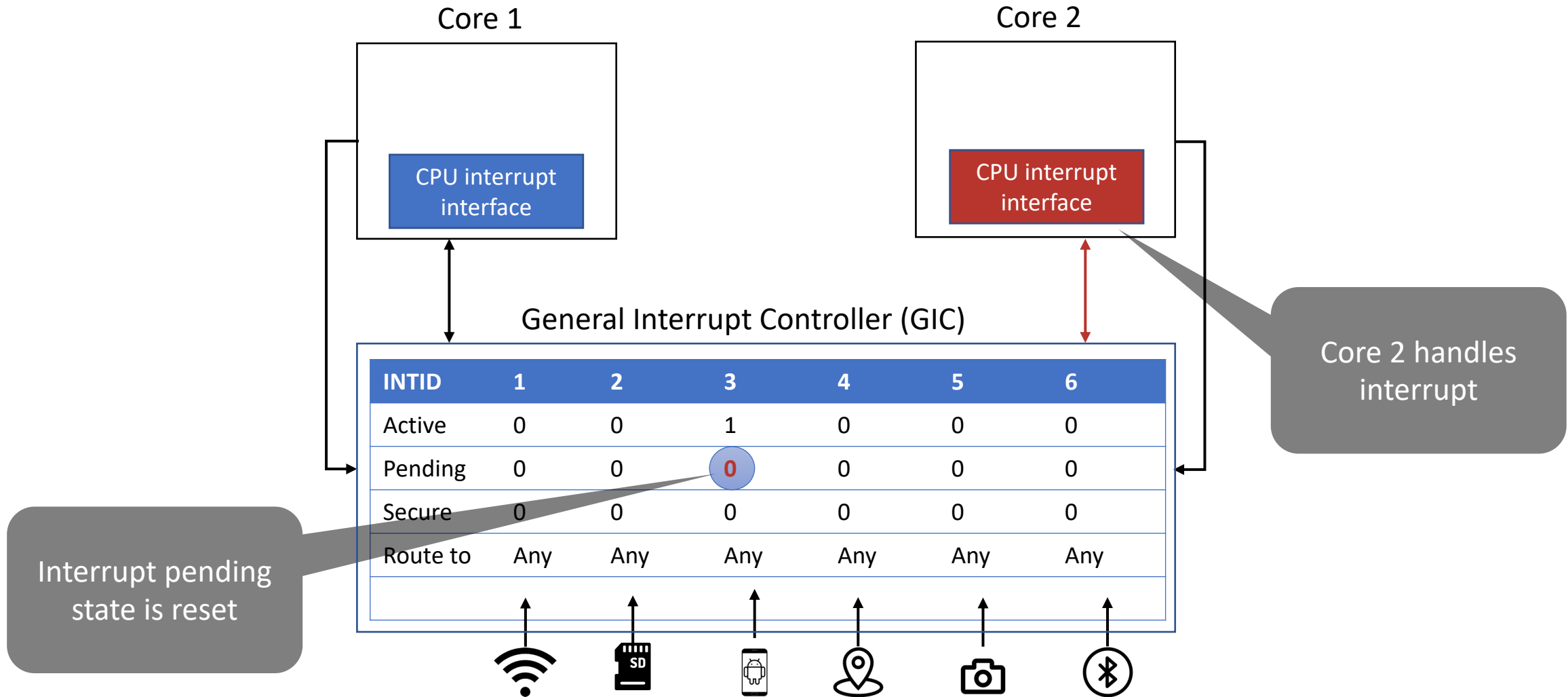
# Typical Interrupt Handling on Arm



# Typical Interrupt Handling on Arm

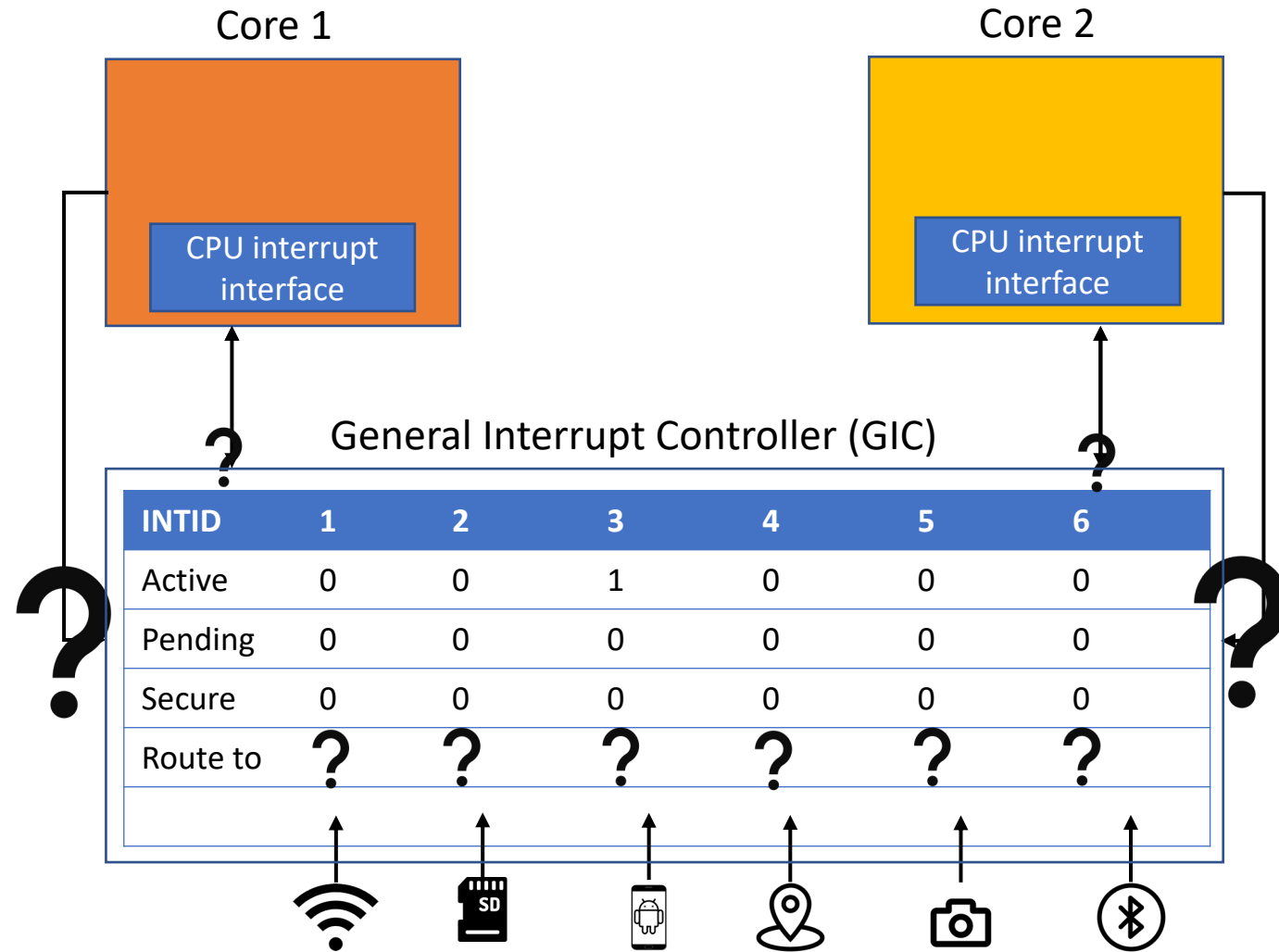


# Typical Interrupt Handling on Arm



# Interrupt Handling with TEEtime

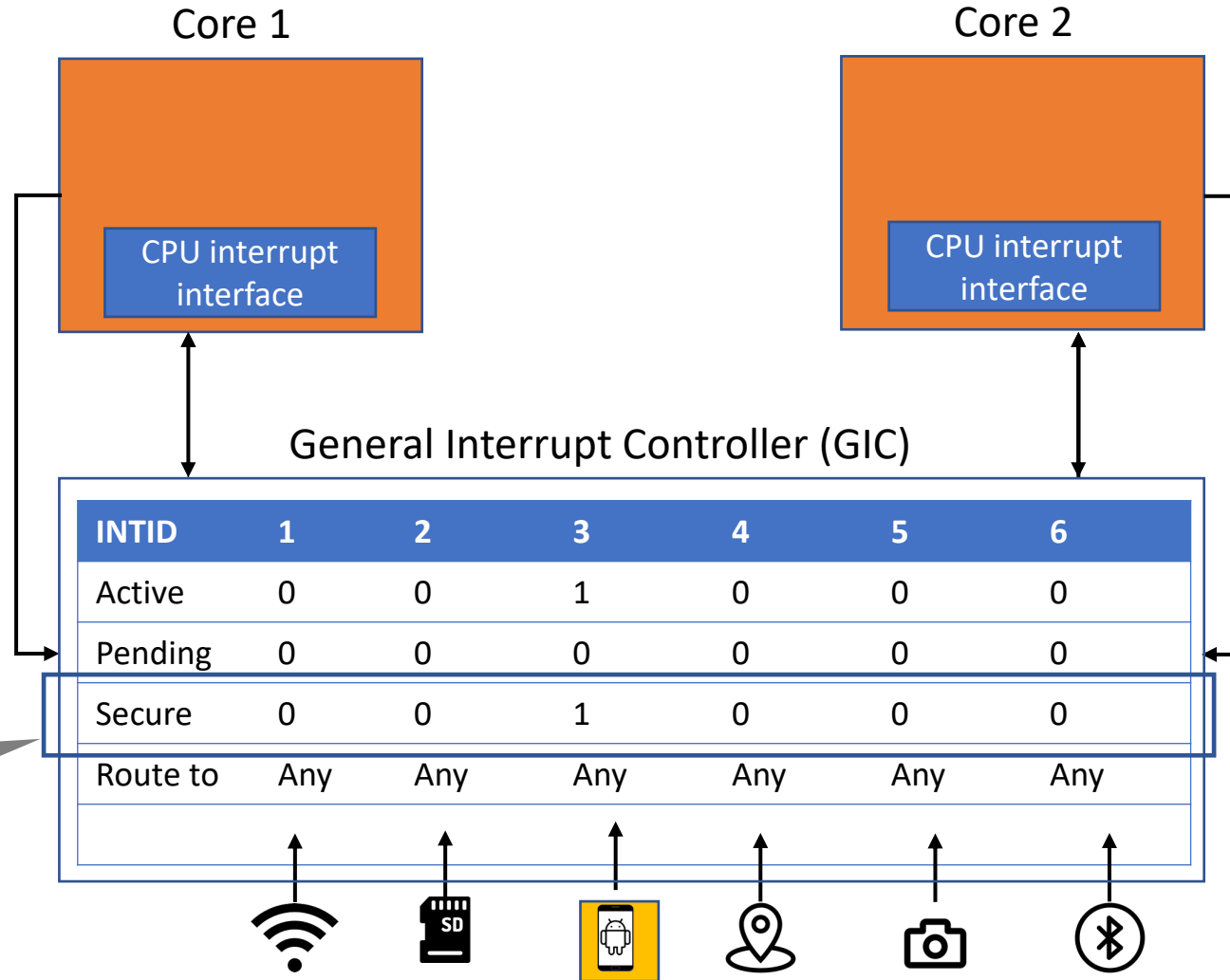
- Legacy Domain
- Sovereign Domain



# TEEtime Temporal Mode: Only 1 core executes at a time



 Legacy Domain

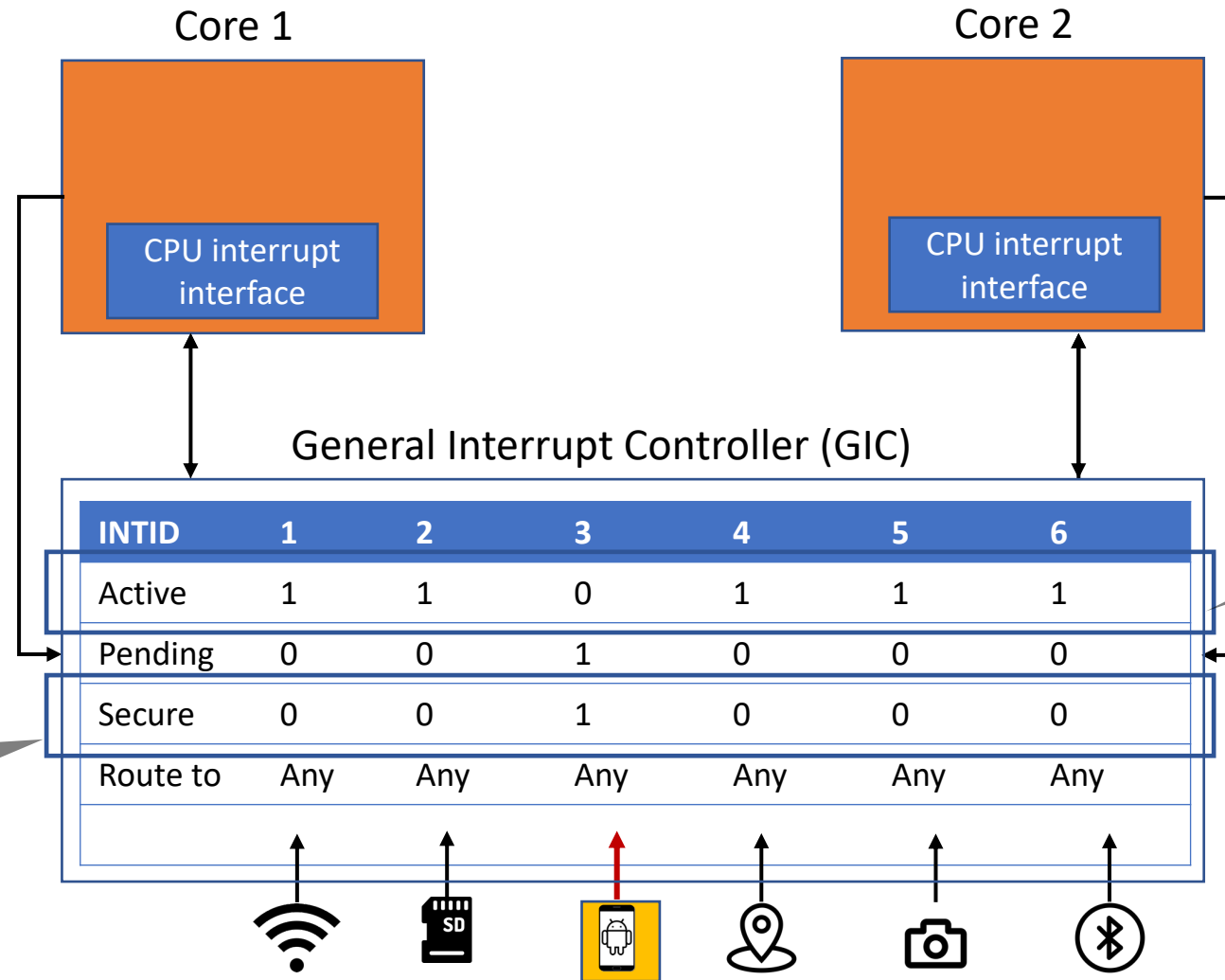
 Sovereign Domain



Stop configuration:  
Interrupts of other  
domains' devices  
are set to secure

# TEEtime Temporal Mode: Only 1 core executes at a time

-  Legacy Domain
-  Sovereign Domain



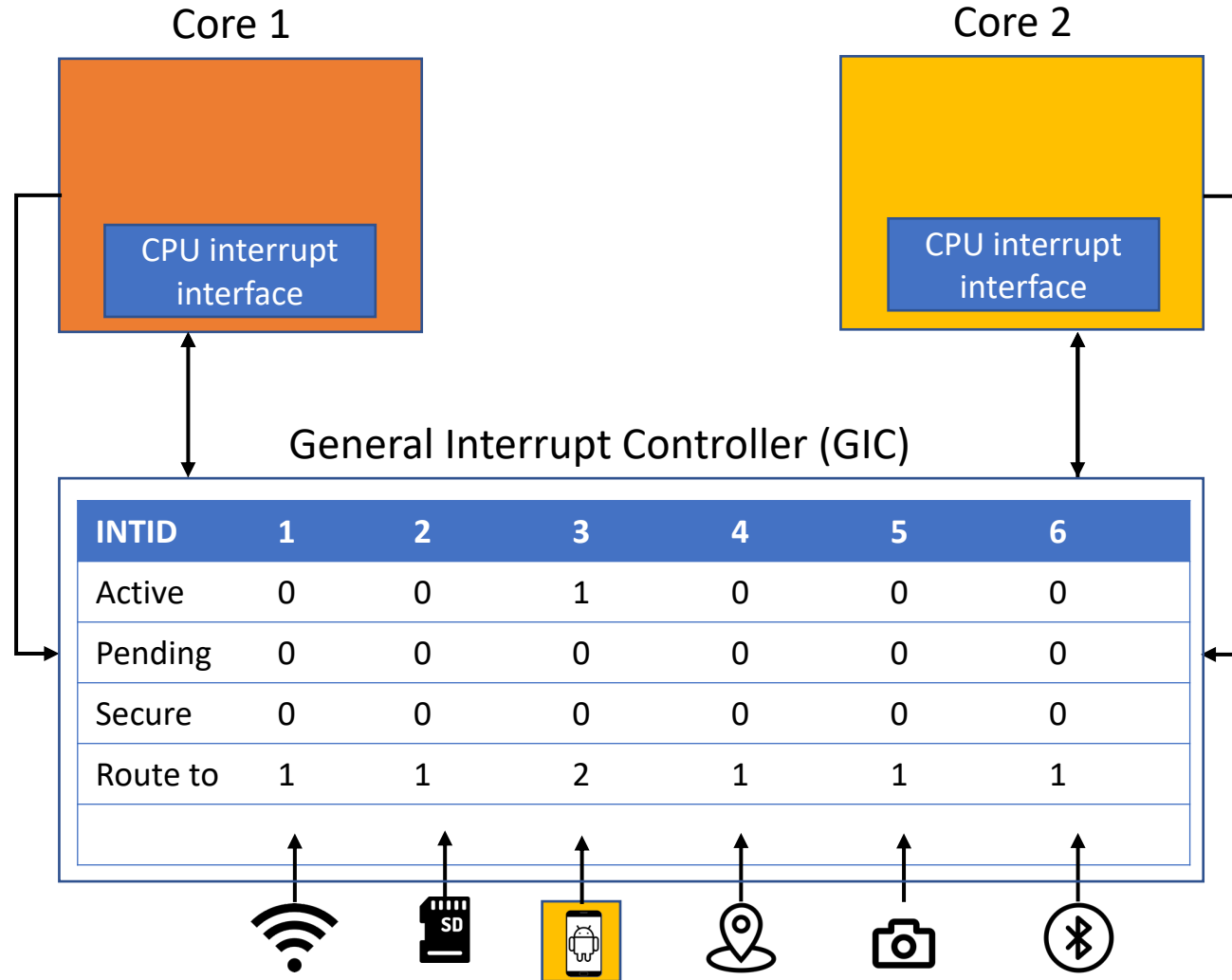
Stop configuration:  
Interrupts of other domains' devices are set to secure

Stop routing:  
Disable interrupts of other domains' devices

# Spatial Mode:

## Cores execute different domains in parallel

- Legacy Domain
- Sovereign Domain





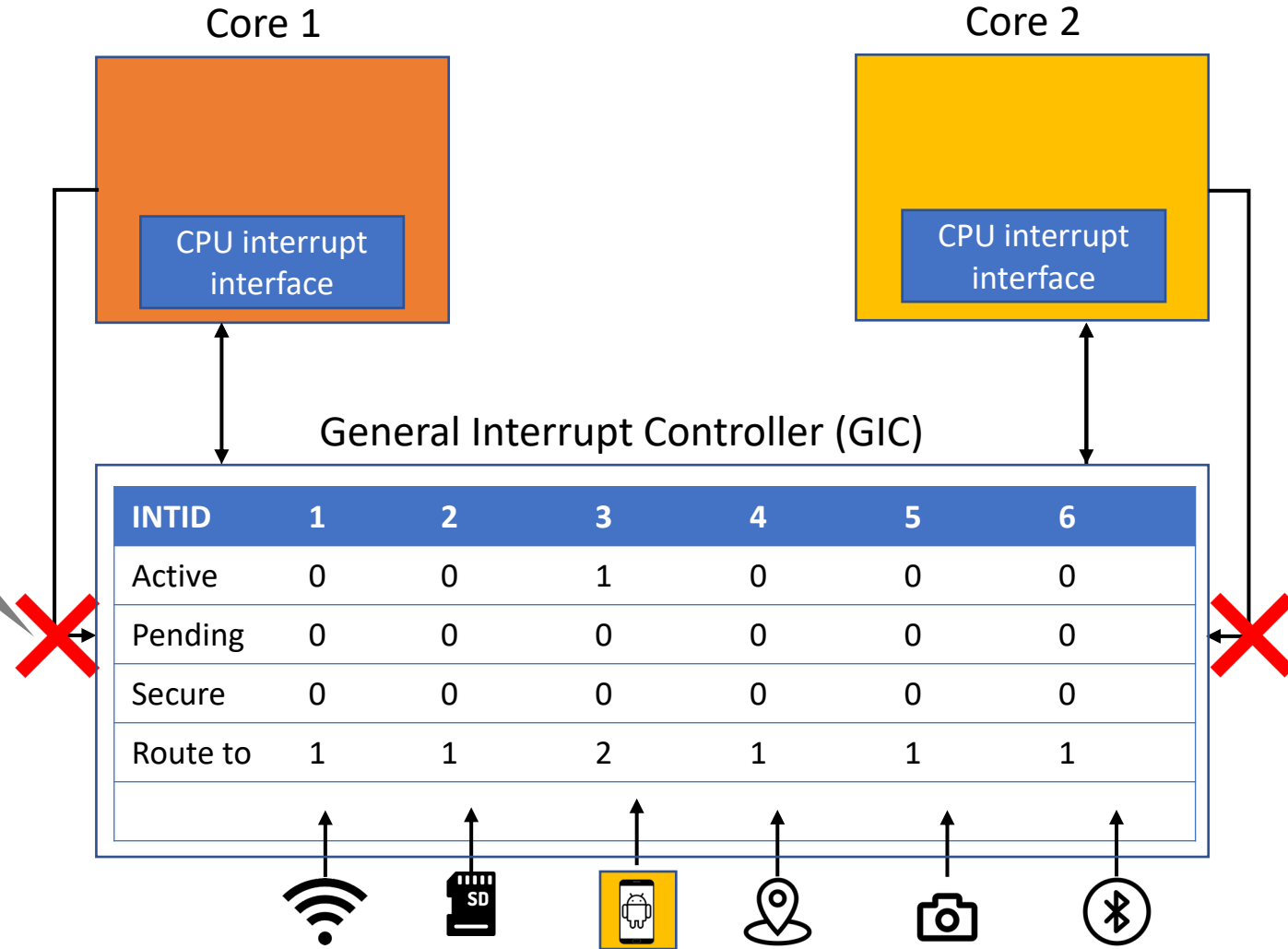
# Spatial Mode:

## Cores execute different domains in parallel

Legacy Domain

Sovereign Domain

Stop configuration:  
Restrict access to  
GIC configuration

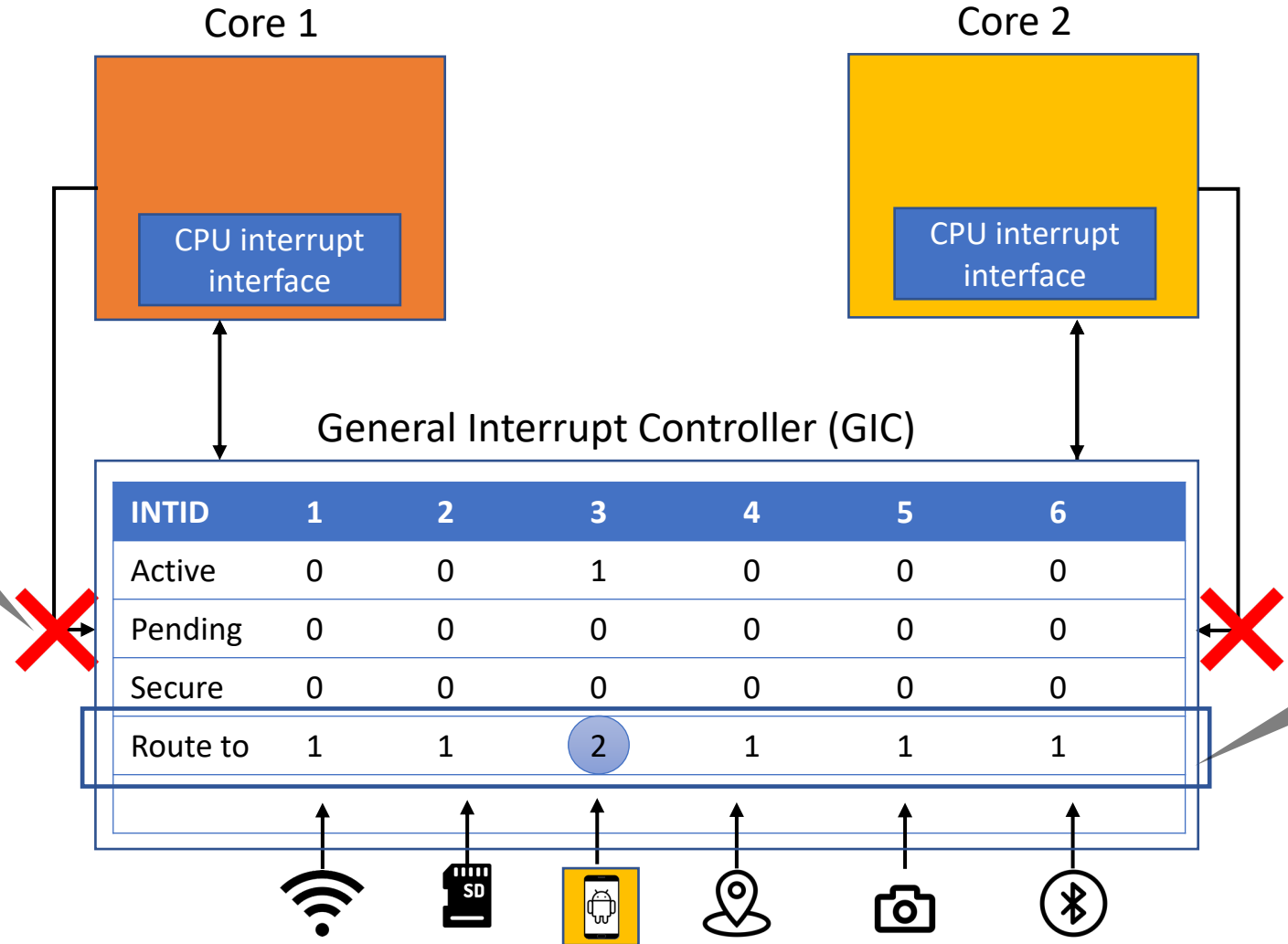


# Spatial Mode: Cores execute different domains in parallel

Legacy Domain

Sovereign Domain

Stop configuration:  
Restrict access to  
GIC configuration



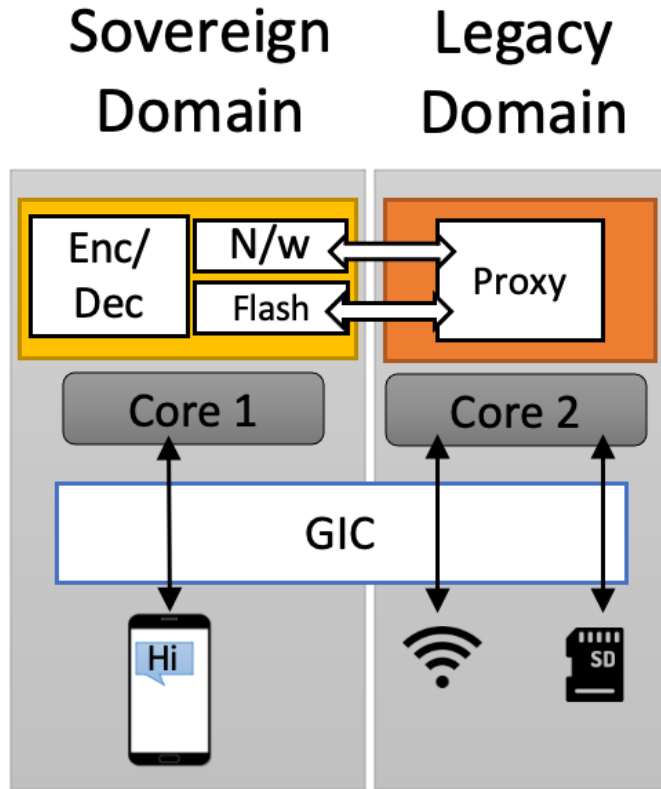
Isolate routing:  
Set explicit  
interrupt routings

# Supported Peripheral Access Modes

- So far: Peripheral can be owned by only one domain at a time
- TEEtime supports different modes of peripheral sharing:  
Exclusive, Handover, Multiplexing, Read Only, Proxy
- Secure Chat app example:

CPU + Memory	Screen	Ethernet, Storage
Spatial	Handover	Proxy

# Example: Chat App in Sovereign Domain

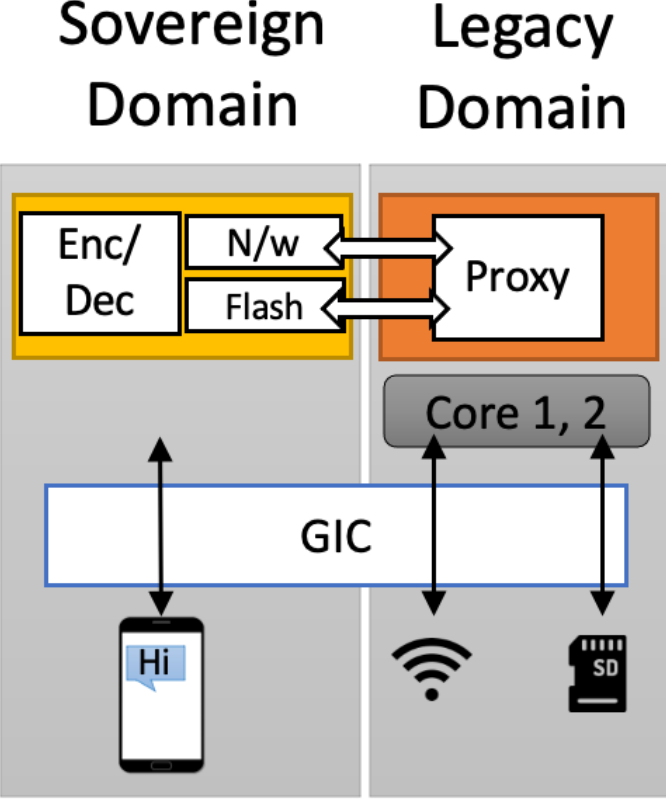
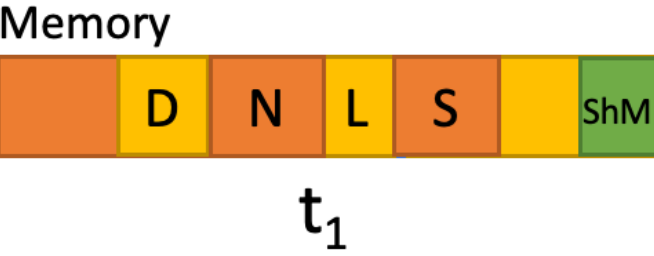
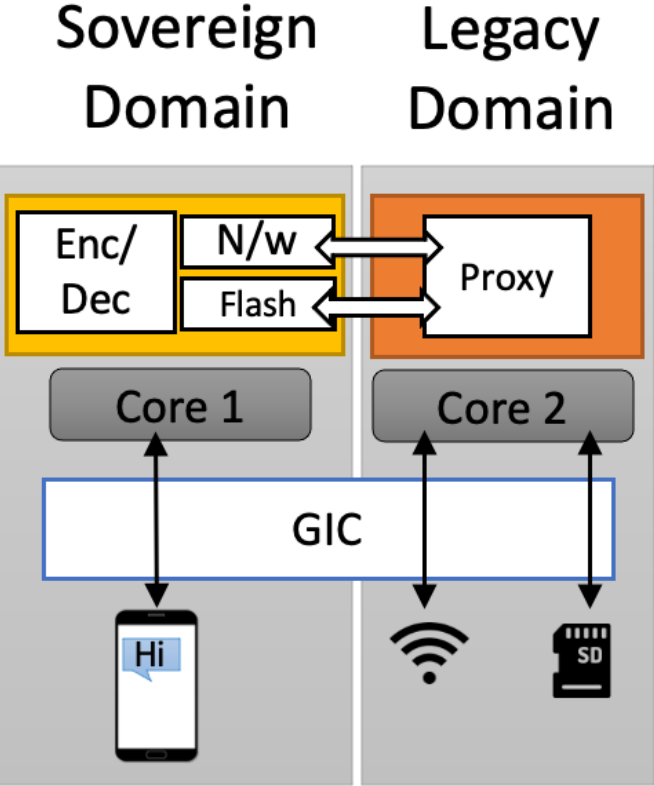


Memory

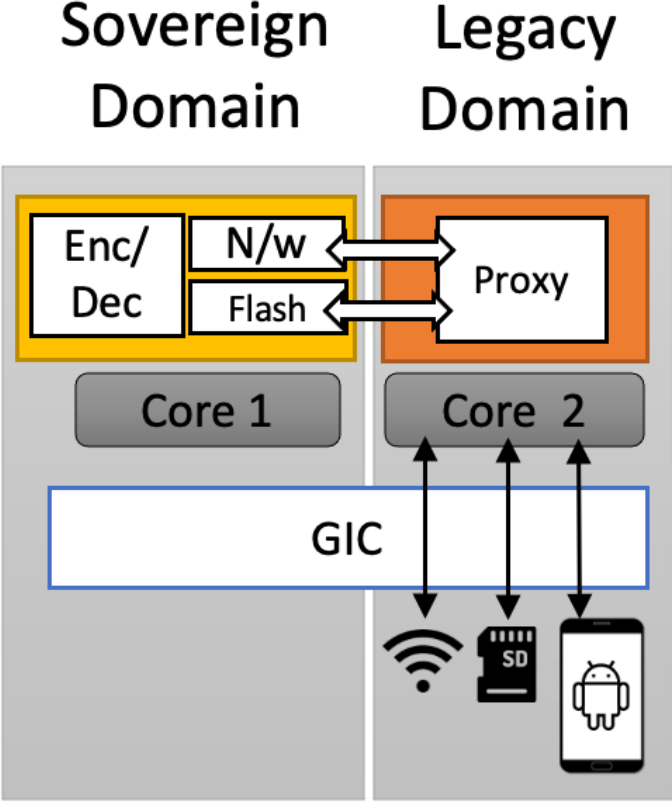
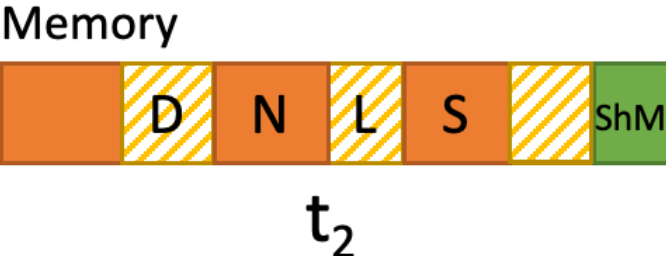
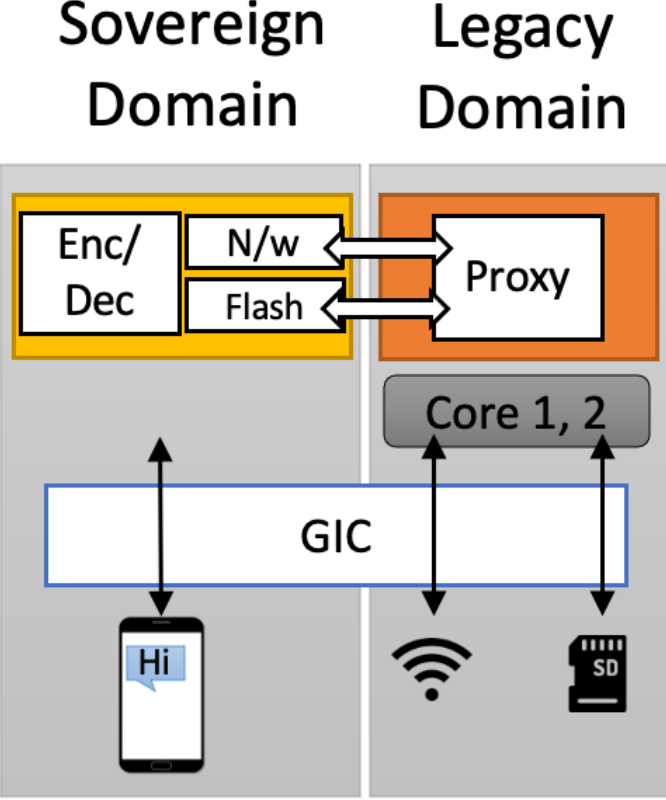
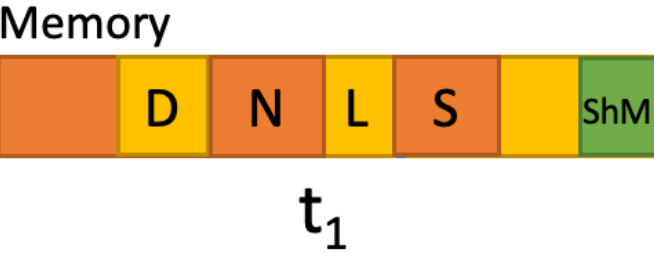
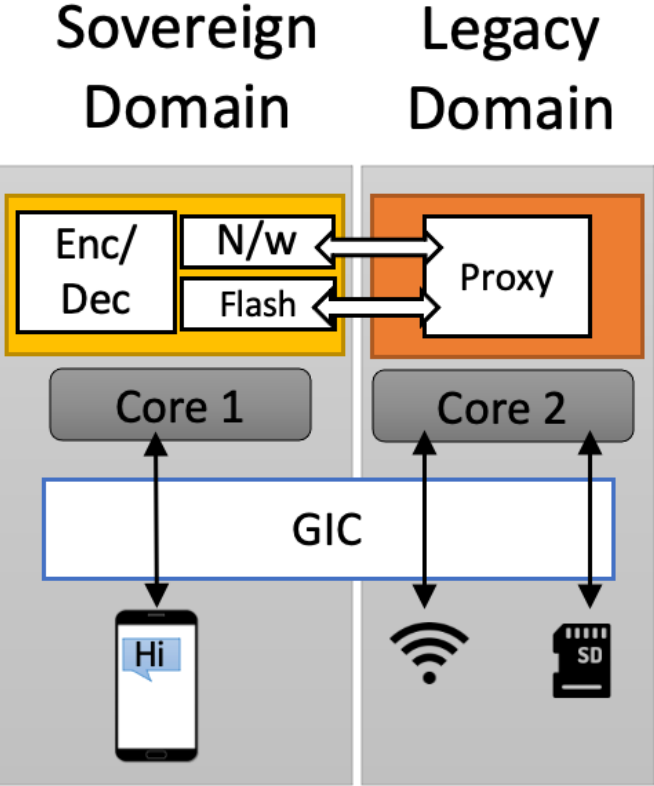


$t_1$




# Example: Chat App in Sovereign Domain



# Example: Chat App in Sovereign Domain






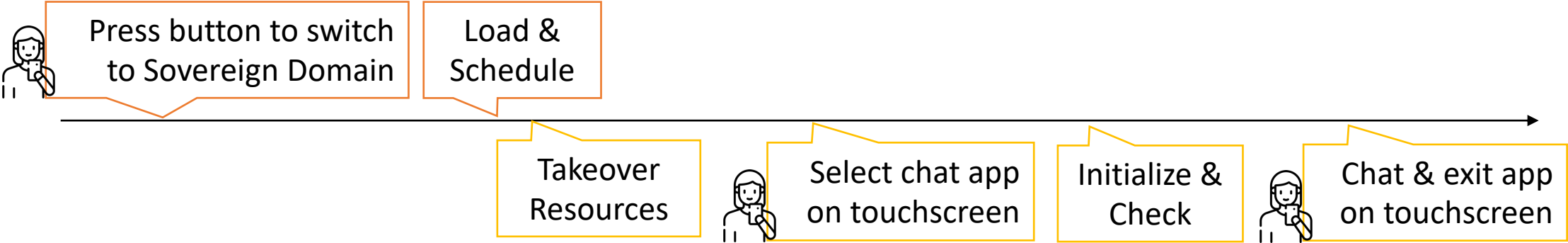
# Putting it together

-  Legacy Domain
-  Sovereign Domain
-  User Interaction






# Putting it together

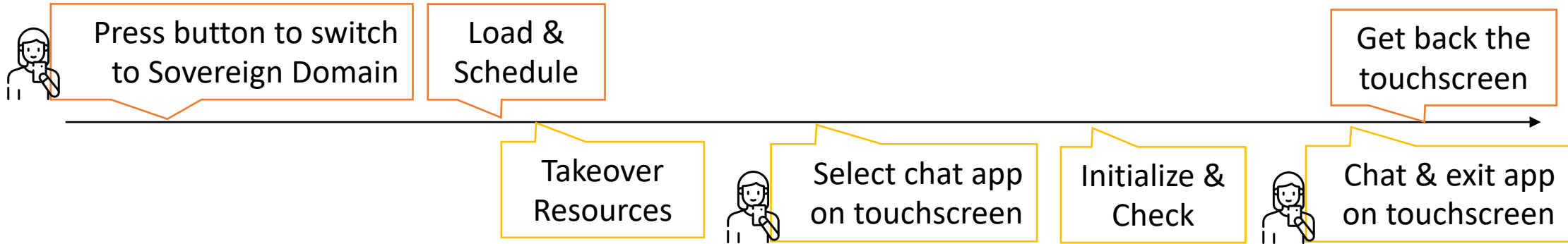
-  Legacy Domain
-  Sovereign Domain
-  User Interaction



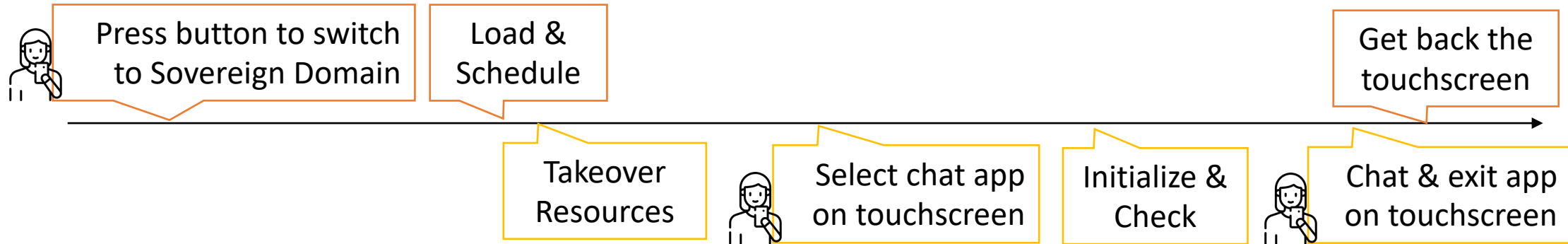
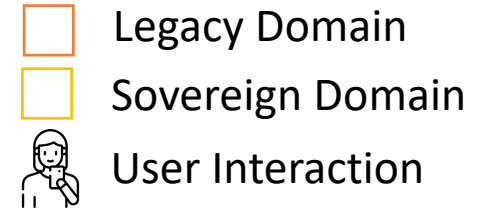


# Putting it together

-  Legacy Domain
-  Sovereign Domain
-  User Interaction



# Putting it together



- Arm platforms
  - Emulator with hardware isolation and peripheral support
  - Phones and development boards
- Sovereign domain bootup is expensive (one time), switching is fast
- Demo  
<https://youtu.be/m80pTgLjIV8>

# More Sovereign Applications

Stakeholder	Sovereign Application	Peripheral (Mode)
<b>User</b>	Secure Chat	Display (E+H), Network (P <sub>L</sub> ), Storage (P <sub>L</sub> )
	Secure Browsing	Network (P <sub>L</sub> ), UART (M)
	Secure Data Vault	Storage (P <sub>L</sub> ), UART (M)
	VPN	Network (P <sub>S</sub> )
<b>Manufacturer</b>	Device Status Check	Network (E), Display (H), Button (H)
<b>OS</b>	Biometric Authentication	Storage (P <sub>L</sub> )

Modes: exclusive (E), handover (H), proxy in legacy (P<sub>L</sub>), proxy in app (P<sub>S</sub>), multiplexing (M)

# Thank you

- For more details, see our paper: <https://arxiv.org/abs/2211.05206>

## It's TEEtime: A New Architecture Bringing Sovereignty to Smartphones

Friederike Groschupp   Mark Kuhne   Moritz Schneider   Ivan Puddu   Shweta Shinde   Srdjan Capkun  
ETH Zurich

- Contact: [shweta.shinde@inf.ethz.ch](mailto:shweta.shinde@inf.ethz.ch)