ASM: A Programmable Interface for Extending Android Security

Stephan Heuser,

Ahmad-Reza Sadeghi

Intel Collaborative Research Institute for Secure Computing at TU Darmstadt, Germany

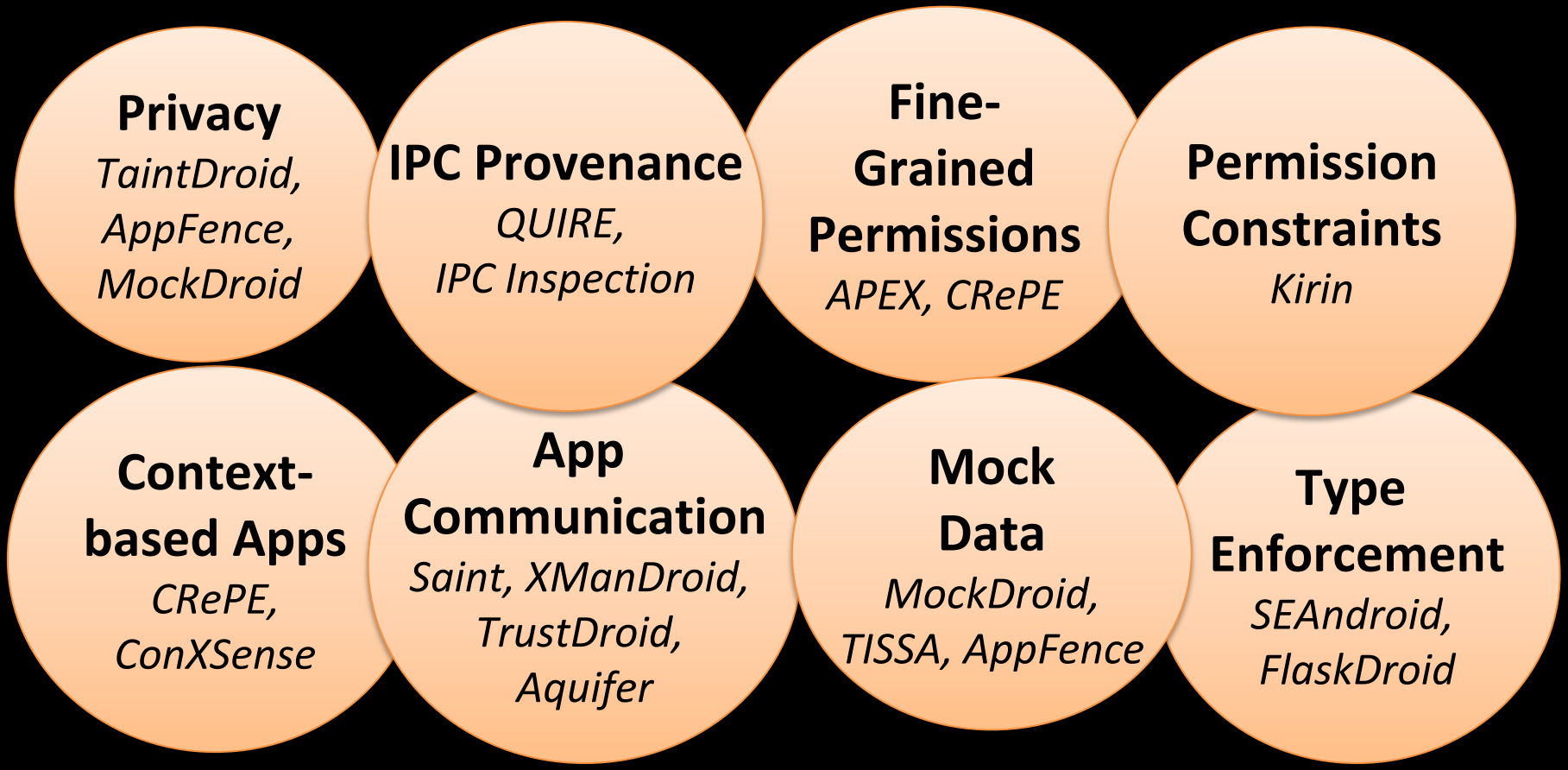
Adwait Nadkarni,

William Enck

NC State University, USA

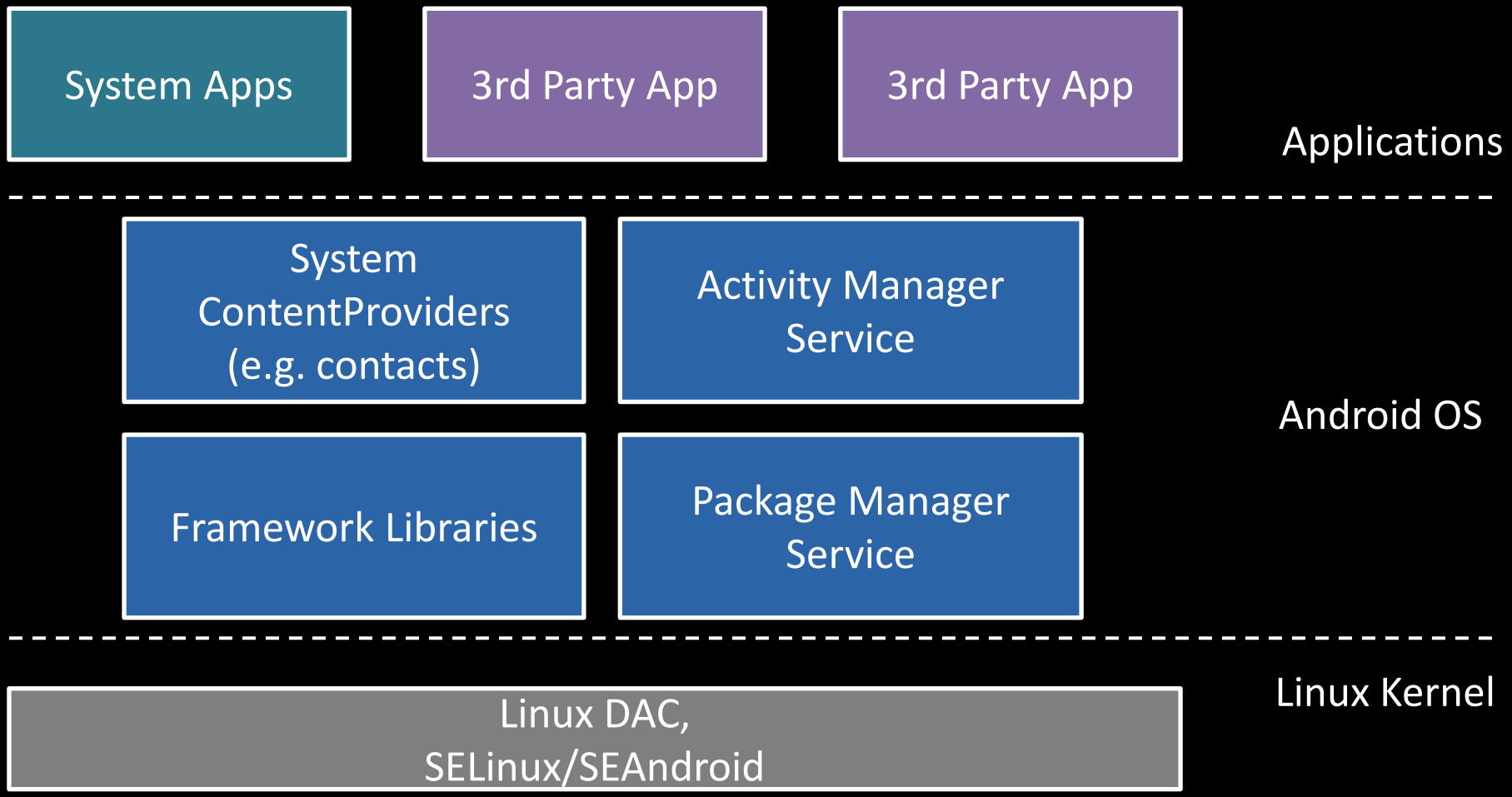
Android Security Extensions (selected)

Security extensions focus on
specific use cases and/or *security and privacy models*



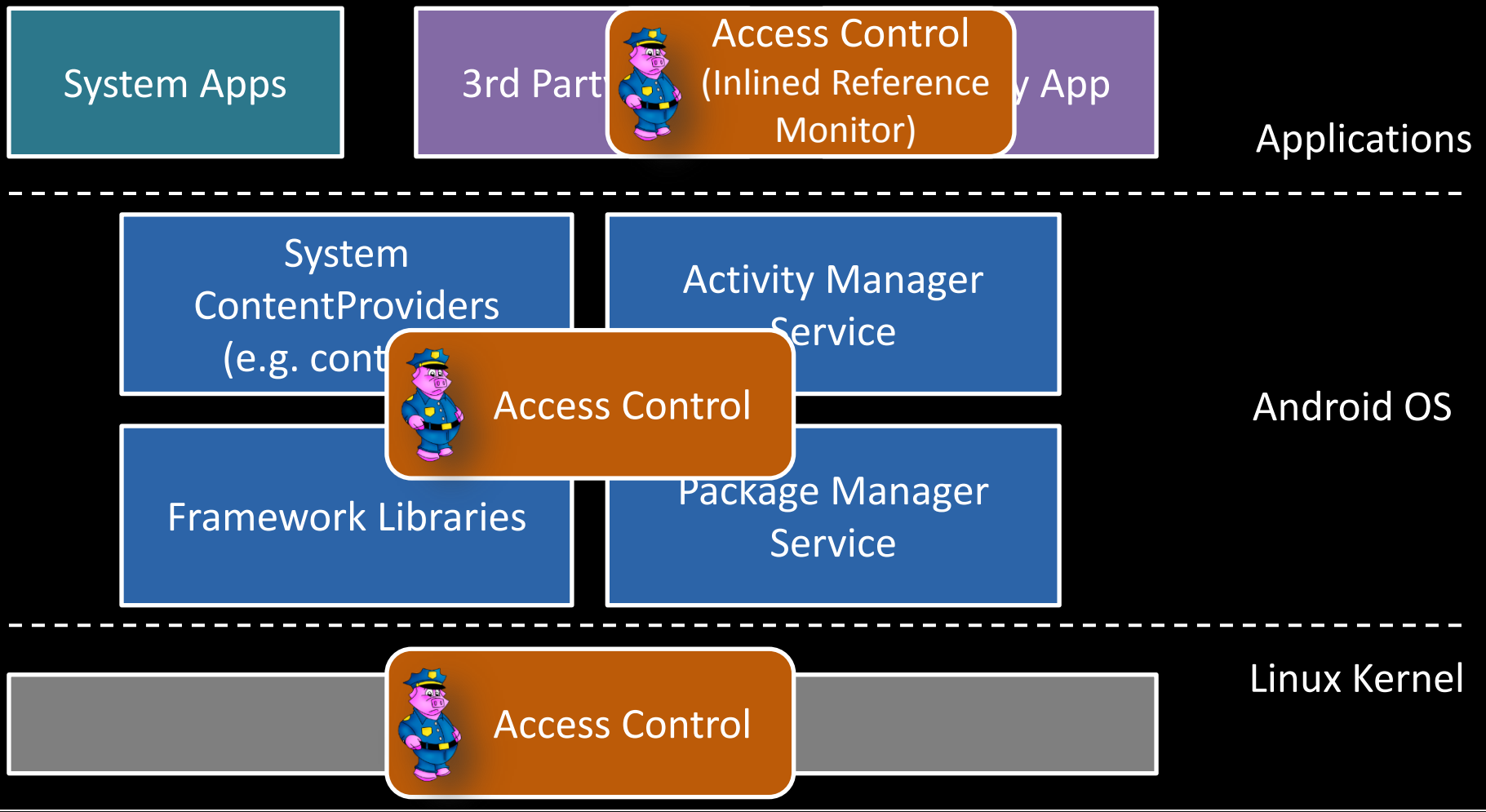
Android Security Extensions

Access control (hooks) are embedded in sensitive components



Android Security Extensions

Access control (hooks) are embedded in sensitive components



Research Question

Is it possible to provide a *programmable* and *generic* security architecture on top of which many of these solutions can be instantiated?

Observations

Diverse Goals, but use similar security hooks and mechanisms

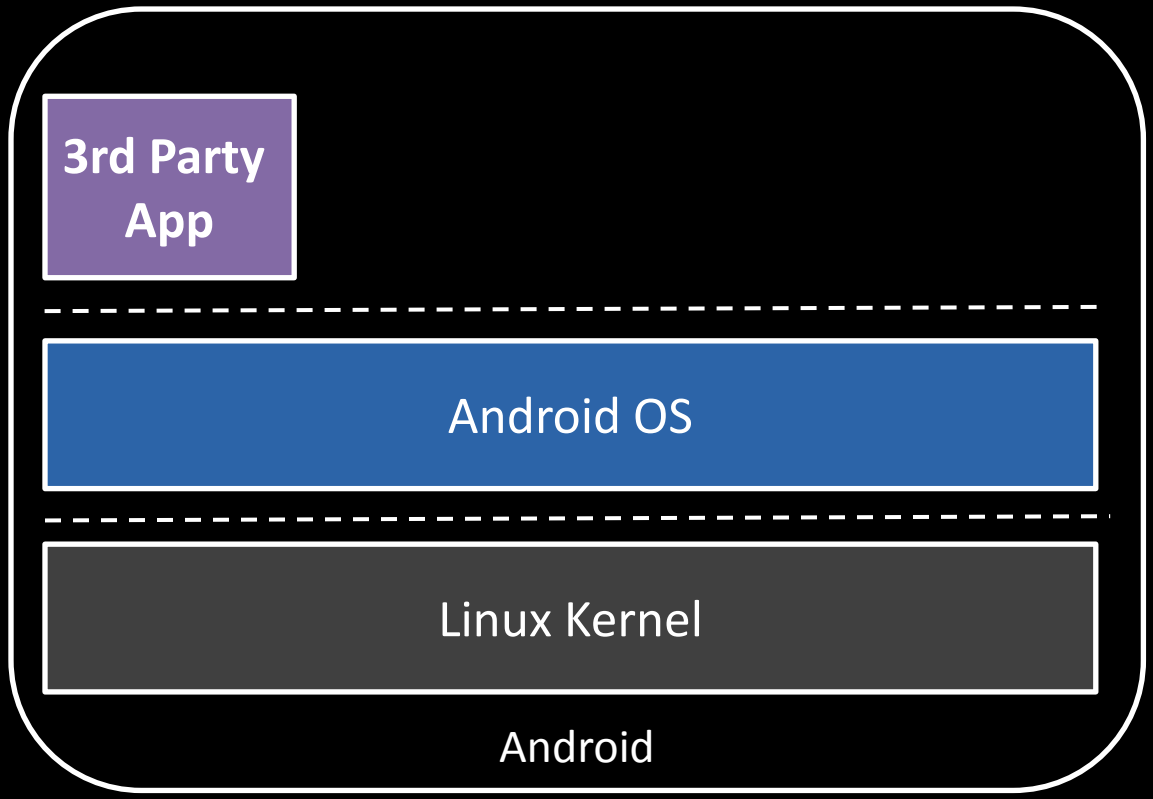
System	Android ICC	Package Manager	Sensors / Phone Info	Fake Data	System Content Providers	File Access	Network Access	3rd Party Hooks
MockDroid		✓	✓	✓	✓		✓	
XManDroid	✓	✓	✓			✓	✓	
TrustDroid	✓	✓			✓	✓	✓	
FlaskDroid	✓	✓	✓	✓	✓	✓	✓	✓
CRePE	✓		✓					
Quire	✓	✓						
TaintDroid	✓		✓			✓	✓	
Kirin		✓						
IPC Inspection	✓	✓						
AppFence	✓	✓	✓	✓	✓	✓	✓	
Aquifer	✓					✓	✓	
APEX	✓	✓	✓					
Saint	✓	✓						✓
SEAndroid	✓	✓				✓	✓	
TISSA			✓	✓	✓			

Observations

Diverse Goals, but use similar security hooks and mechanisms

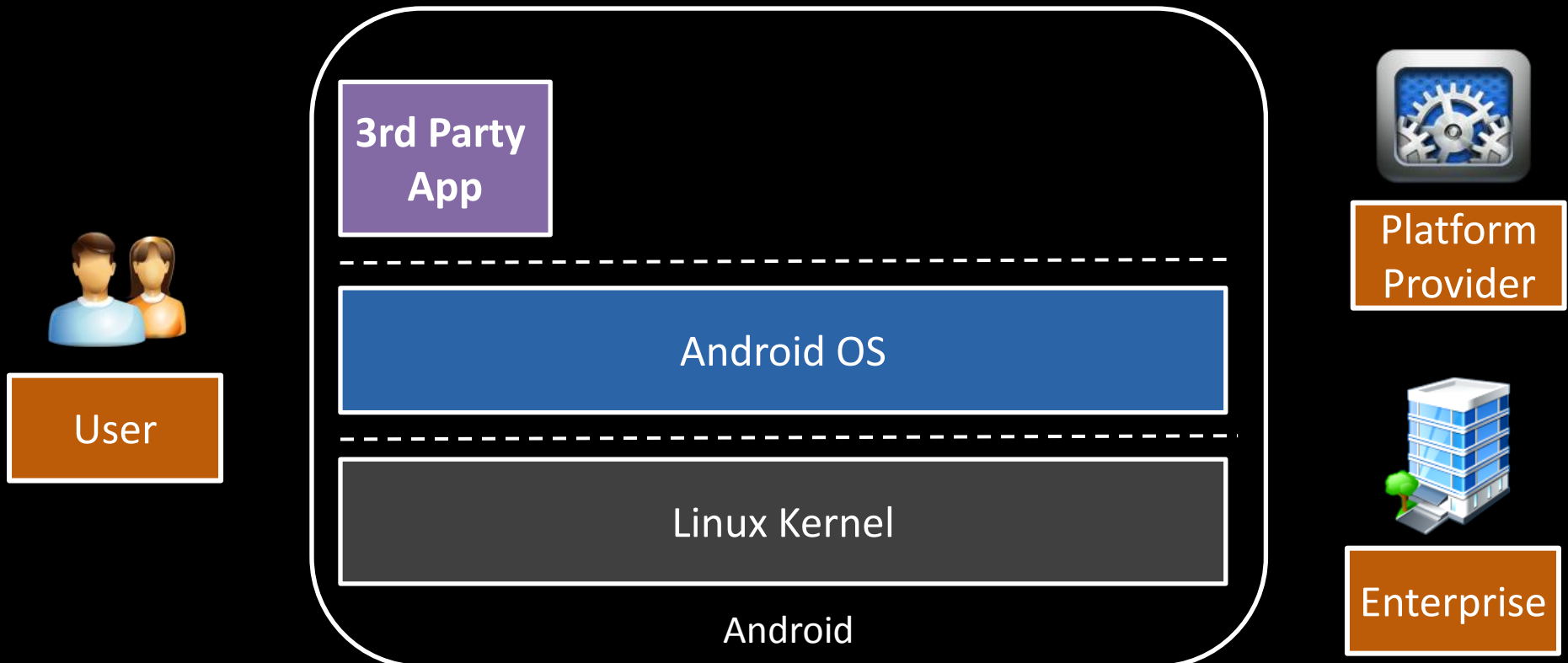
System	Android ICC	Package Manager	Sensors / Phone Info	Fake Data	System Content Providers	File Access	Network Access	3rd Party Hooks
MockDroid		✓	✓	✓	✓		✓	
XManDroid	✓	✓	✓			✓	✓	
TrustDroid	✓	✓			✓	✓	✓	
FlaskDroid	✓	✓	✓	✓	✓	✓	✓	✓
CRePE	✓		✓					
Quire	✓	✓						
TaintDroid	✓		✓			✓	✓	
Kirin		✓						
IPC Inspection	✓	✓						
AppFence	✓	✓	✓	✓	✓	✓	✓	
Aquifer	✓					✓	✓	
APEX	✓	✓	✓					
Saint	✓	✓						✓
SEAndroid	✓	✓				✓	✓	
TISSA			✓	✓	✓			

High-level Idea of ASM



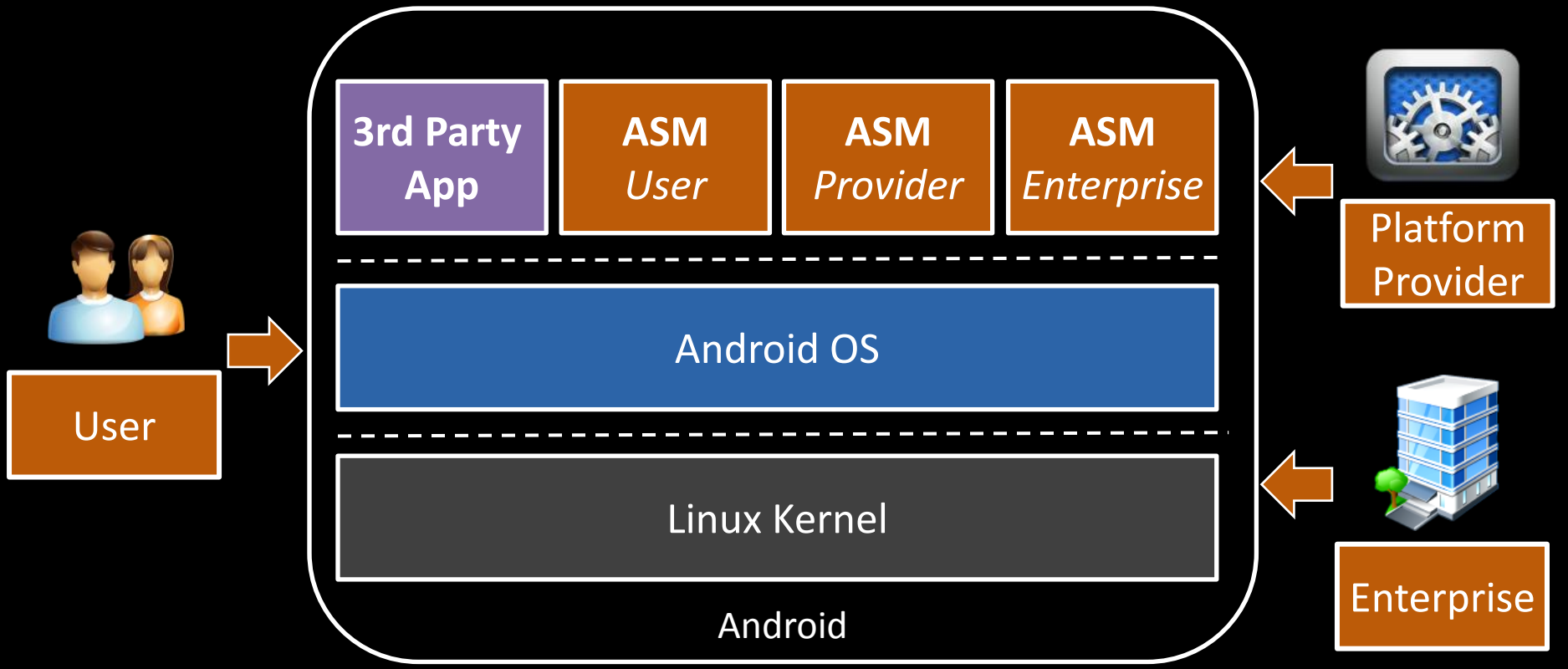
High-level Idea of ASM

- A *modular* access control architecture supporting *multiple stakeholders*



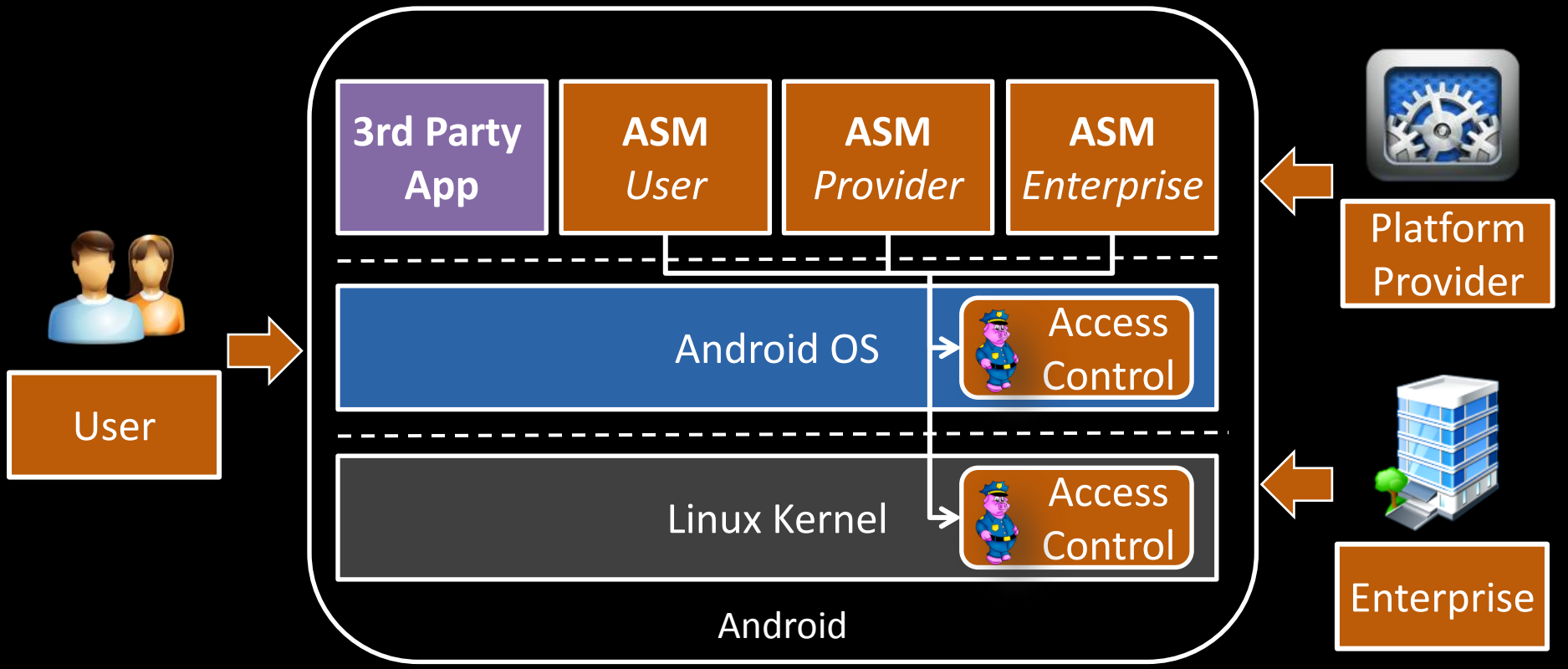
High-level Idea of ASM

- A *modular* access control architecture supporting *multiple stakeholders*
- Deploy *Android Security Modules (ASMs) as apps*



High-level Idea of ASM

- A *modular* access control architecture supporting *multiple stakeholders*
- Deploy *Android Security Modules (ASMs) as apps*

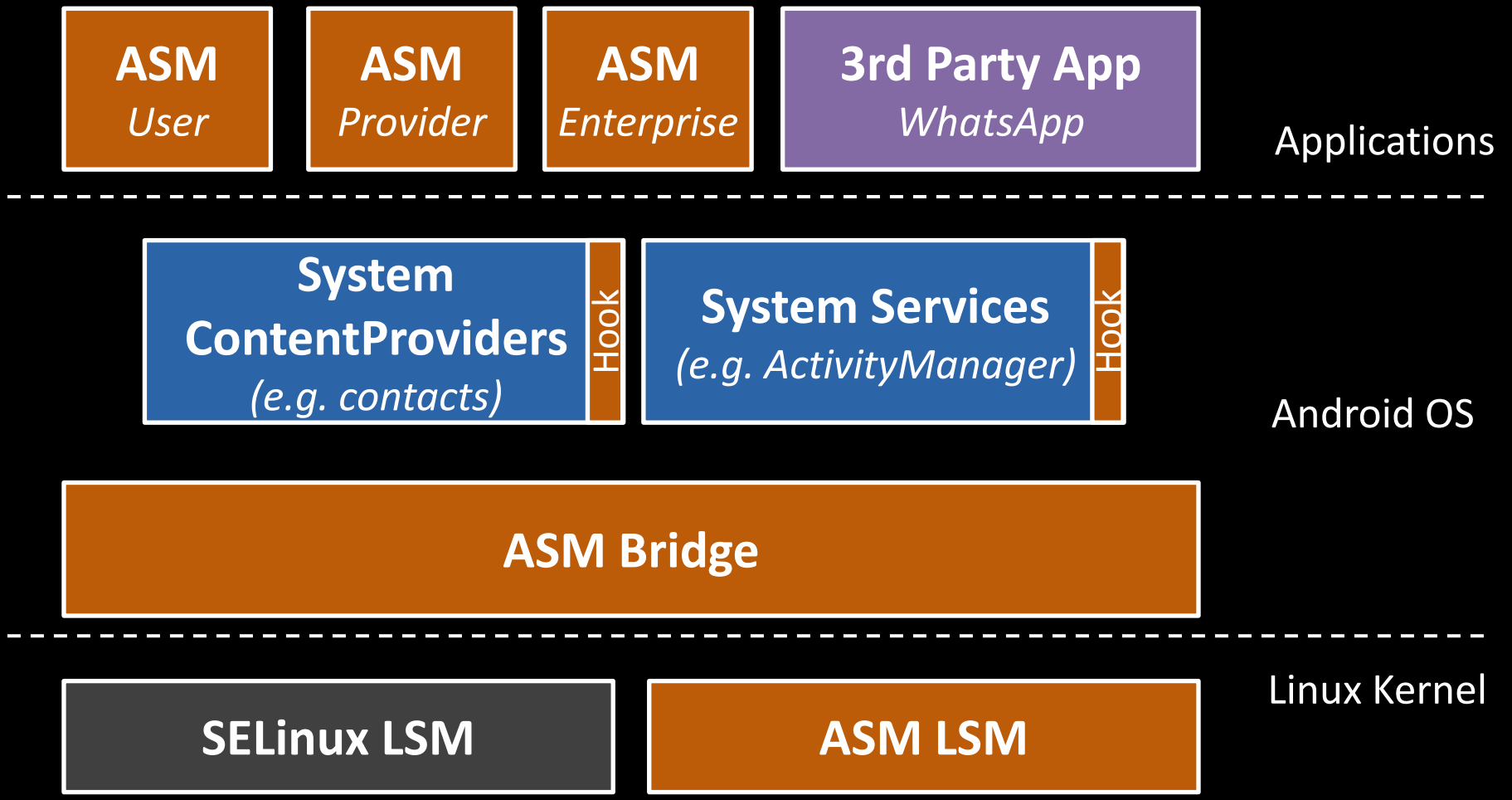


Challenges

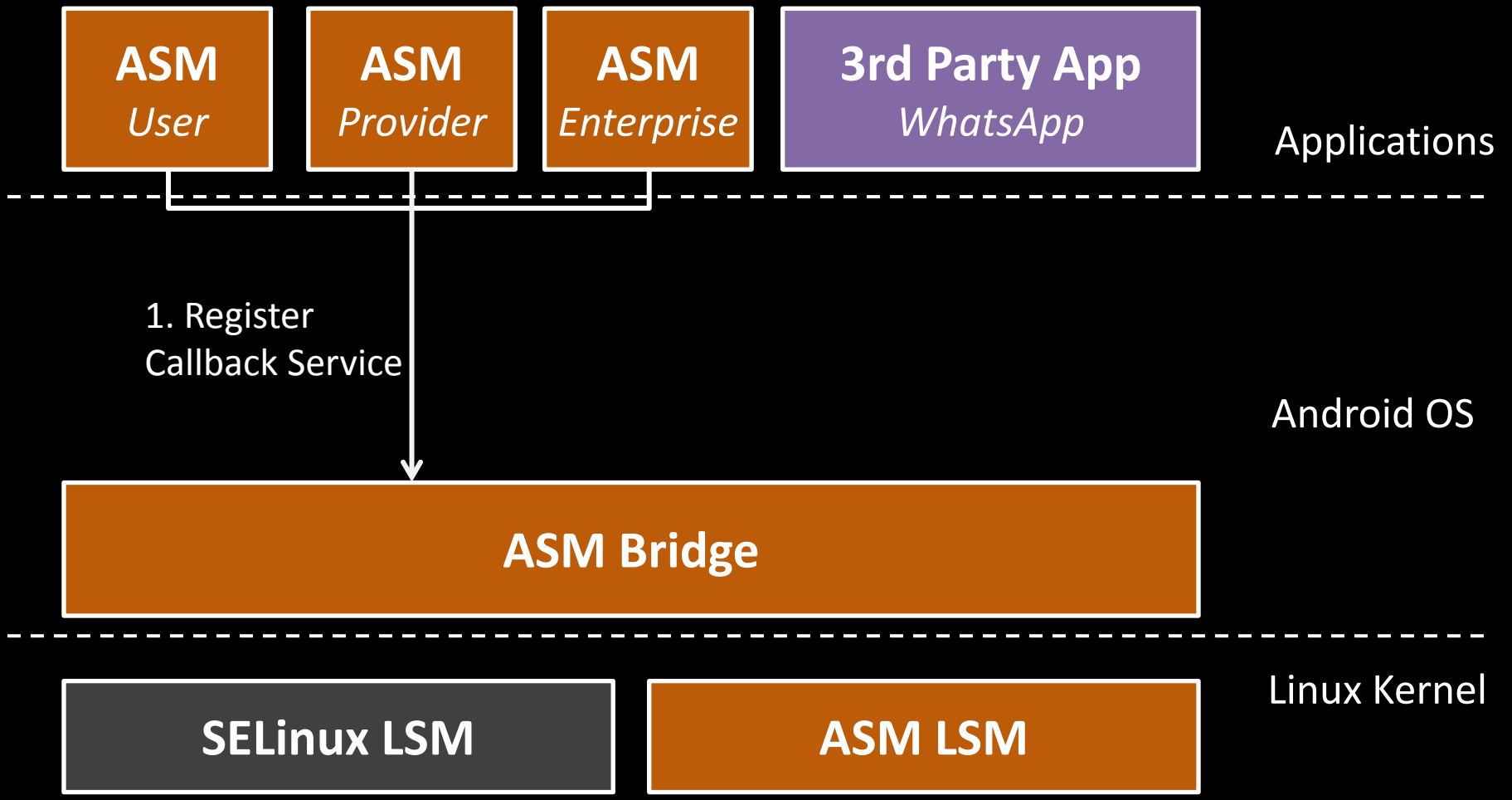
- **Fine-grained access control on all abstraction layers**
  - Handle the *semantics and pecularities* of each layer
- **Preserve existing security invariants**
  - Don‘t overrule *denials* by *default Android access control*
  - Data modification by ASMs only in *well-defined bounds*
- **Efficiency**
  - Only activate hooks when they are *required*
  - Whitelisting for *root processes* and *system apps*
- **Policy Reconcilliation**
  - Handle *decision conflicts* (currently consensus strategy)

Design

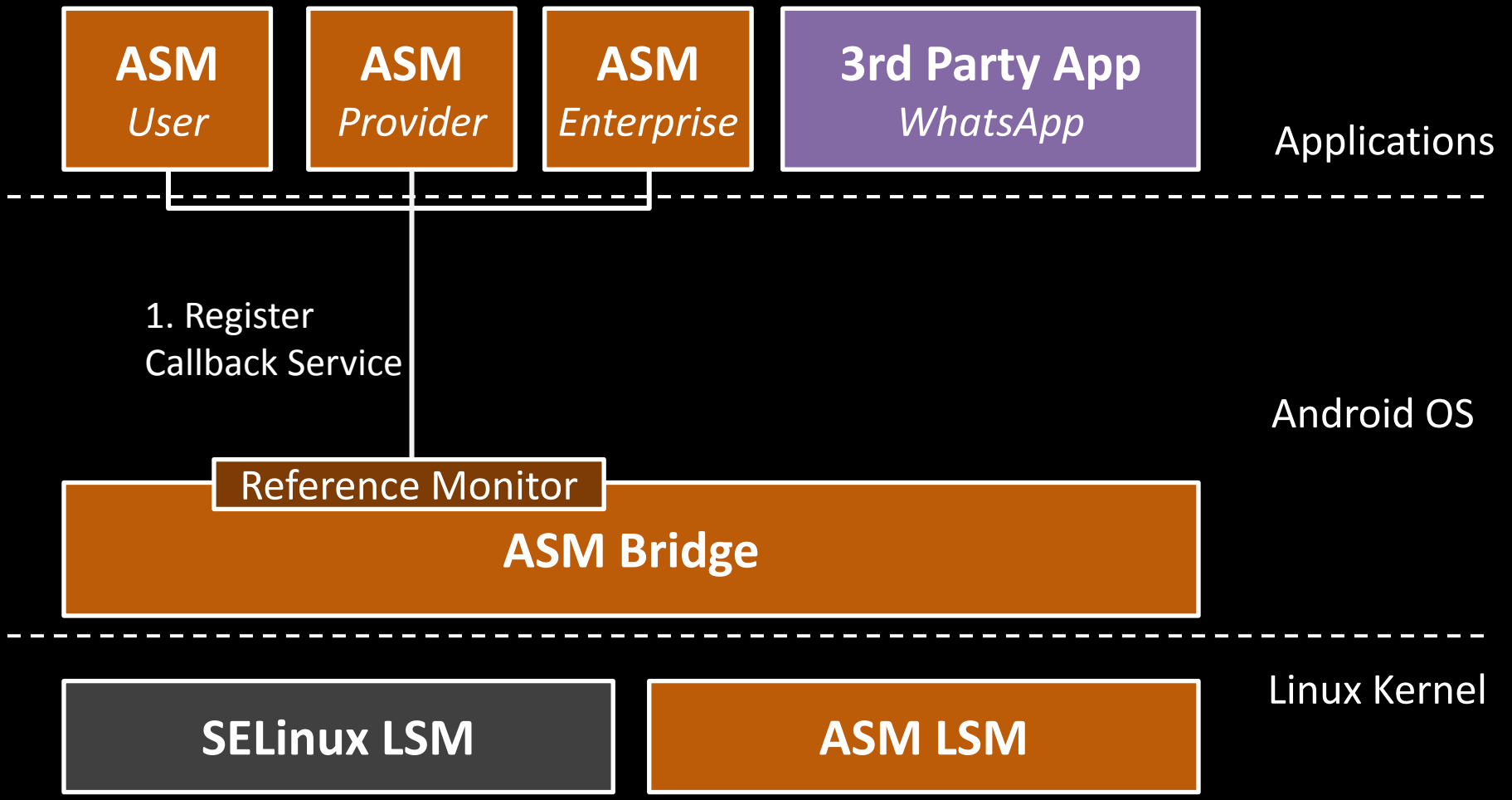
ASM Framework



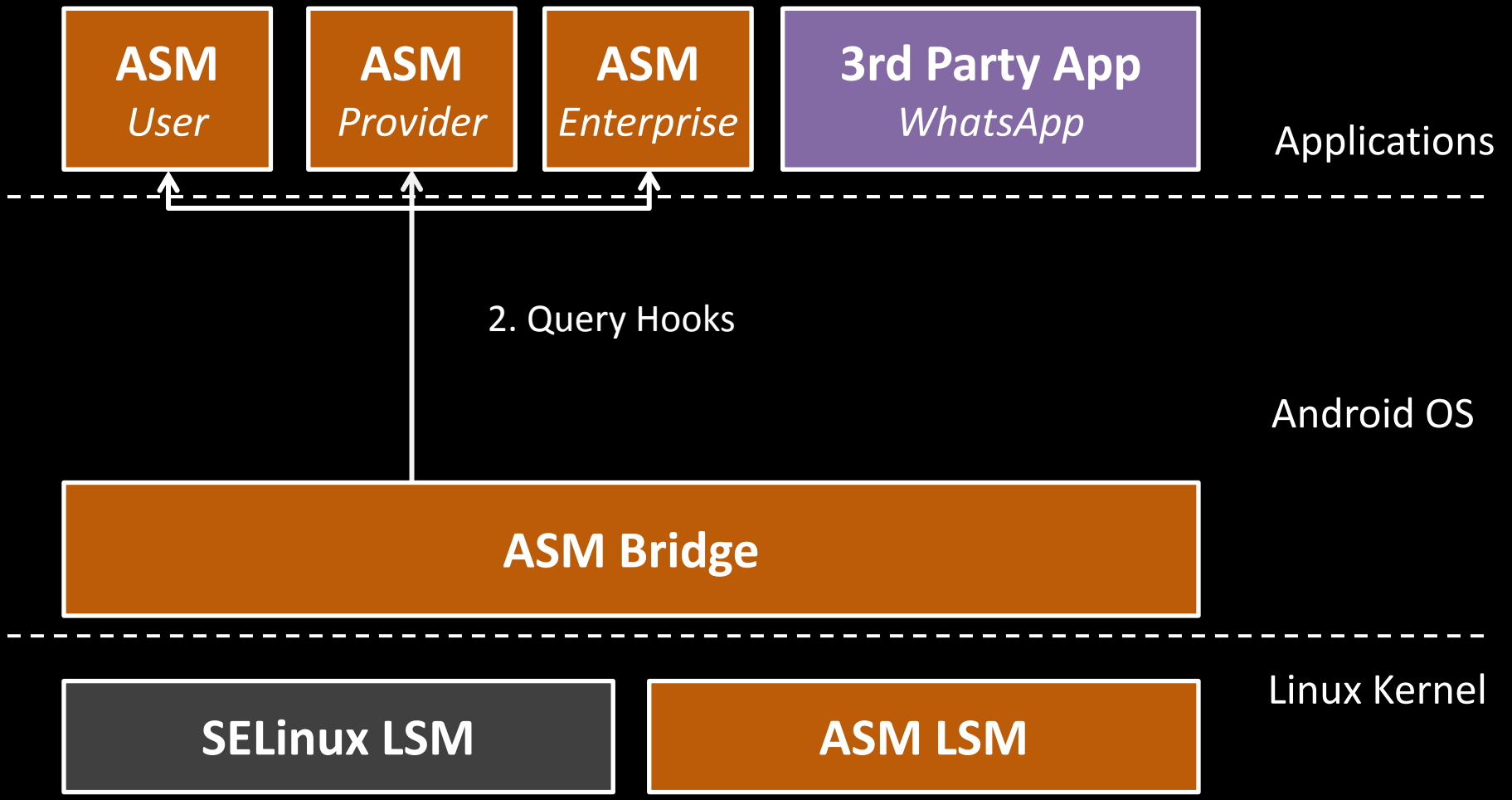
ASM Framework



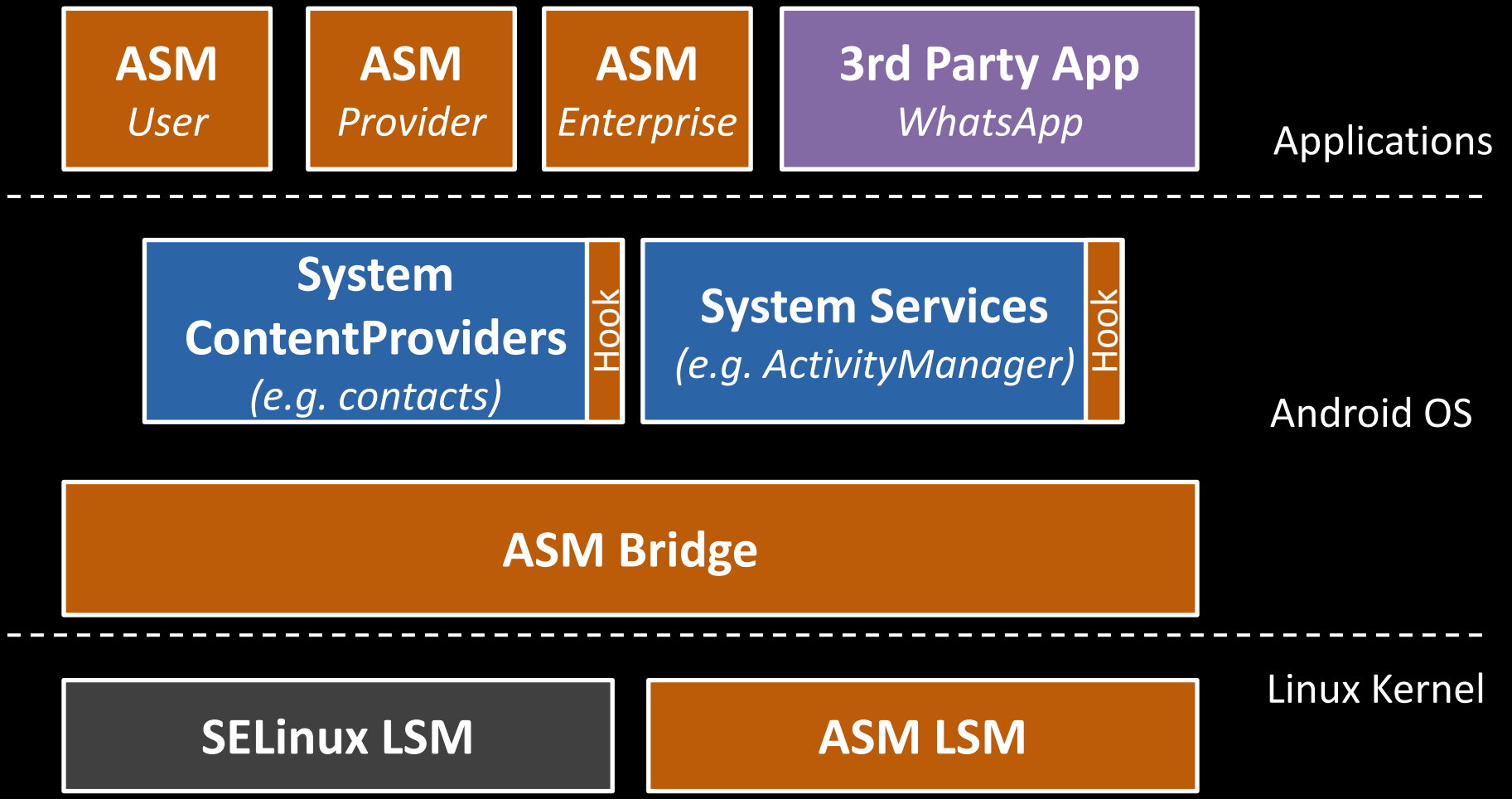
ASM Framework



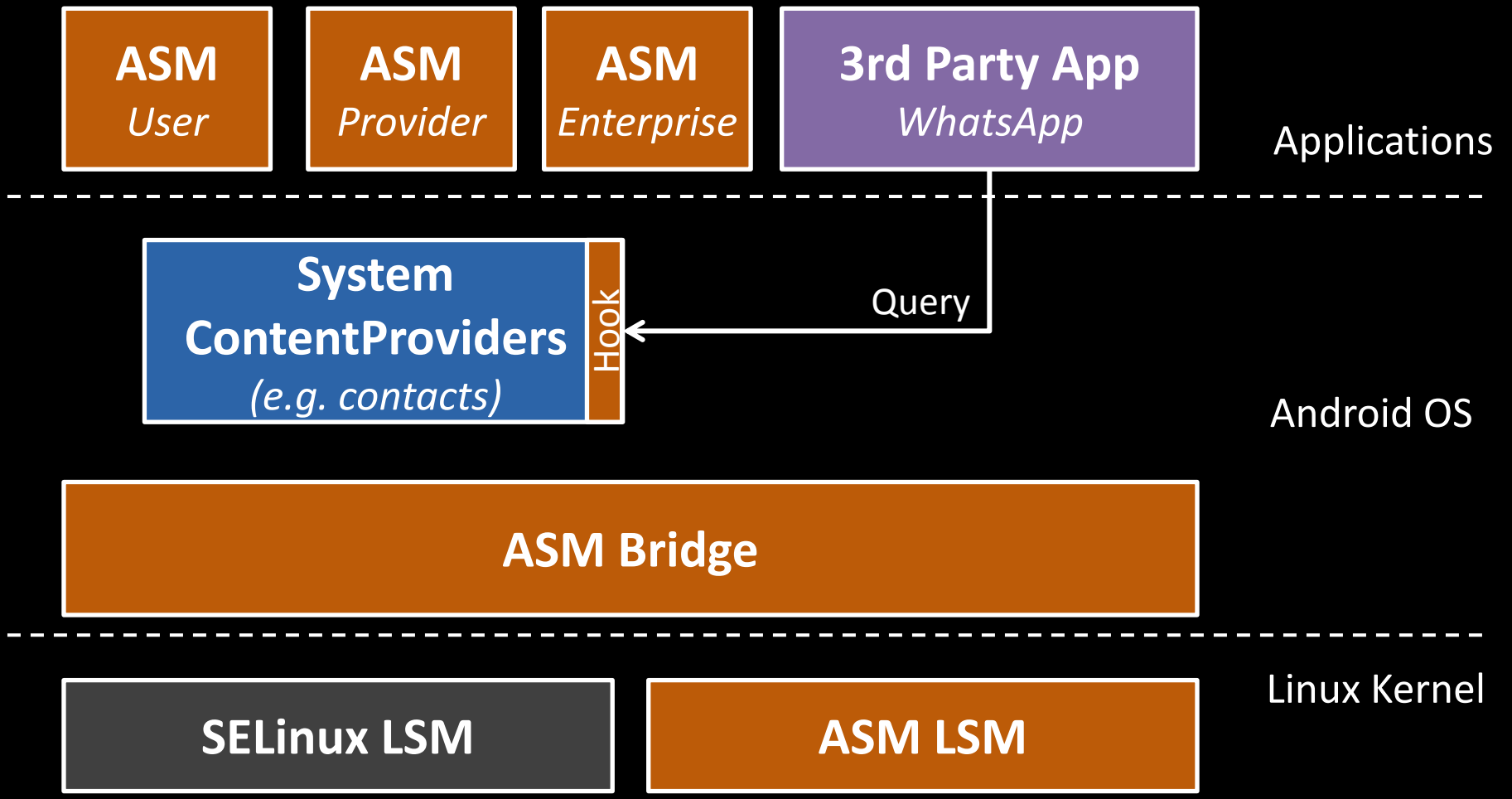
ASM Framework



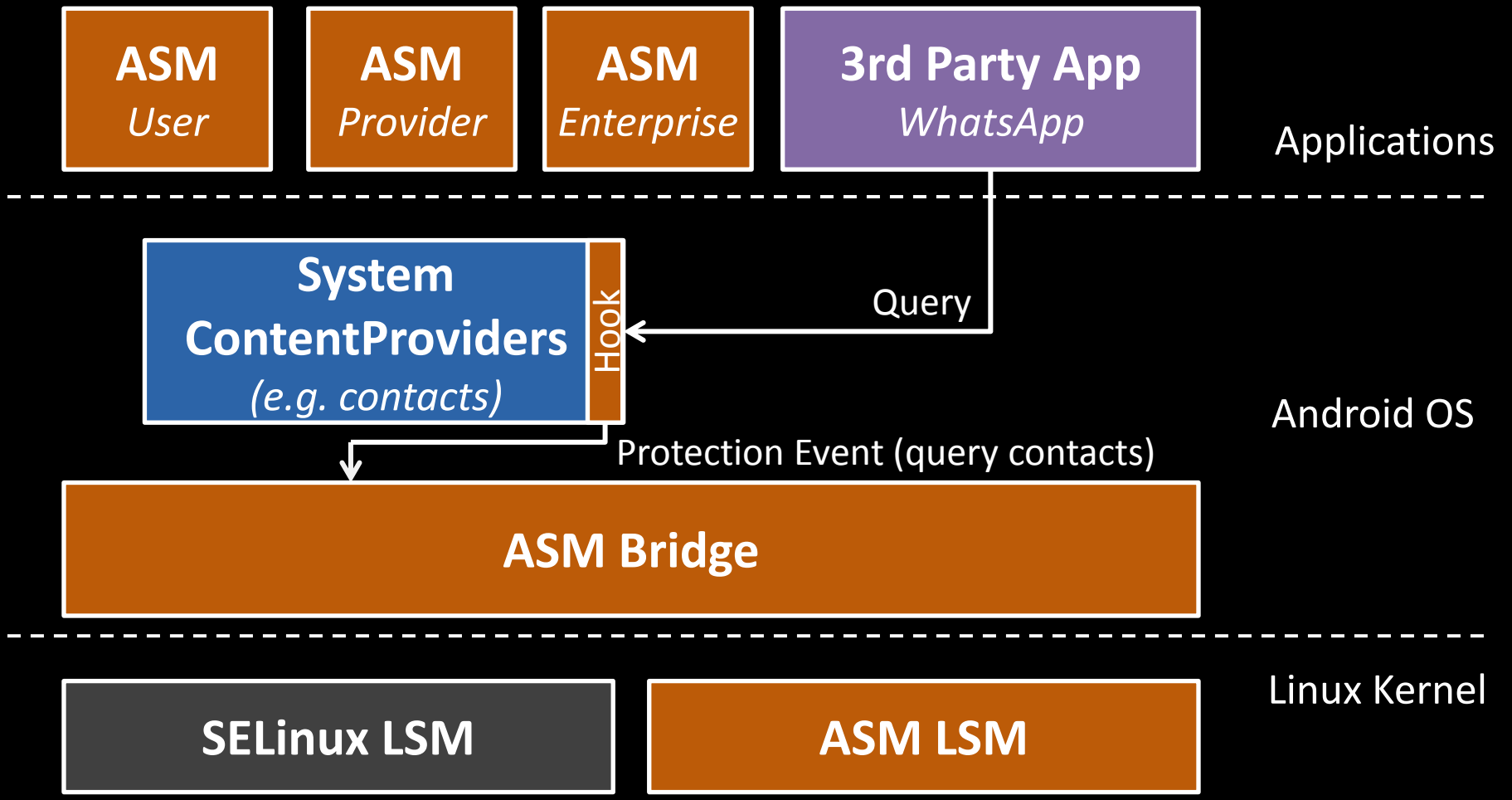
Hook Invocation



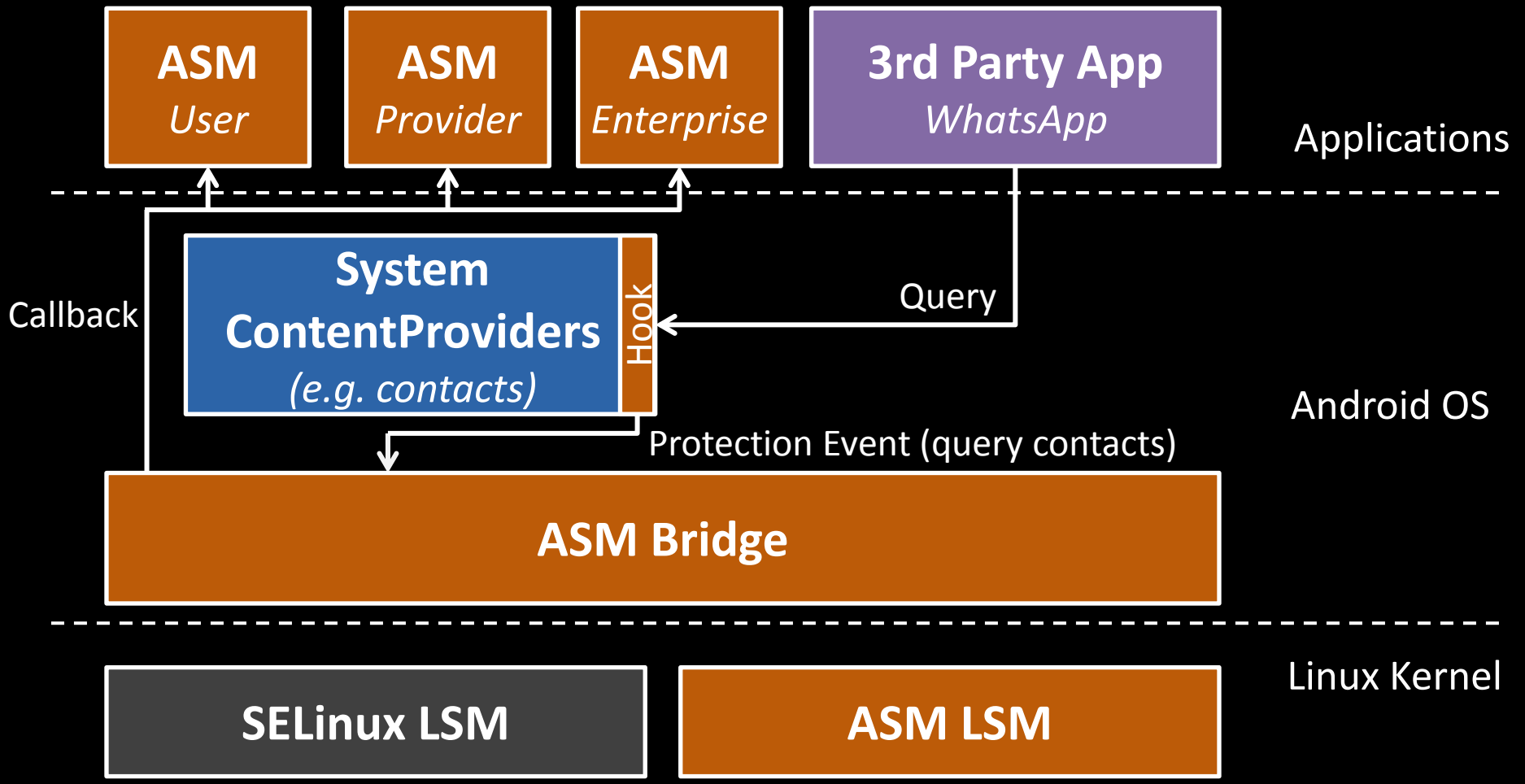
Hook Invocation



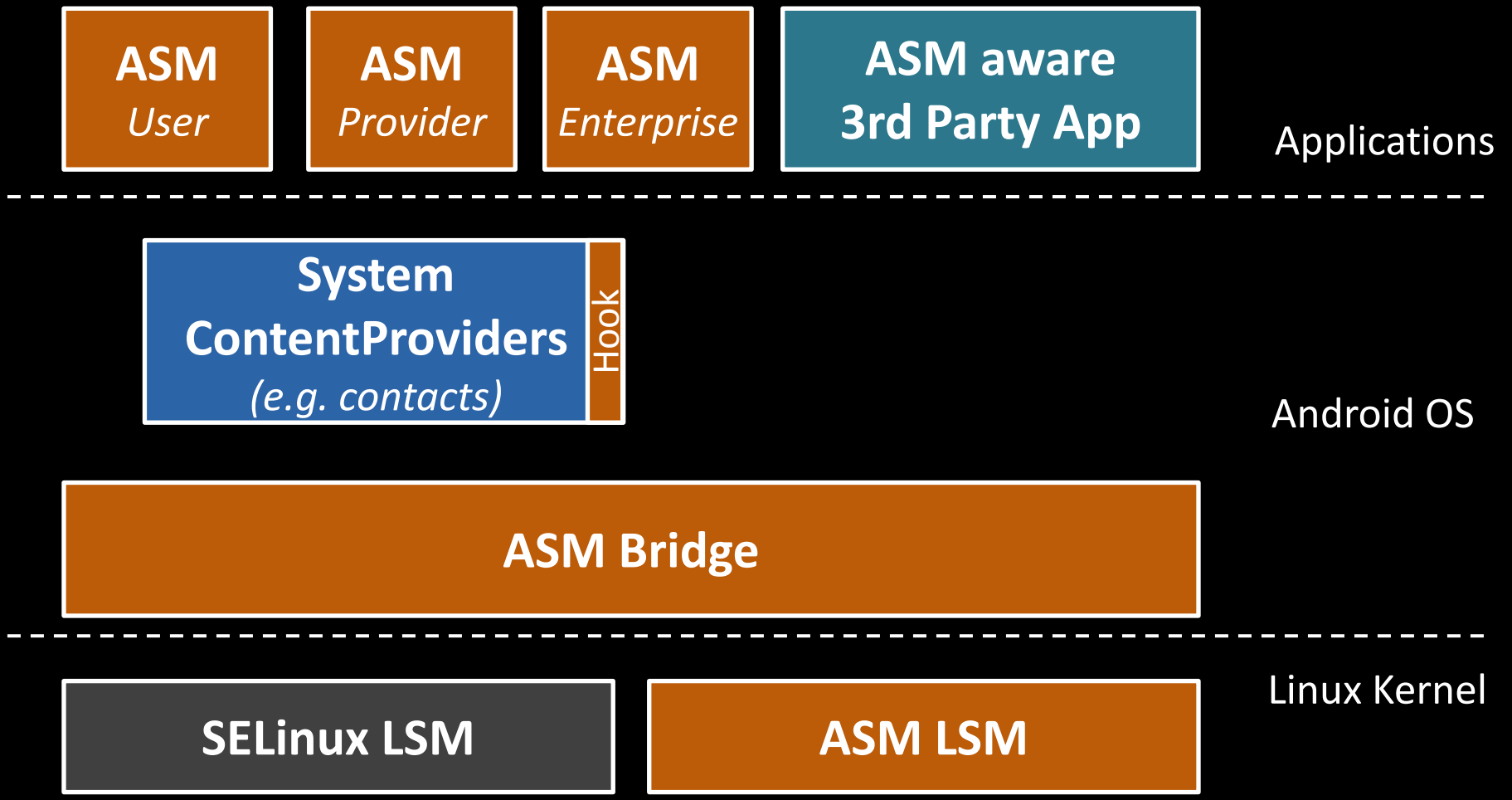
Hook Invocation



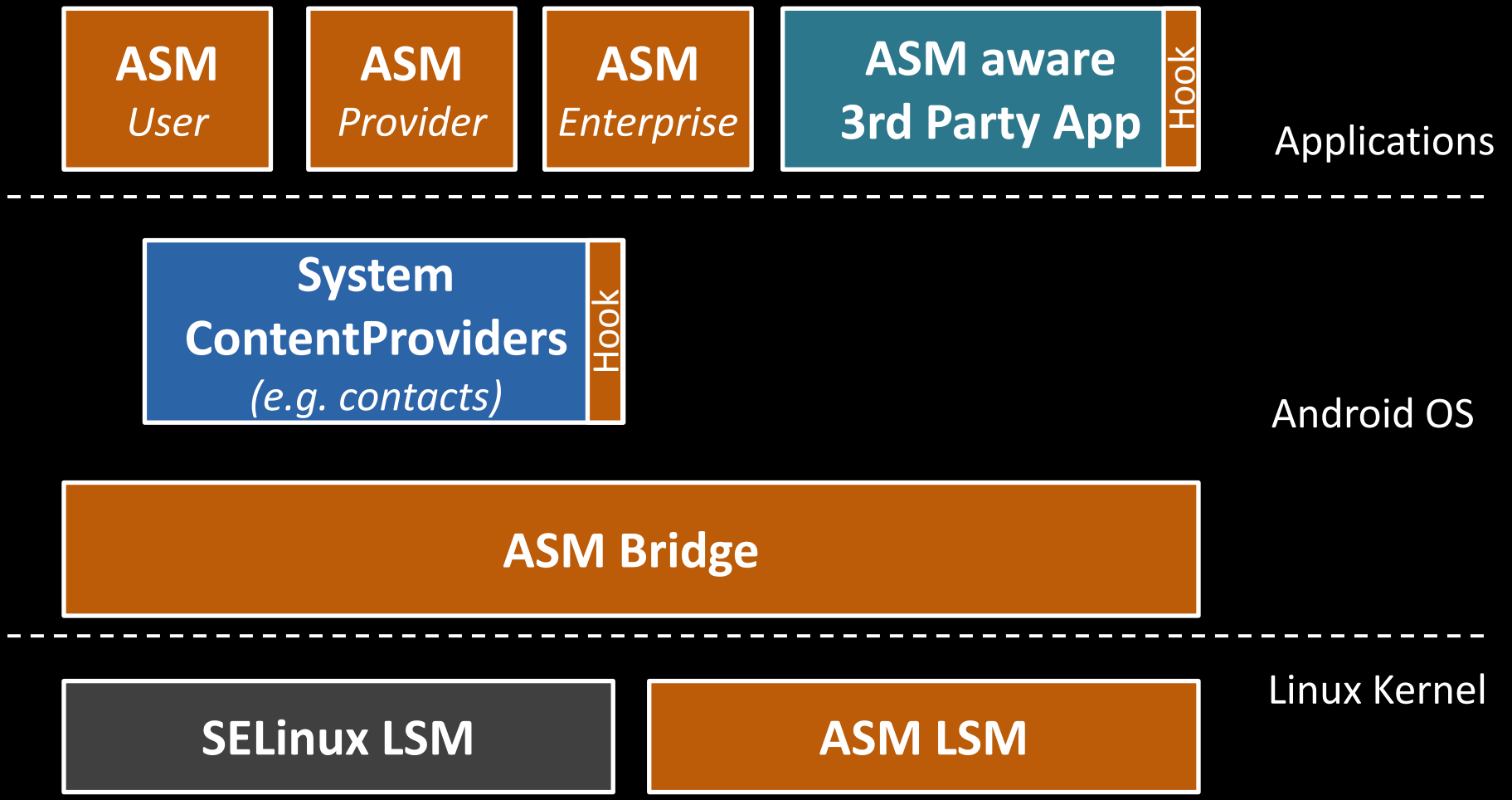
Hook Invocation



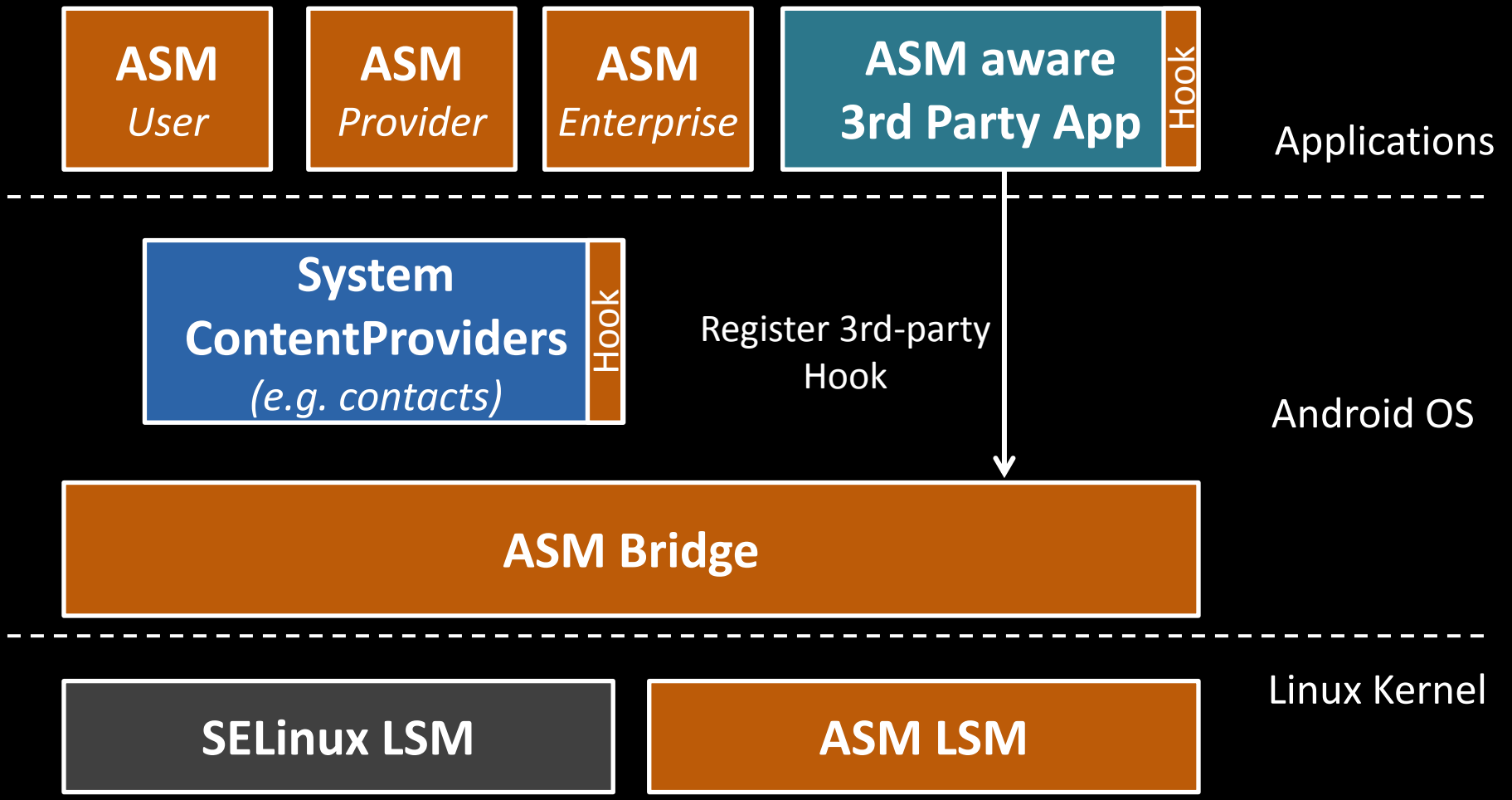
Support for 3rd-Party Hooks



Support for 3rd-Party Hooks



Support for 3rd-Party Hooks



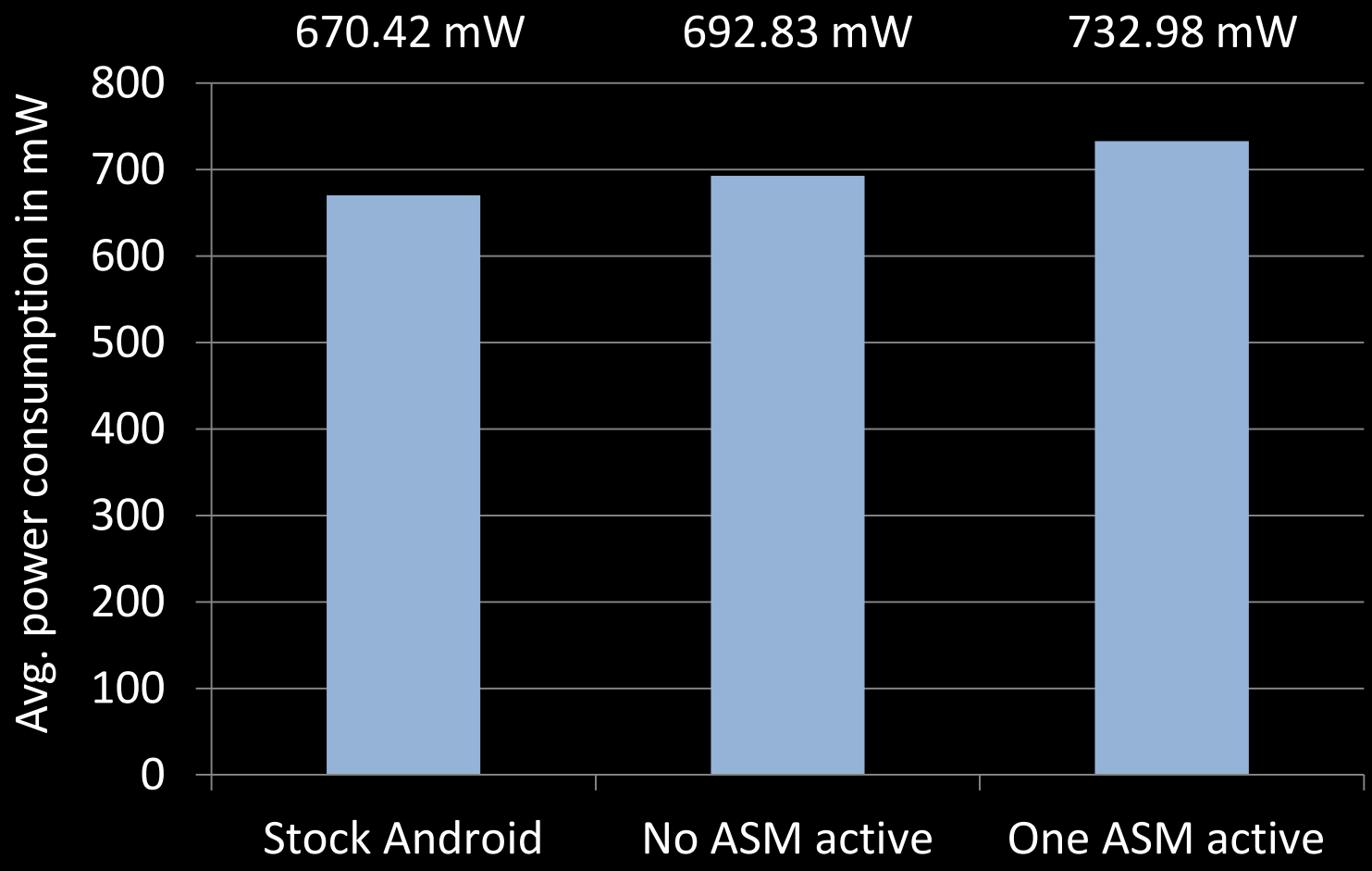
Evaluation

Experiment Setup

- **LG Nexus 4**
- **Android 4.4 (with ASM extensions), Linux MSM Kernel 3.4**
- **Evaluated aspects include User Interface (Activity), Contact, File and Socket operations**
- **Considered impact of a plain ASM**
- **Automated Test Suite**
  - Performance Overhead: Java System.nanotime()
  - Power Consumption: Qualcomm Trepn Profiler

Performance

Power Consumption



Example Use Case

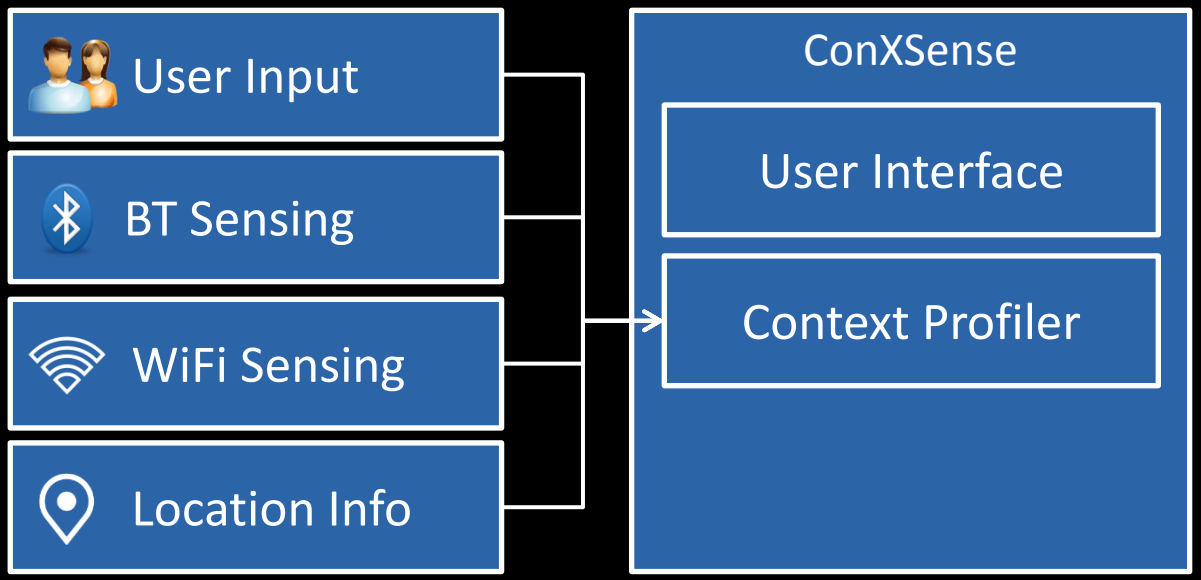
ConXSense
Context Aware Access Control

- Goal: Context-aware access control

ConXSense [ASIACCS 2014]

ConXSense
Context Aware Access Control

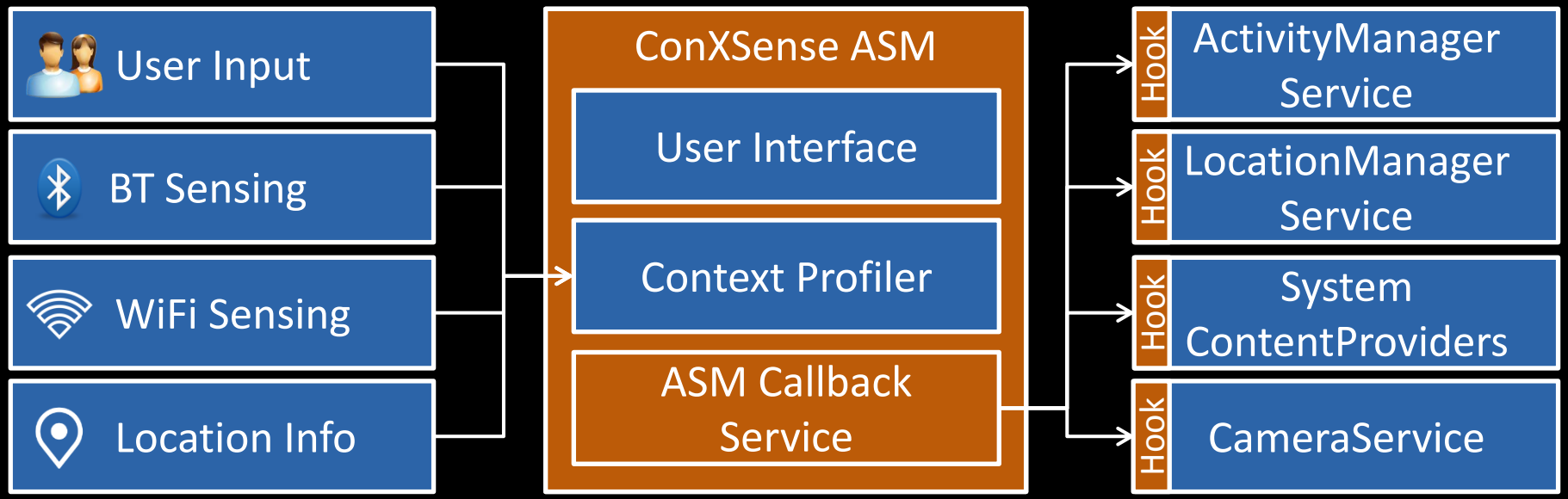
- Goal: Context-aware access control
  - Context-aware access control enforcing policies by user context profiling
  - Includes access control on sensors (e.g., GPS and camera), sensitive information (e.g., contacts) and apps



ConXSense [ASIACCS 2014]

ConXSense
Context Aware Access Control

- Goal: Context-aware access control
  - Context-aware access control enforcing policies by user context profiling
  - Includes access control on sensors (e.g., GPS and camera), sensitive information (e.g., contacts) and apps
- ASM based implementation:



ConXSense [ASIACCS 2014]

Conclusion

- **ASM greatly simplifies use-case specific solutions**
  - Developers don‘t need to modify system components
  - Implementation of security solutions as apps
- **Currently working on further use-cases**
  - Dual Persona Phone
  - Dynamic Application Behaviour Analysis
- **Port to new Android versions**
- **Push ASM to device vendors, AOSP**
  - Google, OEMs – please call us ☺

Thank you!

Questions?

http://www.androidsecuritymodules.org