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

Privacy
- TaintDroid
- AppFence
- MockDroid

IPC Provenance
- QUIRE
- IPC Inspection

Fine-Grained Permissions
- APEX
- CRePE

Permission Constraints
- Kirin

Context-based Apps
- CRePE
- ConXSense

App Communication
- Saint
- XManDroid
- TrustDroid
- Aquifer

Mock Data
- MockDroid
- TISSA
- AppFence

Type Enforcement
- SEAndroid
- FlaskDroid
Android Security Extensions

Access control (hooks) are embedded in sensitive components

Applications

System Apps

3rd Party App

3rd Party App

Android OS

System ContentProviders (e.g. contacts)

Activity Manager Service

Package Manager Service

Framework Libraries

Linux DAC, SELinux/SEAndroid

Linux Kernel
Access control (hooks) are embedded in sensitive components

System Apps

3rd Party App

Access Control (Inlined Reference Monitor)

System ContentProviders (e.g. contacts)

Activity Manager Service

Framework Libraries

Package Manager Service

Access Control

Access Control

Linux Kernel

Android OS

Applications

System Apps

3rd Party App

Linux DAC, SELinux/SEAndroid

ASM - Android Security Modules
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

<table>
<thead>
<tr>
<th>System</th>
<th>Android ICC</th>
<th>Package Manager</th>
<th>Sensors / Phone Info</th>
<th>Fake Data</th>
<th>System Content Providers</th>
<th>File Access</th>
<th>Network Access</th>
<th>3rd Party Hooks</th>
</tr>
</thead>
<tbody>
<tr>
<td>MockDroid</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>XManDroid</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TrustDroid</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FlaskDroid</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CRePE</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Quire</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>TaintDroid</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Kirin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>IPC Inspection</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppFence</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Aquifer</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>APEX</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saint</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SEAndroid</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>TISSA</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Observations

Diverse Goals, but use similar security hooks and mechanisms

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

9/26/2014

ASM - Android Security Modules
High-level Idea of ASM

Android OS

Linux Kernel

Android

3rd Party App
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 peculiarities* 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 Reconciliation**
  - Handle *decision conflicts* (currently consensus strategy)
Design
ASM Framework

Applications

ASM User
ASM Provider
ASM Enterprise
3rd Party App
WhatsApp

Android OS

System
Content Providers
(e.g. contacts)

System Services
(e.g. ActivityManager)

ASM Bridge

Linux Kernel

SELinux LSM
ASM LSM
ASM Framework

1. Register Callback Service

Applications

Android OS

Linux Kernel

ASM User
ASM Provider
ASM Enterprise
3rd Party App
WhatsApp

ASM Bridge

SELinux LSM
ASM LSM

ASM - Android Security Modules

9/26/2014
ASM Framework

1. Register Callback Service

Applications

1. Register Callback Service

Android OS

Linux Kernel

SELinux LSM

ASM LSM

ASM Bridge

Reference Monitor

ASM User

ASM Provider

ASM Enterprise

3rd Party App
WhatsApp
ASM Framework

ASM
User

ASM Provider

ASM
Enterprise

3rd Party App
WhatsApp

Applications

2. Query Hooks

ASM Bridge

Android OS

SELinux LSM

ASM LSM

Linux Kernel

9/26/2014

ASM - Android Security Modules
Hook Invocation

Applications

ASM User
ASM Provider
ASM Enterprise
3rd Party App
WhatsApp

Android OS

System ContentProviders
(e.g. contacts)
System Services
(e.g. ActivityManager)

ASM Bridge

Linux Kernel

SELinux LSM
ASM LSM
Hook Invocation

- **Applications**
  - ASM User
  - ASM Provider
  - ASM Enterprise
  - 3rd Party App (e.g., WhatsApp)

- **Android OS**
  - System Content Providers (e.g., contacts)
  - Query

- **Linux Kernel**
  - SELinux LSM
  - ASM LSM

- **ASM Bridge**
Hook Invocation

ASMs: User, Provider, Enterprise

Applications: 3rd Party App (WhatsApp)

Android OS

System ContentProviders (e.g. contacts)

Protection Event (query contacts)

ASM Bridge

Linux Kernel

SELinux LSM, ASM LSM
Hook Invocation

Applications

Android OS

Linux Kernel

ASM User
ASM Provider
ASM Enterprise
3rd Party App WhatsApp

System ContentProviders (e.g. contacts)

Protection Event (query contacts)

Query

Callback

ASM Bridge

SELinux LSM

ASM LSM
Support for 3rd-Party Hooks

- **ASM User**
- **ASM Provider**
- **ASM Enterprise**
- **ASM aware 3rd Party App**

**System Content Providers** (e.g. contacts)

**ASM Bridge**

**SELinux LSM**

**ASM LSM**

Android OS

Linux Kernel

9/26/2014

ASM - Android Security Modules
Support for 3rd-Party Hooks

- ASM User
- ASM Provider
- ASM Enterprise
- ASM aware 3rd Party App

System ContentProviders (e.g. contacts)

Applications

ASM Bridge

Android OS

SELinux LSM

ASM LSM

Linux Kernel

9/26/2014
Support for 3rd-Party Hooks

- **System ContentProviders** (e.g. contacts)
- **ASM User**
- **ASM Provider**
- **ASM Enterprise**
- **ASM aware 3rd Party App**

Applications

Android OS

Linux Kernel

- **ASM Bridge**
- **SELinux LSM**
- **ASM LSM**

Register 3rd-party Hook
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

- **Activity Start**: Stock Android, No ASM active, One ASM active
- **Contacts Query**: Stock Android, No ASM active, One ASM active
- **File Read**: Stock Android, No ASM active, One ASM active
- **Socket Connect**: Stock Android, No ASM active, One ASM active

**Average time in ms**

- **Activity Start**: Stock Android (15 ms), No ASM active (18 ms), One ASM active (20 ms)
- **Contacts Query**: Stock Android (10 ms), No ASM active (12 ms), One ASM active (15 ms)
- **File Read**: Stock Android (60 ms), No ASM active (65 ms), One ASM active (70 ms)
- **Socket Connect**: Stock Android (1 ms), No ASM active (2 ms), One ASM active (3 ms)
Power Consumption

- Stock Android: 670.42 mW
- No ASM active: 692.83 mW
- One ASM active: 732.98 mW

Avg. power consumption in mW
Example Use Case
ConXSense
Context Aware Access Control

- Goal: Context-aware access control
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
User Interface
Context Profiler
User Input
BT Sensing
WiFi Sensing
Location Info

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 ASM

- User Interface
- Context Profiler
- ASM Callback Service

User Input
BT Sensing
WiFi Sensing
Location Info

ActivityManager Service
LocationManager Service
System ContentProviders
CameraService

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