UNIVERSITÄT
DES
SAARLANDES

Permission Revolution

Shubham Agarwal | May 15th, 2020

Seminar : Selected Topics in Mobile Security, 2020

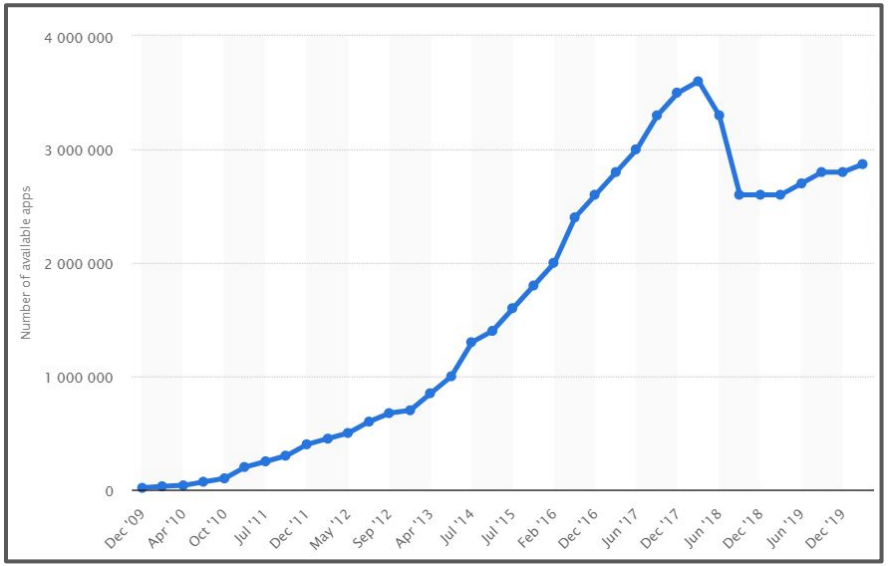
UNIVERSITÄT DES SAARLANDES

Motivation

Current Trends in Mobile Ecosystem

UNIVERSITÄT DES SAARLANDES

- Mobile devices accounted for approx. 52.6% of all Internet traffic (Q4, 2019).
- Mobile space dominated by Android (approx. 71%).
- Approx. 2.5 Million apps on Google Play Store.
- 15+ active mobile app stores.



No. of available applications in the Google Play Store between Dec'09 and Mar'20 - Statista

But, what about user privacy & security?

UNIVERSITÄT DES SAARLANDES

But, what about user privacy & security?


EDITORS' PICK | 129,310 views | Apr 19, 2020, 06:15am EDT

Hacker Claims Popular Android App Store Breached: Publishes 20 Million User Credentials

But, what about user privacy & security?

UNIVERSITÄT DES SAARLANDES


EDITORS' PICK | 935,732 views | May 7, 2020, 05:11am EDT

Samsung Confirms Critical Security Issue For Millions: Every Galaxy After 2014 Affected

Today's Topic of Discussion

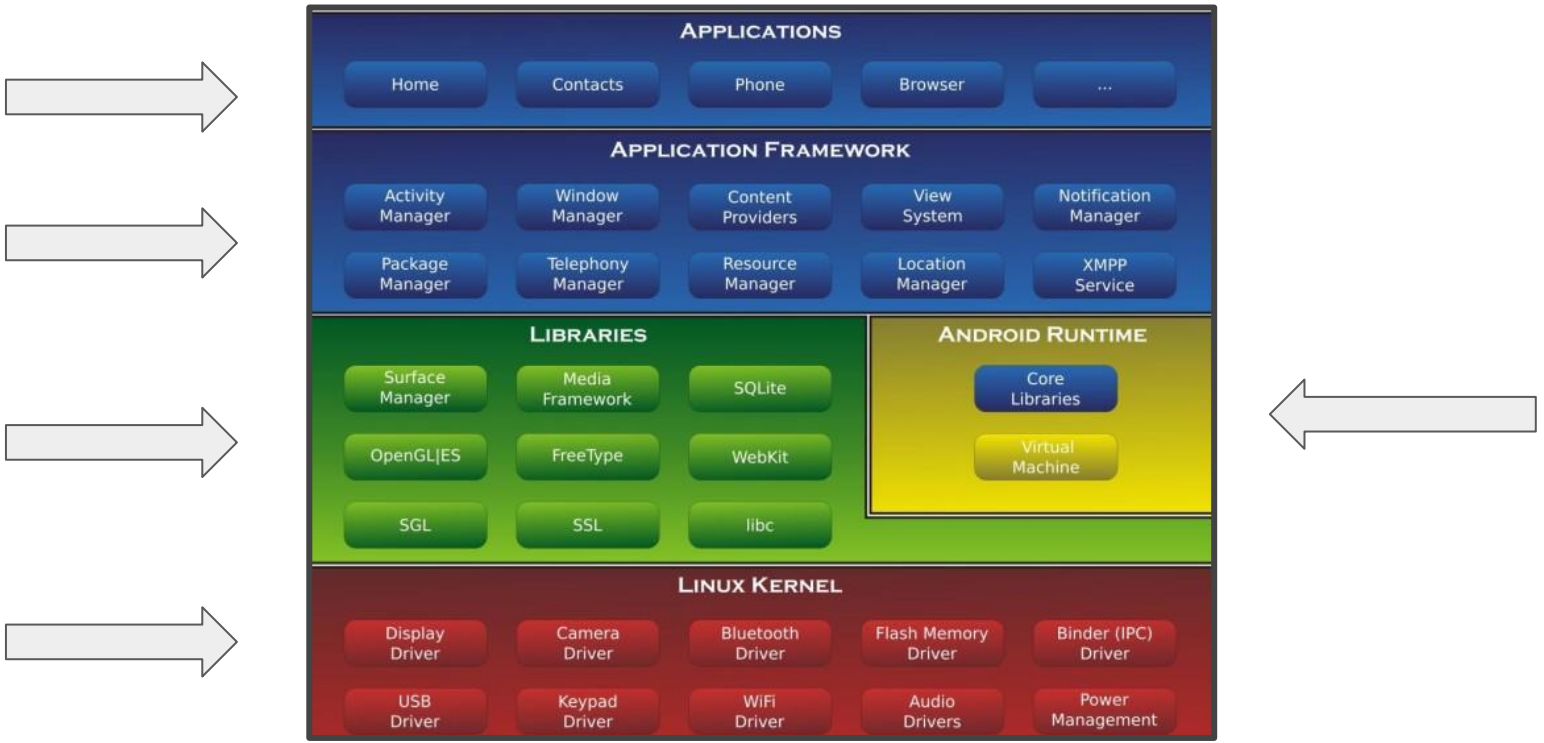
UNIVERSITÄT DES SAARLANDES

1. Rogue applications which steal privacy-sensitive information from the device - Zhou et al.'11 (TISSA).
2. Rogue applications which utilize permission granted to other benign or malicious applications to execute specific security critical operation - Bugiel et al.'12 (extended XManDroid).

UNIVERSITÄT DES SAARLANDES

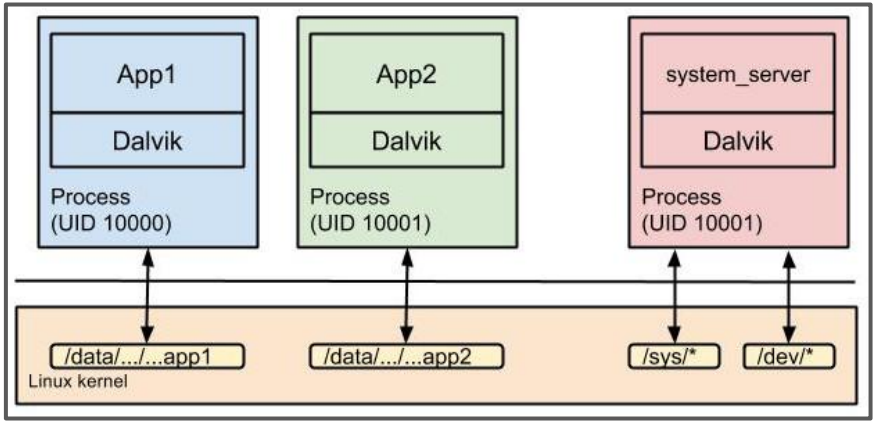
Technical Background

Android Software Stack



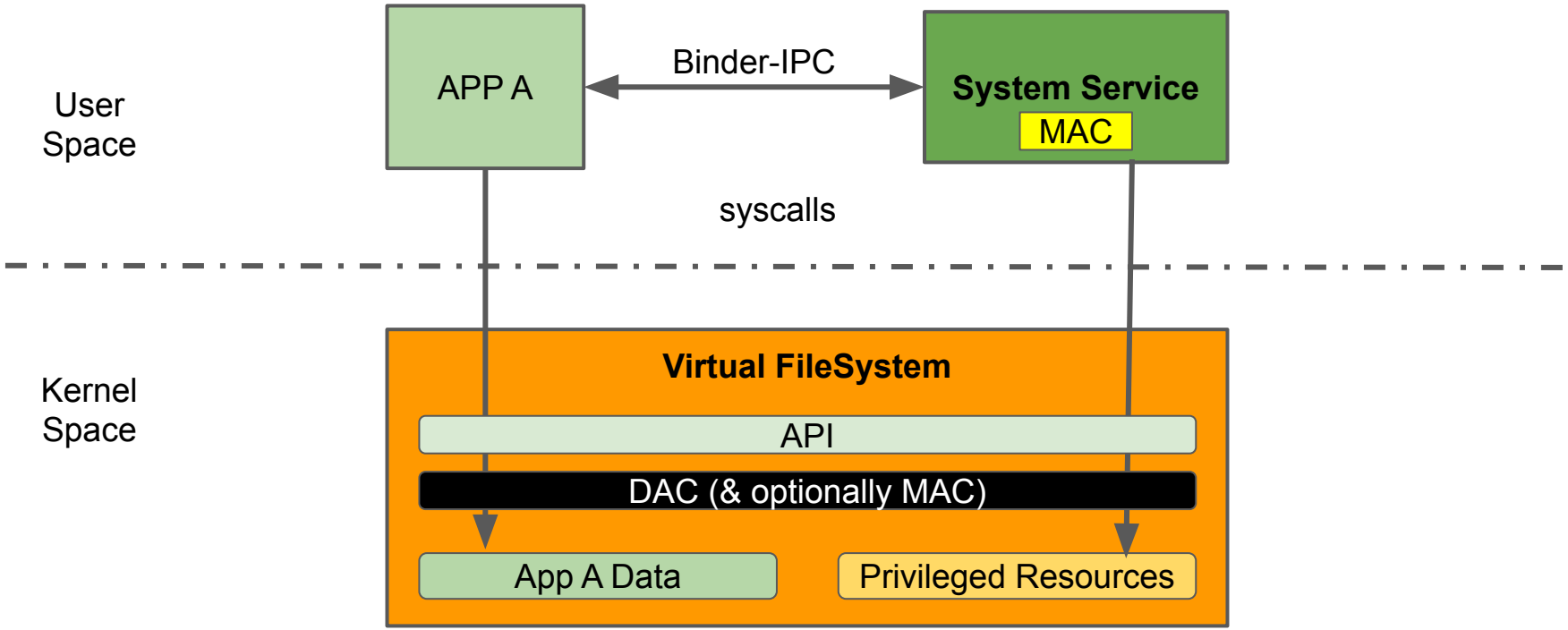
Android Application Sandbox

- Application process & its data
  - confined to the sandbox.
- Applications within one sandbox
  - Share UIDs.
  - Signed by same certificate.



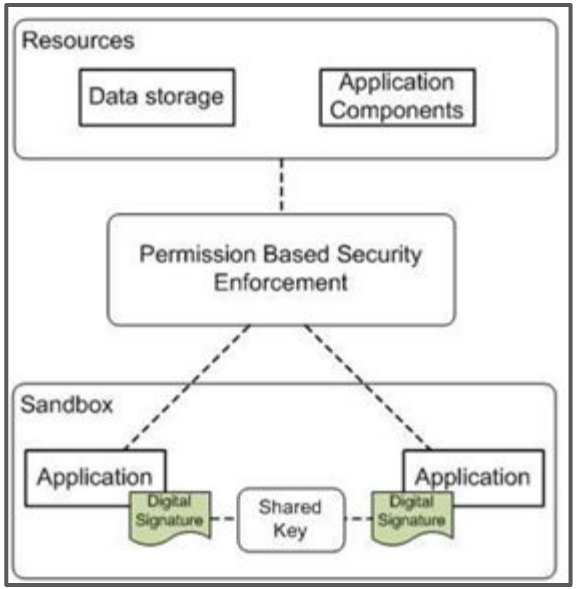
Application Sandbox - Higes

Communication Channels



Android Permissions I

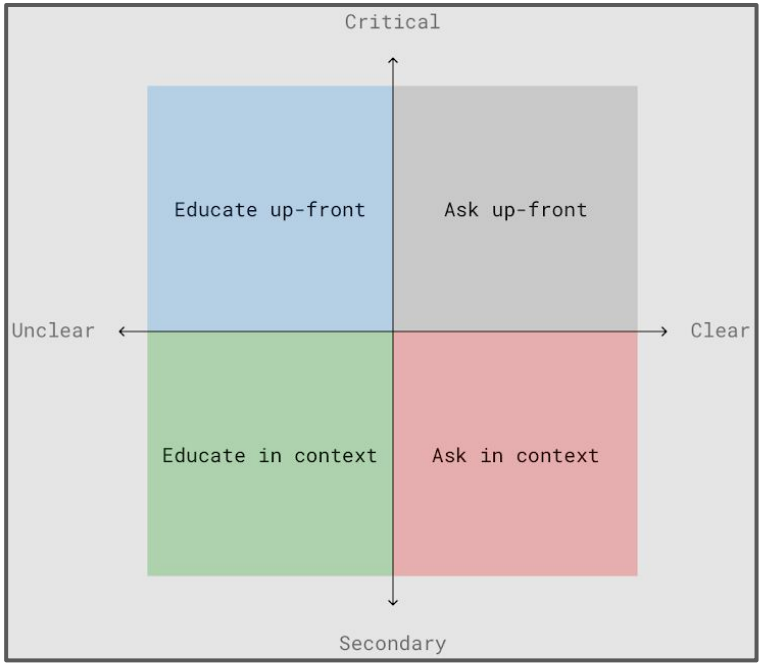
- Functionality of applications - restricted by *permissions* assigned to it.
- *"Principle of Least Privilege"*.



Android Security Model - Medium

Android Permissions II

- Different permission groups.
- Permission Granting Mechanisms:
  - Install-Time.
  - Run-Time (Dynamic).
- Permission Revocation Mechanism.



Permission Granting Scenarios - material.io

What's the fuss all about then?

UNIVERSITÄT DES SAARLANDES

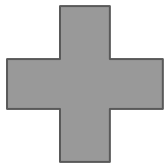
- The app does exactly what it is permitted to, or is at least what it is expected to!
- The concern is the context in which the permission is (ab-)used by the application to process data.
- At times, the applications may even be able to perform operations it isn't permitted to.

Privilege Escalation Vulnerability I

UNIVERSITÄT DES SAARLANDES

Eve

Under-Privileged Malicious App



Alice

Over/Sufficiently-Privileged Benign App

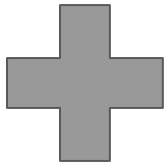
Confused-Deputy Attack

Privilege Escalation Vulnerability II

UNIVERSITÄT DES SAARLANDES

Eve

Under-Privileged Malicious App



Mallory

Another Under-Privileged Malicious App

Collusion Attack

UNIVERSITÄT DES SAARLANDES

Privacy Issues with Permissions

TISSA (Zhou et al.)

UNIVERSITÄT DES SAARLANDES

Research Targets:

- To allow user to control the flow of private information among untrusted third-party applications.
- To allow user to modify the permission configurations for an application after its installation.

TISSA - Research Methodology I

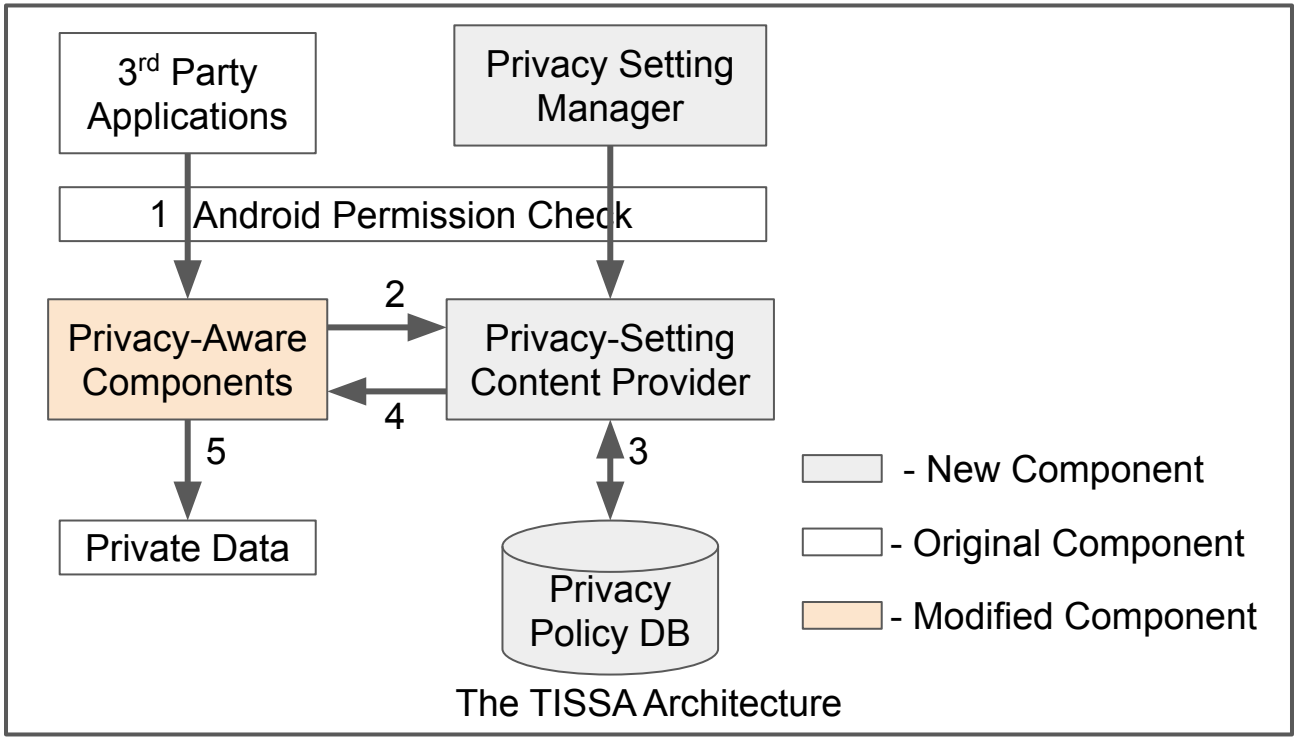
UNIVERSITÄT DES SAARLANDES

Proposed Framework:

- Additional “*privacy mode*”.
- Integration into Android Framework.
- Usability & Backward Compatibility & Performance.

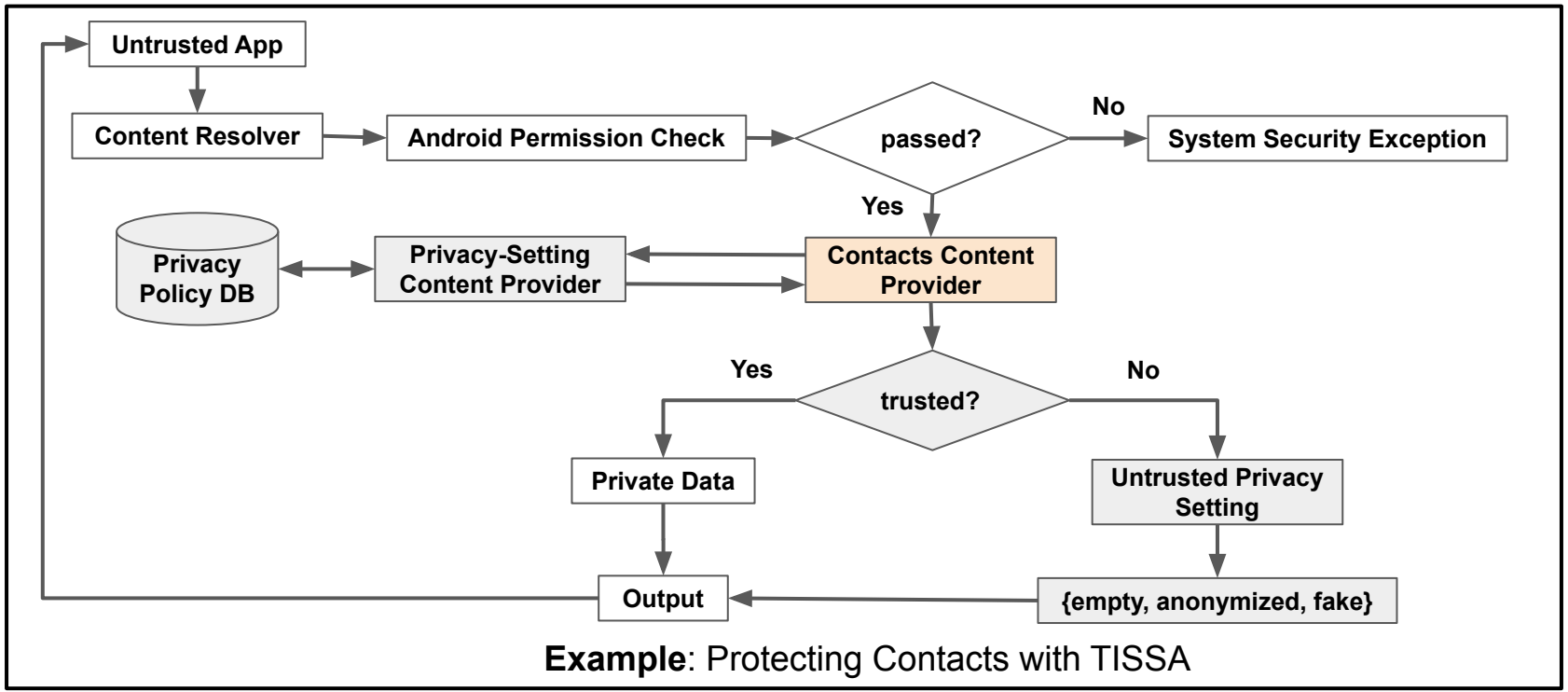
Target: Untrusted 3rd party applications.

TISSA - Research Methodology II



The TISSA Architecture

TISSA - Research Methodology III



Example: Protecting Contacts with TISSA

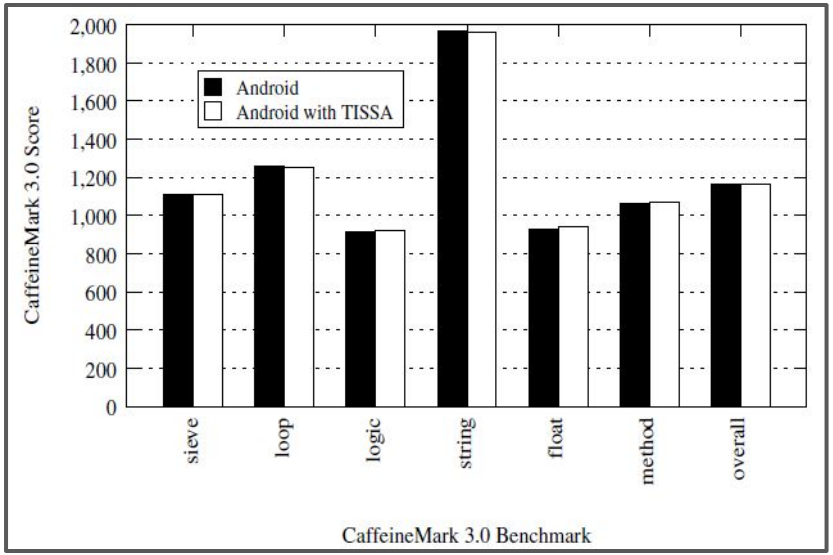
TISSA - Evaluation

UNIVERSITÄT DES SAARLANDES

- Dataset: 24 Apps Selected from Google Play:
  - *Set 1* - 13 apps already known to leak private data.
  - *Set 2* - 11 randomly selected.
- Target Permission: Device Id, Location, Contacts & Call logs.
- Two-step process (*Set 1*):
  1. Find privacy-sensitive data flows.
  2. Modify privacy-settings to replace the flow with empty/fake data.

TISSA - Results

- 14 apps leaked device location.
- 11 apps leaked device identity.
- 6 of them leaked both.
- Performance: negligible overhead.

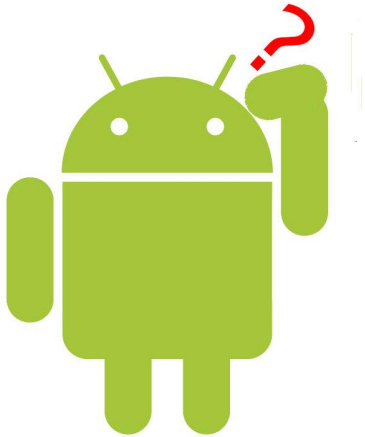


TISSA - Future Works

UNIVERSITÄT DES SAARLANDES

- Additional contextual information for fine-grained permission control needed (Votipka et al., USENIX'18; Wijesekara et al., USENIX'15).
- Similar *personalized privacy assistants* & *plugins* proposed (Liu et al., USENIX'16; Raval et al., MobiSys'19).
- Runtime evaluation and defense from information stealing (Diamantaris et al., ACM'19).
- Heuristic based privacy templates to store privacy preferences.

UNIVERSITÄT DES SAARLANDES



Security Issues with Permissions

XManDroid (Bugiel et al.)

UNIVERSITÄT DES SAARLANDES

Research Targets:

- To establish a system-centric solution to enforce security policies on inter-process communication:
  - Run-time monitoring
  - Kernel-level MAC
  - Kernel to Middleware Communication.
- With legacy compatibility & negligible performance overhead.

XManDroid - Threat Models

UNIVERSITÄT DES SAARLANDES

I.
Known Confused Deputy Attacks via Direct Communication Channel.

Weak Adversary

II.
I. + Unknown Confused Deputy Attacks via Indirect Communication Channel.

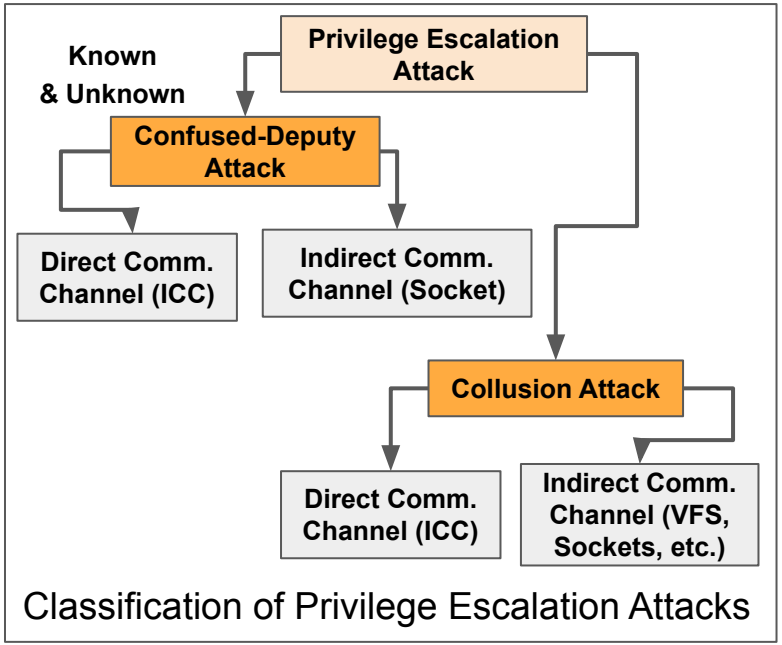
Basic Adversary

III.
II. + Collision Attack via Direct Communication Channel

Advanced Adversary

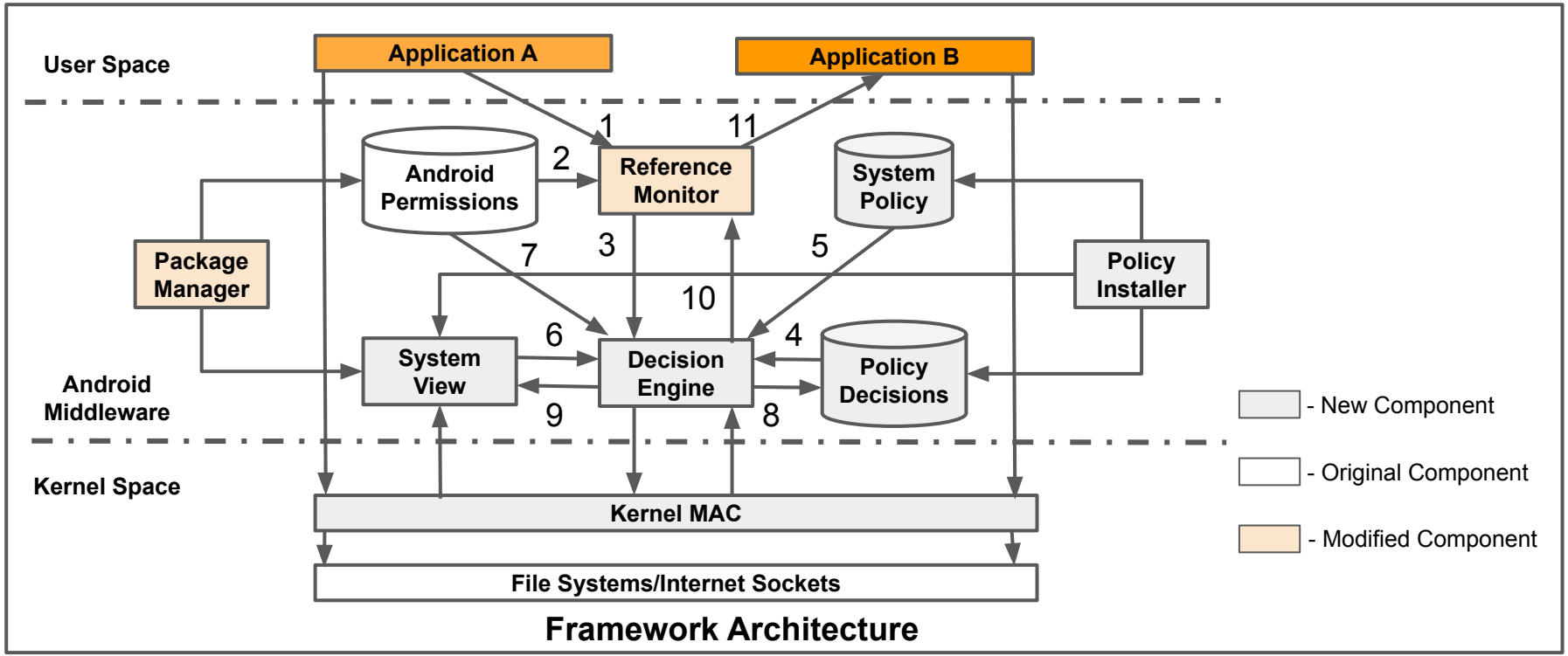
IV.
III. + Collision Attack via Indirect Communication Channels.

Strong Adversary

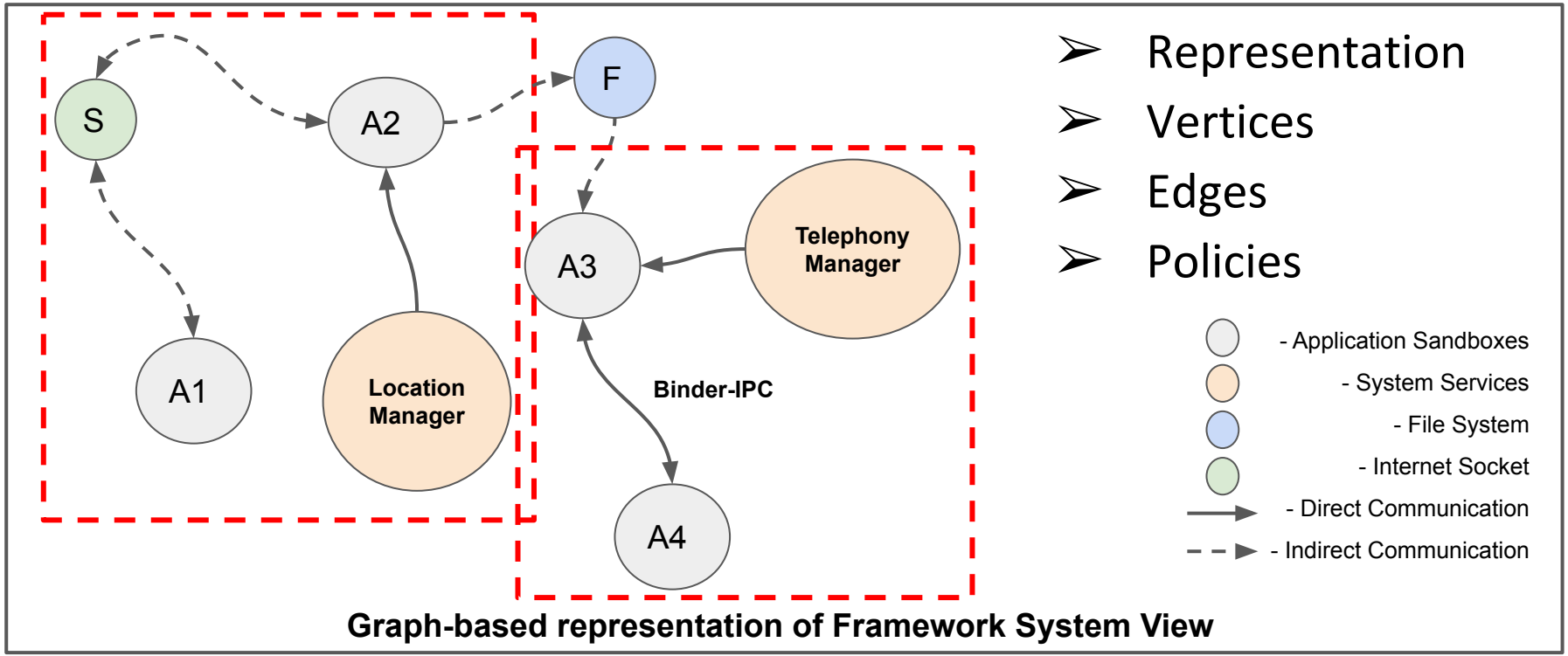


Classification of Privilege Escalation Attacks

XManDroid - Proposed Architecture I



XManDroid - Proposed Architecture II



Graph-based representation of Framework System View

XManDroid - Evaluation I

UNIVERSITÄT DES SAARLANDES

- Dataset: 50 3rd Party Apps.
- Testing Mode: Manual.
- Communication Patterns:
  - ICC.
  - Indirect communication channels.

Attack Detection Efficiency:

- Falsely denied communication.
- Expected result on known cases.
- Sample Applications.

XManDroid - Evaluation II

UNIVERSITÄT DES SAARLANDES

Type	Calls	Average (ms)	Std. dev. (ms)
Original Reference Monitor runtime for ICC			
system	11003	0.184	2.490
DecisionEngine overhead for ICC			
uncached	312	6.182	9.703
cached	10691	0.367	1.930
Intents	1821	8.621	29.011
DecisionEngine overhead for file read			
file read	389	3.320	4.088

ICC Performance Results

Type	Average (ms)	Std. dev. (ms)
Read access to System Content Providers		
total number of accesses: 591		
read	10.317	41.224
overhead	4.983	36.441
Read access to System Services		
total number of accesses: 87		
read	8.578	20.241
overhead	0.307	0.4318

System Component Performance Results

XManDroid - Future Works

UNIVERSITÄT DES SAARLANDES

- IPC provenance information to avoid confused-deputy attacks (Bugiel et al., ACSAC'14).
- Large Scale analysis of malware collusion patterns (Elish et al., IEEE'15).
- Privacy-protecting access control models for apps using SELinux policies (Bugiel et al., USENIX'13; Smalley et al., NDSS'13).
- Inter-process stack inspection to restrict permission usage by third-party libraries (Seo et al., NDSS'16).

UNIVERSITÄT DES SAARLANDES

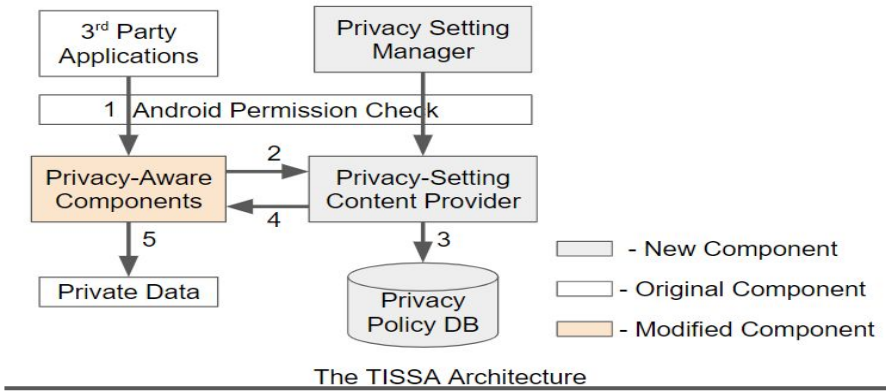
Discussion

Discussion

UNIVERSITÄT DES SAARLANDES

- Key Parameter: Usability & False Positives
- User-involvement: key to contextual integrity.
- Performance overhead: During runtime analysis.
- Vetting: Static (at app store) vs Dynamic (at runtime).

Summary



The TISSA Architecture