Resolving the Predicament of Android Custom Permissions

Güliz Seray Tuncay, Soteris Demetriou, Karan Ganju, Carl A. Gunter

University of Illinois at Urbana - Champaign

#NDSS18
Install-time Permissions
< version 6
Install-time Permissions
< version 6
Install-time Permissions < version 6

Permission Types

- Normal
- Signature
- Dangerous
- SignatureOr System
Install-time Permissions
< version 6

Runtime Permissions
>= version 6
Runtime Permissions

>= version 6

Permission Types

- Normal
- Signature
- Dangerous
Permission Groups
Permission Groups

- read your contacts
- find accounts on the device
- modify your contacts
- precise location (GPS and network-based)
- approximate location (network-based)
- record audio
Custom Permissions

Permission Types

- Normal
- Signature
- Dangerous

App A
- Protect Exported App Components

App B
Prevalence of custom permissions

- 65% apps declare custom permissions
- 70% apps use custom permissions
- 1350 permissions total # of custom permissions
No clear distinction between system permissions and custom permissions
No clear distinction between system permissions and custom permissions

Declared by the system

Declared by 3rd party apps
My_Permission

normal

Microphone Group

My_Permission

record audio
**My_Permission**

**Microphone Group**

- normal

**My_Permission**

- record audio

**App permissions**

CustomPermissionAppUpdateBug

- Microphone
Custom Permission App Update Bug

Custom permission exploit!

START RECORDING

STOP RECORDING

Allow CustomPermissionApp to record audio?

DENY ALLOW

My_Permission

normal

Microphone Group

My_Permission

Granted

record audio
Custom permission exploit!

START RECORDING

STOP RECORDING

My_Permission

dangerous

Microphone Group

My_Permission

record audio

Granted
My_Permission

Microphone

My_Permission

dangerous

Microphone Group

My_Permission

record audio

Granted

Granted
My_Permission

Microphone Group
dangerous

record audio

Granted

Granted
No distinction between custom permissions owners
Skype_Permission

signature

FCFS
App B

Skype_Permission

signature

dangerous

Granted

Skype_Permission

Granted
cusper

“considered to have been born on a cusp between significant generations”
cusper

“considered to have been born on a cusp between significant generations”
Decisions made by principals outside the framework’s Trusted Compute Base affect enforcement at runtime

→ privilege escalation

Custom permissions are claimed on a FCFS basis

→ spoofing

Software testing

Systematically addresses the lack of separation of trust by decoupling system from custom permissions

Provides a backward-compatible OS-level naming convention for tracking ownership of custom permissions

Formally verified to be correct
Decisions made by principals outside the framework’s Trusted Compute Base affect enforcement at runtime

—> privilege escalation

Custom permissions are claimed on a FCFS basis

—> spoofing

Systematically addresses the lack of separation of trust by decoupling system from custom permissions

Provides a backward-compatible OS-level naming convention for tracking ownership of custom permissions

Formally verified to be correct
Decisions made by principals outside the framework’s Trusted Compute Base affect enforcement at runtime

→ privilege escalation

Custom permissions are claimed on a FCFS basis

→ spoofing

Systematically addresses the lack of separation of trust by decoupling system from custom permissions

Provides a backward-compatible OS-level naming convention for tracking ownership of custom permissions

Formally verified to be correct
Cusper enhancements
declaring a custom permission

Skype_Permission
Cusper enhancements
declaring a custom permission

FINE_LOCATION
RECORD_AUDIO
CAMERA
Skype_Permission
Cusper enhancements
declaring a custom permission

Skype_Permission

Permission Type Extension

FINE_LOCATION
RECORD_AUDIO
CAMERA
Skype_Permission

Cusper enhancements
declaring a custom permission

Skype_Permission

Permission Type Extension

FINE_LOCATION
RECORD_AUDIO
CAMERA
Skype_Permission
Cusper enhancements
declaring a custom permission

- Permission Type Extension
- Name Translation

FINE_LOCATION
RECORD_AUDIO
CAMERA

Skype_Permission
Cusper enhancements
declaring a custom permission

- Permission Type Extension
- Name Translation

Microphone Group

Skype_Permission

FINELOCATION
RECORD_AUDIO
CAMERA
Cusper enhancements
grating a custom permission

Skype_Permission

Permission Lookup

FINE_LOCATION
RECORD_AUDIO
CAMERA

:Skype_Permission
Cusper enhancements
granting a custom permission

Permissions:
- Permission Lookup
- Name Translation

Device Permissions:
- FINE_LOCATION
- RECORD_AUDIO
- CAMERA

Permission Status:
- Skype_Permission: Granted
Cusper enhancements
granting a custom permission

Permission Lookup
Name Translation

FINE_LOCATION
RECORD_AUDIO
CAMERA

Skype_Permission

Grant

Grant
installing an app

Runtime (ms)
granting a signature permission to access a service
granting a dangerous permission

2 ms
granting a dangerous permission
effectiveness

Formal Verification
formal verification

Implementation

Alloy Model
formal verification: security properties

Dangerous permissions are never granted without user interaction

An app’s components cannot be accessed by other unauthorized apps
Summary

- Security analysis on custom permissions revealed serious security vulnerabilities (acknowledged by Google).
- Designed CUSPER which introduces mechanisms for separating system and custom permissions.
- Introduced a strategy for tracking permission ownership.
- Introduced the first formal model of Android runtime permissions and used it to formally verify correctness of CUSPER.