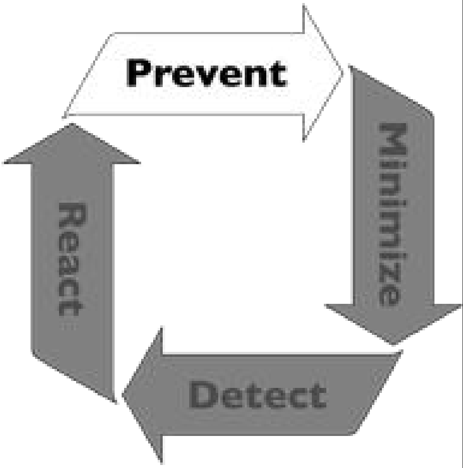
Android Security

Android is the most exploitable smartphone on the market

Security Philosophy

- Finite time and resources
- Humans have difficulty understanding risk
- Safer to assume that
  - Most developers do not understand security
  - Most users do not understand security
- Security philosophy cornerstones
  - Need to prevent security breaches from occurring
  - Need to minimize the impact of a security breach
  - Need to detect vulnerabilities and security breaches
  - Need to react to vulnerabilities and security breaches swiftly



Minimize

- We cannot rely on prevention alone
  - Vulnerabilities happen
- Users will install malware
- Code will be buggy
- How can we minimize the impact of a security issue?
- My webmail cannot access my banking web app
  - Same origin policy
- Why can malware access my browser? my banking info?
- Extend the web security model to the OS

Minimize

- Traditional operating system security
  - Host based
  - User separation
- Mobile OSes are for single users
- User separation is like a "same user policy"
- Run each application in its own UID is like a "same application policy"
  - Privilege separation
- Make privilege separation relatively transparent to the developer

Detect

- A lesser-impact security issue is still a security issue
- Internal detection processes
  - Developer education
  - Code audits
  - Fuzzing
  - Honeypot
- Everyone wants security ⇒ allow everyone to detect issues
  - Users
  - Developers
  - Security Researchers

React

- Autoupdaters are the best security tool since Diffie-Hellman
- Every modern operating system should be responsible for:
  - Automatically updating itself
  - Providing a central update system for third-party applications
- Android's Over-The-Air update system (OTA)
  - User interaction is optional
  - No additional computer or cable is required
  - Very high update rate

Android Security Basics

- Applications, by default, have no permissions
- Permissions list: Manifest.permission
- Applications statically declare the permissions they require
  - Android system prompts the user for consent at the time the application is installed
  - no mechanism for granting permissions dynamically (at run-time)
  - in AndroidManifest.xml, add one or more <uses-permission> tags
  - e.g., <uses-permission android:name=
    "android.permission.RECEIVE_SMS" />

OS protected APIs

- Cost-Sensitive APIs
  - Telephony
  - SMS/MMS
  - Network/Data connections
  - In-App Billing
  - NFC Access
- Sensitive Data Input Devices
  - Location data (GPS)
  - Camera functions
  - microphone
- Bluetooth functions
- Personal Information

Application Signing

- Why self signing?
  - Market ties identity to developer account
  - CAs have had major problems with fidelity in the past
  - No applications are trusted. No "magic key"

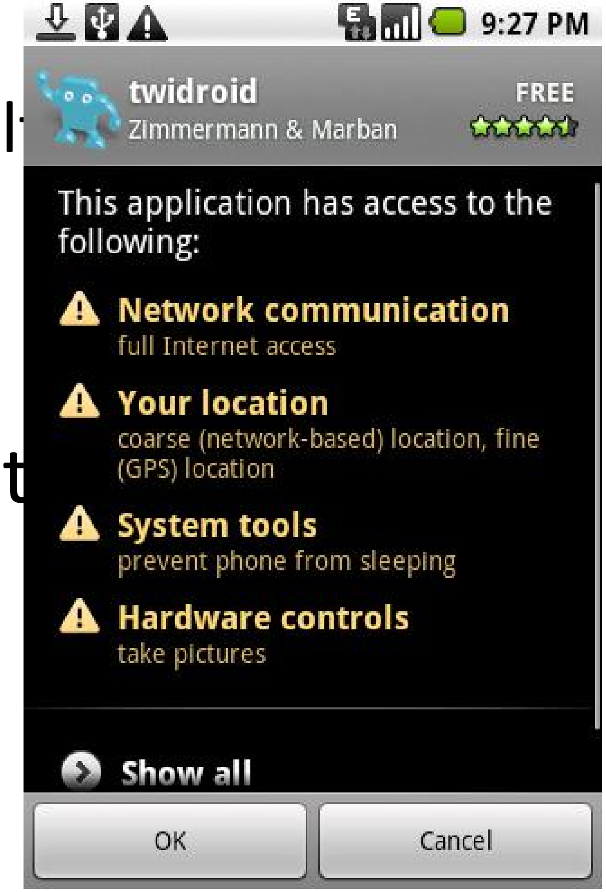
- What does signing determine?
  - Shared UID for shared keys
  - Self-updates

Application Signing

- All .apk files must be signed with a certificate
  - identifies the author of the application.
  - does not need to be signed by a certificate authority
- allows the system to grant or deny applications
  - access to signature-level permissions
  - request to be given the same Linux identity as another application.
- If the public key matches the key used to sign any other APK, the new APK may request to share a UID with the other APK.

Permissions

- Whitelist model
  - Allow minimal access by defaul
  - User accepted access
- Ask users fewer questions
- Make questions more underst
- 194 permissions
  - More ⇒ granularity
  - Less ⇒ understandability



9:27 PM

twidroid

Zimmermann & Marban

FREE

This application has access to the following:

Network communication
full Internet access

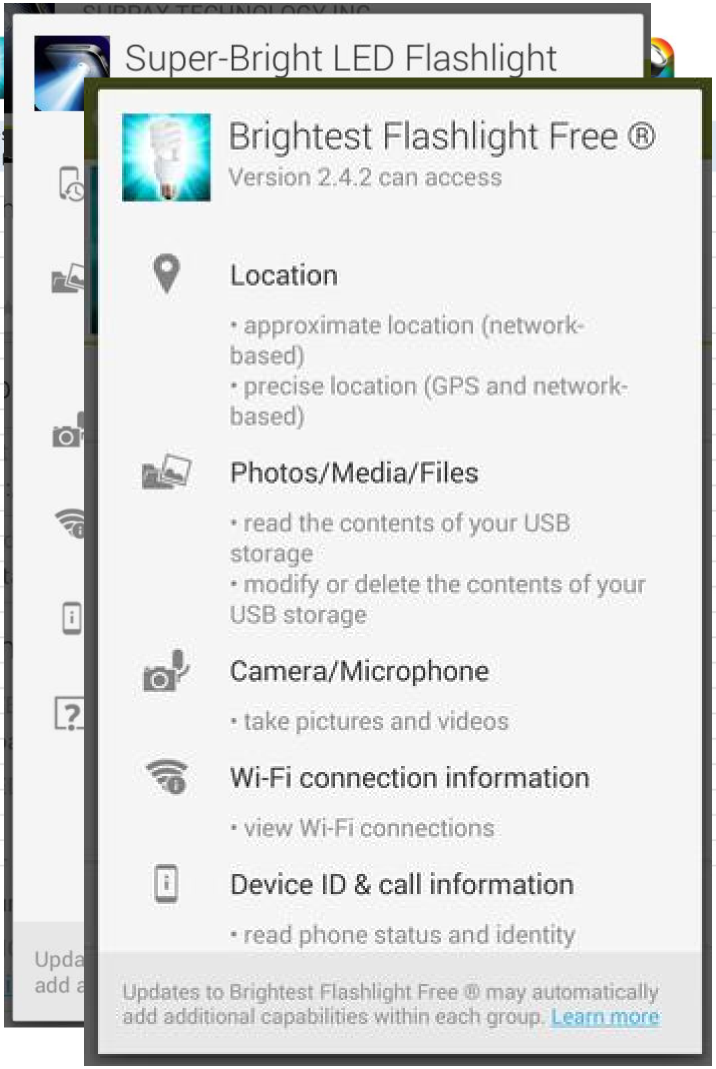
Your location
coarse (network-based) location, fine (GPS) location

System tools
prevent phone from sleeping

Hardware controls
take pictures

Permission Model

Flashlight Apps	Super-Bright LED Flashlight	Brightest Flashlight	High-Powered Flashlight	Flashlight HD LED	Flashlight: LED Torch Light
Permissions					
retrieve running apps	✓		✓		
modify or delete the contents of your USB storage	✓	✓	✓		
test access to protected storage	✓	✓	✓		
take pictures and videos	✓	✓	✓	✓	✓
view Wi-Fi connections	✓	✓	✓	✓	
read phone status and identity	✓	✓	✓		
receive data from Internet	✓		✓		
control flashlight	✓	✓	✓	✓	
change system display settings	✓		✓		
modify system settings	✓		✓		
prevent device from sleeping	✓		✓		
view network connections	✓	✓	✓	✓	✓
full network access	✓	✓	✓	✓	✓
approximate location (network-based)	✓	✓	✓		
precise location (GPS and network-based)	✓	✓	✓		
disable or modify status bar	✓	✓			
read Home settings and shortcuts	✓	✓			✓
install shortcuts	✓	✓			✓
uninstall shortcuts	✓	✓			✓
control vibration	✓				
prevent device from sleeping		✓		✓	✓
write Home settings and shortcuts					✓
disable your screen lock					✓
read Google service configuration				✓	



Super-Bright LED Flashlight

Upda
add a

Brightest Flashlight Free ®
Version 2.4.2 can access

Location
- approximate location (network-based)
- precise location (GPS and network-based)

Photos/Media/Files
- read the contents of your USB storage
- modify or delete the contents of your USB storage

Camera/Microphone
- take pictures and videos

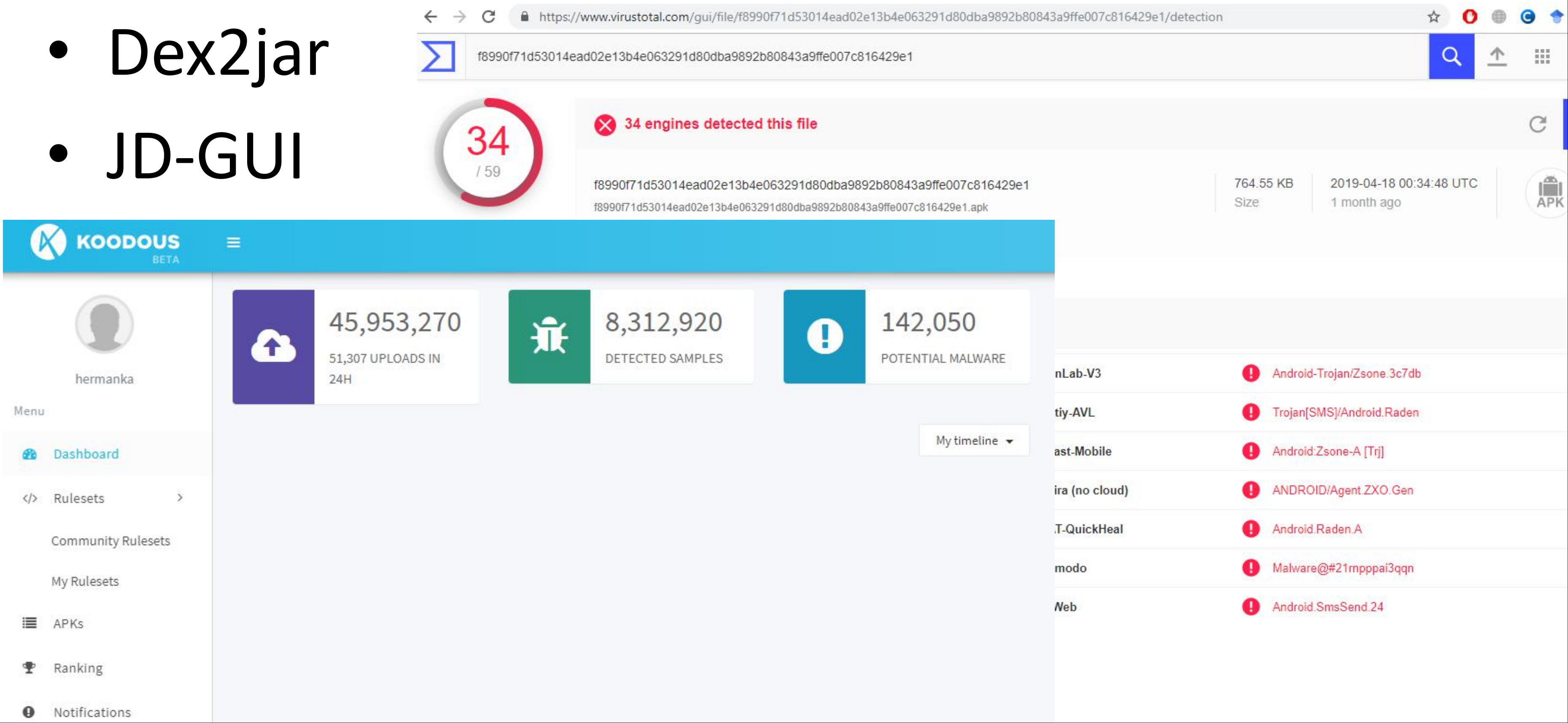
Wi-Fi connection information
- view Wi-Fi connections

Device ID & call information
- read phone status and identity

Updates to Brightest Flashlight Free ® may automatically add additional capabilities within each group. Learn more

App Analysis Tools

- VirusTotal - malicious db
- Koodous - malicious db
- Dex2jar
- JD-GUI



https://www.virustotal.com/gui/file/f8990f71d53014ead02e13b4e063291d80dba9892b80843a9ffe007c816429e1/detection

f8990f71d53014ead02e13b4e063291d80dba9892b80843a9ffe007c816429e1

34 / 59

34 engines detected this file

f8990f71d53014ead02e13b4e063291d80dba9892b80843a9ffe007c816429e1
f8990f71d53014ead02e13b4e063291d80dba9892b80843a9ffe007c816429e1.apk

764.55 KB
Size

2019-04-18 00:34:48 UTC
1 month ago

APK

nLab-V3	Android-Trojan/Zsone.3c7db
tiy-AVL	Trojan[SMS]/Android.Raden
ast-Mobile	Android:Zsone-A [Trj]
ira (no cloud)	ANDROID/Agent.ZXO.Gen
T-QuickHeal	Android.Raden.A
modo	Malware@#21mpppai3qqn
Web	Android.SmsSend.24

KOODOUS
BETA

hermanka

Menu

- Dashboard
- Rulesets
  - Community Rulesets
  - My Rulesets
- APKs
- Ranking
- Notifications

45,953,270
51,307 UPLOADS IN 24H

8,312,920
DETECTED SAMPLES

142,050
POTENTIAL MALWARE

My timeline

How to Analyze an App
Using Reverse Engineer Technique

- Rename apk to zip
- Get class.dex file
- Convert to jar file using dex2jar
- Open jar file using JD-GUI
- Source code ready to analyze