Introduction to Intelligent Security Systems

Alvin Lin

August 2018 - December 2018

Android Colluded Applications Attack

Because of the interconnectedness of online businesses, all of us are generating data and consuming data. This makes data security the biggest factor in data quality, which involves accessibility, security, and privacy. There are many parts that play into this, including data trustworthiness, device security, communication security, and user privacy.

Application Collusion

Colluded applications are applications that may share data through means outside of system processes. RAM usage and CPU patterns may be reflected through this. This is generally a violation of Android security because applications are sandboxed. In order to use the device's resources, an application has to ask for permission first.

Overt communication channels are used for explicit data communications between applications, generally done with Intents in Android which launch an external application to perform a service and transmit data back to the original application.

Attack Scenario

Suppose you have a contact optimizer which has permissions to access a user's contact list and a weather app with permission to access the Internet. The contact optimizer itself cannot leak your private contact data, but it can collude with the weather app through Intents to send your data through the network. Collections of maliciously designed apps can collude to perform malicious actions.

Covert Communication Channels

Covert inter-process communication creates a means for applications to communicate where they should not be able to. Two applications reading harmless data can communicate through the request intervals. This method is often slow however, and not feasible for larger amounts of data.

Colluded Application Attack Detection

- Time Level: reactive (real time prevention), proactive (try to prevent it in advance through analysis)
- Integration Level: standalone applications or library integrated into Android OS to trace your information flow
- Involvement Level: tool usage depends on the firmware, application developer, and device usage.
- Component Level: able to analyze all application components

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech