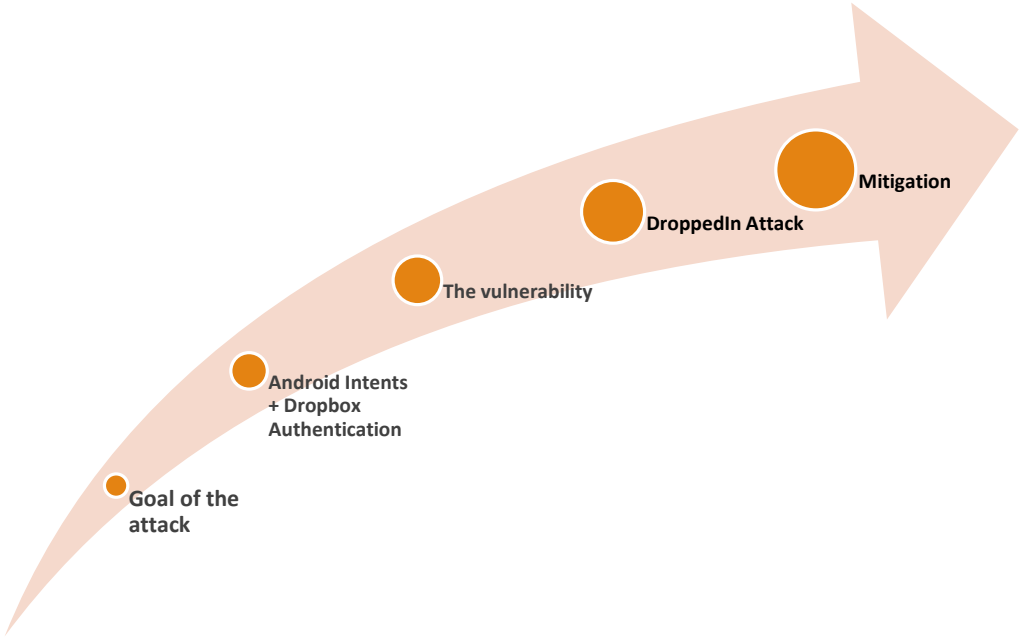
DroppedIn: Remotely Exploiting the Dropbox SDK for Android

(The CVE-2014-8889 Vulneribilty)

TEAM MEMBERS: KEVIN AMORIM, LAMA ALSUWAYAN, HANG XU

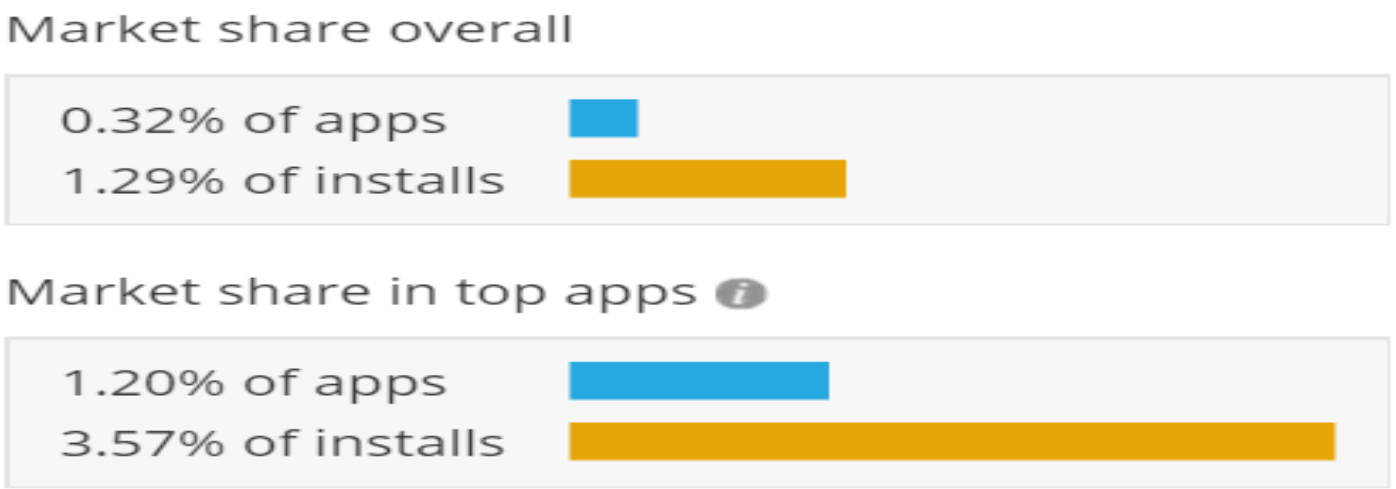
Outline


Mitigation
DroppedIn Attack
The vulnerability
Android Intents
+ Dropbox
Authentication
Goal of the
attack

Data on the Cloud

- World is now storing private personal and business data on the cloud
- Cloud data is not only by the user, but also by apps (photo sharing, storage … etc.)
- Cloud services often provide a framework (SDK) that apps can utilize
  - Example: The Dropbox SDK for Android

Dropbox API - Stats

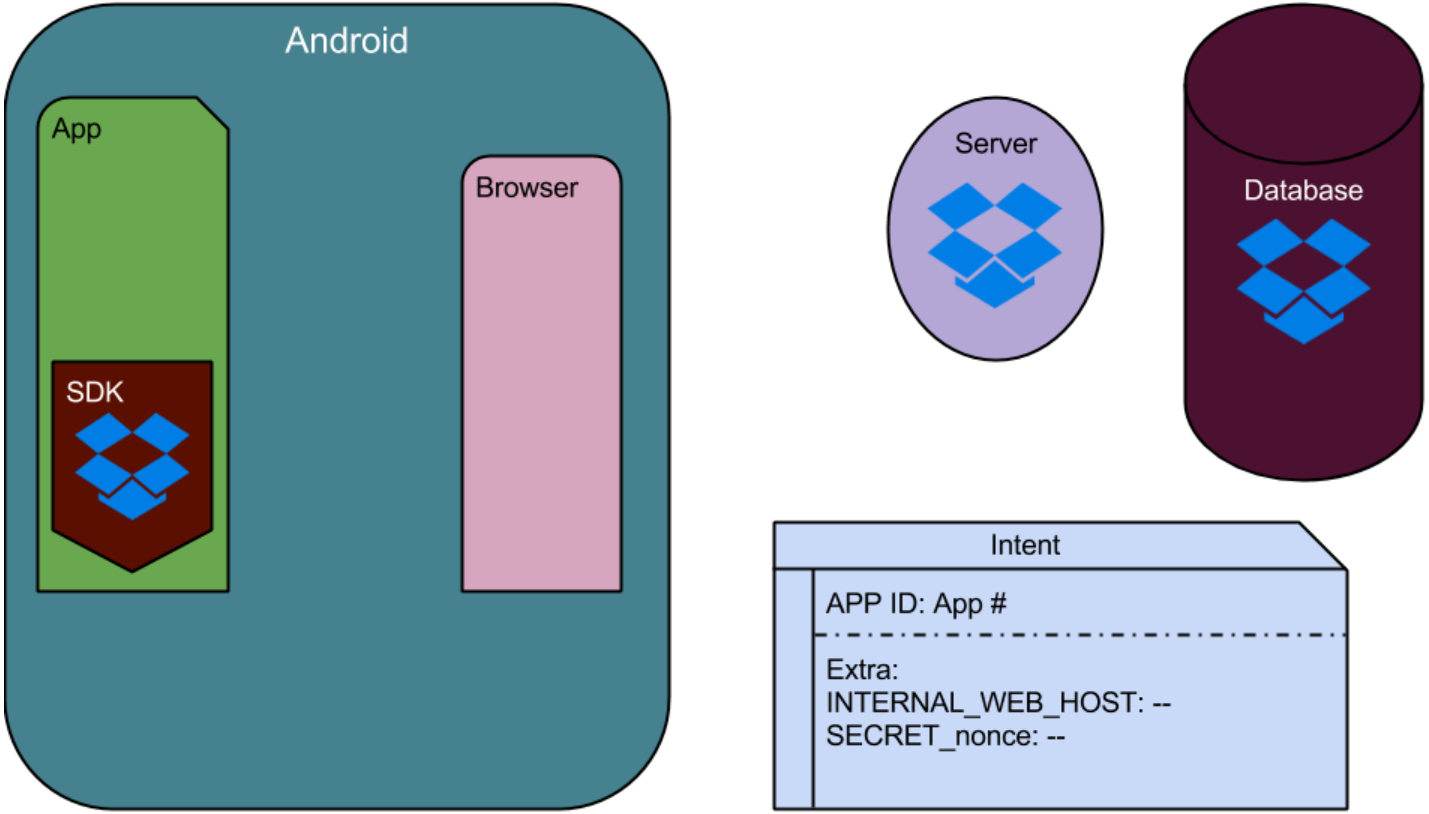


* Stats according to AppBrain

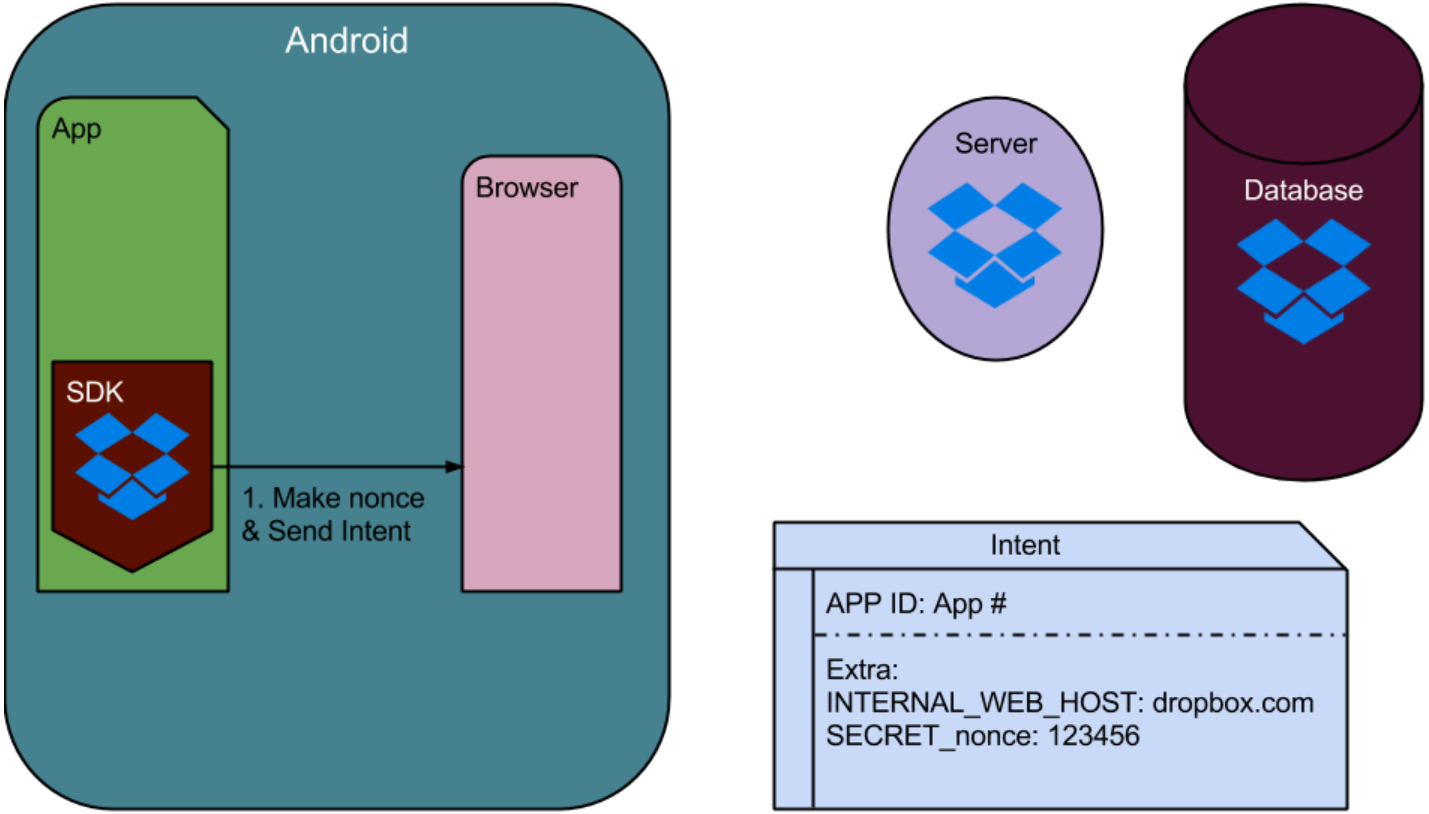
Android & Dropbox

- Android applications execute in a sandbox environment
- Apps can’t access another app’s data directly
- Apps communicate using ‘**Intents**’

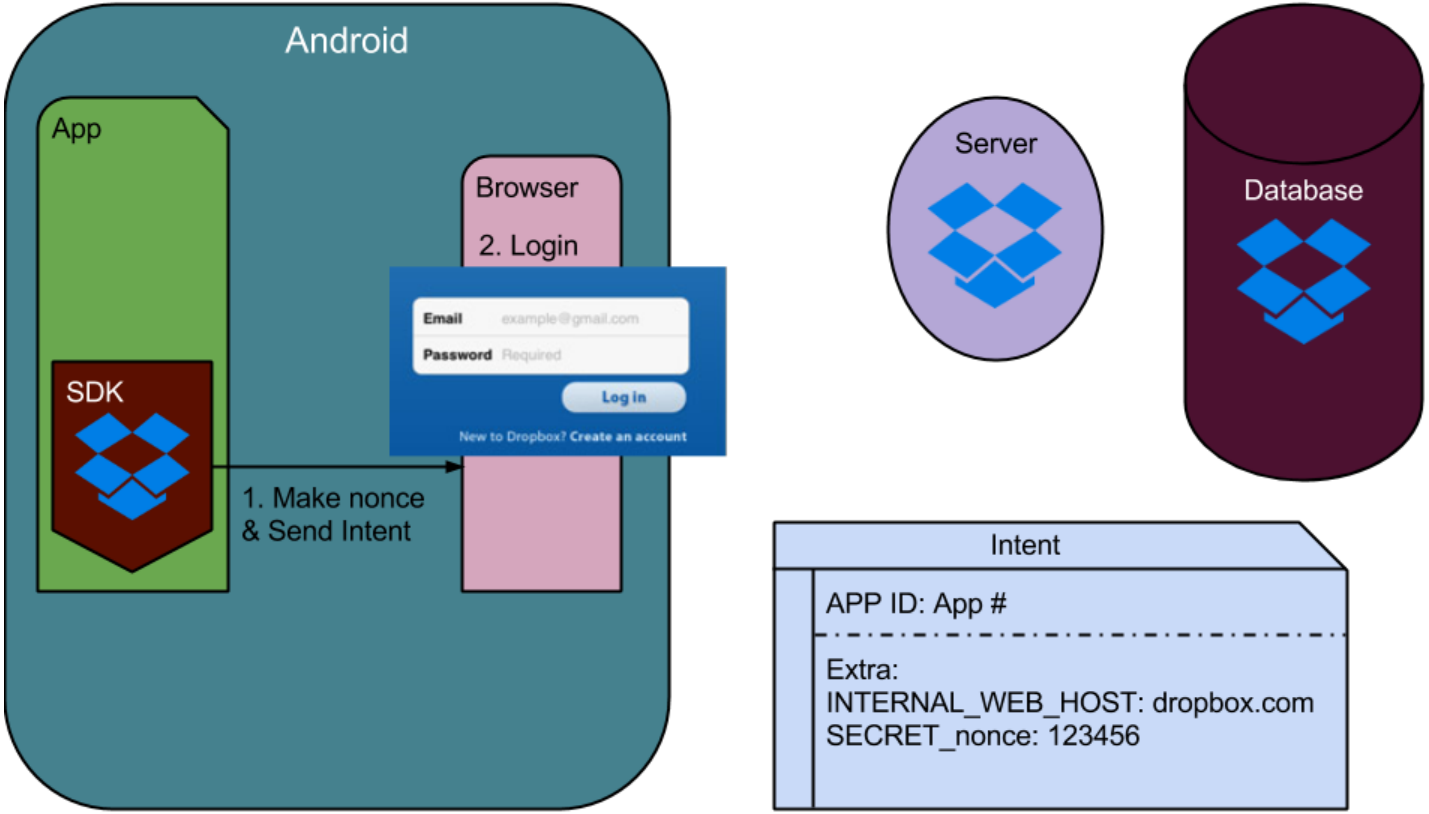
DropBox SDK Authentication (Normal Flow)



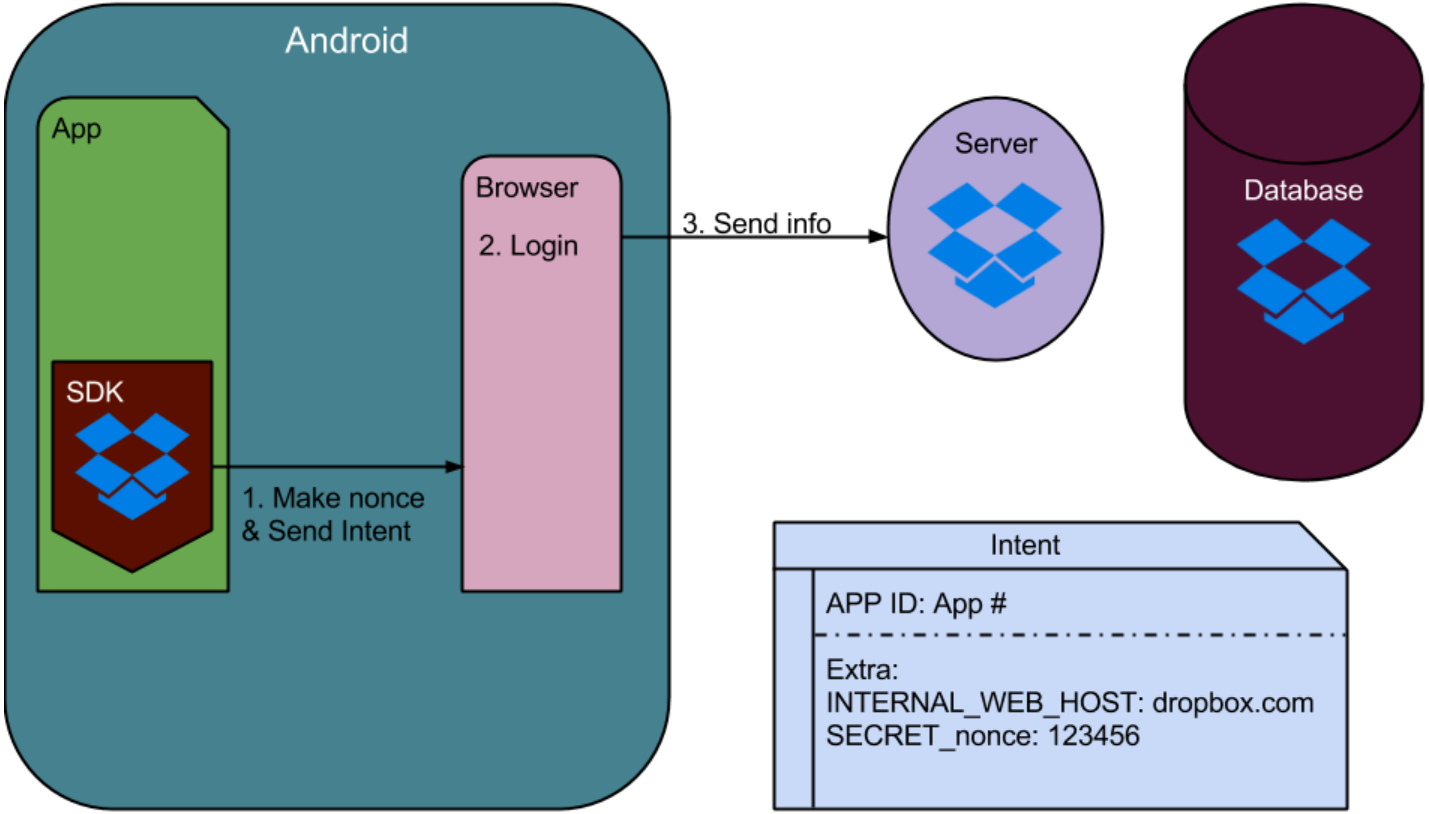
DropBox SDK Authentication (Normal Flow)



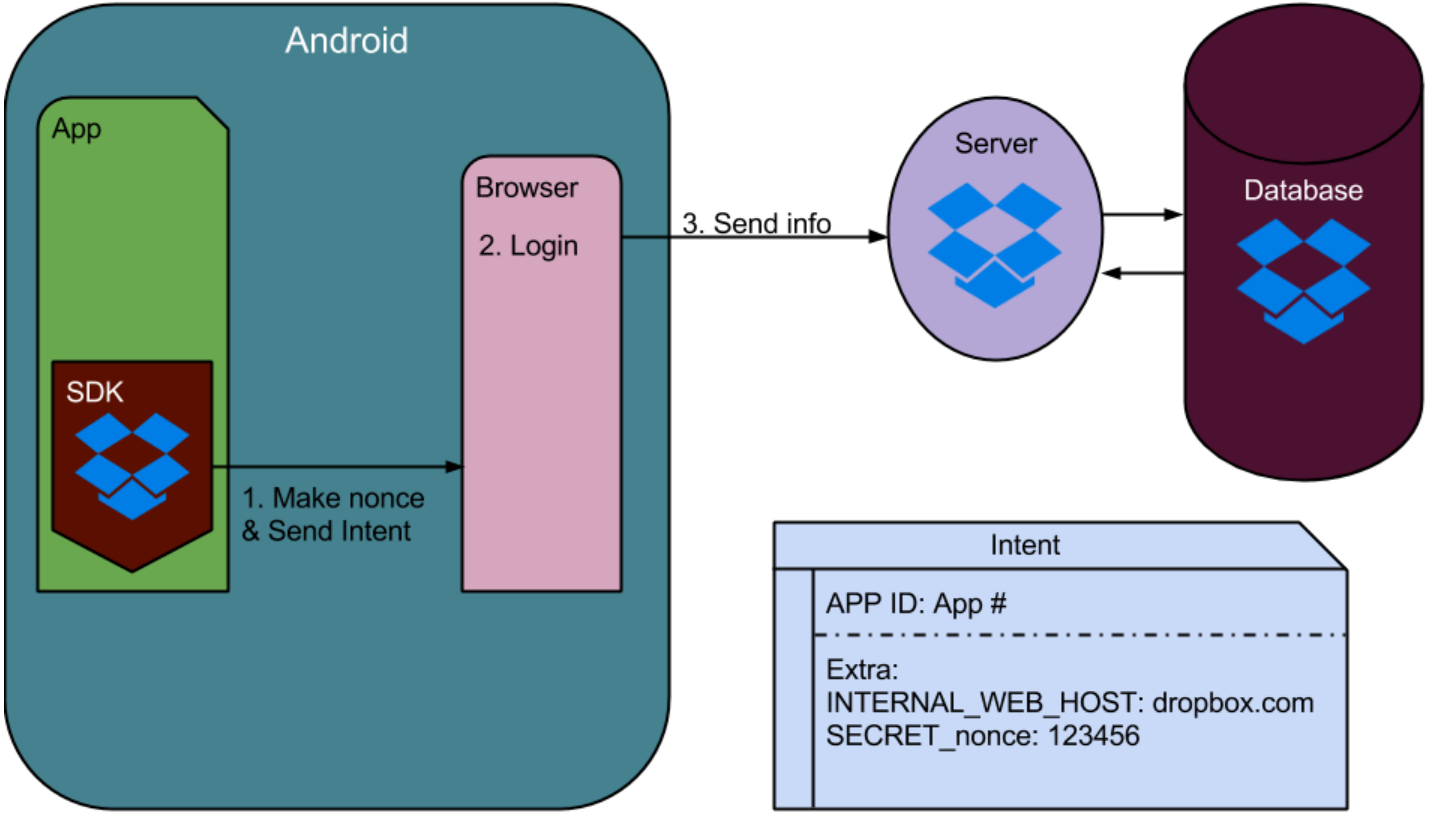
DropBox SDK Authentication (Normal Flow)



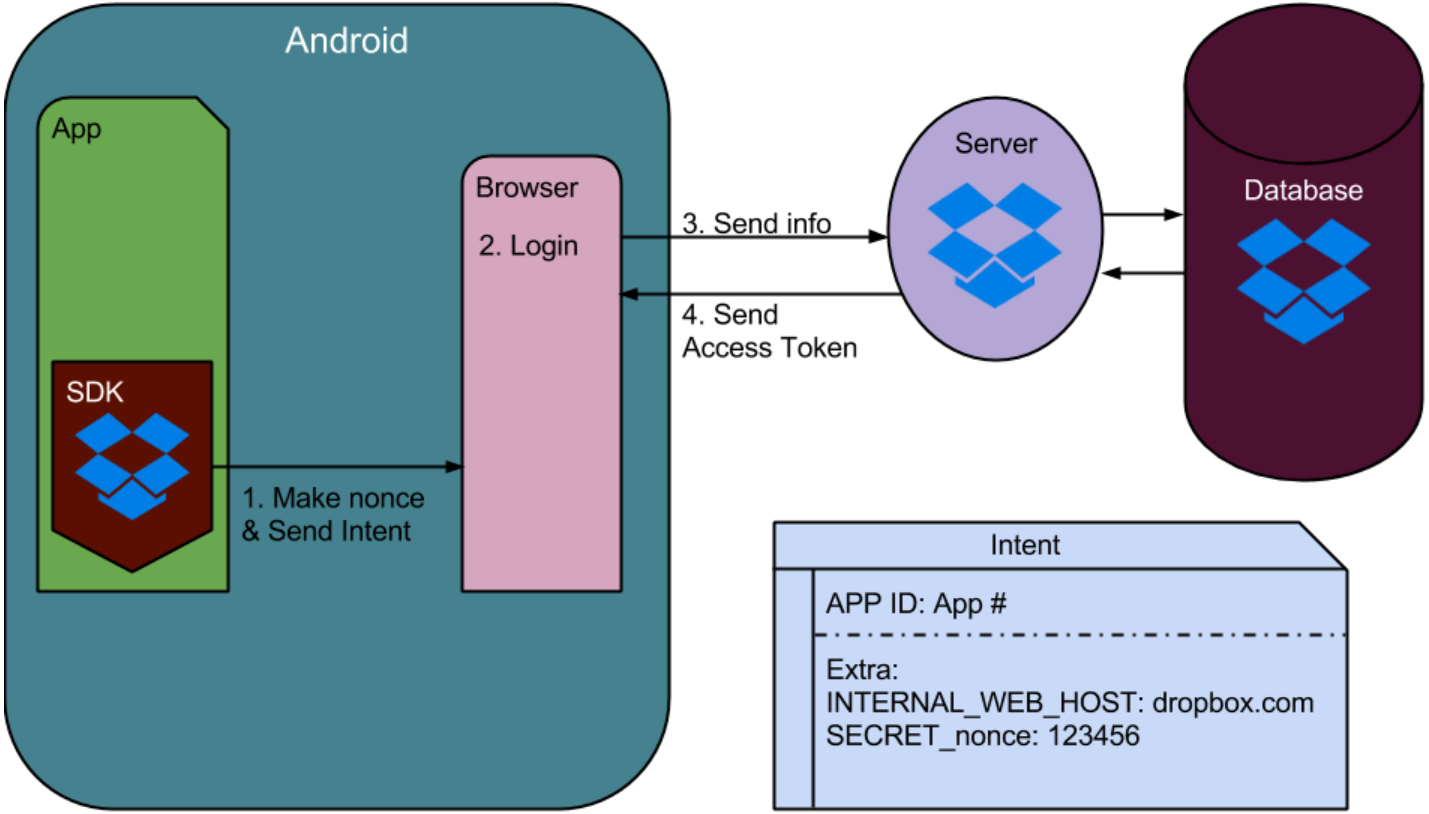
DropBox SDK Authentication (Normal Flow)



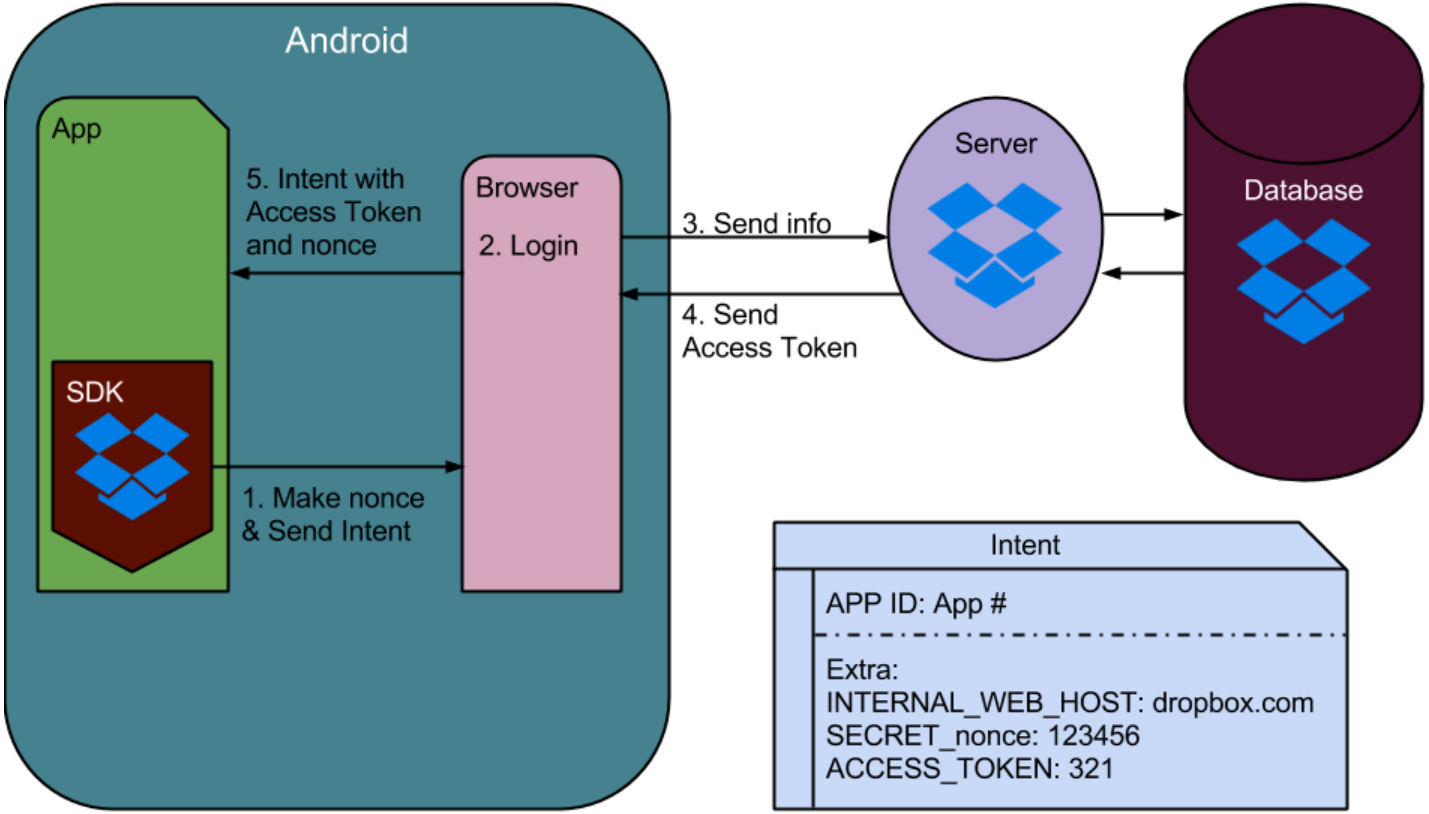
DropBox SDK Authentication (Normal Flow)



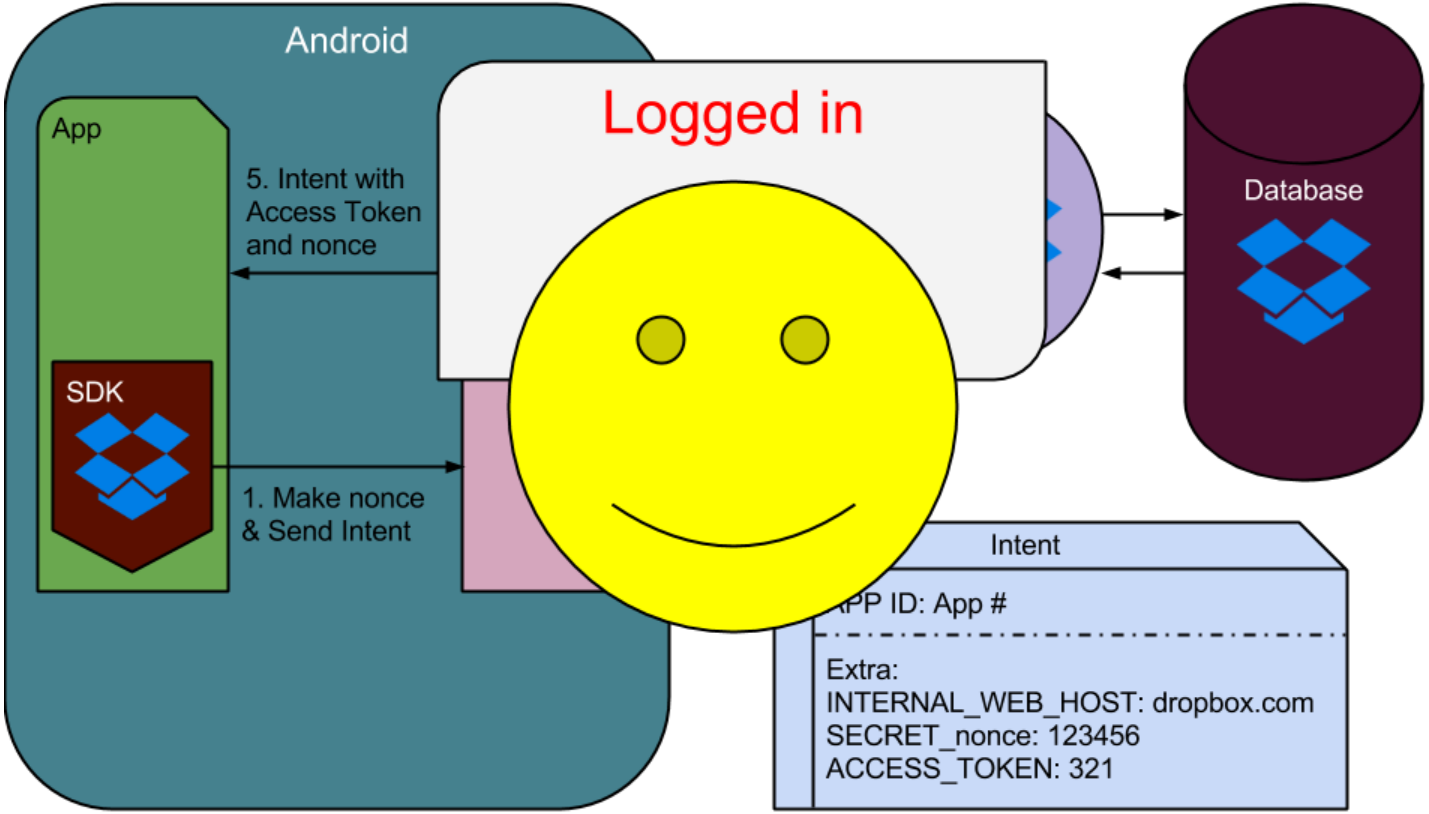
DropBox SDK Authentication (Normal Flow)



DropBox SDK Authentication (Normal Flow)



DropBox SDK Authentication (Normal Flow)



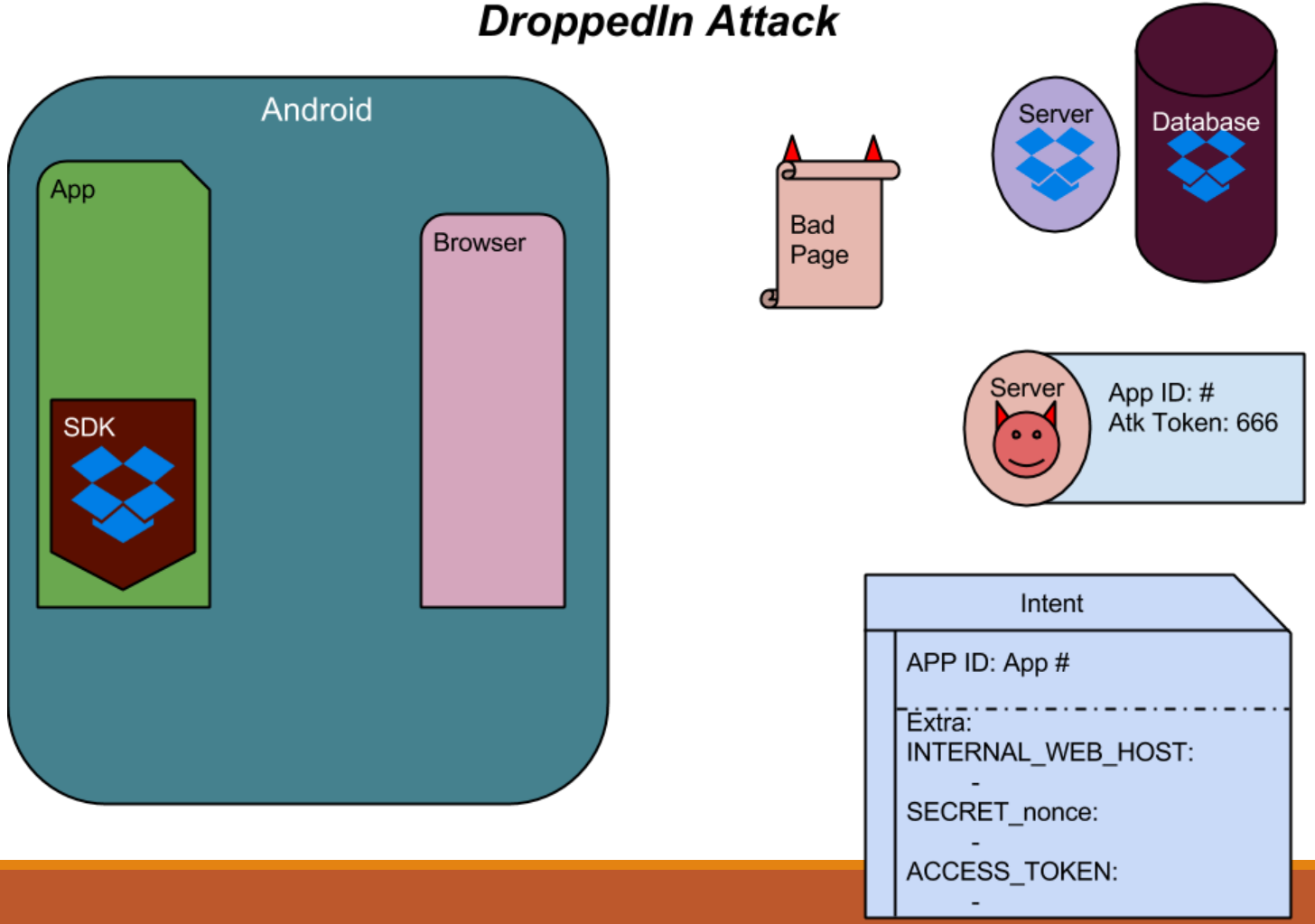
DroppedIn Attack

- Link the app with the attacker's account instead of the victim's to either:
  - have the victim upload sensitive information or
  - download malicious, attacker-controlled data that may be used as part of other attacks.

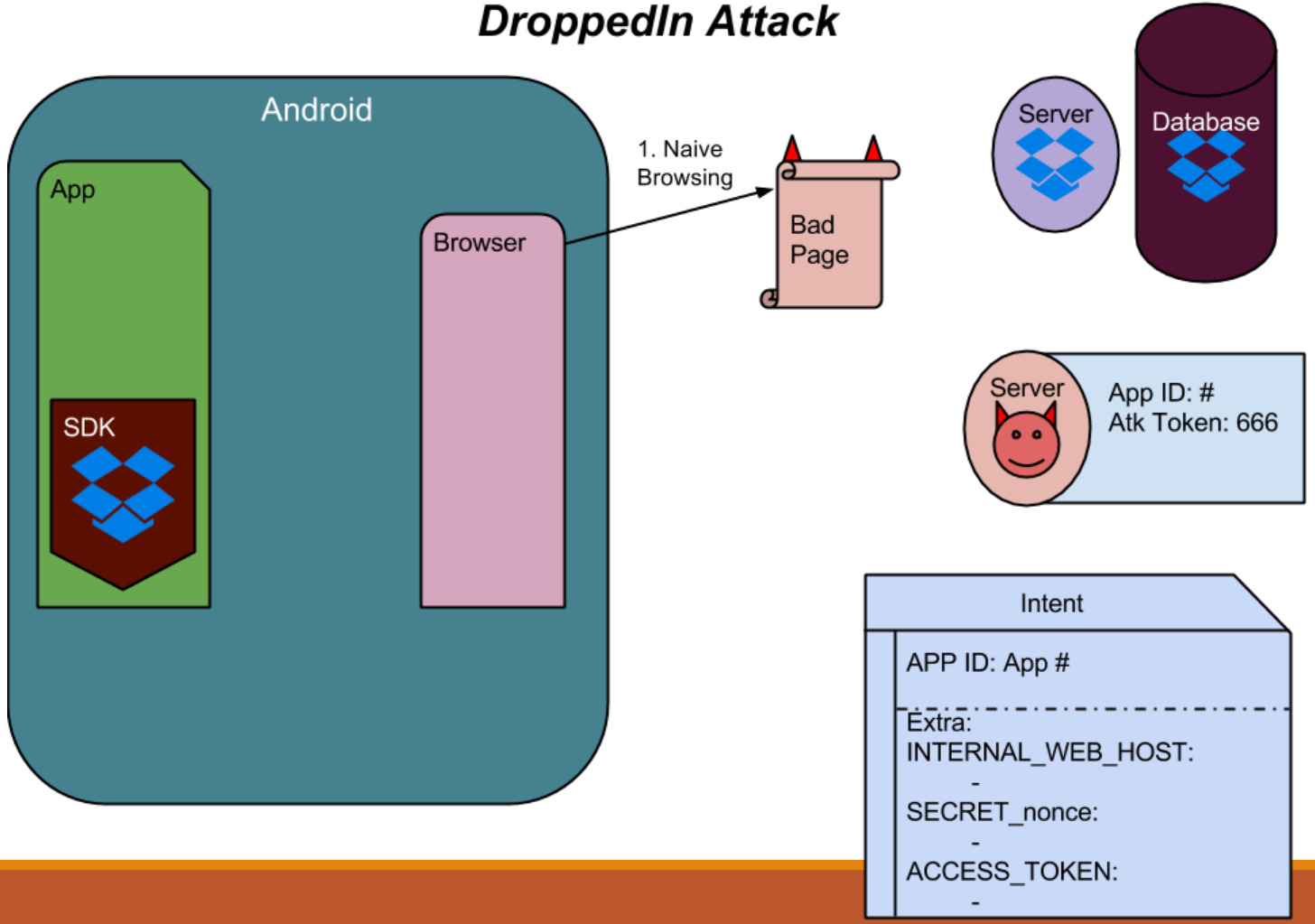
The field "INTERNAL_WEB_HOST" allows this to occur

******Only works when DropBox App is NOT Installed******

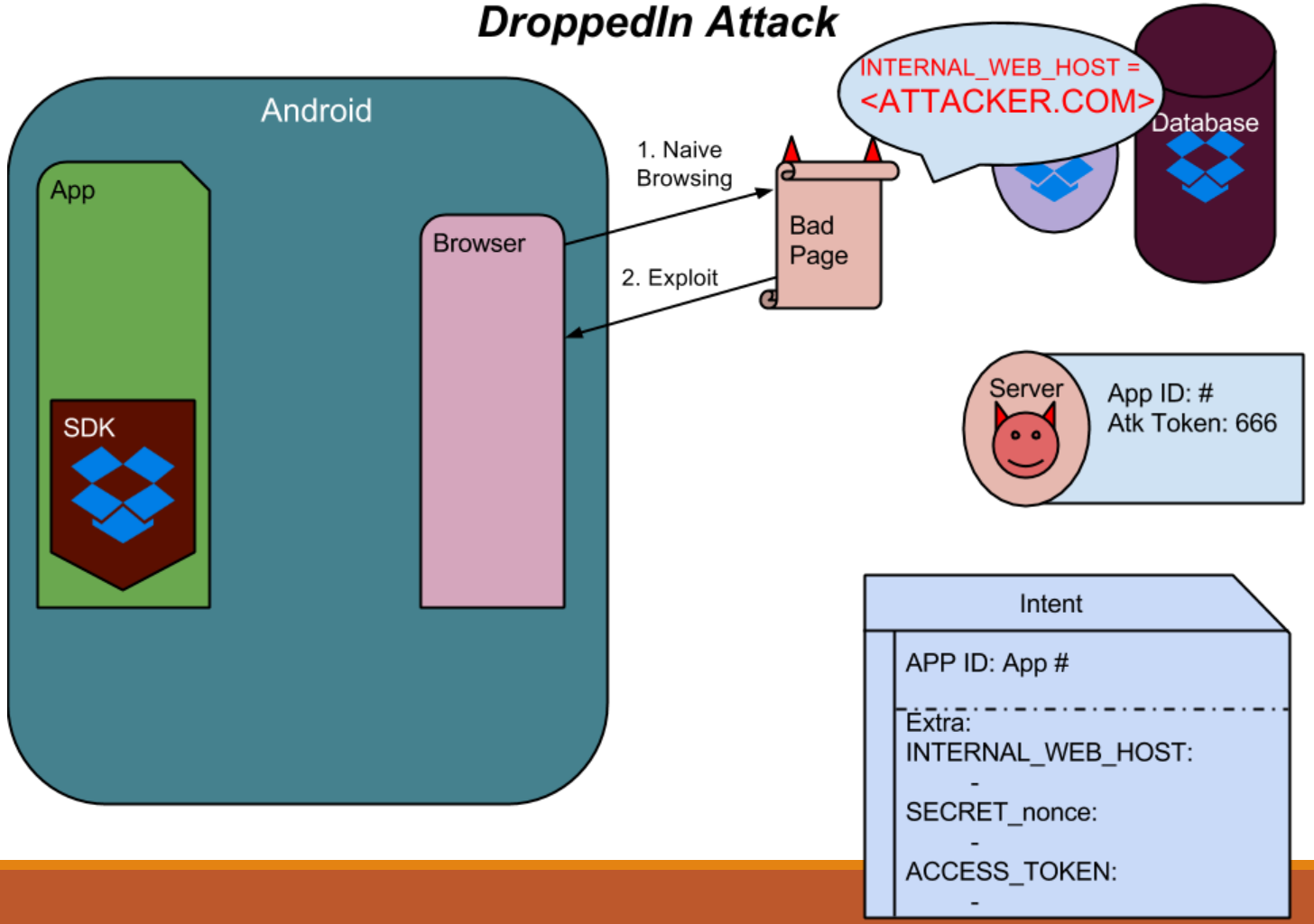
DroppedIn Attack



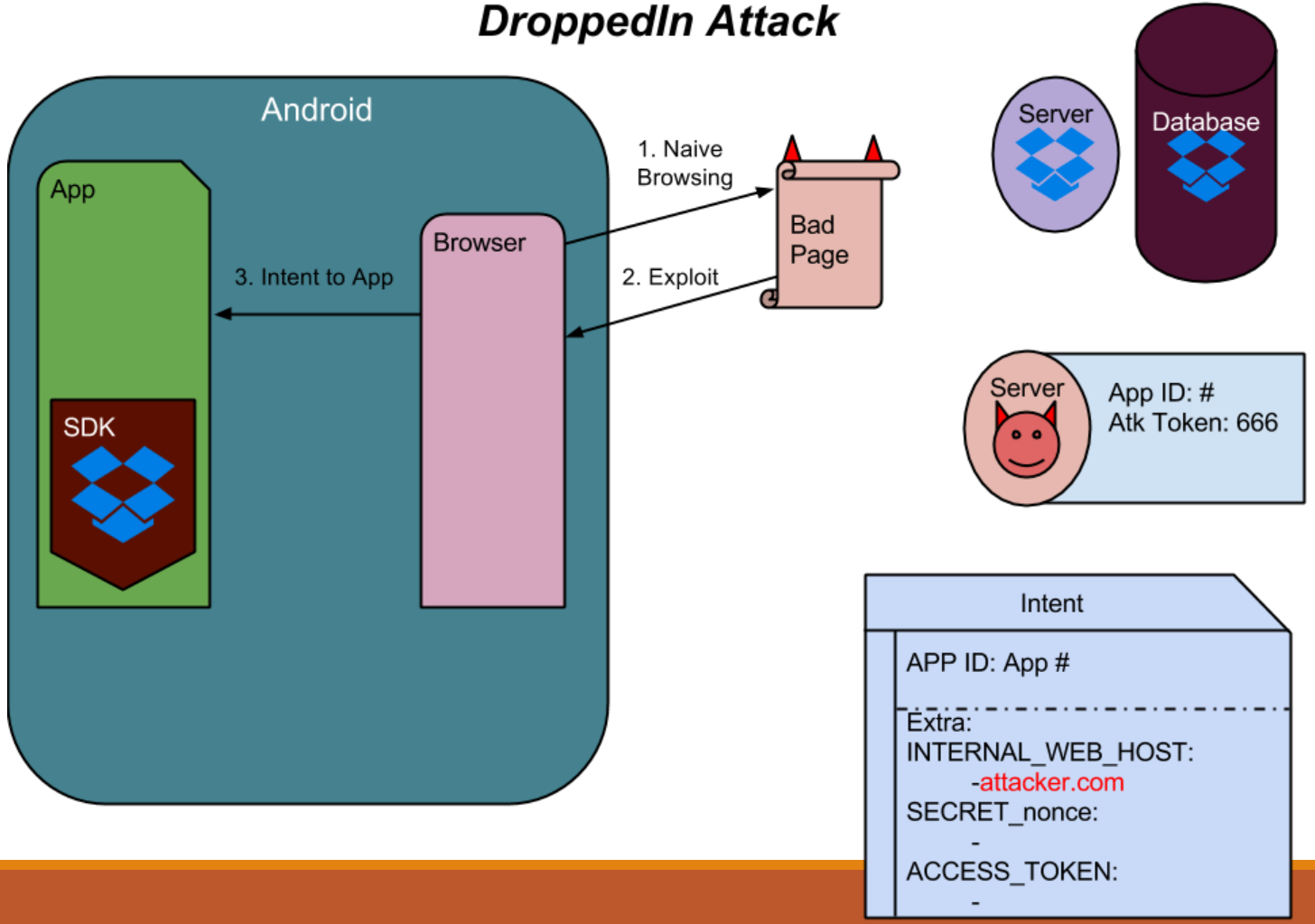
DroppedIn Attack



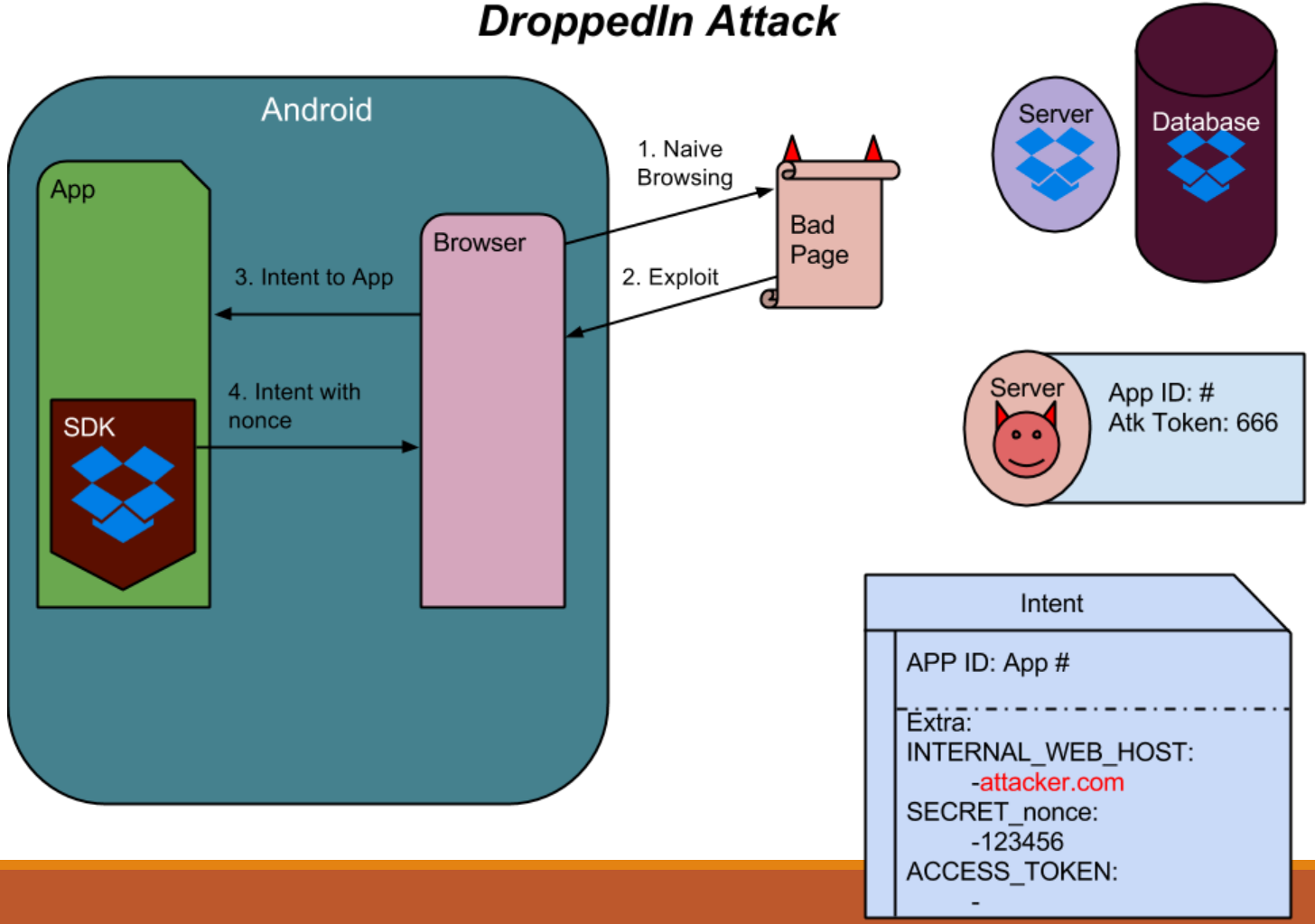
DroppedIn Attack



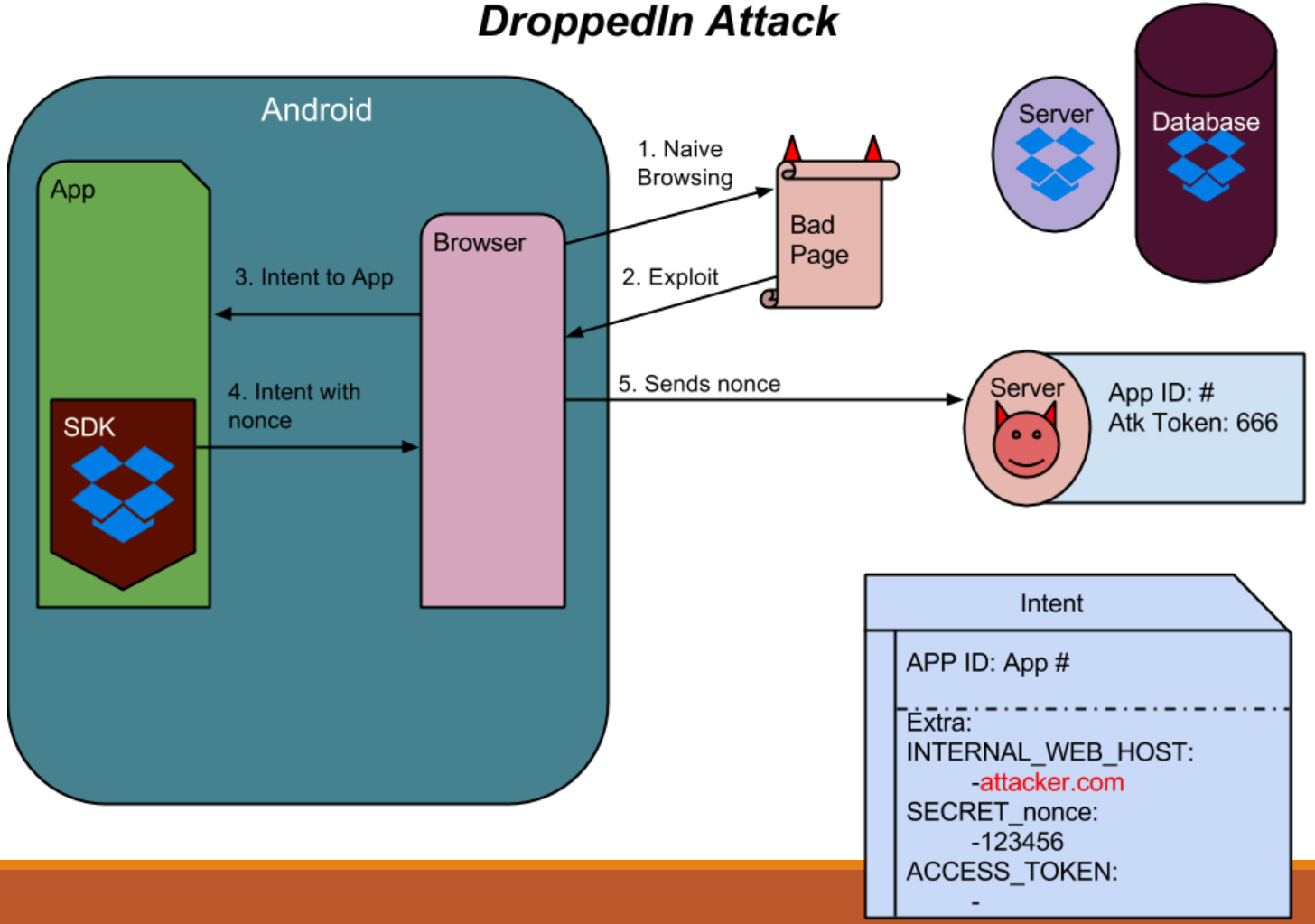
DroppedIn Attack



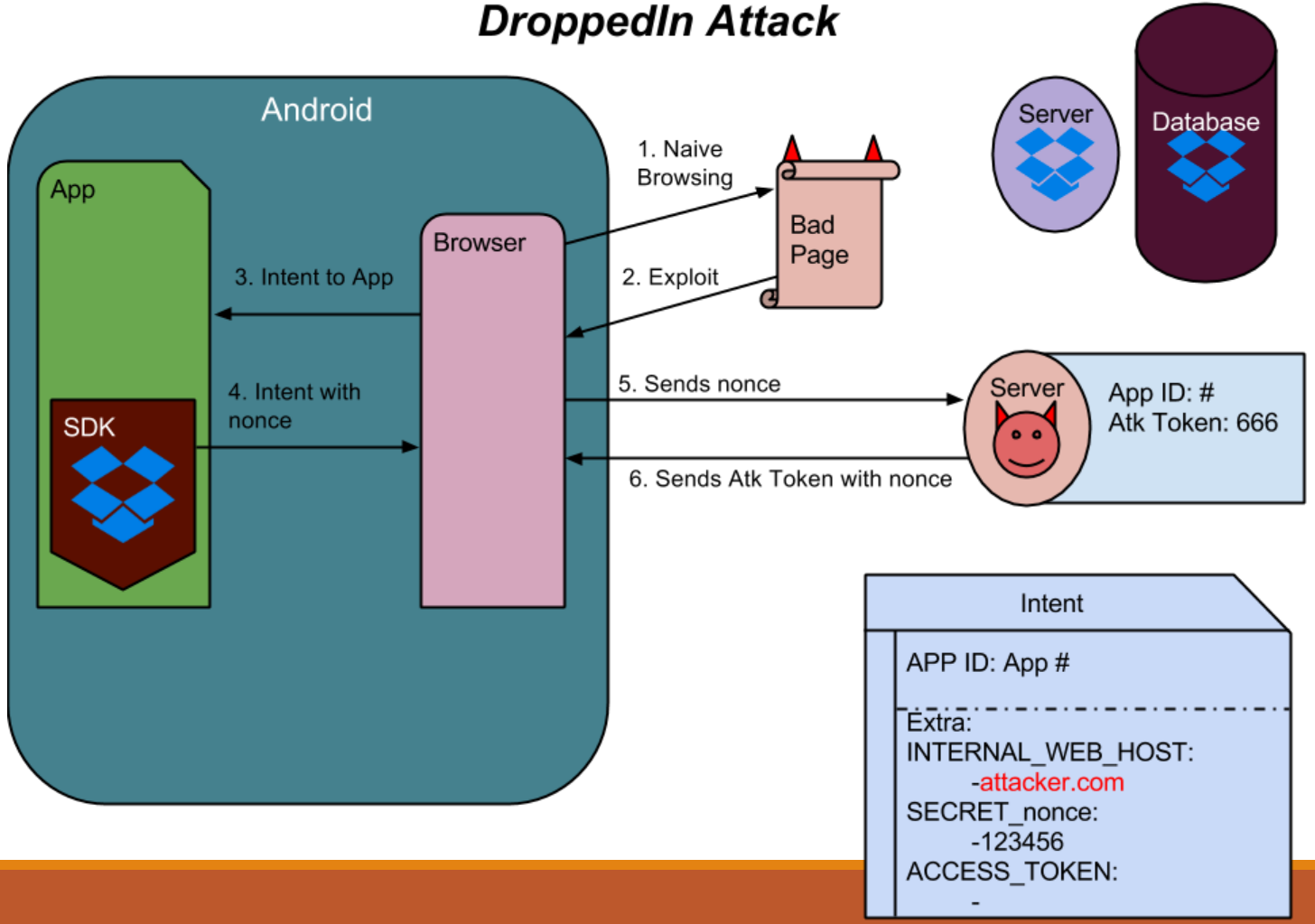
DroppedIn Attack



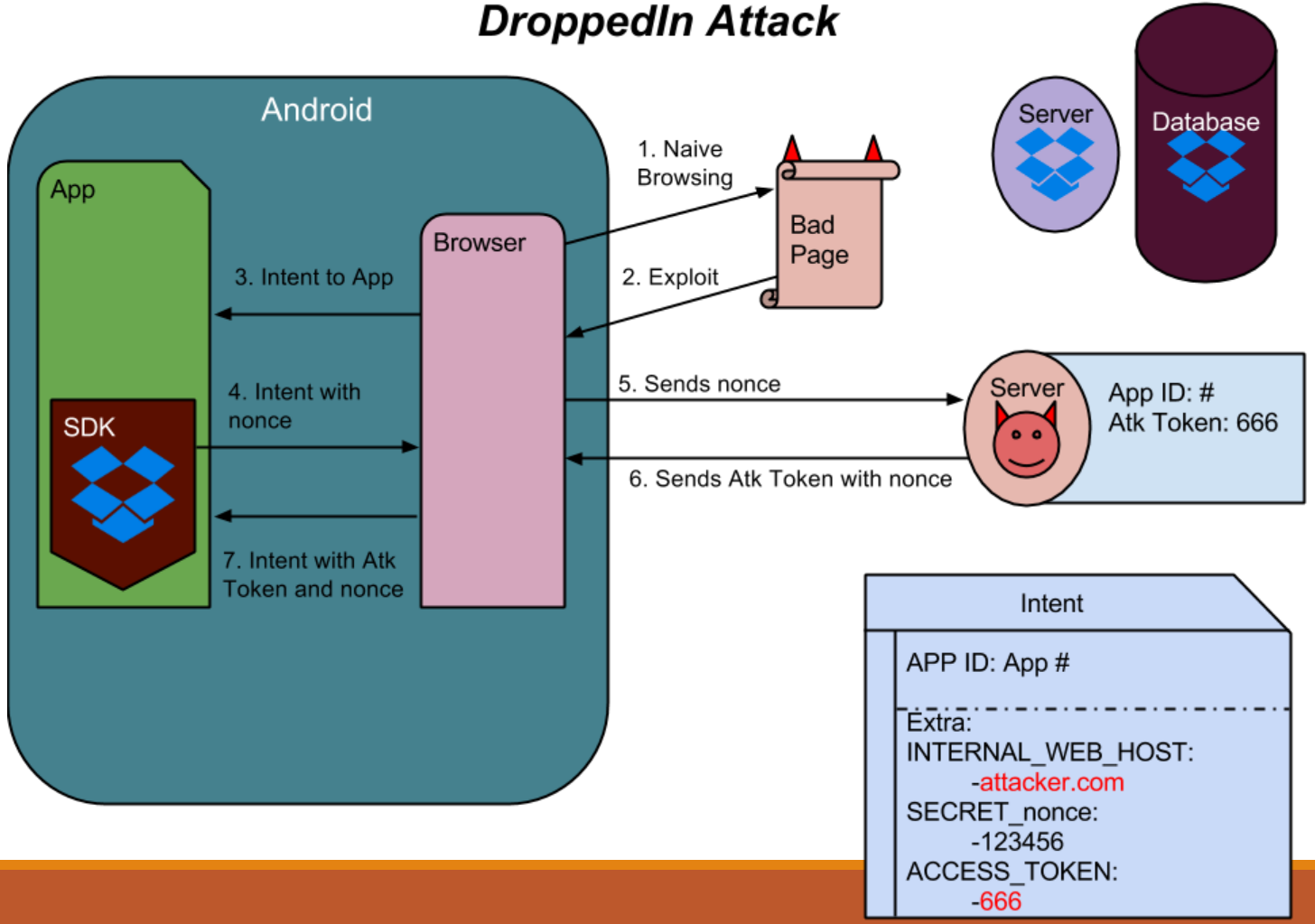
DroppedIn Attack



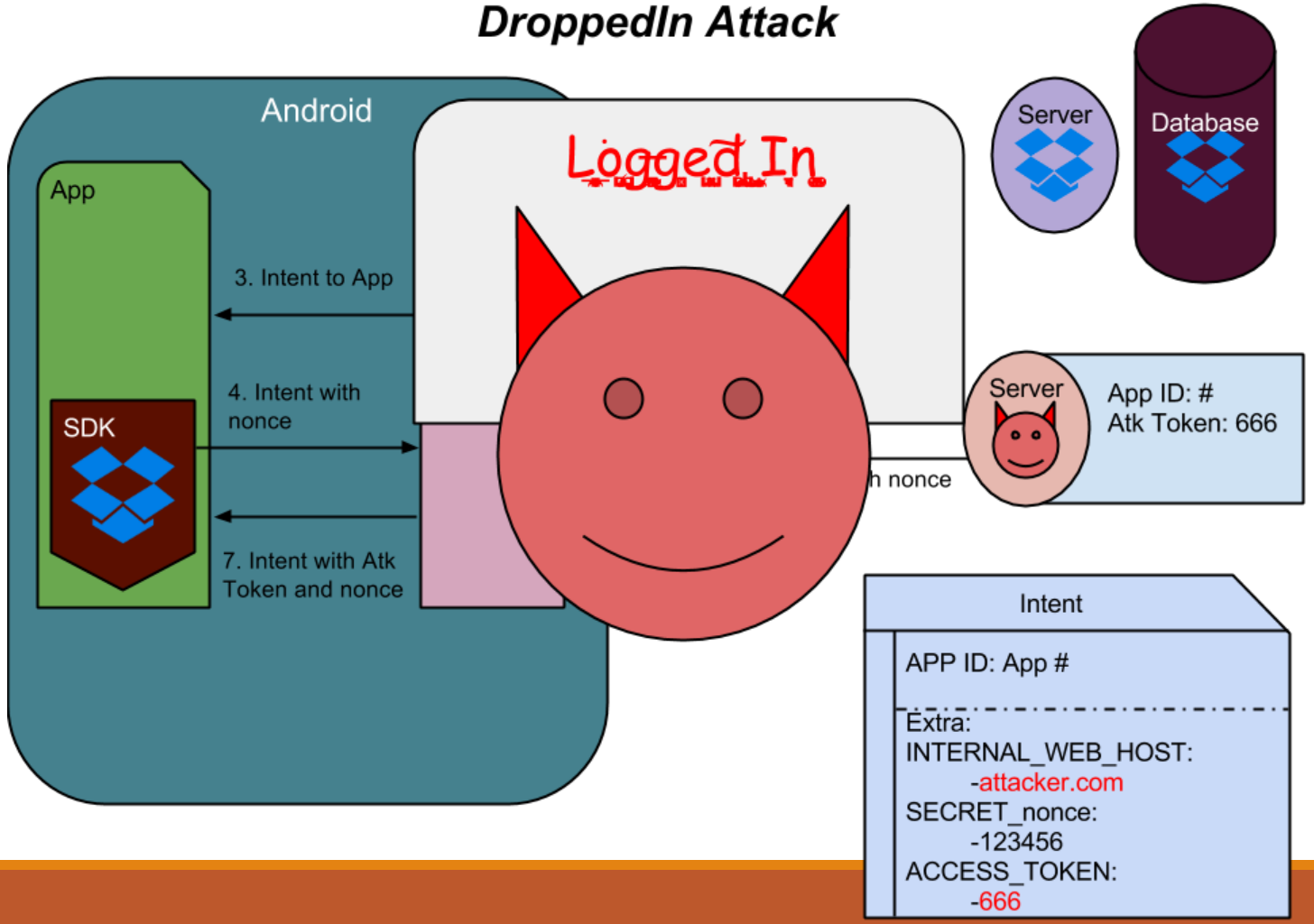
DroppedIn Attack



DroppedIn Attack



DroppedIn Attack



Response from Dropbox

- December 1, 2014 - Vulnerabilities disclosed to Dropbox.
- December 2, 2014 - Dropbox confirmed issue, started working on patch.
- December 5, 2014 - Patch available (Dropbox SDK for Android version 1.6.2)
- March 11, 2015 - Public disclosure

Mitigation

- Authentication no longer accepts input parameters from Intent's extras
  - Don't allow inputs for INTERNAL_WEB_HOST
- As a developer:
  - Update Dropbox SDK for Android to Version 1.6.2 or higher
- As a user:
  - Install Dropbox onto your android device
  - Make sure you update your apps to their most recent version

References

- http://ibm.co/1Hosb02
- http://securityintelligence.com/droppedin-remotely-exploitable-vulnerability-in-the-dropbox-sdk-for-android/#.VQ8rzjCUy1l
- https://blogs.dropbox.com/developers/2015/03/security-bug-resolved-in-the-dropbox-sdks-for-android/