Abusing the IPC of Android apps for fun and profit

András Veres-Szentkirályi
vsza@silentsignal.hu

CampZero
2013
Headfirst into Android
"Content providers manage access to a structured set of data. They encapsulate the data, and provide mechanisms for defining data security. Content providers are the standard interface that connects data in one process with code running in another process."

http://developer.android.com/guide/topics/providers/content-providers.html
drozer allows you to use dynamic analysis during an Android security assessment. By assuming the role of an Android app you can:

▶ find information about installed packages.
▶ interact with activities, broadcast receivers, content providers and services.
▶ use a proper shell to play with the underlying Linux OS.
▶ check an app’s attack surface, and search for known vulnerabilities.

https://labs.mwrinfosecurity.com/tools/drozer/
Case study: Seesmic (social media app)

Longer writeup: http://techblog.vsza.hu/posts/Seesmic_Android_information_leak.html
Case study: MWR BSides Challenge 2013

Challenge:  http://labs.mwrinfosecurity.com/blog/2013/03/11/bsides-challenge/

Tools used:
▶ dex2jar  http://code.google.com/p/dex2jar/
▶ JD-GUI  http://java.decompiler.free.fr/?q=jdgui
▶ apktool  http://code.google.com/p/android-apktool/

Longer writeup:  http://techblog.vsza.hu/posts/MWR_BSides_Challenge_2013_writeup.html
Case study: unnamed e-mail application (fix in progress)

TODO
Conclusion

For developers:

- set exported to false
- set protectionLevel to signature
- use special permissions if nothing else works
- or don’t use content providers at all

For hackers:

- install drozer, start exploring
- profit!
Conclusion

For developers:
▶ set exported to false
▶ set protectionLevel to signature
▶ use special permissions if nothing else works
▶ or don’t use content providers at all

For hackers:
▶ install drozer, start exploring
▶ ... 
▶ profit!
Thanks for your attention!

Facebook
vsza@silentsignal.hu
web
e-mail