COM 402 exercises 2024, session 9: Mobile Security

Exercise 9.1

You are at an Android fanboy/fangirl cocktail party. One of the guests approaches you and starts boasting about his new Samsung Galaxy S24. When he goes into arguing that Android is great because all the software on his phone is open source and can be found in the AOSP, you raise your eyebrow and try to convince him that this is just not the case.

Identify three examples to convince this guest that the software stack on his phone is only partially open source.

Exercise 9.2

Great, you convinced the guest, and he slowly walks away with a thoughtful face. While you were talking to him, another person joined the conversation. She is an app developer, and you have a great conversation about the Android Framework with her. At some point during the conversation, the topic of integrating C/C++ libraries in an Android app comes up.

Let us say you want to implement an image parser in a C/C++ native library to gain more performance and have a better user experience. When loading images directly from the web in your app that uses this library, what could go wrong?

Exercise 9.3

You and the developer agree that native libraries should be used with care in Android apps. As the evening continues, the developer tells you that a couple of months ago, she found a very similar app to one of her apps in the Google Play Store. In fact, the two apps look almost identical. Your blood is pumping faster. This might be a republishing scheme!

Explain to the developer what a republishing scheme is and why it is possible on Android.

Exercise 9.4

You are about to leave the party. On your way out, you stumble into a conversation of security researchers. They are talking about PartEmu and FirmWire, and how these research prototypes enable the dynamic analysis of proprietary software components used on mobile devices. One of the researchers starts to argue that he could just use an emulator (e.g., QEMU) that supports the ARM instruction set of this proprietary software and would be able to achieve the same results. Since you actually read (parts) of the research articles published with these prototypes, you chime in and explain that a CPU emulator alone is not enough to run these components.

Come up with an argument to convince the security researcher.