**Question 1**: Why is the repackaging attack not much a risk in iOS devices?

Answer:

* Because on iOS devices, the App Store does not allow unverified publishers to add applications, because of this there are generally not repackaged apps on iOS, as the publisher would have to be registered and approved with Apple.

**Question 2**: If you were Google, what decisions you would make to reduce the attacking chances of repackaging attacks?

Answer:

* I would attempt to make the apps harder to publish onto the Google Play store, much like Apple, I would go through a process of verification for developers who want to upload content. Or maybe have some sort of icon showing users that a developer is verified, and that apps without the icon come at an inherent risk.

**Question 3**: Third-party markets are considered as the major source of repackaged applications. Do you think that using the official Google Play Store only can totally keep you away from the attacks? Why or why not?

Answer:

* No, Google Play Store cannot totally keep a customer safe from the attacks, much in the same way that antivirus softwares are not always 100% effective. Even if Google was to deploy a built-in malware scanner, it would have to be updated constantly in order to keep up with the newest malware.

**Question 4**: In real life, if you had to download applications from untrusted source, what would you do to ensure the security of your device?

Answer:

* In real life, I would scan the application with my antivirus software as a preliminary check to make sure that it contained no obvious malware. Then, I would look online for any reviews and forums about that particular application to make sure that no one else had encountered any malware while using it.