Talk on ARQUS : Cyber-Security Summmer School 2021

Kushagra Singh BISEN

Université de Lyon

kushagra.bisen@etu.univ-st-etienne.fr

September 10, 2021

Overview

Introduction

I am Kushagra Singh BISEN, a MSc student in Cyber-Physical Social Systems student at Université de Lyon. I present you my work during the days 6-9 September in the Cyber-Security Summmer School organized by Arqus European University Alliance [Home : Arqus].
During the course of 4 days, we were taught different aspects to cyber-security from researchers of different partner universites and were given quizzes and challenges to assess our understanding of the concepts.

Security and Privacy in Android

Security and Privacy is analyzed using two different softwares,

- RiskInDroid
- SPECK

The application to be analyzed was 'xiaomi home app'. Xiaomi home apps are famous for asking for too many permissions, evenif they don't need those. An example of such could be, the home light application asking permissions to access the contacts, and camera. Such extra permissions can be used to spy/sell the data for data mining purposes. This makes us to use softwares to analyze the **APK** file before installing it to our system.

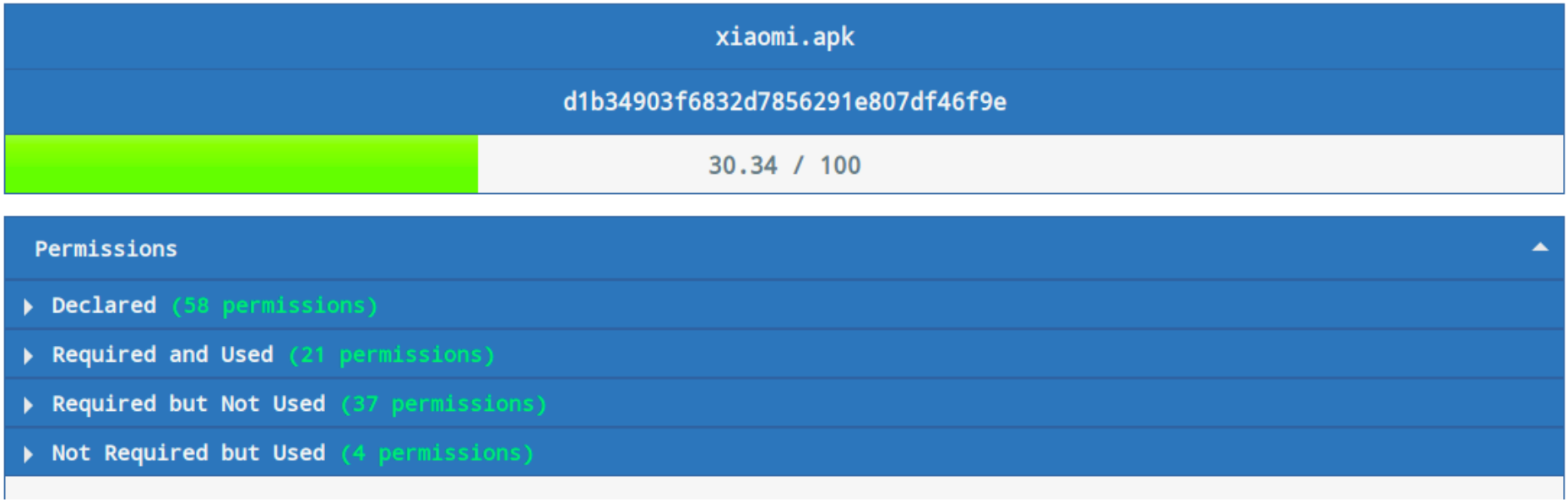
RiskInDroid

Dockerfile is used to run the analysis application. The apk file is selected to result in a score out of 100 based upon different classifiers. The resulting score value is **30.34 / 100**. Regarding the permissions,

- Declared Permissions - 58
- Required and Used Permissions - 21
- Required and not Used Permissions - 37
- Not required but used permissions - 4

Developers can analyze each and every permission, and make decisions or modify the apk for our use.

RiskInDroid



SPECK

The application is downloaded from Github and built using gradle. The python script analyzes the code written in the application, to display the quality of code written with respect to the security of the application. 1719 files were analyzed and code was displayed in 3 classifiers, *INFO, WARNING and CRITICAL*. There are 32 rules which are employed for the analysis, and when you execute they analyze files which depend on the rule. An example of the rule can be, "Store private data within internal storage". Manifest files and main java file are given

Cyber-Security Challenge

The challenge consists the exploitation of a buffer overflow. Unfortunately, I was not able to solve the challenge.

UNIX Quizzes

There were various quizzes given related to file management, networking, file editors, I/O management. I solved the quizzes from section 1 to section 7. Unfortunately, I could not solve the 'init.d' quiz completely, I did solve only 3 of those questions. I could not find the catalog files in my workstation.

Side Channel Analyis with Deep Learning

In this section, I was able to understand and learn Simple Power Analyis. I could not understand Differential Power Analyis and further modules to an extent where I could solve questions related to them.

What I learnt?

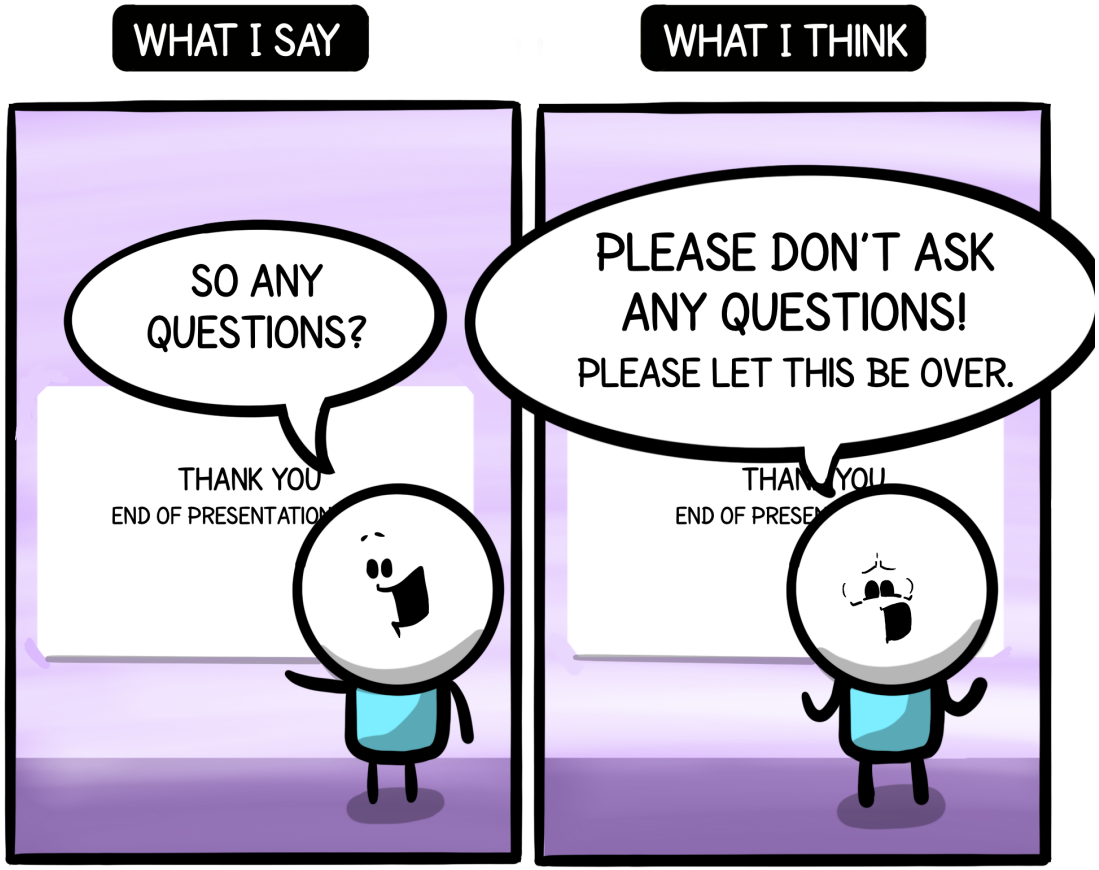
At the end of the summer school, I discovered that Cyber Security is much more than hacking a webpage or getting access to a server. Including Physics, Quantum computing to solve cyber Security problems as well as employing deep learning for cyber-security was a great insight. I wish to rewatch the recordings which will be shared after the school to better understand the concepts to employ later.

References

ARQUS (2021)

Arqus European Alliance. Accessed September 09, 2021. https://www.arqus-alliance.eu/

Thank you for your attention. Any questions?



workchronicles.com

follow on Instagram / Twitter / Facebook