Parte 2 – Exercício 3

De acordo com o que foi interpretado do artigo mencionado no enunciado, os pressupostos do modelo de ameaças são de que não há distinção entre uma falta de cuidado na forma de lidar com os dados, e um atacante a tentar fazer o mesmo. Isto faz sentido, tendo em conta que não há forma de saber identificar a diferença entre o código o que foi feito por um developer erradamente, e alguém com intenções nefastas. Para além disso também é assumido que o ambiente de instalação e os inputs da aplicação podem ser quaisquer, pois isso foge ao controlo da App. Também é assumido que o atacante não tem quaisquer formas de evitar as medidas de segurança da plataforma Android, ou de utilizar canais secundários, de certa forma evitando a necessidade de haver uma preocupação de lidar com dispositivos com Root efetuado.
Por fim, também é assumido que o atacante não utiliza flows implícitos para esconder fugas de dados, e esta assunção é feita porque o FlowDroid não foi desenhado para analisar esses fluxos.

Qual a diferença entre fluxo explícito e implícito de dados?
Como Android suporta Java, e ambos suportam a invocação de métodos nativos em C ou noutras linguagens não controladas, e isto leva a que estes métodos sejam impossíveis de analizar. A forma do FlowDroid lidar com este problema é tendo uma lista dos métodos nativos mais comuns, e uma indicação de como os argumentos afetam o retorno desses métodos. Nesses casos, se os argumentos esperados estiverem manchados (tainted), o retorno também é considerado manchado.

Os fluxos implícitos, são passagens de dados entre componentes Android, através de Intents Android, que são inseridos como argumentos para criação de uma nova atividade pelo sistema operativo. Isto também permite ao componente que chamou o Intent de receber um retorno da nova atividade lançada. Resumidamente o fluxo implícito pode funcionar como um método na medida em que tem argumentos e retorno, no entanto as atividades são definidas pelo programador, pelo que tem de ser feita uma análise dos argumentos caso a caso.