ATTACKS IN THE REAL WORLD

In the first part of this assignment ("Assignment 0.5"), you were asked to find two attack scenarios which exploit vulnerabilities present in Android’s inter-component communication (ICC) process and explain them in detail. These attacks can be implemented and analyzed using specific tools. In this part of the assignment, you are tasked with finding those tools.

LITERATURE REVIEW

You are provided three different published papers about ICC attacks. Review these papers to become familiar with different types of ICC attacks. For the purpose of this part of the assignment, you may assume that these papers describe all known ICC attacks.

For this part of the assignment, you will use these papers in two ways, as described below.

PHASE I – CORRECTING ASSIGNMENT 0.5

You should first use the three papers to evaluate your answers to the first part of the assignment. The goal is to match each of your suggested attacks to a known ICC attack. If you have used other papers in Assignment 0.5, be sure to mention them as your source, as they will be used to evaluate your work. If you find one or more of your vulnerabilities described in Assignment 0.5 incorrect (e.g., the attack you design is not an ICC attack, or you find that your proposed attack is impossible to occur in practice), you can replace them with the most closely related attacks chosen from one of the provided papers.

PHASE II – DETECTION AND PREVENTION

For your updated list of attacks, you are required to

1. find a way to detect instances of those attacks, and
2. determine how those attacks may be prevented.

In your explanations, you should rely on the specific design decisions in the Android OS that made this attack possible (i.e., the underlying architectural causes of each attack). You should be able to find most, but possibly not all, of the information you need. For example, one or more of the papers provided to you may describe ways of detecting a given attack once it has occurred, but not ways of preventing it from happening in the first place.

DELIVERABLES

Your submitted assignment should cover the following for each attack:

1. If you have found any mistakes in your answers to Assignment 0.5, document them. If you have changed the type of attack or its scenario, be sure to mention the reason with details.
2- State the category of each of the attacks based on the provided literature. Remember to include the name of the paper on which you are basing your answer.

3- Explain what Android’s principal design decisions have had to do with the vulnerabilities exploited by your attacks. While you are not required to master Android for this assignment, the underlying causes of the vulnerabilities form the motivation for the publications in the first place, so you should be able to find the answers therein.

4- Name and briefly describe the techniques/algorithms/tools used by the papers’ authors to detect each type of attack, if available.

5- Are there any tools to prevent these attacks mentioned in the articles? Explain it detail.

Although the expectation is that you will draw your answers from the provided papers, you should feel free to add your own solutions. Just be sure to provide enough details to demonstrate that your answer is feasible/correct. Extra credit will be provided for especially creative original solutions (provided that they are correct of course).