專 題 演 講

講 者： 孫宏民教授（清華大學資工系）

題 目： A Static Analysis System for Android Malware Detection Using Machine Learning Recognition

摘 要：

In recent years, with the popularity of smart phones, attracting a large number of developers have put into the development of applications. A wide variety of applications and different types of functions came into being. As smart phones become more powerful, more and more people will use smart phones instead of personal computers. Tens of thousands of applications are downloaded every day, and because of this, they have attracted malicious developers, malicious behaviors in the applications, and hackers' attacks. These malware applications may steal the user's personal privacy information, such as the user's name, mobile phone number, address book and so on. Once the personal privacy information was hacked and leaked, minor impact may be harassed by advertising, while major impact may be scam. In addition, malware applications may also send text messages without permission, and intercept reminding text messages. So how to detect malicious programs has become a big issue. Malware application analysis is divided into two methods, static analysis and dynamic analysis. Static analysis is mainly to disassemble the application, then obtains the information inside the program. By analyzing the internal information of normal and malware applications, extract the features. After preprocessing, find the obvious malicious features. In this paper, we use static analysis method to detect malware application. In order to increase the accuracy of judgment, we will use not only permission but also the other components inside the Manifest file to analysis. We also use n-gram grammar model to analysis the opcode information inside the smali file. Select the obvious malware features, and finally use different machine learning algorithms to classify the malware applications.