（二） 計畫英文摘要。(五百字以內)

總計畫：The Development of Malware's Risk Analysis and User Authentication Technologies for Mobile Applications

The rapid advances of cloud computing and mobile applications facilitate new services commonly known as the “mobile cloud computing”. This new trend of services brings tremendous business opportunity yet triggers new security concerns, as reported in numerous recent studies. For examples, people often store sensitive data in their smart devices that exposes to thread of information leaking when an uncertified app is installed. The current user authentication mechanisms, such as user name and passwords, are often ineffective in mobile environment. Therefore, this proposal consists of three subprojects to encounter each of these research issues individually. Subproject 1, “A Novel Cloud-based Anonymous Aggregation and Risk Assessment of Suspicious Android APPs” addresses the issue of the assurance of a safe operating environment of smart devices; the Subproject 2, “The development of Poses Adaptive and Multimodal User Authentication Mechanism for smart phone users” addresses the issue of assurance of the “right” person to operate the smart device. Both assurances require actions in real time in response to anomaly, as such, both subprojects rely on the reliable cloud service from the third subproject, “ Using Intelligent Platform Management Interface for High Availability Enhancement of Cloud Services”.

Keywords: Mobile Cloud Computing; Mobile APP Malware Analysis; User Authentication; Cloud High Availability

子計畫二：The Development of Poses Adaptive and Multimodal User Authentication Mechanism for Smartphone Users

With the rapid advances in information and communication technologies, smart mobile devices, such as tablets, smart phones, and smart watches, are widely used. These smart devices are often used to store sensitive personal data. Recent surveys show that more than 60% of smart device users opt to turn off their user authentication mechanisms due to their intrusive nature in order to increase usability. We therefore focus on the development of the nonintrusive authentication methods based on the users’ behavior in the past five years. We found that the performance of the proposed authentication method can be improved in three ways: considering the different user operating postures, applying histogram-based features, and using information from multiple sensors. In this two-year proposal, we plan to investigate effective algorithm so that one authentication mechanism can catch a smart phone user’s unique behavior in various operating postures. In the second year, we plan to study method that combines signals from the sensors in smart phone and smart watch to increase the authentication performance effectively, if a user wears a smart watch while using the smart phone.

Keywords: Smartphone; Smartwatch; Multiple Operating Poses; Behavioral Biometrics; Multimodal User Authentication