IDENTITY EXPLOITED THROUGH SOCIAL NETWORK ON SMARTPHONE

Name: Liem Do (Dr. Feng Li, Project Mentor)

Department: Computer Information and Leadership Technology
Purdue School of Engineering and Technology
Indianapolis, IN 46202

Abstract

People tend to leave Wi-Fi feature always on in their Smartphone, which causes many dangerous threats to them. The problem we are trying to approach is how to target Social Networking services on smartphone to exploit identity or steal personal information, such as banking details. For the approach, we will use Man in the Middle Attack methodology along with structural data collection. After the victim’s smartphone connects to the open router which is under the control of an attacker, we will start the attack with ARP poisoning to make the smartphone think us as an actual router and thus it will send data to us. We secretly collect data from the traffic, which will help to determine who the victim is and find out his or her personal information. If the victim uses mobile banking, these banking information including user id and password will be captured. In conclusion, with the study of the attack, we can develop best practice guideline to help smartphone users to prevent from the mobile attack and protect their data. Defense methods will be developed based on the characteristics of smartphones and attacks in this project.