SMARTPHONE-BASED ROGUE ACCESS WIRELESS TETHERING ATTACK
Authored by: Mark A. Mitchell, Jacob Neitling (Dr. Feng Li, Project Mentor)
Computer Information and Leadership Technology
Purdue School of Engineering and Technology
Indianapolis, IN  46202

Abstract

Our project explores how the prolific growth of the smartphone market has forever changed how we are able to communicate with each other. We have also found that this newfound freedom of communication contains many dangers. Much like the original Wireless Revolution, the implementation of smartphones has brought new challenges to security and privacy. We will employ obtaining root access on a device with the Android operating system; this access will allow tethering and data injection and extraction—and, as a result, we will be able to extract desired information or inject malicious code from a target workstation or server. Our studies have shown, thus far, that the true problem facing network infrastructure begins with the fact that smartphones can serve as Wi-Fi hotspots; therefore, other nearby smartphones can easily access the Internet through a tethered smartphone dedicated to providing Internet access. When compared to creating a rogue access point to nullify network boundary defense measures, this attack may lead to the same dire consequences, while presenting new and more difficult challenges in being detected. Consequently, a tethered smartphone becomes a major threat to existing network infrastructure. We plan to test prototypical attack and defense schemes in a real enterprise environment and collect data to study the effectiveness of the prototype schemes. We hope our studies of this attack will illuminate the peril that our society faces from such an attack, and will lead to fruitful countermeasures.

Funding Acknowledgments: Funds for this project were provided by the Multidisciplinary Undergraduate Research Institute at IUPUI.