Rootkits on Smart Phones: Attacks and Implications

ABSTRACT

Smart phones are increasingly being equipped with operating systems that compare in complexity with those on desktop computers. This trend makes smart phone operating systems vulnerable to many of the same threats as desktop operating systems.

This paper examines the threat posed by *rootkits* to smart phones. Rootkits are malware that stealthily achieve their goals by modifying operating system code and data, and have long been a problem for desktops. However, smart phones expose several unique interfaces, such as voice, GPS and battery, that rootkits can exploit in novel ways. These attacks can have serious social consequences, ranging from loss of privacy to denial of service during emergencies.

This paper demonstrates the threat of smart phone rootkits with three novel attacks. We implemented rootkits that allow a remote attacker to: (1) snoop on a victim's confidential conversations; (2) snoop on a victim's geographical location; and (3) stealthily exhaust the battery on a victim's phone. We also discuss the social implications of each of these attacks.