

Detecting Network Intrusion on Mobile Device by Monitoring Power Consumption

James Chung, Dr. Grant Jacoby, Dr. Nathaniel Davis
ECE Department, Virginia Tech

The number of wireless-enabled mobile device is increasing every year, and these devices depend highly on the power obtained from batteries. Without battery power, these devices are completely useless. Nevertheless, most of these devices lack a method to secure themselves from network attacks that could drain the battery power.

The battery power of a mobile device decreases much faster when the wireless mode is enabled. Since the device receives any packet that is directed to it, one could potentially send meaningless packets to the device continuously, draining the battery power much faster than normal. In some commercial and military sectors, without immediate access to AC outlets, drained batteries can cause revenue loss and mission failure, respectively.

A simple method for preventing a network intrusion would be to implement a software-based firewall into mobile devices that monitors the activities of system ports. A potential drawback is that the program must be running in the background constantly to monitor port activities, thus draining the battery. In addition, a firewall does not necessarily point out if the device is being attacked, only if there is an unknown packet at a certain port.

This research proposes a different approach to detecting network intrusion on mobile devices. An early warning system via a host-based form of intrusion detection can be used to alert the user and the security administrators to protect their corporate network(s). This technique operates through the implementation of battery-based intrusion detection (B-bid) on mobile devices by correlating attacks with their impact on device power consumption using a rule-based host intrusion detection engine (HIDE). HIDE monitors power behavior to detect potential intrusions by noting irregularities of power consumption.

In the current generation of mobile devices, HIDE can be used as a remote form of intrusion detection for certain types of viruses or worms. Once an intrusion is detected by a mobile-host, the affiliated network administrator(s) can be notified. This would provide administrators precious extra response time to analyze network traffic, offering an opportunity to recognize and thwart attacks before they spread to inner corporate networks.

For a mobile device, each power state requires a specific range of current from the battery. These power states range from “off” to “busy” states. After a thorough review of many technical documents and then subsequent experiments and research, the ranges of battery current used to sustain various power states can be determined. The dynamic and wide range of power in between states (see Figure 1) provides a means of determining thresholds of normal power levels for activities in each state. Measuring these current ranges over certain periods of time in different power states can determine if the device is in normal operation.

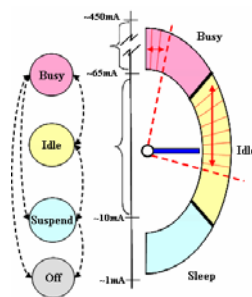


Figure 1: State Power Distribution (Dell Axim) and related B-bid Power Drain Rate Thresholds.

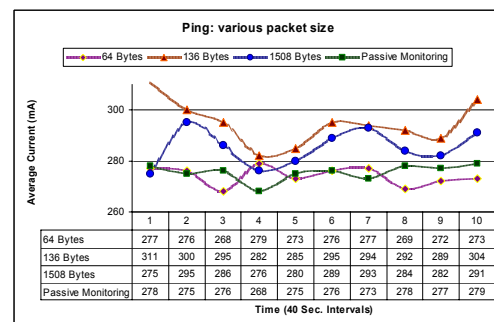


Figure 2: Regular Pinging.

A program was written in C# using .NET Compact Framework. The program logs the instantaneous battery current every few seconds until the user stops the program. The user can set the threshold current as well as the number of consecutive threshold violation required to trigger a warning for a possible intrusion.

In order to determine the threshold current, the program was run on a Dell Axim. Then the device was pinged with three different packet sizes to monitor the battery behavior during a simulated network attack. The results in Figure 2 show a direct connection between increased battery drain as a result of pinging which can be used as a form of intrusion detection.

This research proves that detecting a network intrusion based on abnormalities in power consumption of a device is possible. A further research on this new way of intrusion detection could bring a new set of tools as a defense against an increasing number of viruses and worms.