Securing Android-Based Devices

Researchers

Dr. Asaf Shabtai
shabtaia@bgu.ac.il

Prof. Yuval Elovici
elovici@bgu.ac.il

Publications

Security evaluation
Asaf Shabtai, et al., "Google Android: A Comprehensive Security Assessment", *IEEE Security and Privacy*, Volume 8, Issue 2, Pages 35-44, March/April 2010

Intrusion detection
Asaf Shabtai, et al., "Andromaly: An Anomaly Detection Framework for Android Devices", *Journal of Intelligent Information Systems*, 38(1), 2012, 161-190

SELinux
Asaf Shabtai, Yuval Fledel, Yuval Elovici, "Securing Android-Powered Mobile Devices Using SELinux", *IEEE Security and Privacy*, Volume 8, Issue 3, Pages 36-44, May/June 2010

Goals

The "Securing Android-based Devices" research was conducted six months before the first Android-based mobile devices were distributed by T-Mobile USA. The main goal of the research was to gain essential knowledge regarding the security of the Android platform.

Description

In this research we acquired deep understanding of the Android framework and inherent security mechanisms and identified and evaluated a collection of applicable security solutions for Android.

During the research we carried out a methodological risk analysis process and identified high risk threats (vulnerability to SQL injection, Web attacks, partial code and configuration review, applicability of existing Java and Linux malware). We demonstrated attack scenarios including: developing malware (Denial of Service, PC malware injection), exploiting the Shared-User-ID feature and man-in-the-middle attack on the Android Market's (today, the Play store) protocol.

We demonstrated the applicability of various security solutions such as: SELinux, remotely configurable Firewall, activity-based verification, backup and recovery of applications, and static analysis of applications. In addition, we developed Andromaly, a powerful, modular and reusable intrusion detection framework for Android. We evaluated various Artificial Intelligence methods for detecting abnormal states (Machine Learning and Temporal Reasoning). The CPU consumption of the Andromaly application was in the interval 5.52%±2.11 and the battery measurements showed 10% degradation.