Android Security: A Survey of Issues, Malware Penetration, and Defenses

Abstract

Smartphones have become pervasive due to the availability of office applications, Internet, games, vehicle guidance using location-based services apart from conventional services such as voice calls, SMSes, and multimedia services. Android devices have gained huge market share due to the open architecture of Android and the popularity of its application programming interface (APIs) in the developer community. Increased popularity of the Android devices and associated monetary benefits attracted the malware developers, resulting in big rise of the Android malware apps between 2010 and 2014. Academic researchers and commercial antimalware companies have realized that the conventional signature-based and static analysis methods are vulnerable. In particular, the prevalent stealth techniques, such as encryption, code transformation, and environment-aware approaches, are capable of generating variants of known malware. This has led to the use of behavior-, anomaly-, and dynamic-analysis-based methods. Since a single approach may be ineffective against the advanced techniques, multiple complementary approaches can be used in tandem for effective malware detection.

The existing reviews extensively cover the smartphone OS security. However, we believe that the security of Android, with particular focus on malware growth, study of antianalysis techniques, and existing detection methodologies, needs an extensive coverage. In this survey, we discuss the Android security enforcement mechanisms, threats to the existing security enforcements and related issues, malware growth timeline between 2010 and 2014, and stealth techniques employed...
by the malware authors, in addition to the existing detection methods. This review gives an insight into the strengths and shortcomings of the known research methodologies and provides a platform, to the researchers and practitioners, toward proposing the next-generation Android security, analysis, and malware detection techniques.

EXISTING SYSTEM

Location-based services apart from conventional services such as voice calls, SMS, and multimedia services. Android devices have gained huge market share due to the open architecture of Android and the popularity of its application programming interface (APIs) in the developer community.

DRAWBACK OF EXISTING SYSTEM

- Existing detection methodologies, needs an extensive coverage
- Single approach may be ineffective.
- Security of Android, with particular focus on malware growth.

PROPOSED SYSTEM

Multiple complementary approaches can be used in tandem for effective malware detection. Android security, analysis, and malware detection techniques. Conventional signature-based and static analysis methods are vulnerable in proposed system.
ADVANTAGE OF PROPOSED SYSTEM

- Detect unknown malware
- Signature based on detection is efficiency and simplicity

SYSTEM SPECIFICATION

Hardware Requirements

- System: Pentium IV 2.4 GHz
- Hard Disk: 40 GB
- Floppy Drive: 1.44 Mb
- Monitor: 15 VGA Colour
- Mouse: Logitech
- Ram: 512 Mb

Software Requirements

- Operating system: Windows Family
- Tools: eclipse
- Technology Used: Java
- Backend Used: SQLITE