AndroShield: A Permissions and System Calls-based Android Malware Detection System

Akshay Mathur1, Xinrun Zhang2, Ethan Ewoldt2, Suma S. Sudha1, Quamar Niyaz3, Xiaoli Yang3, Ahmad Y. Javaid1
1. University of Toledo, Toledo, OH; 2. Purdue University North-West, Hammond, IN

1. INTRODUCTION

• Combating malware in Android has been a major challenge.
• Using system call sequences and permissions used by an app can prove significant in determining malicious apps.
• AndroShield app can help novice users understand the utility of permissions and detect malware present on the device using system calls and permissions.
• The app can detect malware apps with an accuracy of 97%-99.
• It utilizes a Client-Server architecture that allows users to check whether a certain application is malicious or benign.

2. METHODOLOGY

3. RESULTS

• Total 6581 traces extracted from the dataset.
• 2001 malware traces and 4580 benign traces.
• Longest system call trace includes 80,000 system calls.
• 90% of benign apps invoked less than 20,000 system calls.
• 90% of malware apps invoked less than 12,500 system calls.

4. AndroShield

5. FUTURE WORK

• Plans to use network traffic data for regularly tracking malware infestations after an app's update.
• Use the app for educating users about permissions and best practices for avoiding malware infestation.
• Continuous monitoring using network traffic-based and system call-based models running as services to alert user of malware presence.

REFERENCES