Mobile Malware Detection By Deception
Héctor Román, Luis Albertorio, José Ortiz Ubarri
Departamento de Ciencia de Cómputos, Universidad de Puerto Rico en Río Piedras

ABSTRACT
Smartphone adoption is increasing at a very high rate every year. Mobile malware is software designed to gain access to sensitive information stored in a mobile device. Mobile malware can also be used to commit cybercrime from a hijacked device. Smartphones application permissions provide the means for a malware application to get access to the files and capabilities of smartphones. Average smartphone users have difficulty identifying suspect malware. In this work we propose a method to detect mobile malware using decoys. The solution proposed to detect mobile malware also serves as protection against malware for mobile users.

METHODOLOGY
The method proposed to detect mobile malware is based on the use of decoys. A decoy in this context is a file or some other type of data that is passively provided to a potential malware application and contains data that seems worthy of stealing. The framework that we propose serves as a protection layer between the software installed in the smartphone and the access to the sensors of the phone; consists of the following:
1) a server application that controls the access to the sensors
2) a client side access API that must be used in the client applications to access the sensors
3) an user space applications that allows to control what will be returned to the client per application
4) a set of monitoring services that detect when the decoys are accessed.

The user should be able to control whether to return the real sensor information, decoy information, or to block access to the sensors. An example of a simple decoy could be made up but enticing emails in the contact list information. A possible way to determine that some application is indeed malware would be to monitor the decoy email address to check if suspicious activity has occurred.

RESULTS
A client/server API was made that handled the data exchange between devices. The multithreaded server receives request from the client and sends the data from the sensors to the client. Sensor data can be real or decoy. Some of the sensors that we managed to access were the accelerometer, gyroscope, light sensor, and contact list.

FUTURE WORK
For future work we will implement a mechanism that will let the user chose whether to send decoy data or real data. Also we will develop methods to trigger alarms in the cases where the decoy information is accessed and the presence of malware or an intruder can be detected.

ACKNOWLEDGMENTS
The authors would like to thank the members of the CSLab and the Computer Science department for their support.

This work is supported by the National Science Foundation under Grant No. DUE-1438838. Presentation of this work has been supported in part by NSF Grant CNS-1042341.

REFERENCES
Justin Cappos†, Lai Wang†, Richard Weiss†Yi Yang†, Yanyan Zhuang‡
†NYU Poly, ‡University of British Columbia Evergreen State College, /Fontbonne University BlurSense: Dynamic Fine-Grained Access Control for Smartphone Privacy