CERIAS

The Center for Education and Research in Information Assurance and Security

Periodic Mobile Forensics

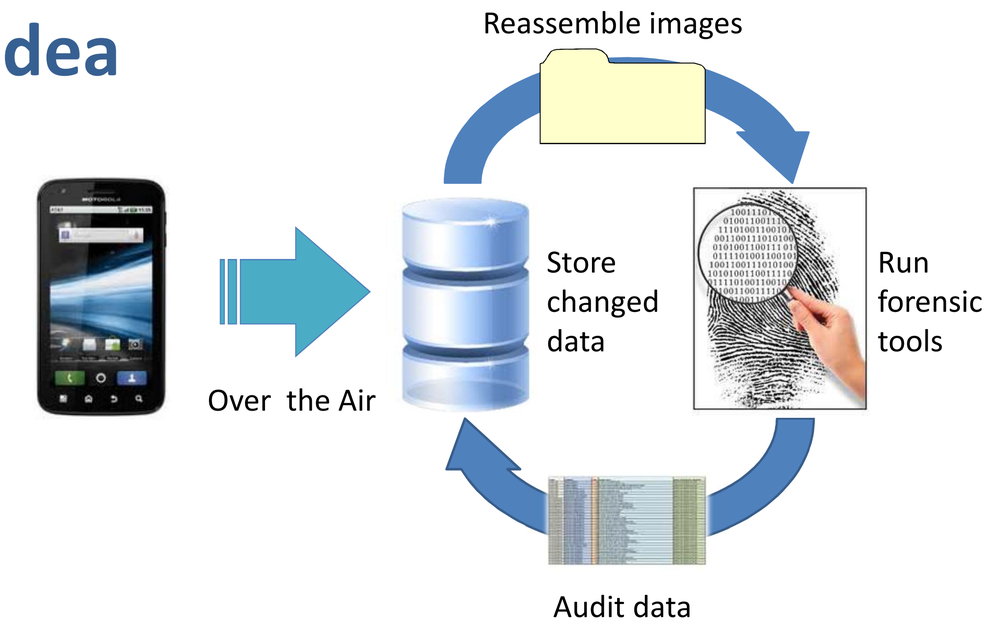
Detecting Malware, Masquerading and Malicious Users

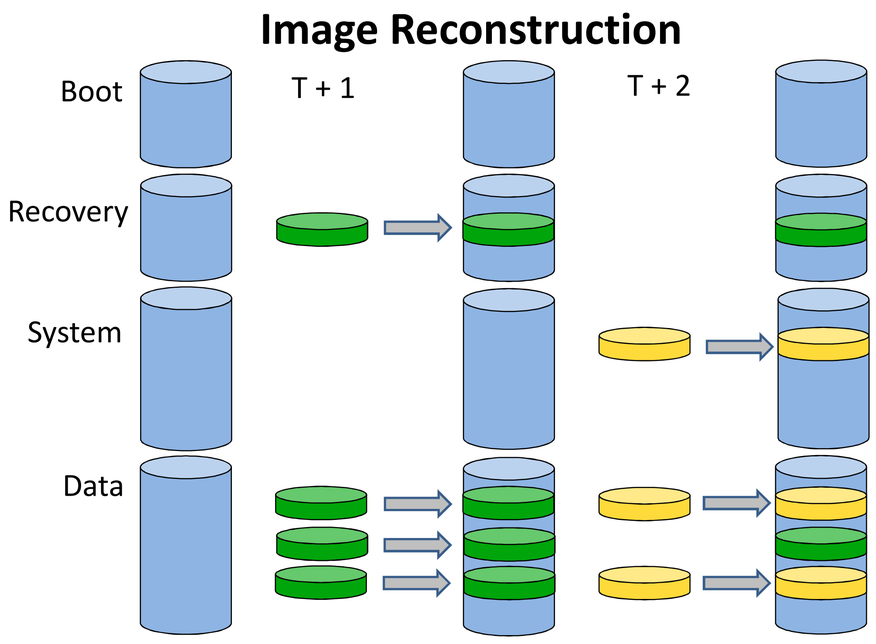
Eric Katz

Problem

Android devices are becoming more pervasive. Currently there are few enterprise methods to identify and measure malicious user and application behavior in order to detect when a compromise has occurred.

Idea

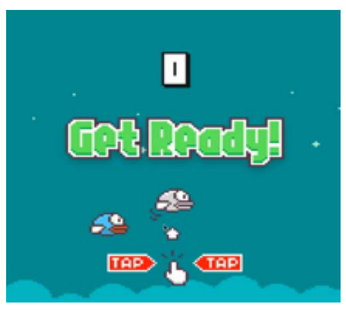




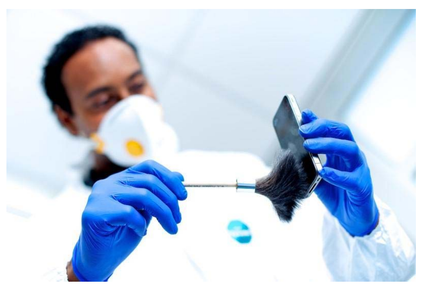
Use Cases

Insider Threat

Evil Maid



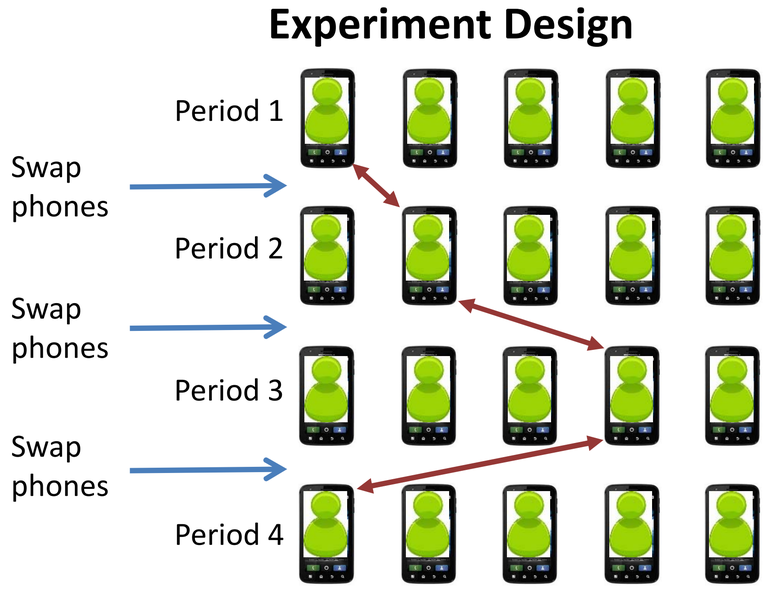
Malicious Application



Insider Threat

Masquerading User Experiment

Conducted at Purdue in conjunction with MITRE, human subjects used phones normally to create a corpus of forensic images. Events are being extracted from the forensic images and statistical comparisons are being used to determine which detection algorithms and events best identify a masquerader on the phone.



CERIAS

MITRE

MITRE Innovation Program

PURDUE UNIVERSITY