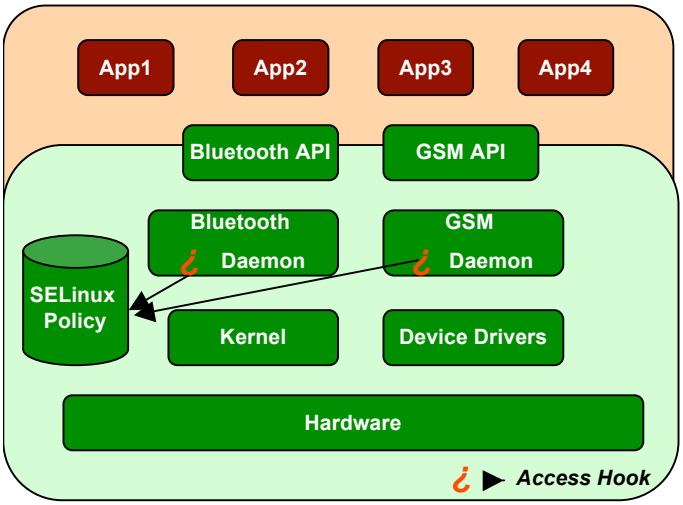
Mobile Phone System Integrity

Divya Muthukumaran, Joshua Schiffman, Anuj Sawani, Mohamed Hassan, Sandra Rueda Rodriguez, Trent Jaeger

Motivation

Over the past few years mobile phones have grown into **Smart phones** supporting additional functionality and services and integrating different networking technologies such as IEEE 802.11, Bluetooth, CDMA and GSM. The **personal nature** of mobile phones results in users storing important information on the handsets like passwords, security codes and other private data. **Untrusted code** and data can penetrate the system via games and applications downloaded by the users. As the phones begin to support advanced applications for **Internet banking** and personal data storage, the integrity of data on the phones become critical

Mediation



The mobile phone has various critical resources that should not be misused. The aim is to mediate access by untrusted applications to these resources. **Access hooks** are inserted into active processes that interact with the resources. Every time an application requests access to a resource, the permission is granted or denied depending on a **policy look-up**.

Also, with the advent of Linux-based mobile phones, the software stack can easily be modified to execute our experiments.

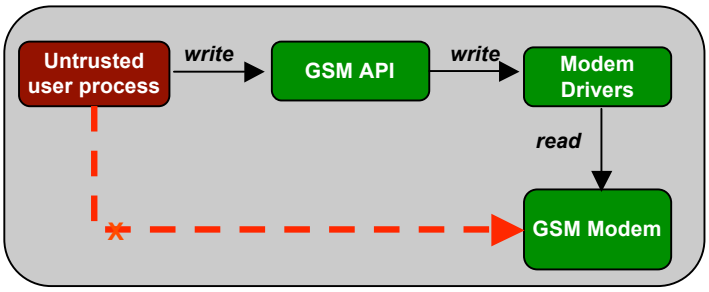
The Goal

Our goal in this project is to preserve the **integrity** of **phone-critical applications** from untrusted code and data. We are leveraging the Trusted Computing Architecture along with SELinux, PRIMA and Information flow analysis to provide integrity guarantees

Information flow measurement

•Integrity property: **Trusted processes should not depend on untrusted ones**

•Inferring information flows:



An untrusted process should not be allowed to write to a trusted object because this can interfere with phone critical applications like the interface for the GSM daemon. We do the following:

- Parse the **binary policy** to get the access rules
- Analyze the rules, obtain the information flows and build the **information flow graph**.
- **Measure** the information flow graph by leveraging **PRIMA (Policy reduced Integrity measurement Architecture)** into the system to facilitate us to make a statement about the integrity of the phone system to a third party

SELinux Policy

We are working on mobile phones running the **Linux 2.6 kernel**. We provide SELinux based access control on these phones. We are working to developing a simple Policy geared towards the phone environment with a minimal rule set.

Sponsored by Samsung