Mobile Phone System Integrity

Divya Muthukumaran, Joshua Schiffman, Anuj Sawani, Mohamed Hassan, Vikhyath Rao, Trent Jaeger

Motivation

- Smart phones have become indispensable devices
- Support a large feature set and applications.
  - Music players, e-commerce, m-banking, GPS, email, web browser etc apart from telephony
- General purpose Operating Systems: Windows and Linux.
- Third-party applications: Download games
  - **What if the games are malicious?**

Integrity of applications

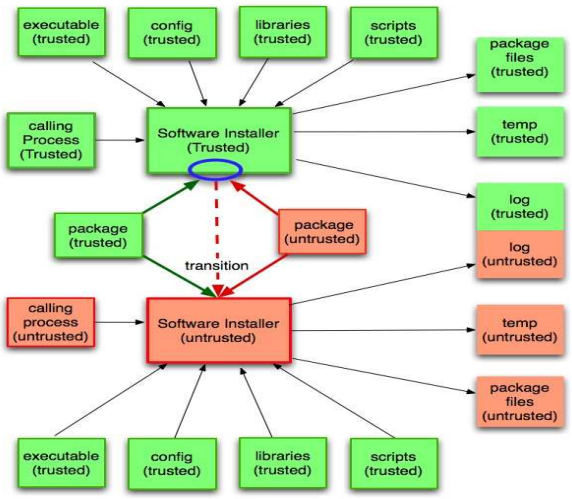
❖Integrity property: ***Trusted processes should not depend on untrusted ones***

❖**Software Installer** is a trusted application. Integrity of other applications depends on the installer. But installer needs to install untrusted packages. How to we protect the installer?

- **Clark-Wilson Lite Integrity Model**
- **SELinux policy**

❖How to prove integrity?

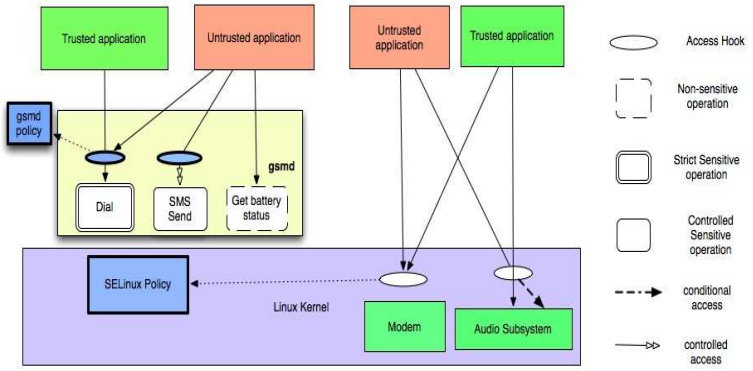
- Measuring Integrity in mobile phone systems[SACMAT '08]
- **PRIMA- Policy reduced Integrity Measurement Architecture**
- Implemented on Openmoko Neo1973 Phone.



Problem

✓How do we know security sensitive applications have not been modified (high integrity)?
✓How do we prove to the bank that our banking client has not been tampered with?
✓How can we protect untrusted applications from misusing telephony?

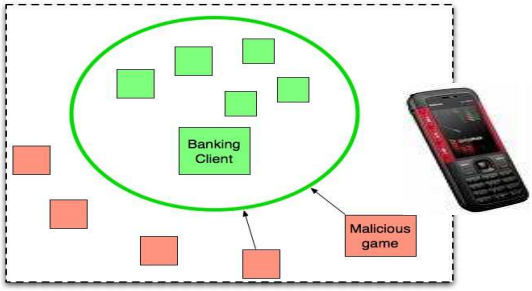
Mediation



✓ ***Untrusted applications should not misuse security sensitive operations in servers.***
  - ✓ Cannot make call
  - ✓ Cannot send SMS to premium numbers
    - ✓ Can query battery

✓ Introduce **Access Hooks** into the telephony server and mediate access to sensitive operations
✓ **Classify operations** and provide **controlled access** to some sensitive operations.
✓ Protect the audio subsystem. *Why?* Untrusted applications can inject noise during a phone call!!

Integrity Perimeter



Sponsored by NSF and Samsung