Practical ROOTS OF TRUST for mobile devices

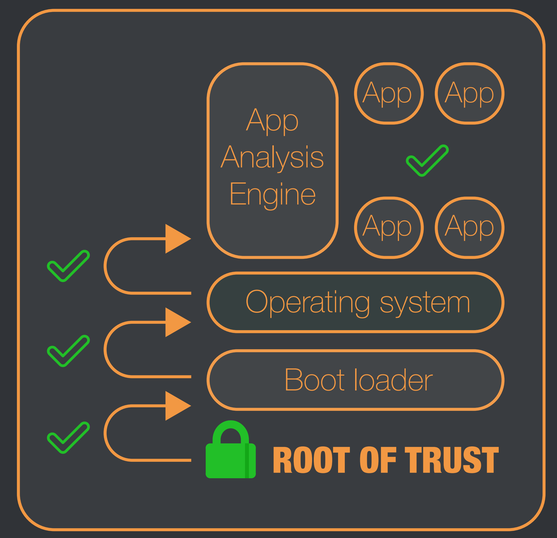
Beyond authentication: Proof that a device is not compromised

A mobile root of trust provides cryptographically strong evidence that the system is configured as it claims. This evidence is a chain of measurements and attestations that starts with a **root of trust**, which forms the trust basis for all evidence for the measurements that follow: the boot loader, the kernel, libraries, subsystems, …all the way to the applications.

Our method

We are developing a portable, software-based root of trust for Android, along with applications that use measurement and attestation to provide a higher level of trustworthiness.

An Android interface to our portable root of trust — one that can be integrated into existing applications — is under development. We are seeking partnerships to integrate our root of trust with applications.



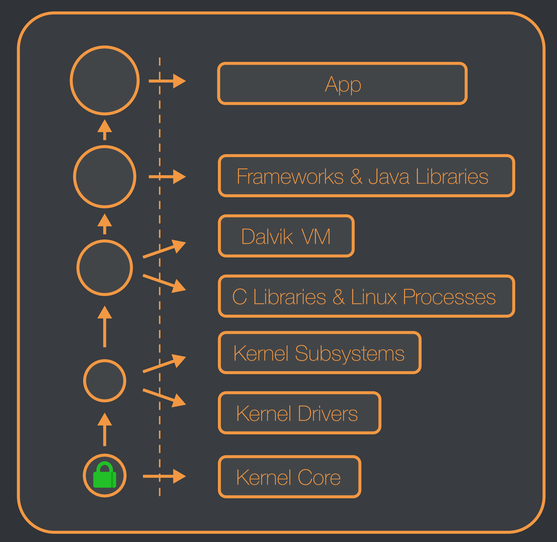
Approach: the evidence chain starts from a trusted root

Example applications

Mobile device management
How can my enterprise trust that mobile device management (MDM) software on our user's phones hasn't been compromised by malware?

Emergency response
How can I trust a potential volunteer's device enough to provision information about critical infrastructure in an emergency?

Secure entry
Can I trust this mobile device to enter a secured facility, in accordance with organizational and building-specific security policy?



A measurement chain for the Android operating system

The Mobile Roots of Trust project is funded by Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division, SBIR H-SB013.2-002: Software Based Roots of Trust for Enhanced Mobile Device Security.
Period of Performance: August 2014 - September 2016

|galois|