ENSURING SECURE CONTENT PROTECTION SOLUTIONS

Type equation here.

RtFence

Kernel Rootkit Defense using TrustZone Technology

Kernel rootkit, as a traditional approach of exploiting, can still be applied to the mobile platform, however. The widening usage of mobile devices has presented a tendency that mobile devices hold information of higher confidentiality. Thus, a successful security attack on mobile devices can leak more sensitive data.

External security mechanism cannot function in this situation, since they relies on certain features provided by kernel, which is no longer a trustworthy component in the software stack.

The integrity of kernel can solely be protected by a component which is independent from the kernel itself.

Product highlights

- Trusted kernel rootkit detection.
- Does no rely on an existing kernel features.
- Online kernel data structure protection.
- Trace analysis of kernel control flow.

Independent Execution Environment Based on TrustZone Technology

ARM®'s TrustZone® technology provides the foundation for the creation of an independent execution environment. By appropriately configuring, TrustZone® technology creates a trusted execution environment whose accesses to hardware resources is absolutely separated from the normal execution environment.

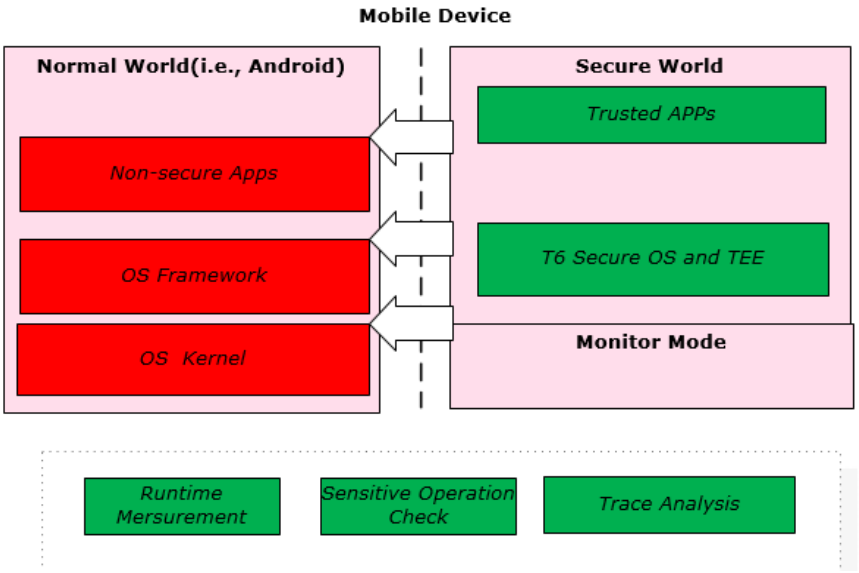
A secure execution environment is more privileged than the one. It holds sensitive data which is inaccessible from normal execution environment and executes only authorized applications, thus preserving the integrity as well as the confidentiality.

Kernel Rootkit Defense with TrustZone

RtFence detects potential kernel rootkit by means of dynamically making snapshot of kernel data structures. By analyzing the snapshot and taking appropriate measures in time, RtFence can stop kernel rootkit before it can cause much damage.

Moreover, certain key kernel data structures is hooked by RtFence. Once modified, the corresponding sensitive operations will be checked online.

RtFence resides in different execution environment with the protected kernel, therefore the integrity of the result it produces is guaranteed.



Architecture of RtFence

Runtime Measurement

Runtime Measurement is performed periodically by RtFence to check whether unreasonable alterations have been made to kernel data structures, which is one of the major indications that a kernel rootkit is undergoing.

Sensitive Operation Check

Certain sensitive operations on the kernel data structures is hooked by RtFence. Once issued, a switch from normal execution environment to RtFence is triggered and this operation is examined in detail to protect data structures from being modified by malicious behaviors.

Trace Analysis

Kernel control flow is monitored in real-time with the processor's built-in performance monitors. RtFence increases the accuracy of kernel rootkit defense by further analyzing the suspected kernel traces.

Learn More

For more information, please visit http://trustkernel.org or email contact@trustkernel.org.

About TrustKernel

Founded in 2013 and headquartered in Shanghai, TrustKernel is focused on next generation mobile and server security solutions and tries to provide these available solutions to end users. TrustKernel's defined goal is to deliver fast and simple IT security solutions for mobile, embedded devices and server to our customers and partners.