November 27, 2018

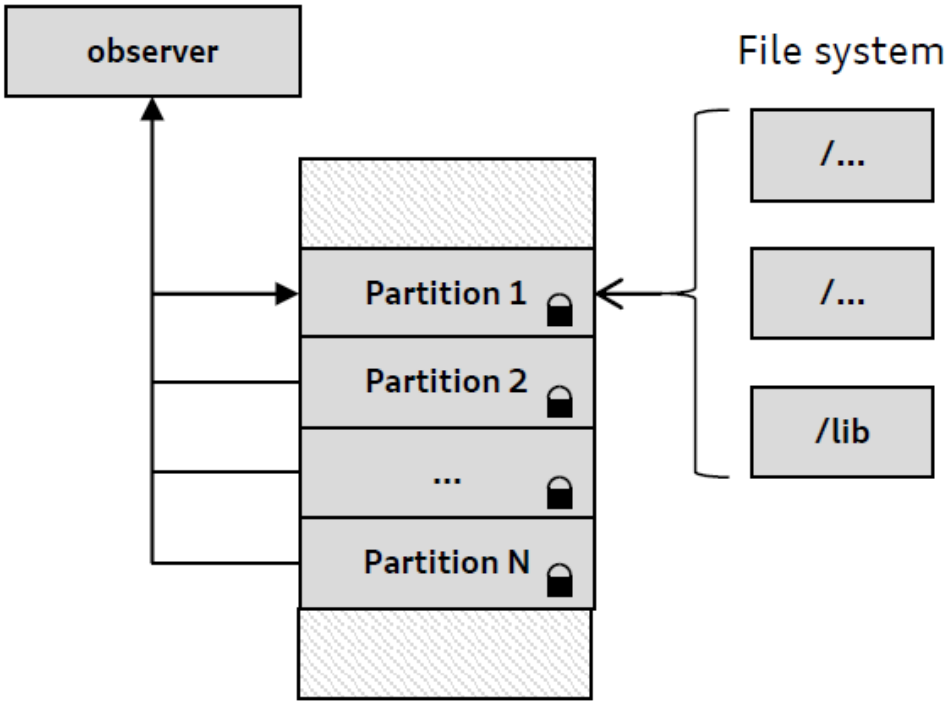
SAFE COMPONENT EXCHANGE IN THE TIVOIZED SYSTEM

Verena Schwaiger
Bertrandt Ingenieurbüro GmbH

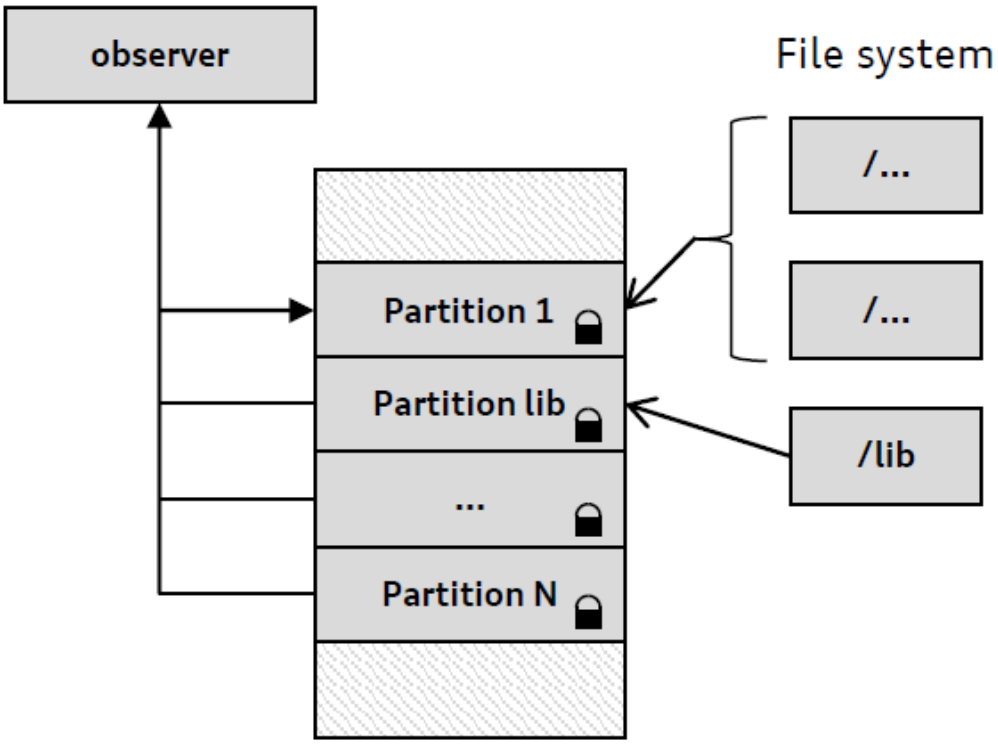
SAFE COMPONENT EXCHANGE IN THE TIVOIZED SYSTEM

Technical Task:
Tivoization is a widely used technique in commercial products to increase security for both user and manufacturer. In such systems, replacement of software components (e.g. binaries or libraries) with cryptographic signatures associated with Secure Boot and Chain of Trust (CoT) is prevented.

Initial Situation:
The figure „state of the art“ shows an example of a system with one or more partitions. In the following example, “partition 1” represents a file system that combines proprietary and public components, e.g. “lib”. All components are protected by a digital signature and are monitored by an observer over the runtime. In the event of a mismatch, the observer may block access to the component in whole or in part, depending on the implementation and use case. On the other hand, many public libraries are offered under licenses that require interchangeability by the user. In order for the user to exchange this library in one of the systems shown below, protection for the entire “partition 1” must be deactivated. Depending on functionality and implementation, this can lead to security threats such as access to critical internal and external interfaces by unverified components or unauthorized sharing of protected system functions.



Solution:
The system proposed in figure "Technical Innovation" solves the problem of the publicly available component, e.g. called "lib", which is nested within a proprietary file system. In the following image, the component "lib" is placed in a separate area (for example, file system partition), which can also be protected by default. The protection for this area can be disabled at the request of the user so that its content can be changed, e.g. by replacing the lib with a functionally equivalent lib. In other words, the solution complies with the licensing terms for this component.



Advantages:

- The big advantage of this idea is that even if the protection for system parts containing "lib" is disabled, the rest of the system including "partition 1" will still be protected by the viewer and its integrity will remain unrestricted.
- In addition, the observer may also pass information about the protection status of the partition "lib" (and thus its integrity and trustworthiness) to other systems such as "partition 1".
  Based on this information, other systems and components may respond accordingly, e.g. by disabling certain functions.