Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis M.Sc.

Trustworthy and tamperproof configuration management of networked devices

Motivation

Today's networks are endangered by numerous threats. One especially problematic type of attacks involves administrative ("root") users: An attacker, for instance, might compromize an honest admin's machine and abuse the credentials stored on this machine to perform undesired or harmful changes in the networked system. The result is, for instance, that the attacker gains access to secret company data. In a different scenario, the administrative user turns evil and abuses her system wide access rights to, for instance, harm her employer.

Approach

In previous work, we investigated how Distributed Ledger Technology (DLT) can help in this context. DLT is able to manage data in a community effort of numerous peers, which can even belong to different, competing organizations. Whenever changes need to be applied to a data asset (create new asset, change an asset's value, etc.), the changes can only be applied when the network reaches a consensus that authorizes the change.
Using DLT as basis, we designed and implemented a trustworthy and tamperproof Configuration Management System (CMS) that acts as an intermediate between administrators and networked devices. In contrast to today's systems (Ansible, Puppet, Chef, ...) a configuration is not directly rolled out to devices but must undergo a validation process controlled by our CMS first. This process mandates that the new configuration is verified by human experts and/or automated processes. After finishing the validation, a configuration becomes active and is applied automatically.
In this thesis, we want to integrate the CMS into a broader scope to cover a new scenario: aircrafts. Aircrafts can be understood as flying computer networks with high security requirements. For this reason, devices cannot be simply reconfigured. Instead, different authorized configuration profiles exist, which are activated, for instance, by incident response systems to counter problems found by anomaly detection systems. Your overall task is to extend the current status of our CMS to fit the new scenario.

Your Tasks

1) Analyze security goals and requirements of the aircraft scenario. **2)** Investigate on related work. **3)** Using the status quo of our CMS, design new CMS functions that help to reach the security goals you defined before. **4)** Implement a prototype of the enhanced CMS.

Contact

Dr. Holger Kinkelin, Cora-Lisa Perner and Heiko Niedermayer
(lastname@net.in.tum.de)