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

Thesis B.Sc.

Thesis M.Sc.

Trustworthy Configuration Management for Networked Elements

Motivation

Today's networks are endangered by numerous threats. Various security problems even emerge from the inside of the network. The maybe most problematic scenario in this context is when administrative personnel ("root" users) become malicious and spy on sensitive data, or perform undesired configurations. This problem arises from the fact that root users virtually have unrestrained access rights that allow them to first perform the undesired configuration and afterwards to remove traces in log files that might reveal their doing.

Approach

In this thesis we strive to change how administration of highly critical network elements is done. Instead of allowing a root user to login to a system via SSH, or to push new configurations to the system using tools like Ansible, systems shall be locked down and accept configurations from a trusted configuration repository only. The repository shall guarantee, that no configuration can ever be modified or removed, which provides a basis for trustworthy configuration accounting/tracking.
However, this approach does not prevent that undesired or even hazardous configurations are issued by administrators. For this purpose, we want to add a property comparable to Bycanthine fault tolerance (BFT) to system configuration. Instead of executing a configuration immediately, a system will accept certain critical configurations only if n additional auditors have checked the configuration proposed by the administrator.

Your Task

In this thesis, the following research questions and ideas shall be elaborated: 1) How is it possible to create an unmodifiable and unerasible repository for, e.g., configurations and also system log information? Target technologies include – but are not limited to – append only file systems, block chains, etc. 2) How can a computer system be hardened in a way that a system administrator cannot directly perform configurations? 3) How can the BFT-like auditing scheme for configurations be implemented based on the chosen repository technology? 4) Which technologies are suitable as basis for the system configuration tool? Example technologies include Ansible, Puppet, etc.

Contact

Dr. Holger Kinkelin kinkelin@net.in.tum.de
Dr. Heiko Niedermayer niedermayer@net.in.tum.de