QNX Security concepts

Introduction

Operating system is the foundation for embedded system and a secure OS can prevent exploits in both underlining hardware and software. Therefore, it is necessary that the security features are baked into the operating system, which can be done by hardening the OS.

It is considered a best practice to harden operation systems and base software. What counts as hardening is up to the particular implementation. Usually this includes at least ensuring that every account / user has only the minimal subset of permissions that are absolutely required to perform its tasks. The exact same goes for groups and for the assignment of group memberships and user permissions for processes.

Objective

Using hardening guides is state-of-the-art for system on the internet, systems in trains, servers and OSs in embedded devices. As QNX claims to be the most secure operating system it neither have a hardening guide available, nor a validation and configuration tool (not just for QNX 7 but for any QNX operating system). Purpose of this project is to identify threats in the system (what could go wrong). Based on these threats, mitigation techniques should be created. These techniques could be to enable/disable related services, ports, protocols, policies or security features. This mitigation techniques will be later used as the base for developing the actual hardening guide.

Workflow

The whole project is divided into 3 main tasks:

1. Identify threat, for this STRIDE model should be implemented.
2. Filter some high-risk threat and create detailed attack tree for those threats.
3. Develop or identify security measures that should be enabled to mitigate these threats.
4. Validation