Linux systemd Forensic Analysis Tool

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Dr. Bruce Nikkel

On Debian like Linux distributions extract the unit and configuration files that differ from their initial installation package. Achieve this by using MD5 checksum comparison. Verify if files' presence is justified. Report suspicious files and state the reason for them being suspicious.

On Debian like Linux distributions (Ubuntu, Debian) systemd is becoming the de facto system manager. It provides a system and service manager that runs as PID 1 and starts the rest of the system. For a service to be compatible with systemd, so called unit and configuration files are used. When a package is installed, default unit and sometimes configuration files are added. These can be altered in different locations overwriting and overriding the default. This work provides a tool to analyze which unit and configuration files have been modified compared to the initial installation.

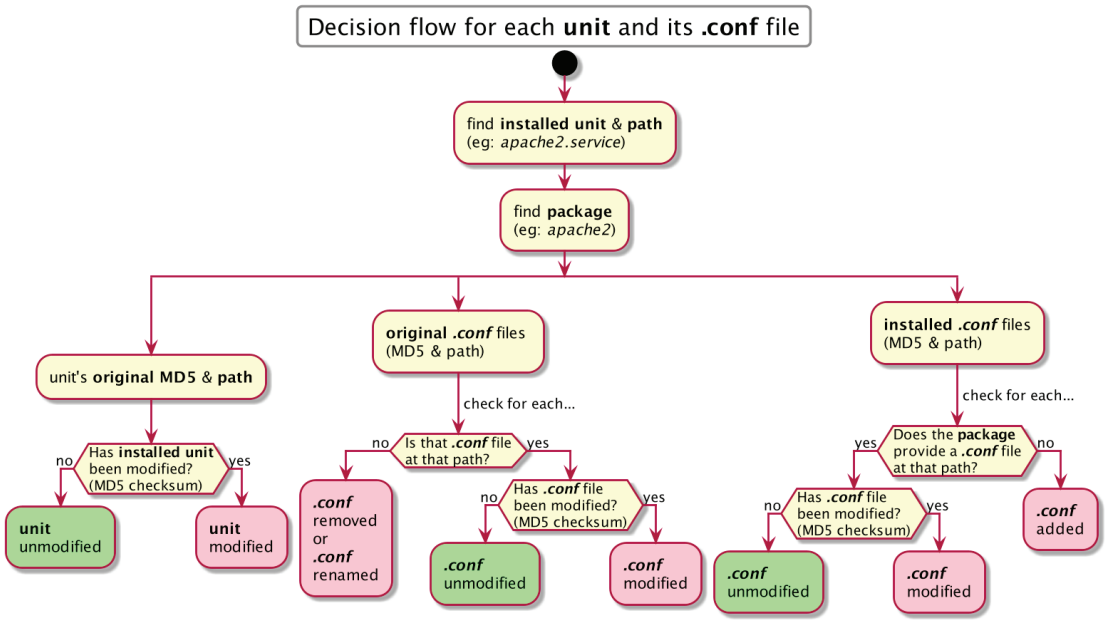
- For all found unit files a MD5 checksum comparison between the installed and the default unit file is computed.
- For all configuration files, it is established if their presence is justified or not. If their presence is justified, a checksum comparison is undertaken.

The checksum comparison is achieved by looking for the MD5 checksums file at 3 locations in the following order:

- /var/lib/dpkg/info/
- if not found at the previous location, search in : /var/cache/apt/archives/
- if not found at the previous location, download the package and search within for the MD5 checksums file.

The suspicious files are listed stating for which reason they are considered suspicious.

Yann Kristen Roth



Find units and configuration files that differ from the initial installation.