Securing the Raspberry Pi OS: An Open Source Security-Configuration Guide

Bachelor's Thesis

Supervisor: Prof. Dr. Alexander Pretschner
Advisor: Patrick Stöckle
Email: {alexander.pretschner, patrick.stoeckle}@tum.de
Phone: +49 (89) 289 - 17314
Starting date: immediately

Fakultät für Informatik
Lehrstuhl 4
Software & Systems Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3
85748 Garching bei München

Tel: +49 (89) 289 - 17314
https://www4.in.tum.de

Context

The secure configuration of systems is still a topic neglected in most organizations and companies. Insecure configuration results in privacy problems or in possible attacks that can threaten different security properties like the confidentiality or the integrity of the data. At the Chair of Software and Systems Engineering, we have been working on this topic in a joint research project with Siemens AG since 2017. In this project, we have made it more efficient to implement existing security-configuration guides [3] and improved the process of maintaining and testing security-configuration guides [4]. As far we know, there is no public example for a state-of-the-art security-configuration guide publicly available yet.

On the other side, the community have difficulties to find out all security problems and make a complete hardening guide out of it such as for the open source system Raspberry Pi OS [2]. Hardening measures include setting secure configuration values for necessary software and services and deactivating or limiting unnecessary or problematic ones. There are many blogs [1] one could see as security-configuration guides that help people to harden their Raspberry Pi OS; However, they have the same problems we have seen for all unstructured security-configuration guides: Human-readable parts, e.g., the description and rationale, are mixed with the machine-readable parts, e.g., scripts to implement the rules. Thus, implementing a guide manually needs annoying more time then an automated one. Furthermore, one can improve the guide only through comments on the website or emails to the authors.

Goal

We want to solve both problems together by publishing a state-of-the-art security-configuration guide for Raspberry Pi OS. The guide should include all rules to harden the Raspberry Pi OS. Each rule should include machine-readable information to implement and check the rule automatically and information about the rationale of the rule. Here, we want to collect information from existing guides and other sources. Using the *existing* Scapolite tools [4], we *can already* generate check and implementation scripts. Raspberry Pi users can use those scripts to harden their Pis when setting them up. Optionally, we might add different profiles, e.g., a high- and a low-security profile.

We will publish the Scapolite files in a git repository, e.g., on GitHub where people can contribute by Merge requests. Furthermore, we will also publish the artifacts, e.g., a PDF version of the guide and the scripts, e.g., as part of a release.

Working Plan

1. Research: Familiarize oneself with security-configuration guides, especially Linux guides.
2. Research: Familiarize oneself with the Scapolite format and the corresponding tools.
3. Research: Collect information about hardening the Raspberry Pi OS.
4. Implementation: Create Scapolite files for the rules.
5. Implementation: Create the check and implementation automations for the Scapolite files.
6. Implementation: Setup the GitHub repository with a CI to produce and deploy the artifacts.
7. Evaluation: Compare vanilla Raspberry Pi OS installation with hardened installation.
8. Evaluation: Compare the effort of manual hardening versus script hardening.

References

[1] Justin Klein Keane and Tom Van De Wiele. Take These Steps to Secure Your Raspberry Pi Against Attackers, 2017. URL https://makezine.com/2017/09/07/secure-your-raspberry-pi-against-attackers/.

[2] Bruce Schneier. Securing a Raspberry Pi, 2017. URL https://www.schneier.com/blog/archives/2017/09/securing_a_rasp.html.

[3] Patrick Stöckle, Bernd Grobauer, and Alexander Pretschner. Automated Implementation of Windows-Related Security-Configuration Guides. In *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*, ASE '20, page 598–610, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450367684. doi: 10.1145/3324884.3416540. URL https://doi.org/10.1145/3324884.3416540.

[4] Patrick Stöckle, Ionuț Pruteanu, Bernd Grobauer, and Alexander Pretschner. Hardening with Scapolite: a DevOps-based Approach for Improved Authoring and Testing of Security-Configuration Guides in Large-Scale Organizations. In *Proceedings of the Twelth ACM Conference on Data and Application Security and Privacy*, CODASPY '22, pages 111–222, New York, NY, USA, 2022. Association for Computing Machinery. ISBN 978-1-4503-9220-4/22/04. doi: 10.1145/3508398.3511525. URL https://doi.org/10.1145/3508398.3511525.

Fakultät für Informatik
Lehrstuhl 4
Software & Systems Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3
85748 Garching bei München

Tel: +49 (89) 289 - 17314
https://www4.in.tum.de

Securing the Raspberry Pi OS: An Open Source Security-Configuration Guide – Bachelor's Thesis