Automatic Security Configuration for Mobile Devices

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: 15.05.2019

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

We at the Chair of Software and Systems Engineering (I4) are developing the Scapolite framework in cooperation with an industry partner. The goal of this framework is to make the specification and management of security-configuration guidelines easier and automate the implementation and the check of the different security-configuration rules. Traditionally, the main focus of security configuration lies on the hardening of servers or PCs, because these have been the devices where sensitive tasks were executed or controlled and sensitive data was stored. Thus, we choose Windows-based systems for our first proof-of-concept of how the implementation and the check of security-configuration rules can be automated. The rationale behind that is that almost 90 % of the desktop or laptop PCs are running a Windows-based system. [2]

Nevertheless, with the spread of smartphones, people are now using them in almost the same way as PCs. Using Apps from third-parties, one can do almost the same things on a smartphone as on a PC. This is reflected by the fact that nowadays 40 % of all devices on the Internet are running an Android OS, but only 37 % a Windows OS. Thus, smartphones are an interesting target for attackers because there might not only contain sensitive information, but also access to the built-in sensors like the camera or the GPS. Therefore, not only PCs should be configured securely, but also smartphones.

Goal

In this Bachelor thesis, we want to develop an approach of how the security configuration of smartphones can be automated. The goal is to automate the check and the implementation of security-configuration rules. The popularity of the Android OS inspired also other people to access this topic: Vecchiato et al. [3] are only dealing with the assessment of the security configuration rules, but not with their implementation. Within this work, we want to find commonalities and differences between the automation of security-configuration guidelines on OSes operating on PCs and OSes operating on mobile devices. Our main focus is based on the Android OS because it is the most widespread OS on mobile devices. For the evaluation, we plan to automate the application of an existing security-configuration guideline, e.g., the Android guideline from the CIS [1], and assess how many rules could be automated and how the security could be improved through the automation of these rules.

Working Plan

1. Research: Other approaches, restrictions on mobile devices, possible solutions
2. Define a format how security-configuration rules for mobile devices can be specified to make them automatable
3. Implement the automation of the implementation and the check of the rules
4. Evaluate the implementation on a existing security-configuration guideline

References

[1] Center for Internet Security: Benchmarks. https://www.cisecurity.org/cis-benchmarks/. Accessed: 2019-04-10.

[2] Operating system market share. https://www.netmarketshare.com/operating-system-market-share.aspx. Accessed: 2019-04-10.

[3] Daniel Vecchiato, Marco Vieira, and Eliane Martins. A security configuration assessment for android devices. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, SAC '15, pages 2299–2304, New York, NY, USA, 2015. ACM. ISBN 978-1-4503-3196-8. doi: 10.1145/2695664.2695679. URL http://doi.acm.org/10.1145/2695664.2695679.