Automatic Selection of Security-relevant Configurations

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

We at the chair of Software and Systems Engineering are currently developing together with an industry partner the Scapolite framework. The idea of the Scapolite framework is the definition of security configuration guidelines in a human- and machine-readable form and the automatic implementation of these guidelines or the automatic check if a system is compliant to a guideline. Usually, the input for a hardening process regarding security configurations is a guideline with many rules. Here, every rule defines a value which has to be set for a specific configuration to make the system more secure.

The selection which configurations are security-relevant and which are not is conducted by experts who should know all security-relevant configurations of a specific system. If the experts who create the security guidelines are not aware of a specific security-relevant configuration or if they simply forget one, this security-relevant configuration may stay in an unsafe state although the system is configured compliantly to the security guideline. Thus, this may lead to open attack points on a system which is regarded to be secure.

Goal

The idea of this bachelor's thesis is to automate this selection of security-relevant configurations. We want to develop a proof of concept which takes as input a set of configurations with additional information, e.g., description, help text, possible values, etc., and returns as output a set of configurations, which are possibly security-relevant. In other words, we want to define a function by rules or learn a function which maps a configuration enriched with its additional information to the security-relevant or not security-relevant.

To our best knowledge, this has not been tried yet. Two main problems here are the lack of the machine-readable definition of the configurations and their additional information and the lack of training data to learn or to deduct which configuration is security-relevant and which is not. During the development of our first proof of concept implementation for the automation of Windows-related security configuration guidelines, we had to reverse engineer the Windows' way of defining possible configurations in the form of administrative template files (ADMX/ADML). Thus, we now have for the Windows context exactly this machine-readable form of the configurations and their additional information needed for the aforementioned approach. Furthermore, with the security guidelines created by the Center for Internet Security (CIS) [1] and the IASE [2], we have the input to derive rules or learn which configurations are security-relevant. Thus, we think that the Scapolite framework is the perfect context to conduct this bachelor's thesis.

Working Plan

1. Research
2. Make familiar with the configuration description format and the guidelines from CIS and IASE
3. Determine set of possible approaches to implement the mapping function
4. Implementation
5. Evaluate on Windows configurations

References

[1] Center for Internet Security (CIS). https://www.cisecurity.org/. Accessed: 2019-01-29.

[2] Information Assurance Support Environment (IASE): Scap content. https://iase.disa.mil/stigs/scap/Pages/index.aspx. Accessed: 2019-04-03.