Automatic and Reproducible Attacks on insecurely configured Systems based on Security-Configuration Rules

Master'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 which is neglected in most of the organizations and companies. The 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. The former can occur if services are configured so that they are sending, e.g., as problem reports, data outside which should be confidential, the latter if the software is configured so that, e.g., old and vulnerable protocols are used. One main problem is that these potential privacy problems and security flaws are abstract and thus they are not taken seriously neither by the persons responsible for the systems nor by their superiors.

On the other side, the state-of-the-art technique of dealing with this problem, the increased security of the application of security-configuration guidelines is abstract, too, whereas the problems resulting from deactivated insecure protocols and services are concrete. If one takes a system and applies all the rules of the corresponding guideline, this might result in a lot of problems because of software which will not work any longer or users which cannot access they systems as easy and comfortable as they were used to. On the other side, the fact that now 2, 3, or more attacks, which are described in the rationales of the applied rules, are not longer possible stays abstract and intangible.

With this master's thesis, we want to improve this situation. We want to find and automate a set of attacks that can be executed as automatically as possible. These attacks should be possible if the system is configured insecurely and impossible if the system has been hardened. The best would be to find as many attacks as possible which are possible if the system is freshly installed and still has the default configuration. The automatic application of these attacks on normal systems would be the perfect argument why the current way of simply ignoring secure configuration is not a viable way.

Goal

We want to use the rationales of the different rules to construct attacks and model them, e.g., in the form of attack trees. These attacks should be

- Automatic
- Possible if the system is configured insecurely or better if the system is in the default state as this is the case for most of the systems
- Impossible if the system is configured as specified in the security-configuration rule. If the attack is still possible although the system has been hardened, the security-configuration guide has to be improved or the attack cannot be blocked by the end user.

The main research object of our project for automating the application of rules and still the most common operating system for desktop computers is Windows 10. Thus, the developed attacks should be attacking a default Windows 10 instance. The attacks should be evaluated by creating new Windows 10 instances, attacking them, applying different security-configuration guidelines or subsets of given guidelines, attacking them again and evaluate, if the attack is still possible or not.

Working Plan

1. Research: find attacks related to insecure configurations
2. Automate attacks, e.g., using Metasploit [1]
3. Evaluate attacks on default and hardened Windows 10 instances

References

[1] https://www.metasploit.com