Monitoring the vulnerability of devices (used in Dutch critical infrastructure)

Bachelor referaat research idea

January 2018

Abstract The goal of this research is to design a monitoring framework that retrieves vulnerabilities described in (online) reports and automatically verifies whether (and when) devices were fixed. As a case study, we intend to apply the proposed framework to devices (e.g., computers and controllers) used in critical infrastructures in the Netherlands. We hope that by exposing vulnerable devices we affect on the average response time of administrators to new vulnerabilities.

Keywords network, security, monitoring, vulnerabilities, critical infrastructure, SCADA

Motivation and Scope Operators of networks controlling critical infrastructures need to design a safe and reliable system, in which messages between the devices are exchanged in a timely manner. However, network which seems safe at some moment in time might be vulnerable at a later point in time, because of flaws of its devices. Vendors, researchers, and white and black hackers constantly search for devices' vulnerabilities in order to warn the users and patch them, or in order to abuse them. For traditional IT networks, performing system updates can be done relatively fast, e.g., within the same day. However, the devices used in critical infrastructures, such as in power distribution, often depend on Supervisory Control and Data Acquisition (SCADA) systems built decades ago, with uptime counted in years. Timely delivered messages are of great importance, which makes scheduling for maintenance and updates hard.

US-CERT is the United States Computer Emergency Readiness Team, which alerts about reported vulnerabilities[1]. An example of a vulnerability

[1] `https://www.us-cert.gov/ncas/bulletins`

can be the Heartbleed[2]. Although reported already in 2014, there are still almost 150 thousand devices still susceptible to it[3]. For critical infrastructure, US-CERT has a dedicated division called the Industrial Control Systems CERT[4], where the reported alerts refer to SCADA devices.

In order to understand how secure is the infrastructure that uses SCADA systems, it is important to track how fast are the new vulnerabilities patched. This can be done, e.g., by constantly monitoring the devices, newly discovered vulnerabilities and their patches. Therefore, the goal of this research is to create a framework for monitoring a set of devices for new vulnerabilities.

Goal The research questions to be addressed in this assignment are as following:

RQ1: What are the most well-known vulnerabilities of equipment used in SCADA systems?

- RQ1.1: What are the best practices to prevent or overcome those vulnerabilities?
- RQ1.2: How can you list and find the newest vulnerabilities and their patches?

RQ2: Design and implement a framework for monitoring a device for vulnerabilities, upon releasing new vulnerability for that specific device (vendor).

- RQ2.1: What is the average time of response of the discovered vulnerable devices on the announced vulnerabilities?

Type of assignment This assignment is aimed to bachelor students of computer science and or electrical engineering interested in network monitoring, security and SCADA networks.

More information Justyna Chromik (j.j.chromik@utwente.nl) and Jair Santanna (j.j.santanna@utwente.nl)

[2] `https://www.us-cert.gov/ncas/alerts/TA14-098A`

[3] `https://www.shodan.io/search?query=vuln\%3ACVE-2014-0160&language=en`

[4] `https://ics-cert.us-cert.gov/`