Software Vulnerabilities: Exploitation and Mitigation
—
Lab 1

Alexandre Bartel

The report for the lab should consist of a single pdf file. Please use the following filename:

`lab1_${FIRSTNAME}_${LASTNAME}.pdf`

Send the report to alexandre.bartel@uni.lu with the following subject:

`MICS-SOFTVULN2019 Lab1 ${FIRSTNAME}_${LASTNAME}`

The deadline is the day before the next lecture at 23:59.

1 Lab1 (33 P.)

1.1 Software and Computers

Read this paper on the history of software to answer to the following questions.

Question 1.1 Before computer ”machines”, what was a computer? 2 P.

Question 1.2 Who was the first programmer? 2 P.

Question 1.3 4 P.

- What was the first programming language?
- Is it still used today? Why?

Question 1.4 What was the first use of the ENIAC? 2 P.

1.2 CIA

Recall that a software vulnerability can have an impact on the confidentiality, integrity and/or availability of a software system.

Question 1.5 Describe each of the following vulnerabilities (type of vulnerability, specific conditions to exploit the vulnerability) and explain if they can have an impact on the confidentiality, integrity and/or availability: 9 P.

1. CVE-2014-0160
2. CVE-2016-9079
3. CVE-2018-20343 [a]

[a] eip, is the instruction pointer register. If the attacker controls it, he can execute arbitrary code (to simplify we suppose there are no countermeasure in place)

1.3 Non-disclosure

Read this article and answer to the following questions.

Question 1.6 4 P.

1. Does this article describe someone or an organization using non-disclosure?
2. What is ”EternalBlue”?

The article above mentions this document. Go through it and answer to the following questions.

Question 1.7 Under which circumstances is a vulnerability not reported to the vendor? 3 P.

1.4 Where is the Flaw?

A few years back there have been famous attacks against WEP, a wireless encryption protocol. Read this paper and answer to the following questions.

Question 1.8 What kinds of WEP flaws does the paper mention? Are these design or implementation flaws? 4 P.

Question 1.9 Suppose we are 100 years into the future and we can finally write code without any implementation bug. Can an implementation of WEP be secure? Why or why not? 3 P.

Note on plagiarism

Plagiarism is the misrepresentation of the work of another as your own. It is a serious infraction. Instances of plagiarism or any other cheating will at the very least result in failure of this course. To avoid plagiarism, always properly cite your sources.