Mittuniversitetet
MID SWEDEN UNIVERSITY

Laboratory Assignment: Malicious Software

Daniel Bosk*

malware.tex 2169 2015-01-14 22:37:01Z danbos

Contents

1 Introduction

This laboratory work will cover the topic of malicious software, or malware. Malware comes in many different forms; viruses which infect other programs, worms which actively spread themselves through networks, logic bombs which does nothing until a given criteria is fulfilled.

To counter these we can use several approaches. One is antivirus software, which tries to detect all sorts of malware – not just viruses – despite the name. Another approach is to configure access control and other mechanisms to prevent running these programs, e.g. by never executing programs on USB-sticks, programs received by email, or programs downloaded from the Web, and so on.

2 Aim

After completion of this assignment you will:

- Be able to reason about the detection of malware.
- Have an understanding for how malicious software and antivirus softare work.

3 Theory

To be able to do this assignment you should first read chapters 5, 7, 10 in *Computer Security* [1]. Then you should read section 21.3 in *Security Engineering* [2]. Finally you should read Ken Thompson's classic paper "Reflections on trusting trust" [3].

4 Assignment

This section covers the work to be done and the next section covers how it will be examined, and what to be done to pass it.

The first part of this assignment consists of implementing Thompson's idea for including malicious code in the C compiler and then removing it from the source code. The C compiler should be modified so that it injects a printf-statement printing the line "May the Source be with you ...\n" in the beginning of all programs it compiles. This means that after the compiler itself is recompiled it will also be printing this line when compiling programs. It also means that once the compiler is compiled with this code, we can restore the original source code and the compiler will continue to do this despite recompiling it with its original source code.

This first part of the assignment will be solved together during a full-class hackathon in the computer lab. There will be a projector with the code for all to see, then we will rotate who will be by the keyboard writing what the rest of the class is saying. This way we will discuss together and write the code together, everyone will thus participate in the process.

The second part of the assignment is to dicsuss the consequences of this, among other things we will discuss the following two questions:

- How can we possibly detect if this attack has occured somewhere?
- What would happen if this attack was directed at e.g. an open source project?

5 Examination

To pass this assignment you must first actively participate in the hackathon lab session. If you cannot participate in the lab session you have to solve the lab yourself, then orally present your solution during one of the lab sessions after the course-end.

You must also actively contribute to the post-coding discussions. For those who cannot attend the hackathon there will be post-coding discussions during the lab sessions after the course-end.

References

[1] Dieter Gollmann. *Computer Security.* 3rd ed. Chichester, West Sussex, U.K.: Wiley, 2011. ISBN: 9780470741153 (pbk.)

[2] Ross J. Anderson. *Security Engineering. A guide to building dependable distributed systems*. 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: http://www.cl.cam.ac.uk/~rja14/book.html.

[3] Ken Thompson. "Reflections on trusting trust". In: *Communications of the ACM* 27.8 (1984), pp. 761–763. URL: http://dl.acm.org/citation.cfm?id=358210.