Obligatory exercise 1: Trusted path

Written by, Ole Eivind Parken, StudentID: 121086

September 1, 2014

1 Introduction

We have been given an assignment were we are going to explore different (non Microsoft Windows) operating system to find out how they manage trusted path (if they does). I have chosen Linux, because this is the operating system I am most familiar with. Again, I have almoste no knowledge about Linux security from before.

2 Trusted Path, what is that?

Trusted path is were the user can be absolutely sure that he is communication directly to the operating system, and no attackers can manipulate or stop the information communicated. Examples of this can be if the user initiate ctrl+alt+del in Windows systems(SAK).

3 SAK, Secure Attention Key

When SAK is initiated by a user all other user processes are suspended or shutdown, and only the trusted path remains running.

Since Linux kernel version 2.2 and later there have been included support for a Secure Attention Key. The pattern for initiating the SAK is different between systems. When the pattern is pressed, the SAK will kill a running X server, force exit programs that tries to connect to the current virtual terminal. [1]

As a user, you should allways invoke SAK before you login to a system or entering your login information in the terminal, to be sure that you have trusted path and there are no software listening.

To make SAK work, the kernel have to be compiled with sysrq support [2]

4 TPE, Trusted Path Execution

Trusted Path Execution is to grant user to run software outside of /bin and /usr/bin. If a user of the system is creating software that may cause damage to the system, and tries to execute this outside of these two directoryes, the TPE will check if either the user og the given path is configured as trustworthy, if not, the user will be given a -EACCESS error, else the program will run start. [3]

This feature is not implemented by default to Linux, but there exists a framework that is built into the kernel called "Linux Security Modules". Linux

Security Modules was designed to give specific needs of everything needed to implement a mandatory access control module. The most know is: AppArmor, SELinux, Smack and TOMOYO Linux

References

[1] B. Toxen, "Real World Linux Security: Intrusion Prevention, Detection, and Recovery," http://books.google.no/books?id=bv2n6o_6LaQC&pg=PA329&lpg=PA329&dq=linux%2Bsecure%2Battention+key&source=bl&ots=c1qXYGAoJD&sig=-WO1qNUdLYHzWDdZzTUA2cIGLWQ&hl=no&sa=X&ei=MysEVPK1FajmyQOws4DQDA&ved=0CFAQ6AEwBQ#v=onepage&q=linux%2Bsecure%2Battention%20key&f=false, 2003, [Online; accessed 01.09.2014].

[2] A. Morton, "Linux 2.4.2 secure attention key (sak) handling," https://www.kernel.org/doc/Documentation/SAK.txt, 2001, [Online; accessed 01.09.2014].

[3] N. A. Rahimi, "Trusted path execution for the linux 2.6 kernel as a linux security module," https://www.usenix.org/legacy/event/usenix04/tech/freenix/full_papers/rahimi/rahimi.pdf, 2004, [Online; accessed 01.09.2014].