IMT3501, software security, excercise #01

Jan Samuelsen Lindemann, 120926

September 3, 2014

Abstract

This article describes if and how trusted path is implemented in linux.

1 What is Trusted Path

Trusted path is a way to ensure that the user is interacting with what the user thinks he is interacting with, this is to ensure that no information communicated can be intercepted or modified[3]. A well known instance of trusted path is the ctrl-alt-delete at boot-up on Windows which gives you the login screen. Most modern smart-phones have trusted path implemented by pressing the home button.

2 Trusted Path in linux?

A feature like ctrl-alt-delete in windows does not exist in the same way in linux, this particular sequence of characters is usually used for restarting the machine, Linux did however implement a feature meant to combat login-spoofing around year 2000, Secure Attention Key.

2.1 Secure Attention Key

Secure Attention Key(SAK), is a mechanism implemented in Linux kernel 2.2 and later for restarting the x-server, which causes any processes that might claim to be a log-in prompt to restart with it.[2]

2.2 Trusted Path Execution

TPE checks if the parent directory of a file being executed is root, if this is the case the path is trusted. Also uses trusted user ACLs to determine if a file owned by a certain user in the ACL can be executed. If both of these checks fail, the execution of the file is denied.[1]

References

[1] Niki A. Rahimi, IBM, *Trusted Path Execution for the Linux 2.6 Kernel as a Linux Security Module*. 2004.
https://www.usenix.org/legacy/event/usenix04/tech/freenix/full_papers/rahimi/rahimi.pdf

[2] Andrew Morton, *Linux 2.4.2 Secure Attention Key (SAK) handling*. 2001.
https://www.kernel.org/doc/Documentation/SAK.txt

[3] Wikipedia, *Trusted path*. 2001.
http://en.wikipedia.org/wiki/Trusted_path