Name: Cezar Augusto Contini Bernardi

Student ID: 140139

Obligatory exercise 1

2014-08-31

Task: Choose an operating system, not Windows, and describe how does it implement the concept of trusted path execution (TPE)

1. Trusted Path Execution

> *“A trusted path is a mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base. This mechanism can only be activated by the person or the Trusted Computing Base and cannot be imitated by untrusted software.”* - The Orange Book (TCSEC), page 113. [1]

A few examples of this are the Windows Ctrl+Alt+Del and Smarthphones home button.

2. TPE in Linux Kernel

TPE is not implemented by default on the linux kernel [2], however, there is a framework called Linux Security Modules built into the kernel. Using it, is possible to load several modules like SELinux and AppArmor, as well as user coded modules.

These modules make use of a set of hooks into the kernel and use a sysfs pseudo-filesystem to interact between user space and system. The TPE implemented by Niki Rahimi [3] uses a hook to monitor the execution of files and performs a check on the path that the executable resides and the user executing it. With this information, it tries to define if this execution is trusted or not.

Regarding the path, to confirm that it is trusted or not, the parent folder is evaluated. In case it is owned by root and it is neither other user or group writable, then the path is trusted.

To evaluate the user trying to execute it, an ACL is created containing the trusted users that are authorized to run executables from any folder [3]. The root user has the power to include and exclude users from this ACL.

[1] Department of Defense Standard, Trusted Computer System Evaluation Criteria. Available at http://csrc.nist.gov/publications/history/dod85.pdf

[2] The Linux Documentation Project, Set Up a Trusted Path. Available at http://www.tldp.org/HOWTO/Secure-Programs-HOWTO/trusted-path.html

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