Obligatory Assignment #1: Trusted Path

Brage Celius - 120920
September 3, 2014

I. Trusted Path

Trusted Path is a mechanism that provides confidence that the user is communicating with what the user intended to communicate with. [2] It ensures that attackers can't intercept or modify whatever information is being communicated. An example of this is Ctrl+Alt+Del in Windows.

II. Linux and Trusted Path

The concept of Trusted Path is by default not implemented in stock Linux distributions. [2] However, two different realizations of this concept are available for implementation. These realizations are called "Secure Attention Key" and "Trusted Path Execution".

III. Secure Attention Key

The "Secure Attention Key"(SAK) seeks to protect the login sequence from trojan password capturing programs. This is achieved by immediately diverting and handling the login sequence as a special case in an alternate path. For that purpose, the SAK is hard coded into the kernel. Upon pressing the SAK combination, it is immediately detected by the kernel and redirected to a path that handles this special case, thereby creating a trusted path. [3] This way, no userspace application can trap the SAK combination or prevent the kernel from redirecting the sequence to an alternate path.

SAK implementation in Linux is approached in two ways. The first way is through a feature called "Magical System Request"(sysrq) [5] Sysrq defines a key combination that can be pressed to which the kernel will respond regardless of what it is doing. In order to use the sysrq feature, the kernel must be configured with support for sysrq.

The second way is to define a key combination at the end of the /etc/rc.sysinit file. The rc.sysinit file is run as part of the initialization process of the system, and is the last file to be executed before the login sequence starts. [8] Adding the following line enables and sets SAK to ctrl+alt+pause: [6]

```
echo "control alt keycode 101 = SAK" | /bin/loadkeys
```

By adding this line to the rc.sysinit file, the system initialization sequence will pause and prompt for the SAK combination key before initiating the login sequence.

IV. Trusted Path Execution

"Trusted Path Execution" (TPE) is a feature that seeks to prevent execution of malicious code by prematurely checking if the execution is deemed secure. This check is achieved by utilizing a kernel hook within the Linux Security Module. [7] Upon execution of a file, TPE checks the user and path to see if either is deemed "trusted". In the case that neither the user nor the path is deemed to be trusted, execution of the program is denied and an error -EACCESS will be returned. [7] If either the user or the path is evaluated to be trusted, the program is allowed to execute.

The evaluation of whether a path is secure is based on several conditions. For example if the file is root owned and neither group-writeable or world-writeable, the path is considered trusted. [7] For a user to be considered trusted, they must either be the root user or listed in an access control list. [7]

	Trusted User	**Untrusted User**
Trusted Path	**Execution Allowed**	**Execution Allowed**
Untrusted Path	**Execution Allowed**	**Execution Denied**

Figure 1. Trusted Path Execution Chart

References

[1] Wikipedia Article on Trusted Path
Available: https://en.wikipedia.org/wiki/Trusted_path

[2] Secure Programming for Linux and Unix HOWTO, Chapter 7.12
Author: David A. Wheeler, March 2003.
Available: http://www.tldp.org/HOWTO/Secure-Programs-HOWTO/trusted-path.html

[3] Lwd.net article on SAK.
Available: http://lwn.net/Articles/489186/

[4] Wikipedia article on grsecurity.
Available: https://en.wikipedia.org/wiki/Grsecurity

[5] Kernel documentaion on sysrq.
Available: https://www.kernel.org/doc/Documentation/sysrq.txt

[6] Kernel documentation on SAK.
Available: https://www.kernel.org/doc/Documentation/SAK.txt

[7] Usenix article on Trusted Path Execution.
Available: https://www.usenix.org/legacy/event/usenix04/tech/freenix/full_papers/rahi

[8] Glennastory.net article on Linux System Process Initialization.
Available: http://glennastory.net/boot/init.html