Obligatory assignment 1: trusted path

Author: Joachim Hansen
<joachim.hansen@hig.no>
Student number: 120483

Abstract

This article will cover a brief explanation of the concept of trusted path, give some reasons for why this concept is important in operating systems (OS), present examples for some OS that have trusted path and provide some insight on how this is implemented on Solaris OS.

What is a Trusted path?

"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" - Orange Book [1, page 113]

Figure 1: The Secure Attention Key (SAK) is the means for how we trap the kernel to invoke the trusted path.In a windows based OS, the SAK is a combination of these keystrokes ctrl + alt + delete on the keyboard. When the user is using the SAK he can be sure that he is communicating directly with the kernel, without any interference by malicious software.[2, Page 6-9], [3, page 1]

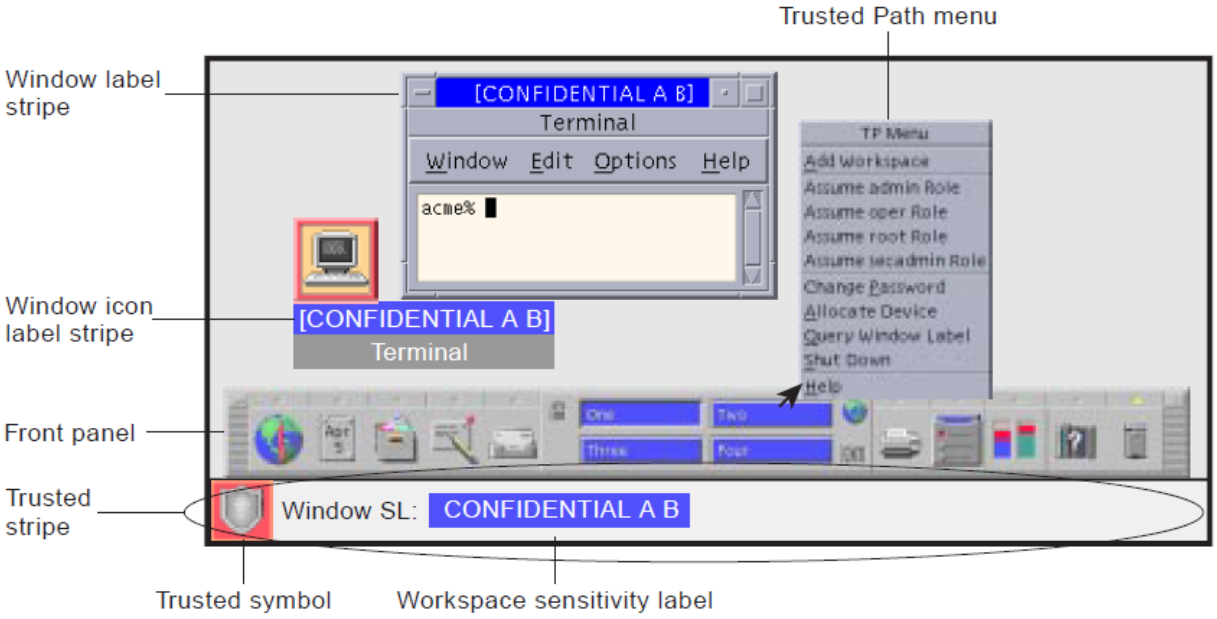
Trusted path in other Operating systems

Scomp Trusted Operating Program (STOP) and Solaris are examples of OS that have their own implementation of the trusted path, yet this is not true for

all OS; e.g. Linux is one of the major players in the OS market that currently have no support for the concept of trusted path. The reason behind this can perhaps partly be explained by a quote from Dennis Ritchie: "The first fact to face is that UNIX was not developed with security, in any realistic sense, in mind; this fact alone guarantees a vast number of holes."[4, page 40,46],[5, page 8], [2, page 14]

Trusted path in Solaris

Figure 2: illustration of Solaris trusted path menu and trusted stripe - **Source(s):** [6, page 22]



The SAK in Solaris OS differs from Windows based OS, in that it's not being initiated by a set of keystrokes. For the user to activate the SAK he must left click with the mouse on the screen stripe shown at the bottom in the above picture or by clicking the trusted label in a window. [2, page 20] [7]

When the users are directly communicating with the trusted computing base, then the trusted path symbol appears to the user. This can reassure the user that no malicious software is forging this screen, as it cannot be forged. [6, page 19] [8, page 22] [6, page 76]

The trusted path menu will be used in the authentication process of administrative roles, setting security labels and passwords. In short the trusted path is needed whenever there is an action that effect security.[7]

References

[1] (DECEMBER l985). Trusted computer system evaluation criteria (alias: orange book, [Online]. Available: http://csrc.nist.gov/publications/history/dod85.pdf.

[2] S. A. Bartram. (2000-06). Supporting a trusted path for the linux operating system, [Online]. Available: http://calhoun.nps.edu/bitstream/handle/10945/32937/00Jun_Bartram.pdf?sequence=1.

[3] H. Langweg. (1NOV 2004). Building a trusted path for applic ations using cots components, [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a448490.pdf.

[4] J. Morris. (2009). Linux kernel security overview, [Online]. Available: http://namei.org/presentations/linux-kernel-security-kca09.pdf.

[5] C. S. E. Canada. (2012). Certification report eal 4+ evaluation of bae systems stop os™ v7.3.1, [Online]. Available: https://www.commoncriteriaportal.org/files/epfiles/383-4-176%20CR%20v1.0e.pdf.

[6] I. Sun Microsystems. (2000). Trusted solaris user's guide, [Online]. Available: http://docs.oracle.com/cd/E19109-01/tsolaris8/805-8115-10/805-8115-10.pdf.

[7] I. Sun Microsystems. (2014). The trusted solaris™8 operating environment (short), [Online]. Available: http://www.oracle.com/technetwork/server-storage/solaris10/overview/ds-ts8-150124.pdf.

[8] ——, (2000). Trusted solaris™ 8 operating environment, [Online]. Available: https://info.aiaa.org/tac/isg/SOFTC/Public%20Documents/Technical%20Working%20Groups/Trusted%20Computing/Trusted%20Solaris.pdf.