Obligatorisk Oppgave: 1)
K. Borge
120919

Intro:
This assignment is about the concept behind trused path, and how the OS implements trusted path. I started out trying to look into Android. But I found out that Android is build up on mostly linux, so I figured out I should change it into Solaris instead. Solaris is a Unix operating system[3]. Solaris strongest points are that it scale really good, and have the ability to adapt [1]

Trusted Network:
Solaris has some exstentions that are focusing on security which is called “Trusted Extensions”[4], which can distinguish what kinds of hosts or network that shall be allowed to transmit their IP packets. What makes this special is that with the “Trusted Extentions” it will automaticly sent with the labels of the sender, because it’s required by the program. This makes it easy to see that all the packages are coming from a trusted host.

Trusted path:
The trusted path is showing whenever the the user want to change, cut or paste across label boundaries[1], because this require full authorization for the “Object label management”. It is possible through the Trusted path menu, to assign different kinds of roles. The roles are there to let the machine know who got access to what, like for example who is allowed to change the origin of files.

This is done by estabilishing a new workspace and log into secadmin role, which should as default be the only role available. After the authentification and the trusted path recognince the workspace, this workspace will be locked and set for this specific user.
To give out an example of how you can know that you are using “a trusted path” is by the secure attention key (SAK); which means that you click a special compination on your keyboard. One example of this is window’s “ctrl” + “alt” + “delete”.

Basiclly Trusted path is a menu where whatever you do, you know it is fully trusted. By this I mean, there is no change of any trojans having any controll of these functions. One example is that you can access devices, and different kinds of devices need different kinds of autentification. From what I understood, by which role you have, you can get access to devices that are plugged physically into the computer. If you don’t have that access you won’t be able to select the device from the menu.

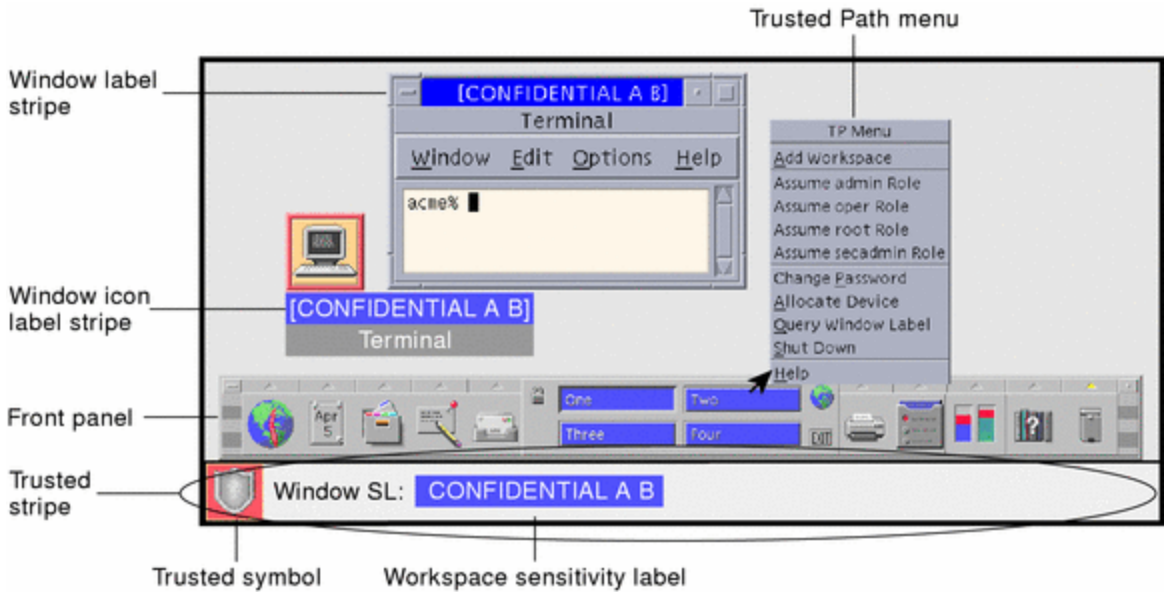

figure 1 [2]: *This is the basic setup for the trusted path on Solaris. In the menu you can see what I mentioned earlier bout the admin roles and the choice for accessing devices.*
You can clearly see the labels which cannot be constructed by any kind of virus and malware.

The way you actually get into the trused path is to use the menu. Whenever you click the menu you will get into the trusted path environment, and you'll automaticly see the trusted path stripe and icon. This will work as a SAK, where you actually have to click with the computer mouse to get into the trusted path.

If by any means the trusted stripe isn't visable, there might be a problem with the system. [2] This should allways be visale when handling a security action. Even if the shild-icon, the trusted symbol is gone, there might be a problem. This is one of the main visabilities implemented to help the user to see that he really is using the trusted path.

If you would like to change the clock or change some of the files you really need to be an administratior.

Resources:
[1]http://books.google.no/books?id=yXD0O_6f8QUC&pg=PT397&lpg=PT397&dq=trusted+path+solaris&source=bl&ots=vQlbCtPDQ_&sig=vWWlAD_RAwU9QQcdTQZs09b6jbw&hl=no&sa=X&ei=pMMEVIbYH5HmaliagdgJ&ved=0CEYQ6AEwBA#v=onepage&q=trusted%20path%20solaris&f=false

[2]http://docs.oracle.com/cd/E19109-01/tsolaris8/805-8115-10/6j7klujc1/index.html

[3]http://no.wikipedia.org/wiki/Solaris_(operativsystem)

[4]http://en.wikipedia.org/wiki/Solaris_Trusted_Extensions

[5] https://www.mail-archive.com/security-discuss@mail.opensolaris.org/msg02294.html