Linux Secure Attention Key (SAK) handling

Date: 18 March 2001
Author: Andrew Morton

An operating system's Secure Attention Key is a security tool which is provided as protection against trojan password capturing programs. It is an undefeatable way of killing all programs which could be masquerading as login applications. Users need to be taught to enter this key sequence before they log in to the system.

From the PC keyboard, Linux has two similar but different ways of providing SAK. One is the ALT-SYSRQ-K sequence. You shouldn't use this sequence. It is only available if the kernel was compiled with sysrq support.

The proper way of generating a SAK is to define the key sequence using `loadkeys`. This will work whether or not sysrq support is compiled into the kernel.

SAK works correctly when the keyboard is in raw mode. This means that once defined, SAK will kill a running X server. If the system is in run level 5, the X server will restart. This is what you want to happen.

What key sequence should you use? Well, CTRL-ALT-DEL is used to reboot the machine. CTRL-ALT-BACKSPACE is magical to the X server. We'll choose CTRL-ALT-PAUSE.

In your rc.sysinit (or rc.local) file, add the command:

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

And that's it! Only the superuser may reprogram the SAK key.

Note

1. Linux SAK is said to be not a "true SAK" as is required by systems which implement C2 level security. This author does not know why.
2. On the PC keyboard, SAK kills all applications which have /dev/console opened.

   Unfortunately this includes a number of things which you don't actually want killed. This is because these applications are incorrectly holding /dev/console open. Be sure to complain to your Linux distributor about this!

   You can identify processes which will be killed by SAK with the command:

   ```
   # ls -l /proc/[0-9]*/fd/* | grep console
   l-wx------    1 root     root           64 Mar 18 00:46 /proc/579/fd/0 -> /dev/console
   ```

   Then:

   ```
   # ps aux|grep 579
   root       579  0.0  0.1  1088  436 ?        S    00:43   0:00 gpm -t ps/2
   ```

   So `gpm` will be killed by SAK. This is a bug in gpm. It should be closing standard input. You can work around this by finding the initscript which launches gpm and changing it thusly:

   Old:

   ```
   daemon gpm
   ```

   New:

   ```
   daemon gpm < /dev/null
   ```

   Vixie cron also seems to have this problem, and needs the same treatment.

   Also, one prominent Linux distribution has the following three lines in its rc.sysinit and rc scripts:

   ```
   exec 3<&0
   exec 4>&1
   exec 5>&2
   ```

   These commands cause **all** daemons which are launched by the initscripts to have file descriptors 3, 4 and 5 attached to /dev/console. So SAK kills them all. A workaround is to simply delete these lines, but this may cause system management applications to malfunction - test everything well.