X server privileges on Solaris

Alan Coopersmith
Solaris X11 Engineering Team
X servers in Solaris

- Which ones are included?

- Solaris 2.3 through 10 included Xsun
  - Forked from X Consortium sources, upgraded through Solaris releases to final version based on X11R6.6
  - Solaris 7 through 10 also include Xprt using these sources
  - Solaris 9 & 10 also include Xvfb & Xnest using these sources

- Solaris 10 and later include servers built from X.Org releases
  - Upstream + patches, not forked like Xsun was
  - Solaris 10 uses xorg-server 1.3
  - Solaris 11 uses xorg-server 1.10
  - Includes Xorg, Xephyr, Xvfb, and Xvnc
# X servers in Solaris

*Which set-id bits are set?*

<table>
<thead>
<tr>
<th>X server</th>
<th>Set-id bits</th>
</tr>
</thead>
</table>
| Xsun                           | SPARC: setgid root  
x86/x64: setuid root                      |
| Xnest & Xvfb based on Xsun     | none                                             |
| Xorg                           | setuid root                                      |
| Xephyr & Xvfb based on Xorg    | none                                             |
| Xvnc                           | setgid root                                      |
X server privileges

- Why were these set-id bits used?
- setgid root
  - Was used to protect access to creating transport endpoints in `/tmp/.X11-pipe/` and `/tmp/.X11-unix/` in the past – have now moved to use of sticky bit like other platforms.
  - Solaris kernel allows processes with gid 0 to control power management and give priority boosts to processes in the IA scheduling class.
  - This is all Xsun needed on SPARC, since kernel frame buffer drivers handled all privileged device access – no general bus access was needed.
X server privileges

- Why were these set-id bits used?

- setuid root
  - x86/x64 requires for direct PCI register access via /dev/xsvc mapping and SYS_IOPL setting
  - Xorg (both platforms) requires for write access to /var/log to move /var/log/Xorg.<display>.log to .old and create new log file
  - Some SPARC drivers ported from Xorg still rely on kernel drivers for device access (ast, radeon), others now also use libpciaccess to minimize porting differences (mga)
Dropping privileges

- *Currently Solaris-added patches*

- On startup, Xorg creates a named pipe in `/var/dt/sdtlogin/` (directory only readable & writable by root).
- When it receives the X server ready signal, gdm opens the pipe for writing.
- When gdm is finished authenticating the user, it writes key=value pairs to the pipe for uid, gid, home directory, projects.
- When Xorg receives data on the pipe, it sets uid, gid, etc. to the values from the pipe, and chdir’s to the given home directory.
- Sets both uid & euid, gid & egid, but keeps saved id values so it can return to root when needed at VT switch & server regeneration.
Input device access as non-root user

- Currently Solaris-specific

- `/etc/logindevperm` is a list of files that is chown’ed to the user who logs into `/dev/console` (since approx. Solaris 2.0) or `/dev/vt/console_user` device (Solaris 11 & later only)
  - `/dev/vt/console_user` is a kernel maintained symlink to the currently displayed VT
  - Handled in login program currently – gdm or `/bin/login`.

- When devices are hotplugged, they are also checked against the logindevperm device list and chown’ed accordingly.
  - List includes most USB devices, including all HID types.
VT switching handling of privileges

- Currently Solaris-specific

- When Xorg receives user login information from gdm in Solaris 11, it also now informs the kernel of the user via a new ioctl on the VT device, `VT_SETDISPLOGIN`.

- Other user space programs, such as vtdaemon or hald can query this to get the uid of the user currently owning a given VT, including `/dev/vt/console_user` for the currently active one.

- Allows passing ownership of devices from current X server to the one being activated on VT switch.

- Currently Solaris-specific
Appendix

Links to sources, patches, & docs
Dropping privileges

- **Currently Solaris-added patches**

- **Original specification (from 1995, for CDE’s dtlogin & Xsun):**
  - [https://java.net/downloads/solaris-x11/docs/Login.Xserver.Pipe.txt](https://java.net/downloads/solaris-x11/docs/Login.Xserver.Pipe.txt)

- **Xorg server new source file:**
  - [https://hg.java.net/hg/solaris-x11~x-s11-update-clone/file/tip/open-src/xserver/xorg/sun-src/os/dtlogin.c](https://hg.java.net/hg/solaris-x11~x-s11-update-clone/file/tip/open-src/xserver/xorg/sun-src/os/dtlogin.c)

- **Xorg server patch:**
  - [https://hg.java.net/hg/solaris-x11~x-s11-update-clone/file/tip/open-src/xserver/xorg/dtlogin-userinfo.patch](https://hg.java.net/hg/solaris-x11~x-s11-update-clone/file/tip/open-src/xserver/xorg/dtlogin-userinfo.patch)

- **gdm patch:**
  - [https://hg.java.net/hg/solaris-desktop~spec-files/file/2c32b1660d58/patches/gdm-03-sdtlogin.diff](https://hg.java.net/hg/solaris-desktop~spec-files/file/2c32b1660d58/patches/gdm-03-sdtlogin.diff)

*Updated Sept. 2013 to change URL’s from decommissioned opensolaris.org to new java.net site*
Input device access as non-root user

- *Currently Solaris-added patches*

- logindevperm(4) man page:

- gdm patch:

*Updated Sept. 2013 to change URL’s from decommissioned opensolaris.org to new java.net site*
VT switching handling of privileges

- Currently Solaris-added patches

- Original specification (from OpenSolaris vconsole project):
  - https://java.net/projects/solaris-x11/downloads/directory/docs/vconsole

- Xorg server new source file:
  - https://hg.java.net/hg/solaris-x11~x-s11-update-clone/file/tip/open-src/xserver/xorg/sun-src/os/dtlogin.c

- Xorg server patch:
  - https://hg.java.net/hg/solaris-x11~x-s11-update-clone/file/tip/open-src/xserver/xorg/vt.patch

Updated Sept. 2013 to change URL’s from decommissioned opensolaris.org to new java.net site