Security Improvements Needed in Debian

Russell Coker <russell@coker.com.au>
Internet and Security Consulting

- Could one person at the front please monitor the conference IRC channel and forward comments/questions to me as appropriate

Resources:

- #selinux on irc.freenode.net
- http://etbe.blogspot.com/ My Blog
- http://www.nsa.gov/selinux/ Official SE Linux web site
- http://www.coker.com.au/selinux/ My SE Linux web pages

Capabilities

- Need more capabilities in the Linux kernel code

- SYS_ADMIN and NET_ADMIN allow many accesses, any process that needs one of the actione permitted by one of those capabilities gets all the access

- Not specific to Debian

PolyInstantiated Directories

- Programs create predictable file names in public directories such as /tmp (through bugs and through mis-use)
- Users act predictably
- Programs perform unknown/unexpected operations on behalf of users (EG editors creating files under /tmp or /var/tmp)
- For strong separation of users we need a different instance of /tmp and /var/tmp for each user

Specific Attack Scenarios for PI-D

- Attack by user on user
- Attack by user on daemon
- Attack by non-root daemon on user
- Attack by root daemon on user (can only be prevented with SE Linux)

Previous attempts at restricting /tmp usage

- Restrictions on creating links - OpenWall

- Hiding file names, only works for the case where file names are secret, not for boolea file names

Linux implementation

- New systemcall unshare() to create private name-space for filesystems (among other things) - can be called from PAM module to work with unmodified programs

- Directory such as /tmp/.inst/tmp.inst-rjc-rjc is created and bind mounted to /tmp

- /proc/self/mounts shows the filesystems mounted for a process, /proc/mounts links to /proc/self/mounts

- PAM setting

session required pam_namespace.so

- Option unmnt_remnt for su and comparable programs (probably suexec, maybe MTA local delivery)

Shared-subtrees

- Allow autofs and sys-admin mount commands to work

```
mount --make-shared /
mount --bind /tmp /tmp
mount --make-private /tmp
```

- Only works on mount points, bind mount of /tmp needed for /tmp in root FS
- If PI directories are not excluded from the shared name space then things go horribly wrong
- Need start-stop-daemon to have PI support for non-root daemons
- Need wrapper for root daemons to prevent attacking users on SE systems, also protects the daemon in question from being attacked on a non-SE system
- Need PAM support for user login and cron jobs

How well the problem is solved in Fedora

- Non-root daemons started via runuser will have PI
- User processes from regular login and cron jobs have PI
- Support for excluding some users from PI, to prevent them from attacking PI users an daemons all directories are under /tmp/.inst which is a mode 000 directory
- Adds significant integrity and confidentiality benefits both with and without SE Linux
- On SE Linux systems there is an option of instantiating based on context, UID, or both

Exec-Shield

- Prevents application from executing code on their stack or mapping a memory region with write and exec access

- On a SE Linux system there are extra access controls on it, otherwise it just uses flag in shared objects to control it’s operation

- Default functionality in Fedora and RHEL for years, doesn’t cause problems for them..

ioctl(fd,TIOCSTI,&c)

- Allows pushing characters to the controlling tty
- If hostile user tricks sysadmin into su’ing to their account then they can own the sysadmin shell
- Fedora has "su -c" protected against this via setsid() - we need the same
- Need to have start-stop-daemon call setsid()
- Daemons should never be started with su unless it’s a modified code path that calls setsid()
- NB "ssh user@localhost" is better than "su - user", but "exec su - user" can do the job

Xen support in installer

- For a server install I want everything in a domU for better debugging options in the case of suspected penetration
- Ideally an install option would include a minimal install of the base system with Xen and a server install in domU in the same operation

SE Linux

- Base support is in Etch
- Want to have it in the default install in Etch+1 (as done in Fedora)
- Am considering creating my own netinst ISO for Etch to include SE Linux by default
- Want to have developers using it (among other things it results in the discovery of more security bugs)

Q/A

- #selinux on irc.freenode.net
- http://etbe.blogspot.com/ My Blog
- http://www.nsa.gov/selinux/ Official SE Linux web site
- http://www.coker.com.au/selinux/ My SE Linux web pages

Russell Coker <russell@coker.com.au>
Internet and Security Consulting