



Production Environment Issues

27th Linux User Meeting
2004-01-21
Knut Woller

- **Kernel Updates and Update Policy**
- **New application software deployment scheme**
- **A few words on acron**
- **Notebook Acquisition Statistics**



Recent Kernel Bugs and Updates

- **December 2003: do_brk**
- **local root exploit, exploit code available**
- **three attack vectors, could not be intercepted by module (a la ptrace)**
- **patch ist a trivial two line bounds check**
- **needed to update all kernels**
- **decided to roll out 2.4.22 to all systems, starting December 09, 2003**
- **more info on**

http://www-it.desy.de/systems/linux/desy-4/do_brk_fix.html

Recent kernel bugs and updates

- **January 2004: do_mremap**
- **very similar to do_brk**
- **local root exploit, exploit code available**
- **two attack vectors**
- **patch is trivial two line bounds check**
- **needed to update all kernels**
- **decided to roll out 2.4.24 starting January 14, 2004**
- **more info on**

http://www-it.desy.de/systems/linux/desy-4/do_mremap_fix.html



Status of Kernel Updates

- **900 DESY Linux 4 hosts have received the 2.4.24 RPM in the last days**
- **200 have already installed it**
- **Two servers had problems related to their network interface numbering and did not come back up by themselves**
- **Desktop updates seem uncritical so far, but there are some “exotic” configurations out there which may fail (e.g. dual processors with software mirrored SCSI disks)**

If your system receives cron updates, it is waiting for a reboot now to fix a gaping local root exploit

- **In case of problems, contact linux@desy.de**

Kernel Update Policy (DL4 & DL5)

We basically have two choices:

Stable Kernels:

- Stick with one version
- Apply patches if needed
- Do not break compatibility

Unstable Kernels:

- Roll out new versions
- Update instead of patching
- Update 3rd party kernel modules

Pros:

- Stable environment for VMware and similar

Pros:

- no backporting of patches
- benefit from new features
- better support for new hardware
- less lifetime issues



Kernel Update Policy

- **Our Proposal (and so we did it):**
 - **We will use new kernels every once in a while and provide automated kernel updates to all systems to keep them in sync**
 - **We will not roll out new kernels just because they are there, but ...**
 - **change versions if new hard- or software require it or if we need the new features**
 - **provide patches only for the latest production kernel**
 - **We will provide timely security updates for production systems**
 - **We will try to support you with kernel modules for standard applications (e.g. VMware)**
 - **Kernel updates require a reboot. No fixed policy yet, different scenarios are possible**



New application deployment scheme

- As presented here before, we are changing the software distribution scheme from “AFS centric” to “locally installed”
- DESY add-ons now come as RPM
- DL5 will be fully RPM based
- For DL4, the packages maintained in the new scheme (e.g. pine, perl, ...) are also provided in AFS
- This requires a compatibility symlink
`/opt/products -> /afs/desy.de/@sys/products`
- This symlink has been created on all DL4 systems which receive updates in early January and should be fully transparent to the user
- If your PC did not get it, you may be missing software updates.
- In case of problems, contact linux@desy.de

A few words on the acron service

- **acron is a cron-like scheduler with token renewal support for running jobs on AFS directories and remote execution**
- **the software has been written at CERN and is about ten years old now**
- **we have roughly 70 active acron users at DESY (including myself), plus a number who would use it – if it worked**
- **most of us have been frustrated recently because acron did not work as expected or not at all**



How should acron work?

- While holding a valid Kerberos TGT, you create an acrontab file using the “acrontab” command
- A valid entry looks like

```
56 * * * * pal02.desy.de /usr/local/bin/klis;usr/afsws/bin/tokens
```
- This creates a cron job on the acron server, which folds your TGT with a dummy token for later execution
- At execution time, an AFS token is generated and you job is executed on the target host using ARC



Why did acron stop working?

- **Because ARC is broken. The reason is not quite clear. It probably never worked right on Linux**
- **This became very obvious when puls and x4u2 went out of service and all users migrated to pal**
- **Several factors contribute to the malfunction of acron:**
 - **the (mis-) implementation of process accounting groups in the Linux kernel**
 - **history of user and root logins**
 - **time of creation of your acron job**
 - **spurious YP failures**



What do we do about it?

- **Christian Hüttig is working on an acron successor: k5cron**
- **Software is currently in alpha test and running quite reliably**
- **k5cron server is still a test system and needs to migrate before we go beta**
- **users who do not mind creating their jobs over again after server migration can test now (send a message to unix@desy.de)**
- **description and technical note will follow very shortly**



Notebook Acquisition Statistics

- **76 Notebook orders passed the computing committee in 2003**
- **70 of them went to DELL, 31 of those were DELL Latitude D600**
- **3 Apple Powerbook, 2 ASUS, 1 SONY**
- **We made a standard recommendation in favour of the DELL D series in May 2003**
- **Since then, more than 50% of the new notebooks are DELL Latitude D600**
- **We will focus on the D600 as the first DESY Linux Notebook**