Quattor and CERN's computer centre security

Luis Fernando Muñoz Mejías

11th Quattor Workshop

Disclaimer

- I don't work for CERN anymore
  - I cannot engage CERN into any actions
  - ... but I'm leaking a good bunch of configs for you ;)
- What I present here is the work of many other people
  - Manuel Guijarro
  - Jan Iven
  - Stefan Lüders
  - Gavin McCance
  - Remi Mollon
  - Ricardo Salgueiro
  - Steve Traylen
  - Jan van Eldik
  - Romain Wartel
  - ... and me
- I accept job offers ;)

Disclaimer

- I don't work for CERN anymore
  - I cannot engage CERN into any actions
  - ... but I'm leaking a good bunch of configs for you ;)
- What I present here is the work of many other people
  - Manuel Guijarro
  - Jan Iven
  - Stefan Lüders
  - Gavin McCance
  - Remi Mollon
  - Ricardo Salgueiro
  - Steve Traylen
  - Jan van Eldik
  - Romain Wartel
  - ... and me
- I accept job offers ;)

Disclaimer

- I don't work for CERN anymore
  - I cannot engage CERN into any actions
  - ... but I'm leaking a good bunch of configs for you ;)
- What I present here is the work of many other people
  - Manuel Guijarro
  - Jan Iven
  - Stefan Lüders
  - Gavin McCance
  - Remi Mollon
  - Ricardo Salgueiro
  - Steve Traylen
  - Jan van Eldik
  - Romain Wartel
  - ... and me
- I accept job offers ;)

Disclaimer

- I don't work for CERN anymore
  - I cannot engage CERN into any actions
  - ... but I'm leaking a good bunch of configs for you ;)
- What I present here is the work of many other people
  - Manuel Guijarro
  - Jan Iven
  - Stefan Lüders
  - Gavin McCance
  - Remi Mollon
  - Ricardo Salgueiro
  - Steve Traylen
  - Jan van Eldik
  - Romain Wartel
  - ... and me
- I accept job offers ;)

Disclaimer

- I don't work for CERN anymore
    - I cannot engage CERN into any actions
    - ... but I'm leaking a good bunch of configs for you ;)
- What I present here is the work of many other people
    - Manuel Guijarro
    - Jan Iven
    - Stefan Lüders
    - Gavin McCance
    - Remi Mollon
    - Ricardo Salgueiro
    - Steve Traylen
    - Jan van Eldik
    - Romain Wartel
    - ... and me
- I accept job offers ;)

Security with no collaboration

Outline

1. Introduction
   - Overview of the security at CERN's computer centre
   - Security baselines for servers
2. Consistently managing security
   - Software updates
   - Account management
   - Access management
   - Keeping traces
3. Monitoring
   - Security-related sensors and metrics
4. Conclusion

Some (known) CERN figures

- A handful of computer centres
  - At least one of them has general connectivity to the Internet
- 50K network devices (and growing fast)
  - Office desktops
  - Printers
  - SCADA systems
  - Usually in a private network
  - Calculation nodes
  - Mobile phones
- 2K network switches (and growing)

The challenge

- 25K users allowed to run arbitrary, unreviewed, uncertified code in 10K state-of-the-art machines
  - $\sim 80K$ CPUs available for abuse
  - $\sim 200PB$ storage available for abuse
- CERN computer security team has only 8 people
  - Two of them are students
  - One of them is not a CERN employee
- ... and yet the organisation works. :)

Too complex environment

- The computer security team can't enforce any concrete security feature
  - SELinux? AppArmor? Tomoyo?
  - McAfee? Norton? ClamAV? Microsoft?
  - Windows? Linux? Mac? Android? BSD?
  - Block module loading after boot?
- Normal users need simple, understandable guide
  - No resources to guide every possible choice
- Smart users are not that smart ;)

Can't handle all this alone!

Helping users (or asking users for help)

- The computer security team provides a set of high-level, portable requirements

  > *Minimize the usage of local accounts. (Local accounts often become neglected and/or have outdated and/or obvious weak passwords.)*

- Service managers have to return an implementation document with the specifics for each requirement.
  - Or they have to justify why it should be derogated in their case
- Some requirements were already implemented, even before the baselines formalised them

What comes next

- How Quattor helps in implementing these baselines
- Plus some geeky stuff ;)

What comes next

- How Quattor helps in implementing these baselines
- Plus some geeky stuff ;)

Applying software updates

- General use case was well discussed at RAL
- CERN can't upgrade the whole site (nor even a whole stage) at once
  - Experiments are extremely conservative when it comes to changes
- IT generates snapshots with default versions every week
  - Users choose their best snapshot
- The security team mandates updates in case of major security problem
  - And then, Lemon is used to detect systems that don't comply

Managing 250,000,000 accounts

- Users have a personal account, and maybe several service accounts
  - Same account for logging into Linux, Windows services, web services, mail...
  - Impossible to have local accounts in every possible service/box
- Access to services has to be restricted to the correct groups of people
  - Listing the correct users one by one is a nightmare
    - ncm-useraccess ACLs
  - UNIX groups are not the right thing to use

LDAP-based authentication

- LDAP server in Microsoft's Active Directory
  - But I bet most features are available in any other LDAP implementation

  e-group: logical name assigned to a set of accounts
  - Recursive
  - Simpler to maintain than Pan nlists. ;)
- LDAP authentication nicely integrated in SL5 and SL6
- ncm-authconfig does all the work

ZUUL

- Quattor templates configuring LDAP authentication
    - Link given at the end of the talk, just adapt it to your needs
- CERN constants hardcoded
    - But it's a good example

TODO

- What about services that don't support LDAP?
  - .k5login?
- Pending the ability to generate Pan variables from LDAP contents

Access to users accounts

- Usually with their Kerberos ticket
  - PAM context
- SSH public keys discouraged
  - When stolen in off-CERN incidents, attacker compromises CERN account
  - Difficult to check if a compromised key is banned in all machines
- No local passwords

Access to privileged accounts

Who can access to them

- Without password
  - No need to change the password if someone leaves the group

```
"/.../ssh/daemon/options/PermitRootLogin"=
    "without-password";
```

- List of tickets allowed to log into the account in `$HOME/.k5login`
  - ncm-useraccess

```
    ‘‘/software/components/useraccess’’ =
        = allow_root_access(‘‘homer’’);
```

  - Need a way to derive this from LDAP

Access to privileged accounts

Restricting their scope

- They can't SSH out
    - All SSH servers configured with

      ```
      ‘‘/.../ssh/daemon/options/DenyUsers" =
          ’root@*’;
      ```

    - Need to restrict even more accounts
        - oracle
        - apache
- Pending: restrict the origin of connections to privileged accounts
    - pam_access.so?
    - may ncm-pam help?

Multifactor authentication

- In progress
- I hope the templates will be published, when ready :)

Extra logging

- In especially sensitive machines, we log all commands and arguments executed
- Transparent wrapper around `execve` (snoopy)

```
'/software/packages' = pkg_repl('snoopy');
```

- Plus, we monitor it is enabled in /etc/ld.so.preload
- Commands are sent to the central syslog

```
Mar 11 19:00:01 narusegawa snoopy[32116]: [uid:0
sid:31408 tty:/dev/pts/7 cwd:/
filename:/usr/bin/tail]: tail /var/log/secure
```

SELinux sensor

- SELinux must be in "enforcing" mode in all SLC5 systems
- See links at the end of the talk

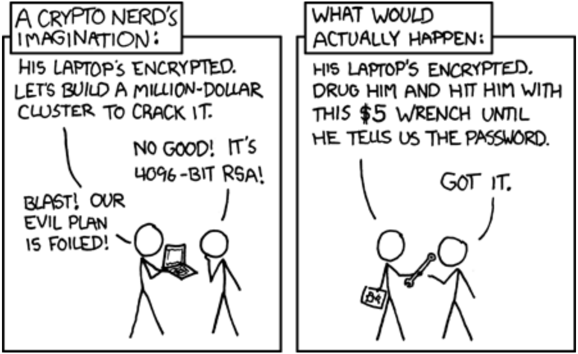
Security-sensitive files

- Some files need very tight permissions
  - /etc/shadow
  - /etc/ssh/sshd_config
- We actively monitor 12 files
  - Users are welcomed to suggest more, or to monitor more on their clusters
- See links

Wrap-up

- A large computer facility must be consistent
    - Quattor is a big help in this
- We can apply many security-related changes without disturbing service managers
- Service managers have good tools to control access to their services
- Much more than 8 people contribute to the security of CERN's computer centre
- CERN needs a way to configure LDAP-unaware services with LDAP contents

We have to protect it all


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

More information

- Security baselines for servers
- ZUUL Twiki
- Snoopy configuration
- SELinux monitoring template
- Monitoring of file permissions
- The problem of managing 236 million user accounts