Introduction, bilan 2005

Journées Informatiques

Valpré septembre 2006

Le thème Sécurité aux Journées Informatiques

- http://ji.in2p3.fr

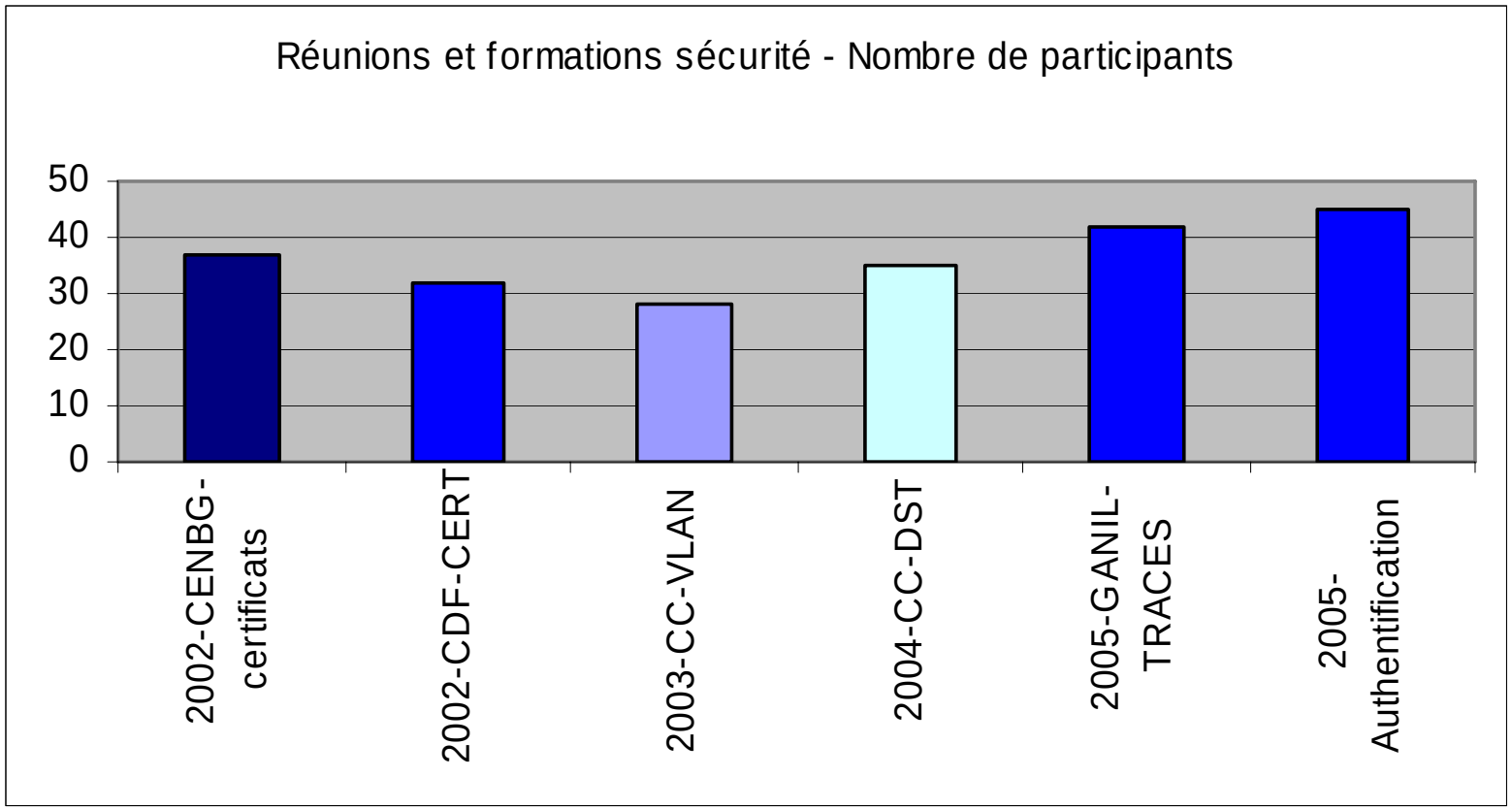
Bilan de l’année 2005

- Groupe sécurité IN2P3
- Infrastructure des réseaux des laboratoires
- Filtrage en entrée
- Surveillance réseau et détection d’intrusion
- Evolution de la menace et incidents
- Conclusion

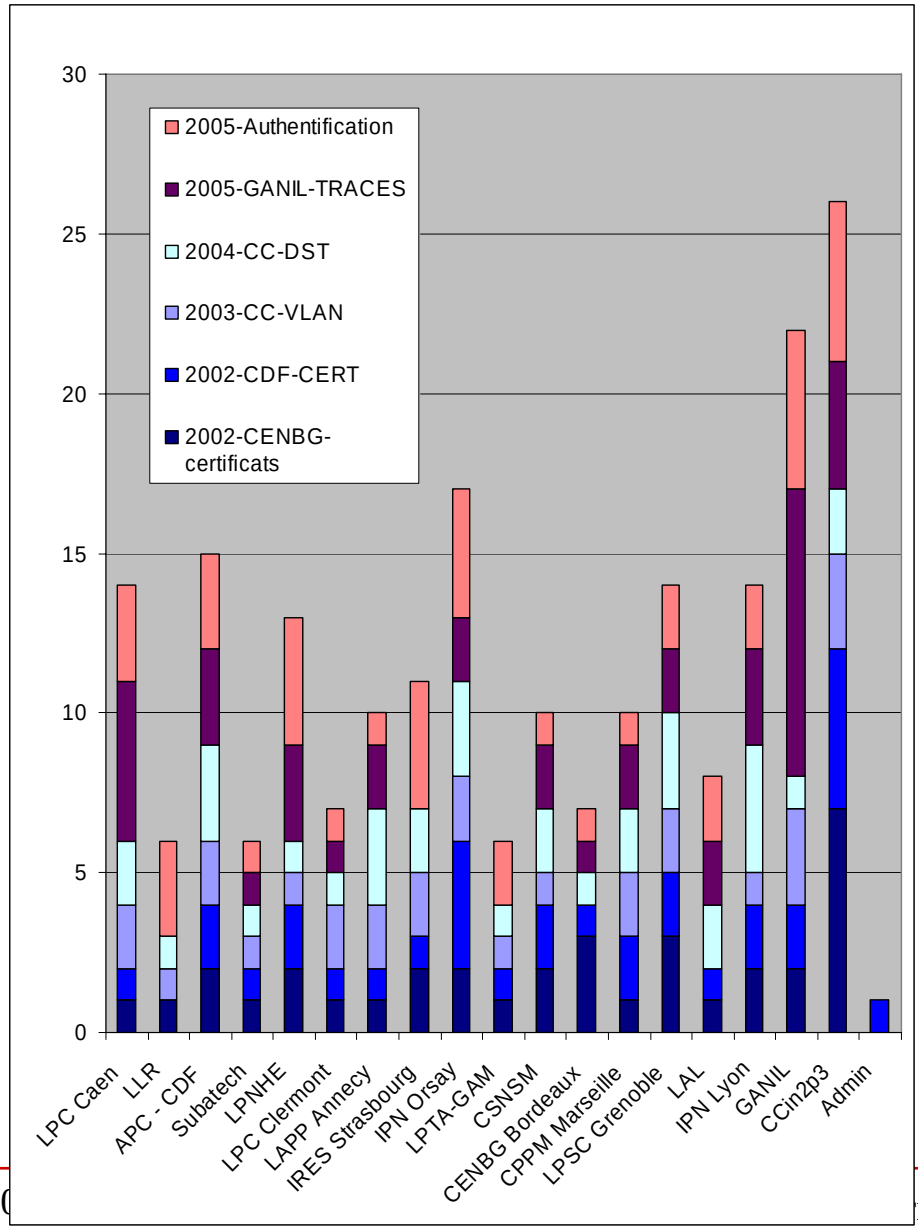
Le groupe sécurité

- 70 personnes
- Existence antérieure à 10 ans
- Liste SECURITE-L@in2p3.fr
- Quelques participations, contributions SIARS

Participation aux JS

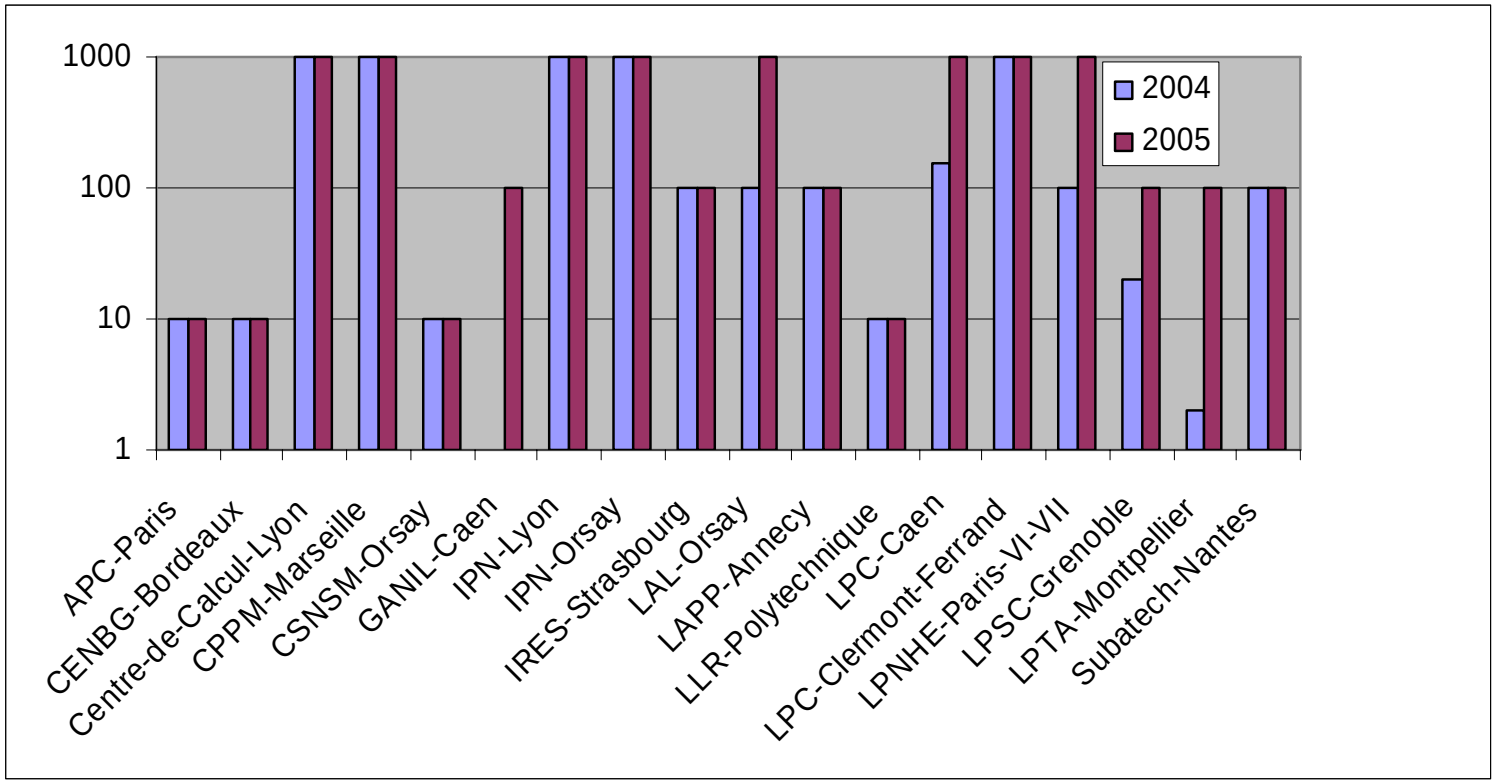


Répartition par laboratoire



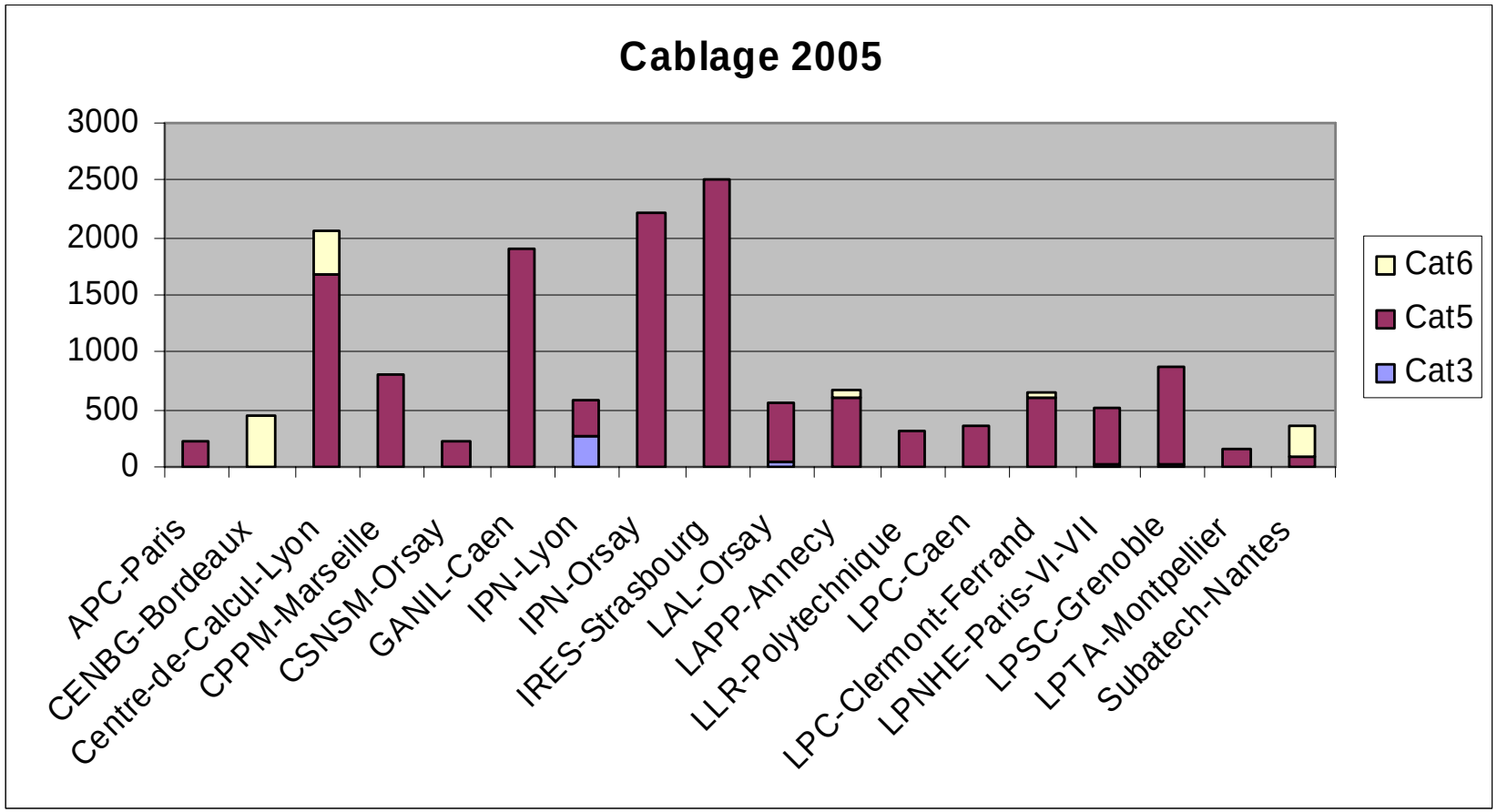
Infrastructure des réseaux de laboratoire 1/6

- Renater



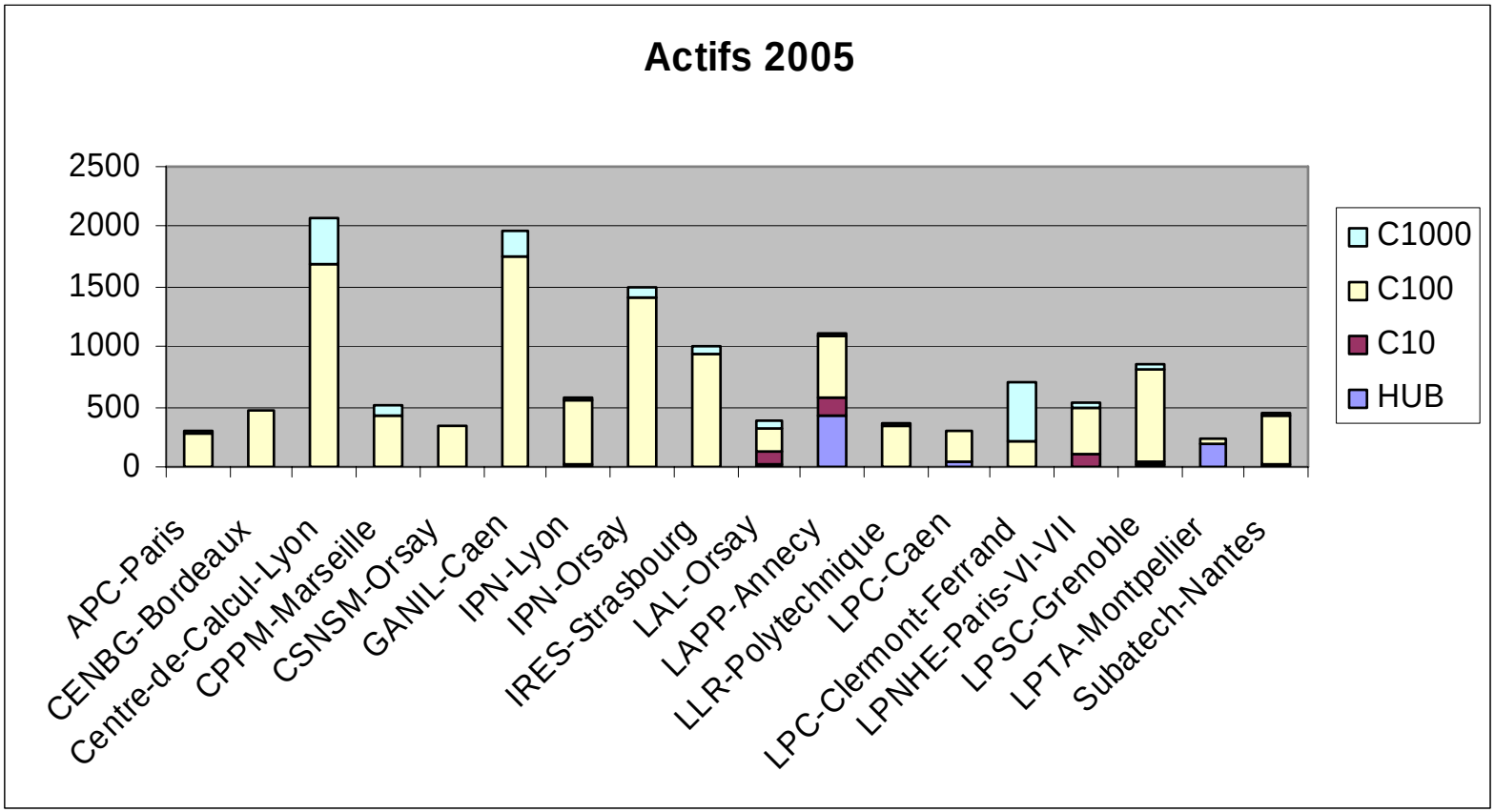
Infrastructure des réseaux de laboratoire 2/6

- Câblage



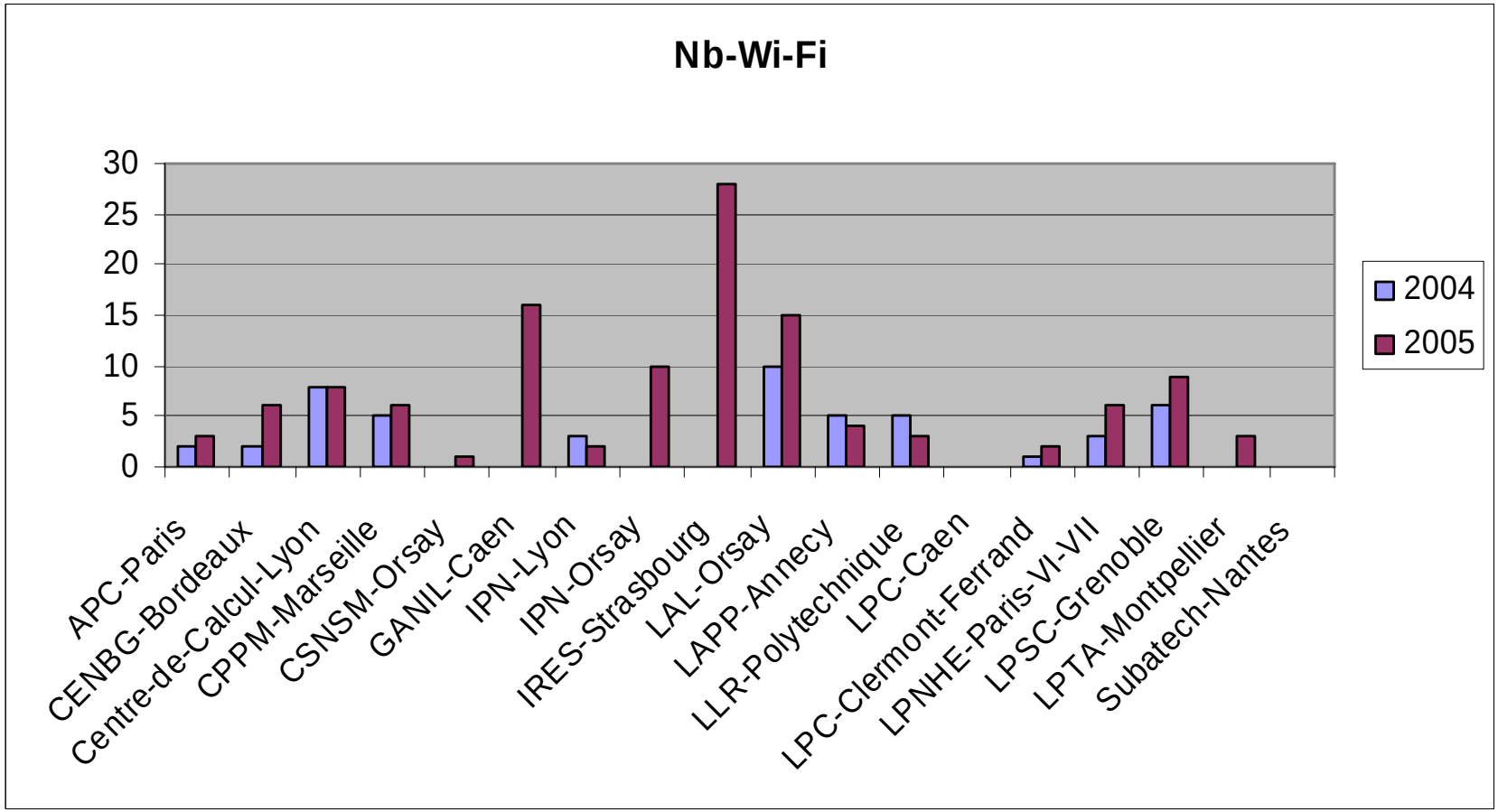
Infrastructure des réseaux de laboratoire 3/6

- Eléments actifs



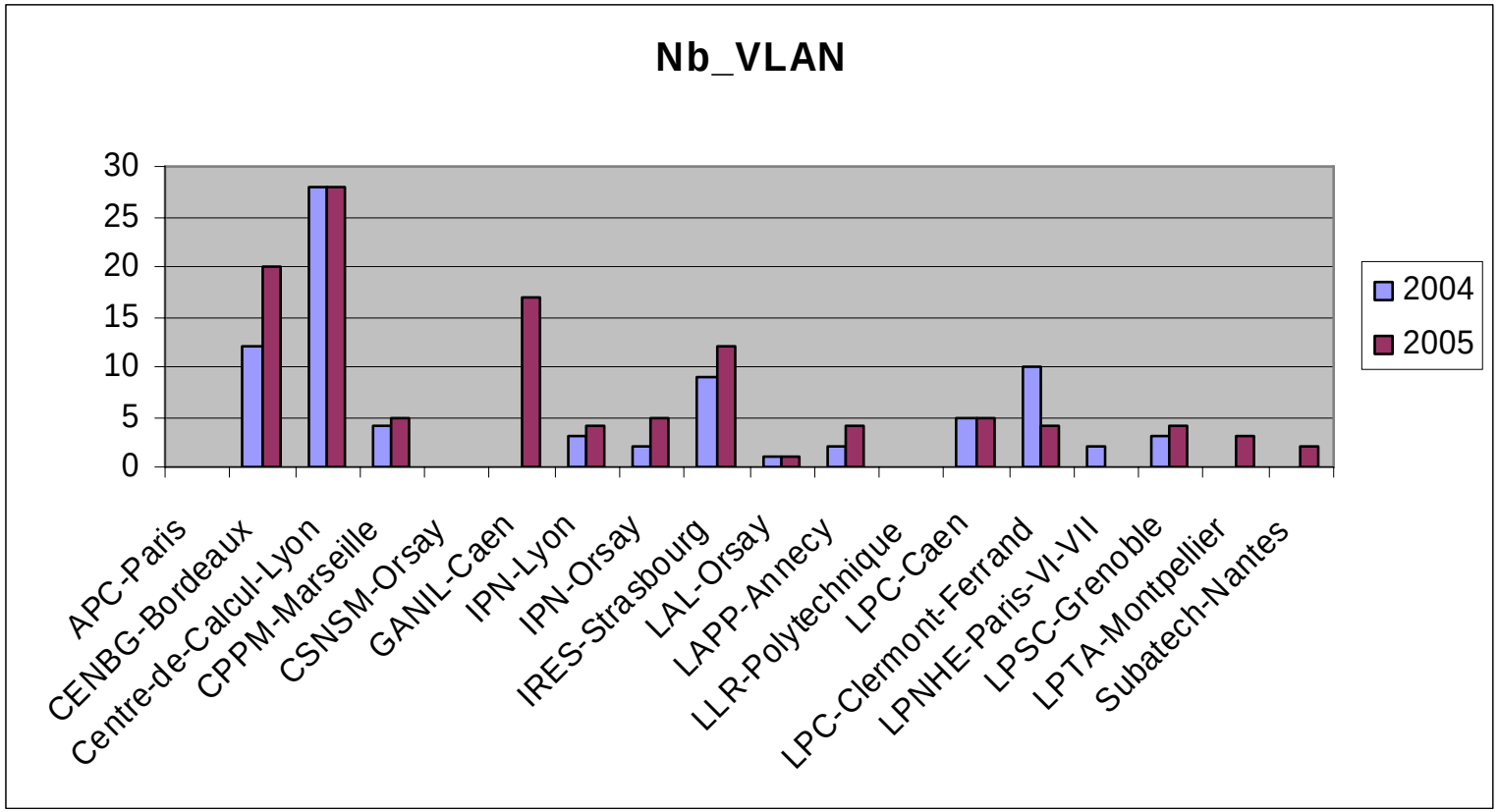
Infrastructure des réseaux de laboratoire 4/6

- Wi-Fi



Infrastructure des réseaux de laboratoire 5/6

- Cloisonnement

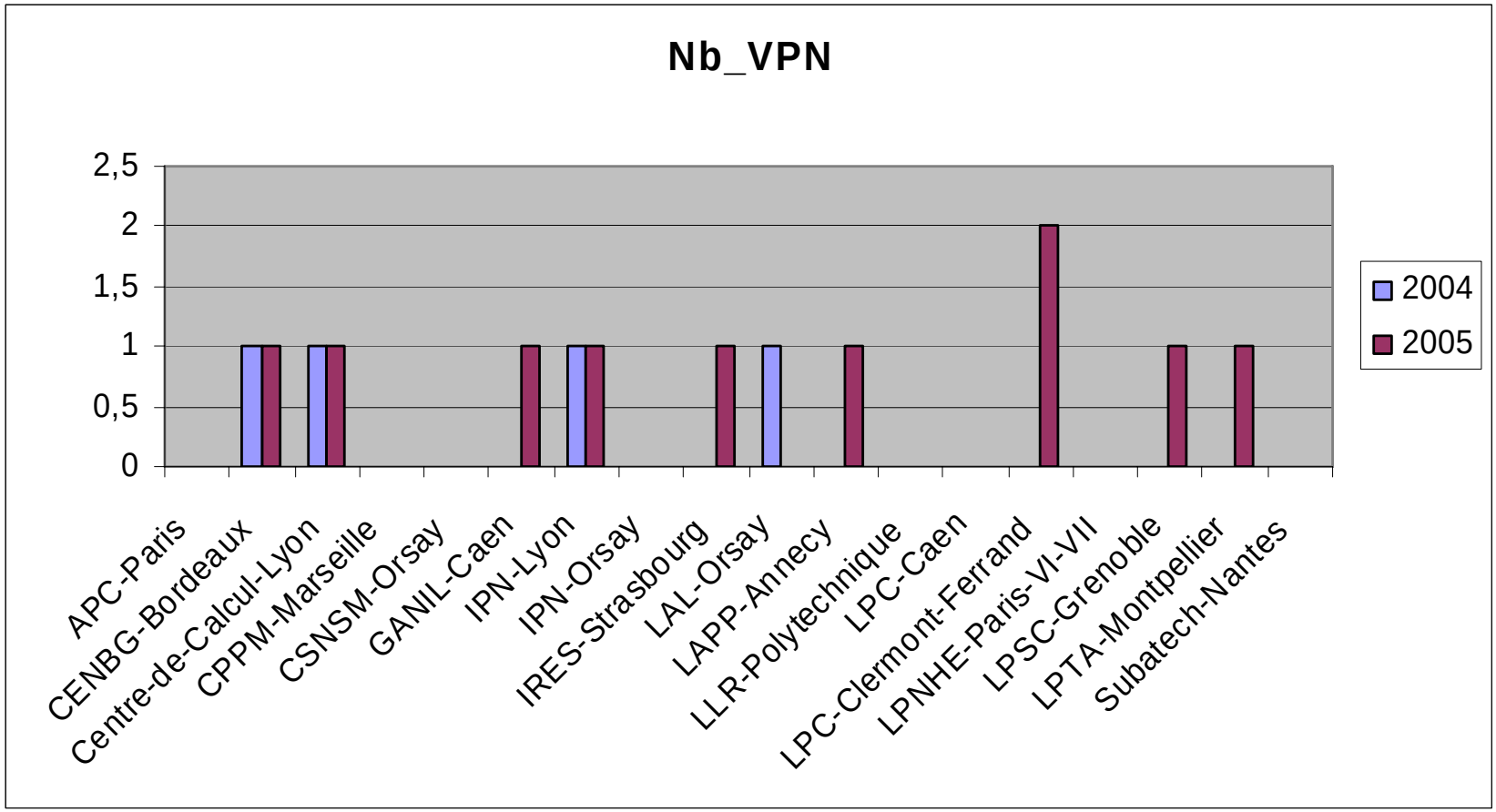


Contrôle de l'accès au réseau

- ***Filaire*** *:*
  - 11 laboratoires ne contrôlent pas l'accès au réseau filaire.
  - 6 laboratoires effectuent un contrôle tel que :
    - Activation des prises à la demande
    - Verrouillage des adresses MAC (Subatech).
    - VMPS (CC-IN2P3, CENBG, LPSC, IPNL).
- ***Wi-Fi :***
  - 9 laboratoires sur 10 effectuent un contrôle d'accès pour le Wi-Fi, le 10ème a placé le Wi-Fi dans une zone à part.
  - Ce contrôle d'accès met en œuvre une ou plusieurs des techniques suivantes :
    - la non diffusion du SSID,
    - le chiffrement WEP
    - le contrôle des adresses MAC
    - WPA

Infrastructure des réseaux de laboratoire 6/6

- VPN



Filtrage en entrée 1/2

- Exposition des laboratoires et efficacité des actions en terme de filtrage.
- Nombre total de service (TCP) ouverts vers l'extérieur est de 998.
- Extrait des ACL des routeurs de laboratoire
- Fermeture des services non chiffrés (en rouge dans le tableau).
- Tableau du filtrage en entrée de site

Filtrage en entrée 2/2

- *Evolutions depuis 2005*
  - POP et IMAP fermés depuis l'extérieur (au profit de POPS et IMAPS)
    - 2 en 2005
    - 9 en 2006.
  - Il ne reste plus qu'un TELNET ouvert au lieu de 22 dans 6 sites en 2005.
  - Il n'y a plus de SHELL ouvert.
  - Il subsiste un nombre important de serveurs FTP, il faudrait vérifier que la plupart ne sont accessibles qu'en lecture seule et en mode *anonymous*.

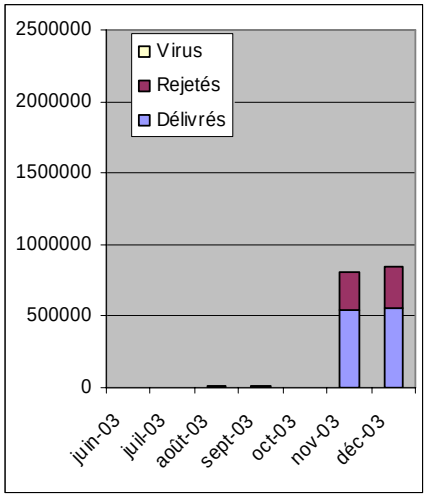
Surveillance réseau et détection d'intrusion

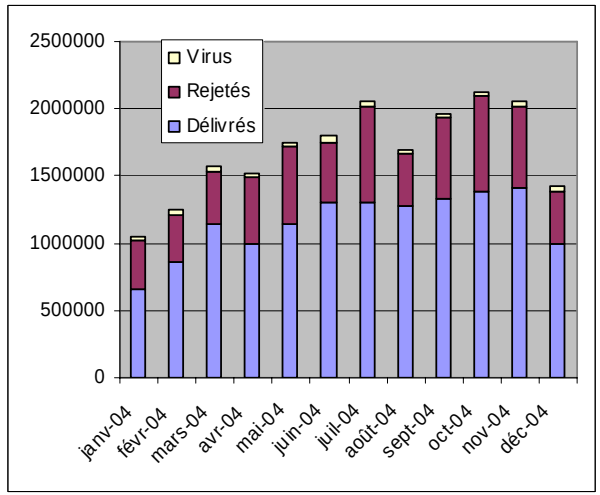
- Extra est déployé dans tous les laboratoires.
- Scripts déclenchés automatiquement pour la surveillance
  - Virus test les connexions sortantes sur les ports Windows, envoie des mails d'alerte
    - Virusday 060612
      - IP Port NbHits
      - 134.158.40.1 445 16295
  - Extrastat comptabilise les scans (une machine externe echange des paquets avec N machines/ports internes), resultats stockés dans une bdd, pour l'instant non exploité.
- Détection des attaques « brute force » SSH, pot de miel pour capturer les mots de passe, alerte en cas d'attaque venant de l'IN2P3. (voir présentation de Jean-Michel).

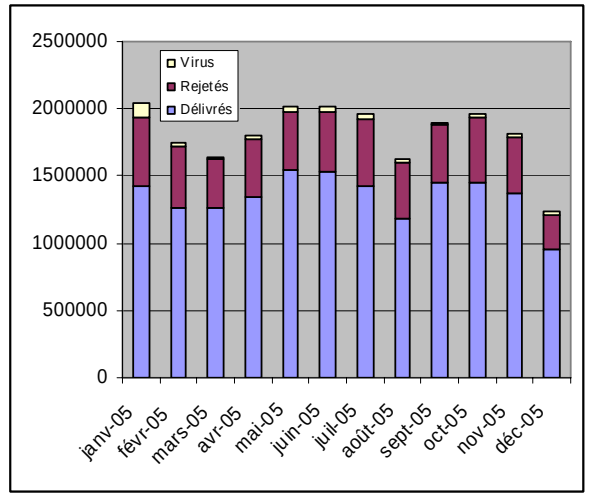
Menace et incidents

- Passerelle antivirus du Centre de Calcul

2003 2004 2005

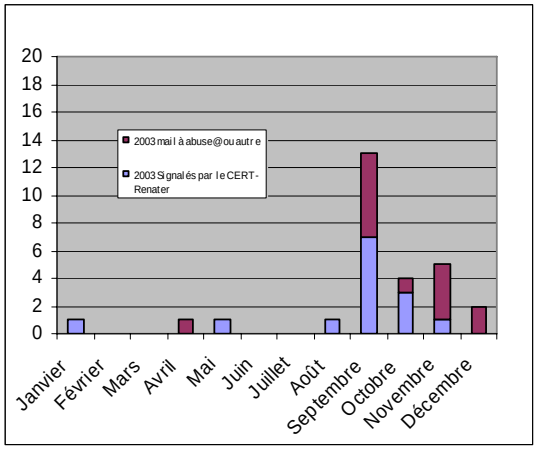


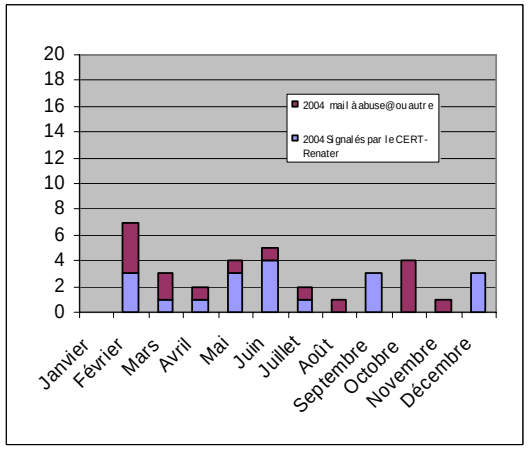


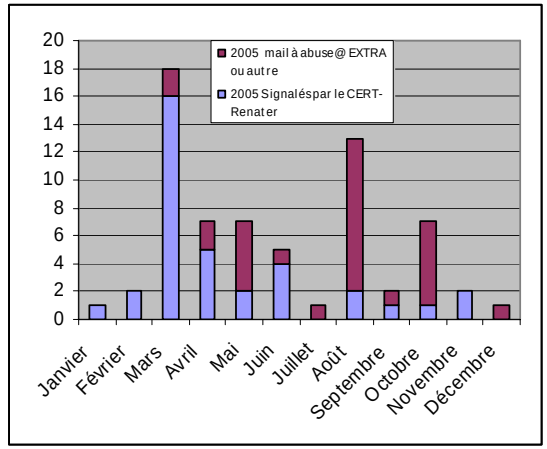


Menace et incidents

- Virus reportés malgré l'antivirus (mail CERT-Renater, mail reçu à abuse@in2P3.fr, détection par extra).

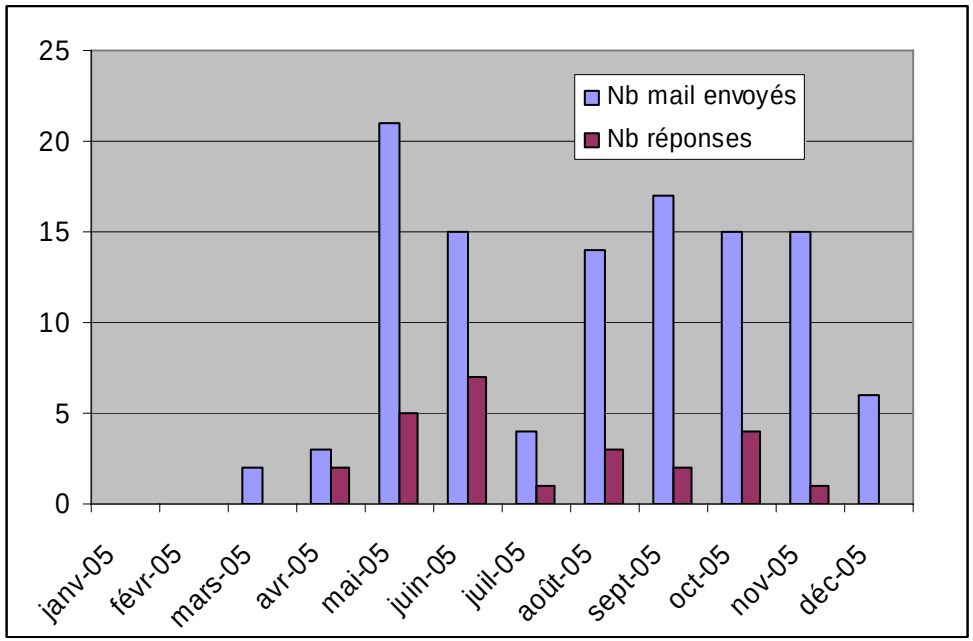






Menaces et incidents
Intensification des attaques SSH

- Voir présentation de Jean-Michel Barbet
- Peu de retour sur les protestations à abuse@



Menaces et incidents

- Compromission de machines
  - - xyzt268 : compromission découverte suite à l'implication de la machine dans un DDOS. Utilisation de AWStats.pl 2005/VULN095 CERT-Renater. Compromission du compte apache, pas de passage root,
  - - 134.158.xyz.219 et 134.158.xyz.70 compromises suite à une perte d'ACL due à un bug dans IOS Cisco 12.2.25SEB en cas d'activation des sondes RMON. Compromission du compte root, sniffer et *backdoor* sur la machine 219.
  - - xyz.in2p3.fr, xyz01, xyz02, xyz03 compromission d'un compte utilisateur, robot IRC et *keyboard logger*, pas de passage root.
  - - xyzs1, xyzs9, xyzs8 *rootkit suckit*, compromission du compte root, nombreux mots de passe sniffés.

Menaces et incidents

- rootkit Suckit
  - installé à partir d'une faille dans la routine p_trace.
    Ce rootkit peut être détecté avec une simple commande ls

    ls -li /sbin/telinit /sbin/init
    1599495 -rwxr-xr-x 1 root root 27036 Feb 10 2003 /sbin/init
    1599503 lrwxrwxrwx 1 root root 4 Apr 29 2004 /sbin/telinit -> init

    Si les deux inodes sont différents la machine n'est pas infectée.
    Si les deux inodes sont identiques la machine est infectée ce qui peut être confirmé par un cat /proc/1/maps qui fait apparaître un autre processus à la place de /sbin/init (genre /sbin/initxyz)

Conclusion

- Filtrage
- Cloisonnement 14/18
- Extra
- Authentification