La sécurité des systèmes d'information à l'IN2P3

JI08 – Obernai - 2 octobre 2008

Th.Mouthuy

Chargé de mission SSI à l'IN2P3

La question...

Que voulez-vous savoir sur la sécurité à l'IN2P3 ?

- Sommes-nous en sécurité ?
  - Oui ? Et je peux arrêter mon exposé...
  - Non ? J'arrête mon exposé pour retourner travailler...

La sécurité des systèmes d'information ?

- Pourquoi ?
- Comment ?

La question : Pourquoi ?

- Pourquoi de la sécurité ?

  Préserver VOS données !

  - C'est obligatoire (légal – voir CNIL)
  - C'est une nécessité pour le CNRS

  En sécurité, on parle en terme de :

  - Confidentialité
  - Disponibilité
  - Intégrité

La question : Comment ?

- Comment ?
  - Ce n'est pas que « un problème technique »...
  - Structure organisationnelle à l'IN2P3 (et CNRS)
  - Education des utilisateurs – c-à-d aussi VOUS !

Groupe sécurité de l'IN2P3

- Structure organisationnelle à l'IN2P3
  - Plus de 10 ans d'ancienneté... et d'expérience
  - 1 Chargé de mission sécurité auprès de la direction
    - Bernard Perrot (~1996 ? → 2001)
    - Bernard Boutherin (2001 → 2008)
    - Thierry Mouthuy (2008 → ?)
      - + 1 suppléant (Benoit Delaunay)
  - ⭐ Coordination des actions
  - ⭐ Mettre en place la politique de sécurité
  - ⭐ Garantir un niveau de sécurité commun

Groupe sécurité de l'IN2P3

- Des correspondants sécurité dans chaque laboratoire (déjà en place depuis plus de 10 ans)
- 70 personnes de tous les labos :
  - Liste de diffusion SECURITE-I@in2p3.fr
  - Réunions de sécurité 1 à 2/an (30 à 50 participants)
  - Des actions concertées

Quelles actions ?

- Avant 2001: Fermeture des services non sécurisés (telnet/ftp)
- 2002: Filtrage « tout sauf... »
- 2002: Antivirus sur les emails
- 2003: Mise en place des VLAN
- 2005: Déploiement Extra
  - Enregistrement automatique des logs routeurs
  - Analyse des logs et alertes
  - Possibilité de tracer une connexion
- 2008: Relations avec la chaine organisationnelle CNRS

Bilan 2007/2008

- Chaque année un bilan « sécurité » est présenté à la direction...

1. Infrastructures des labos

  - Tendance au 10 Gbps (actuellement 1 Gbps /labo)
  - Suppression des HUBS en interne (17/18)
  - Cloisonnement presque partout (16/18) (wifi, visiteurs,DMZ,...)
  - VPN en augmentation (14/18)

- Pas de difficultés en vue

Bilan - suite

2. Filtrage tout sauf...

Année	Nb de ports ouverts
2005	1887
2006	2514
2007	2948

Tendances :

- Augmentation de SSH
- Augmentation de HTTP et HTTPS
- Augmentation de MYSQL !!!
- Augmentation Visioconférence
- Stabilisation des ports pour les grilles de calcul

- Plus de telnet, de X11, de ICA
- Encore trop de IMAP, POP, FTP

Attaques vues

3. Scans :

- 7000 machines/heure
- Ports 135 (10M/an), 1433 (6M/an) et 22 (6M/an)

  ⇒ Ouvrir uniquement ce qui est nécessaire

- 10000 mots de passe différents/mois essayés par SSH

  ⇒ Attention à la solidité des mots de passe

4. Virus : 3M vus par mois au CC
   (Les Greylist en rejettent 80 %)

Alertes ou incidents 2008

5. Alertes EXTRA ou incidents en 2008...

Nb	Ports	Raison	Origine
8	4672	P2P	Visiteur
2	16800	TV	Visiteur
1	8000	P2P	
3	445-139	Virus	Visiteur
1	80	Site communautaire	
1	1433	Virus	?
1	Bcp	Virus	?
3	80	? Skype ?	Visiteur
1	25	Virus	Visiteur

8	Différents	Erreurs de config ou cas particulier.

3	Défiguration de site
4	Vols de portable

Actions sur les incidents...

- Problème classique d'hébergement de visiteurs
  - Filtrage en interne – Vlan
  - Filtrage en sortie – Quelques essais
- Quelques dérapages internes – à recadrer
  - P2P, sites particuliers
- Quelques erreurs de config (pas trop graves)
- Quelques problèmes de site web (forums, listes)
- Problèmes des portables et des données...

Problèmes des PC portables

- Menace : Vol du portable
  - Problème de confidentialité ↣actions
  - Problème de disponibilité ↣précautions
- Protection des données p.ex. des données classifiées, à caractère personnel,...
- Respect des clauses d'un contrat de recherche
- Préserver des résultats de recherche
- Nouvelle menace !! : Passage de frontière

Politique de chiffrement pour les portables

- Projet pilote CNRS à l'IN2P3 (F.Morris et ThM)
- Mettre en place l'organisation pour le chiffrement des portables à l'IN2P3
- Accord du directeur de l'IN2P3

➔ Tous les nouveaux portables seront chiffrés...

Quels autre dangers ?

En vrac....

- Acceptation d'émails dangereux
- Clic sur des sites malveillants

- Applications Web mal écrites
- Service non corrigés (patch !)
- Fuite d'information...

- Services gratuits sur Internet ?

Services gratuits d'internet ?

- Gratuité ?
  - Publicité, utilisation de la bande passante, interruption de service sans préavis
- Confidentialité ?
  - Google mail, Google agenda, Blackberry, Doodle, et aussi le download de fichier sur Free.fr

- Sensibiliser les utilisateurs sur les informations qu'il rend publique !!!

Quelques exemples à proscrire...

- GMAIL : Proscrire
  - Adresse professionnelle !
- WEB hébergé : Proscrire
  - Risques de compromission en cascade
- Externalisation du stockage
- Exemple d'un labo de chimie stockant, sur un wiki Free.fr, les résultats de manip, les idées etc

Conclusions : La sécurité dans l'institut

- Milieu relativement homogène
- Problématiques très similaires dans chaque labo

- Structure « institut » bien adaptée
- A permis des actions concertées et bien ciblées
  - ➔ A préserver donc... !

- Comment combiner la SSI CNRS (régions) et la SSI IN2P3 ?
  - Accord J.Illand et R.Longeon
  - Schémas fonctionnels

Comment interagir ?

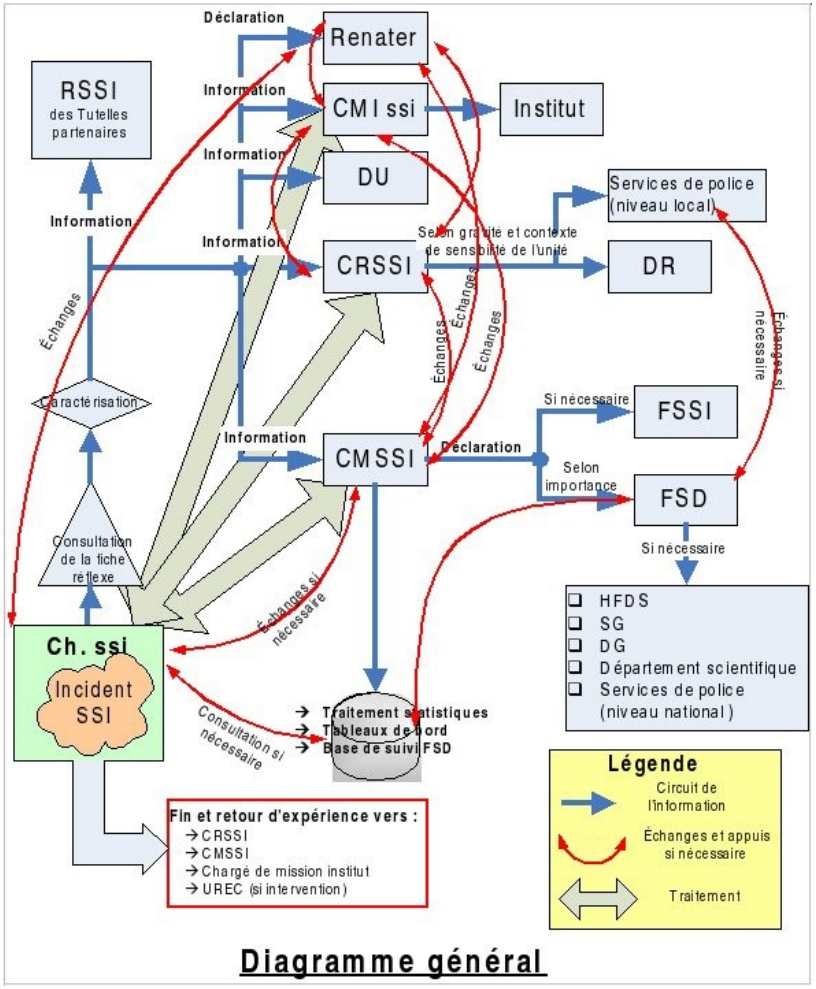
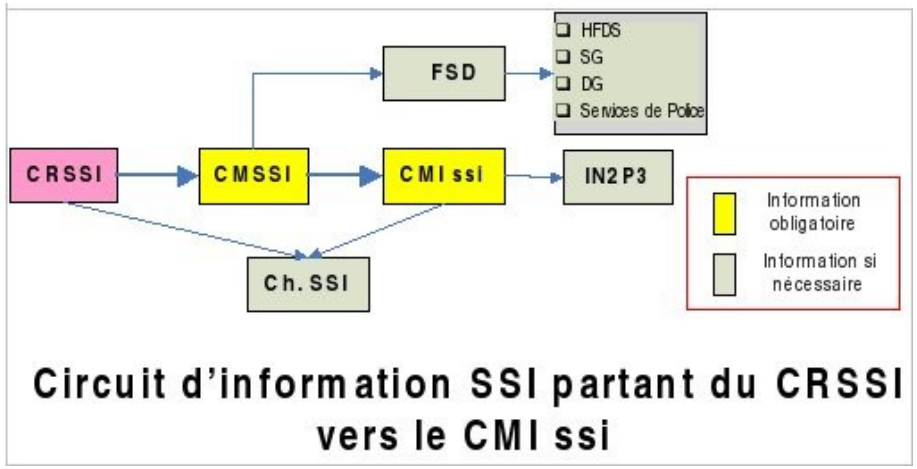
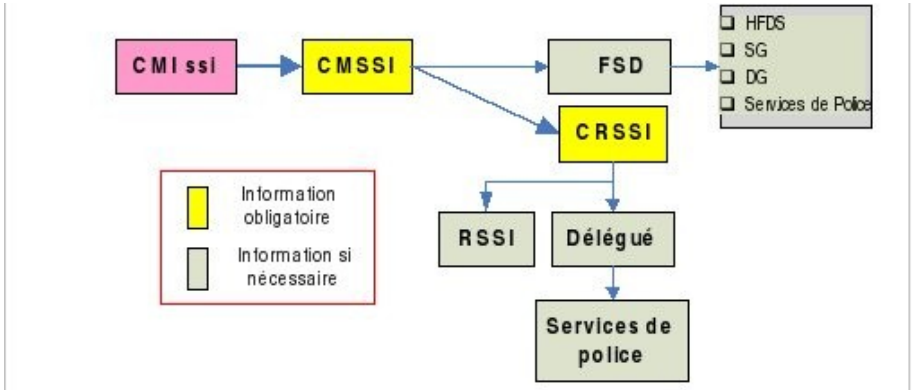


Diagramme général

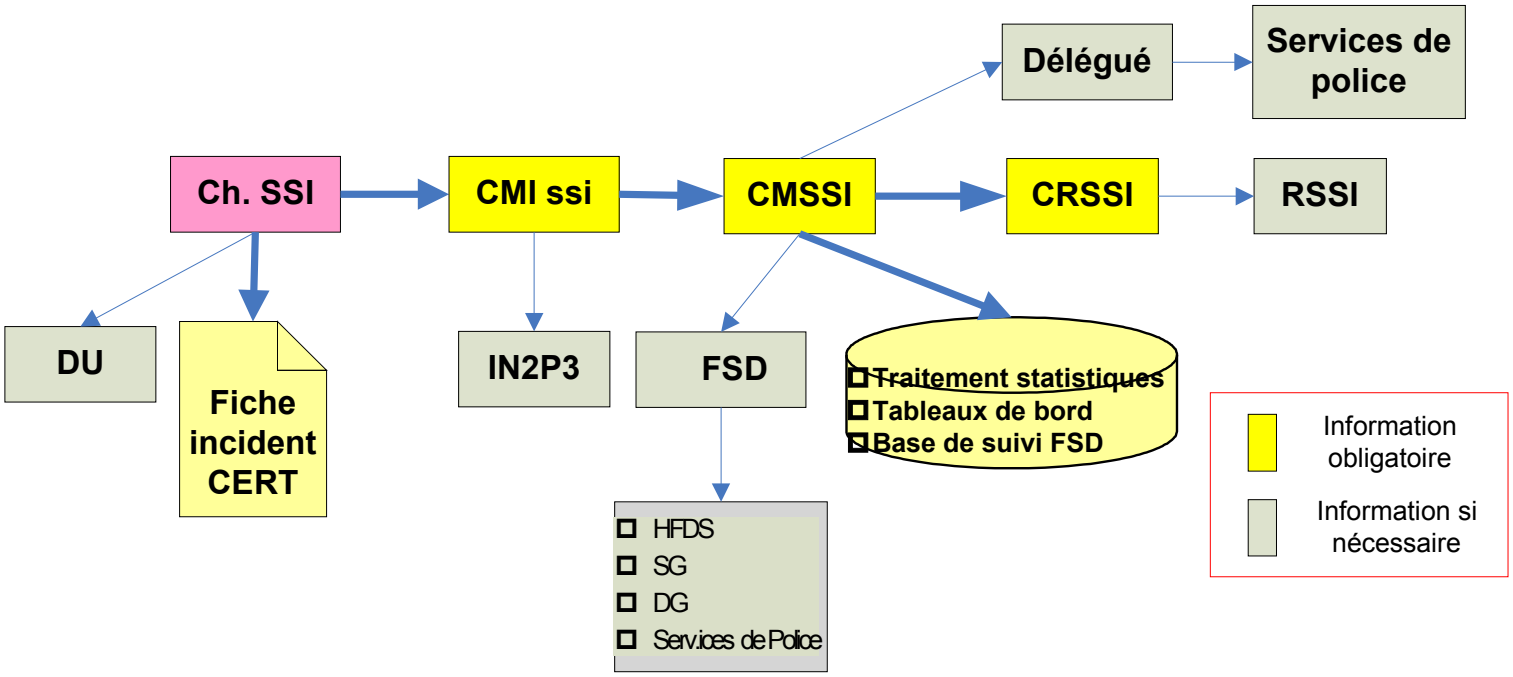


Circuit d'information SSI partant du CRSSI vers le CMI ssi



Circuit d'information SSI partant du CMI ssi vers le CRSSI

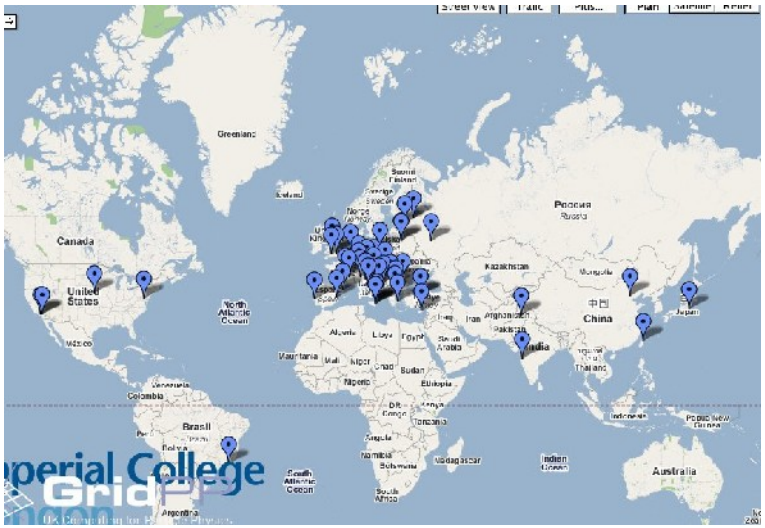
Chaine fonctionnelle



Information ascendante d'un incident de SSI (à partir du Ch. ssi)

Nouvelle problématique – La grille

- Traitement de données important (1PB/an)
- Mise en commun des moyens de calcul et de stockage
- Projets EGEE et LCG
- Des utilisateurs de tous pays...



GRILLE – Nouvelles problématiques

- Nouveaux problèmes de sécurité:
  - Connexion par certificat
  - Appartenance à une organisation virtuelle (VO)
  - Droits génériques par VO permettant :
    - Le calcul
    - Le stockage
- On ne connait pas les personnes...
- On ne sait rien des applications...
- Il faut surveiller les sites... et faire confiance !

GRILLE – Nouvelles chaines

- Nouvelles chaines de correspondants, internationales cette fois.

- Différents groupes :
  - OSCT : Operational security coordination team
  - MWSG : Middleware security group
  - JSPG : Joint security policy group
  - SCG : Security coordination group
  - EuGridPMA : Autorités de certification

- Un correspondant (générique parfois) par site
- Des listes de diffusion

Conclusions

- Des nombreuses chaines...
  - Au sein de l'institut IN2P3
  - Avec le CNRS – FSD – Régions – Universités
  - Dans les GRILLES
- Les personnes qui participent sont souvent les mêmes... Heureusement !!!