

La SSI à l'IN2P3

Réunion des CRSSI – Paris 11 septembre 2008

Th.Mouthuy

Chargé de mission SSI à l'IN2P3

L'IN2P3

IN2P3 = Institut du CNRS

★ Acteur majeur en Physique Hautes Énergies

- ★ 19 laboratoires
- ★ 1 Centre de Calcul
- ★ 3 sites (Ganil, Modane, La Seyne)

IN2P3

INSTITUT NATIONAL DE PHYSIQUE NUCLÉAIRE
ET DE PHYSIQUE DES PARTICULES



Particularités de l'IN2P3

- ★ 700 Chercheurs/Enseignants chercheurs
- ★ 1800 Ingénieurs, Techniciens et Administratifs
- ★ Contacts forts avec :
 - IRFU (CEA)
 - Sites étrangers : CERN, FNAL, SLAC, DESY
- ★ Très fortes relations internationales...

p.ex. Collaboration Atlas :

- 2200 personnes
- 177 laboratoires
- 37 pays



Groupe sécurité de 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 Bouterin (2001 → 2008)
 - ◆ Thierry Mouthuy (2008 → ?)
 - ◆ + 1 suppléant (Benoit Delaunay)
- ★ Coordination des actions
- ★ 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

Exemples de réunions / formations

- ◆ 2001 : Charte IN2P3, connexion sécurisée
- ◆ 2002 : CENBG – Présentations des certificats
- ◆ 2002 : CDF – CERT-Renater
- ◆ 2003 : CC – VLAN et VPN
- ◆ 2004 : CC – Présentations de la DST (Jaillet)
- ◆ 2005 : Ganil – Aspects juridiques (Longeon) et politique de sécurité au CEA (Zuccolini)
: Aussois – Authentification centralisée et SSO
- ◆ 2006 : JI06 – sécurité des systèmes de contrôle-commande
- ◆ 2007 : Nantes – Sécurité au CNRS, IN2P3 et PSSI CNRS

Des actions – Avant 2001

- ◆ Fermeture des ports « sensibles »
 - ★ Utilisation de SSF (B.Perrot) au lieu de Telnet
 - ★ Fermeture de FTP

Un peu de grogne chez les utilisateurs, mais grâce à l'action collective, plutôt bien passé.

Actions 2001 - 2004

- ◆ 2001 : Définition d'une charte informatique IN2P3 (suivi de peu par la charte CNRS)
- ◆ Janvier 2002 : Filtrage « Tout Sauf... »
Surveillance des logs des routeurs
- ◆ Octobre 2002 : Filtre antiviral des emails (central si souhaité)
Filtres réseau sont actifs partout
- ◆ Janvier 2004 : Retour sur les implémentations VLAN
Présentation de EXTRA - planning

Actions 2005 - 2008

- ◆ Janvier 2005 : Mise en place de EXTRA
 - ★ Enregistrement automatique des logs routeurs
 - ★ Analyse des logs et alertes
 - ★ Possibilité de tracer une connexion
- ◆ Octobre 2007 : Discussions sur les interactions entre groupe de sécurité IN2P3 et la structure CNRS
- ◆ Avril 2008 : Définition de la chaine organisationnelle

Bilan

- ◆ 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

Attaques vues

3. Scans :

- ★ 7000 machines/heure
- ★ Ports 135 (10M/an), 1433 (6M/an) et 22 (6M/an)
- ★ 10000 mots de passe/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
3		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...

Politique de chiffrement pour les portables

- ◆ Déjà présenté précédemment (cfr talk de Fr.Morris)
 - ◆ Mettre en place l'organisation pour le chiffrement des portables à l'IN2P3
 - ◆ Pour le moment en attente de la lettre de missions du directeur de l'IN2P3
- ➔ Tous les nouveaux portables seront chiffrés...

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 ?

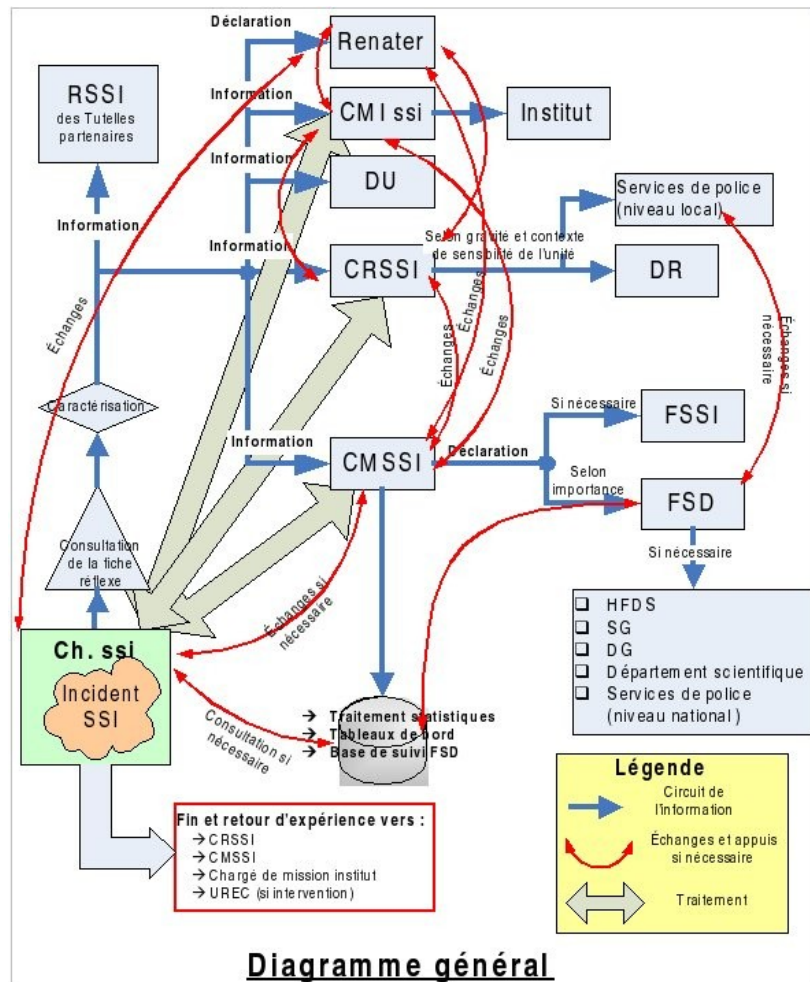
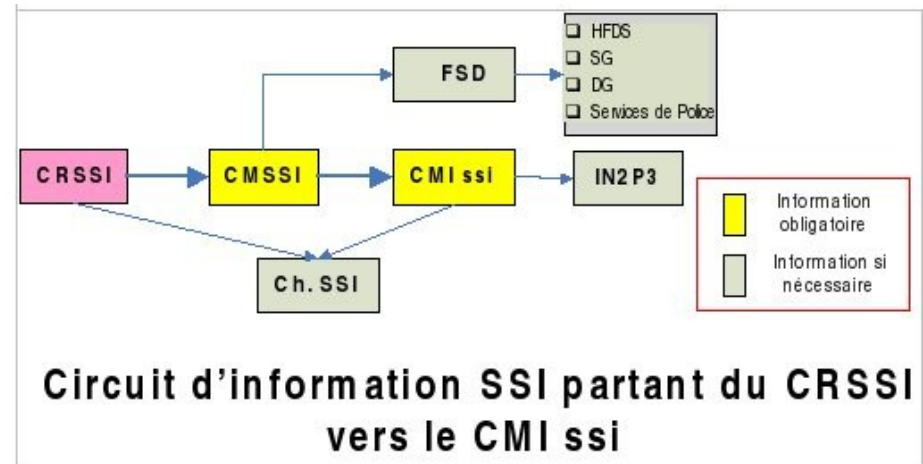
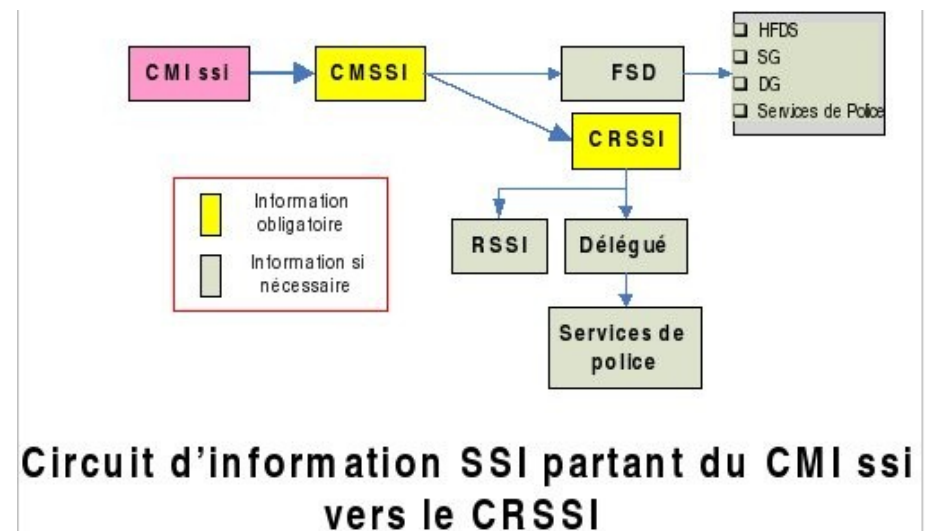


Diagramme général

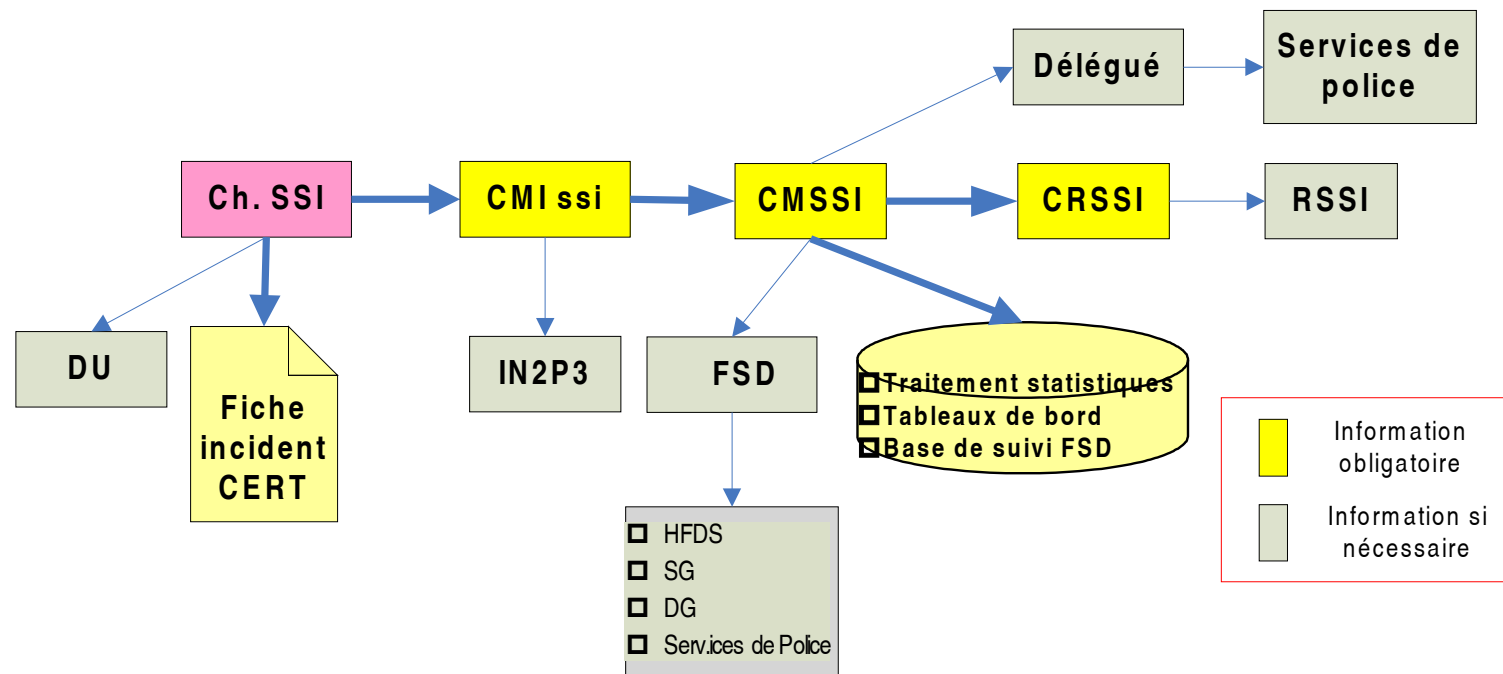


Circuit d'information SSI partant du CRSSI vers le CMI ssi



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

Chaîne fonctionnelle



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

Nouvelle problématique – La grille

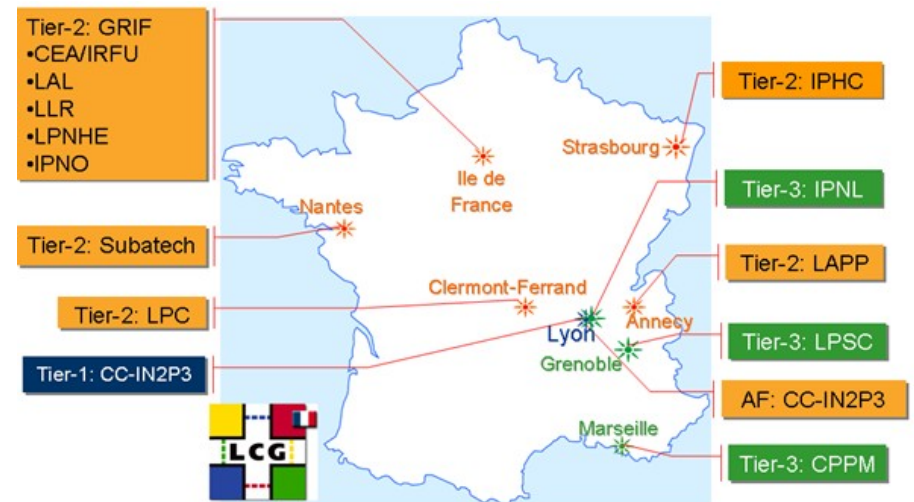
- ◆ Traitement de données important (1PB/an)
- ◆ Mise en commun des moyens de calcul et de stockage
- ◆ Projets EGEE et LCG
- ◆ Des utilisateurs de tous pays...



La GRILLE en France

◆ Des laboratoires français :

◆ CGGVeritas	Paris
◆ GRIF	CNRS, Ile de France (IRFU, LAL, LLR, LPNHE, IPNO)
◆ IBCP-GBIO	CNRS, Paris
◆ CC	IN2P3, Lyon
◆ CPPM	IN2P3, Marseille
◆ IPNL	IN2P3, Lyon
◆ IRES	IN2P3, Strasbourg
◆ LAPP	IN2P3, Annecy-le-Vieux
◆ LPC	IN2P3, Clermont-Ferrand
◆ LPSC	IN2P3, Grenoble
◆ SUBATECH	IN2P3, Nantes
◆ IPGP	CNRS, Paris



◆ Institut des grilles (CNRS) à Paris

GRILLE (LCG)

- ◆ Mais aussi, des contacts étroits entre...

Tier1 (CC) et Tier2 (Belgique)

Tier2 (Japon - Tokyo)

Tier2 (Chine - Pékin)

Tier2 (Roumanie)

Tier2 (GRIF) et Tier2 (Sénégal)

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 connaît 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
 - ★ Dans les GRILLES
- ◆ Les personnes qui participent sont souvent les mêmes... Heureusement !!!