



# *L'Unité Réseaux du CNRS*

*Journée des CRSSI 2007*

Bernard.Rapacchi @ urec.cnrs.fr

Marie-Claude.Quidoz @ urec.cnrs.fr

---

# *L'Unité Réseaux du CNRS*

- Créée en 1990
- Christian Michau : directeur 1990-2002
- Jean-Luc Archimbaud : directeur 2002 – 2006
- D'abord rattachée au département SPI, STIC, Ingénierie, ST2I
- Rattachée au Secrétaire Général depuis novembre 2006

# *Les missions de l'UREC (1)*

- Assurer **l'assistance à la maîtrise d'ouvrage**
  - Actions concernant la mise en œuvre
  - Maintien et à l'optimisation de la performance

des systèmes et réseaux informatiques et de télécommunication pour l'ensemble du CNRS

- Organiser les réseaux informatiques au CNRS
- Développer les services qui leur sont associés
- Apporter son expertise technique à la communauté qui les administre.
- Missions directes auprès :
  - DG, SG, Départements Scientifiques, Délégations Régionales, Directeurs d'Unités

# *Les missions de l'UREC (2)*

- **Cellule**
  - D'expertise, de développement et de validation de solutions techniques.
- **Mission également**
  - De diffusion des connaissances et des pratiques,
  - Notamment par des actions de formation de la communauté des administrateurs système et réseau (ASR) du CNRS
  - Elle participe au pilotage de la fédération des réseaux régionaux de métiers d'ASR avec la MRCT et la DRH
- **Travail en collaboration**
  - Direction des Systèmes d'Information, le CC-IN2P3, les services du Fonctionnaire de Sécurité de Défense
  - GIP RENATER, Comité Réseaux des Universités

# *Trois pôles de compétences techniques*

- **Infrastructures et services réseaux**

- Expertise / consultance des projets réseaux dont ceux soumis au Comité des Infrastructures du CNRS, (SIRESv2)
- Définition des spécifications techniques des cahiers des charges RENATER ou réseaux métropolitains (RAP)
- Services nationaux : DNS cnrs.fr et un service de listes de diffusion

- **Intergiciels (Middleware) et applications**

- L'identification, l'authentification, les autorisations, les annuaires.
- Logiciel IGC du CNRS
- Rappel :
  - Formation des autorités d'enregistrement CNRS-Plus (dans les DR)
  - Mais aussi celles des AE CNRS-Standard (dans les unités)

- **Expertise technique de sécurité informatique**

---

# *Pôle de compétence technique en sécurité*

- Cellule d'Expertise Technique en Sécurité (CETESSEC)  
**==> À destination des Administrateurs Systèmes et Réseaux**
  
- Trois personnes
  - Gaël Beauquin                      tél : 04 76 63 59 78
  - Nicole Dausque                      tél : 01 44 27 42 80
  - Marie-Claude Quido                tél : 04 76 63 55 96
  
- Adel                                      [cetesecc@urec.cnrs.fr](mailto:cetesecc@urec.cnrs.fr)
  
- Site : <http://www.urec.cnrs.fr/> onglet Sécurité

# *Expertise / soutien (1)*

- Aspects techniques des incidents de sécurité
  - Analyse et compilation d'informations diffusées par les CERTs : objectif --> **prévenir** (ex. *Vulnérabilités Web sur PHP*)
  - Acquisition d'informations sur incidents : objectif --> **réagir** (ex. *A2IMP* Aide à l'Acquisition d'Informations sur une Machine Piratée)
    - Savoir acquérir en situation d'urgence les bons réflexes pour sauvegarder les données indispensables
  - Analyse post mortem : objectif --> **comprendre** (ex. *A3IMP* Aide à l'Analyse des Actions Intentées sur une Machine Piratée)
    - Récupérer des informations (fichiers, processus...) à partir d'éléments sauvegardés (traces, sauvegarde disque dur...) et en tirer bénéfice pour la travail au quotidien
  - Aides techniques aux incidents de la vie courante : objectif --> **fournir** des boîtes à outils (ex. *Récupérer un disque endommagé*)

## *Expertise / soutien (2)*

- Suivi des évolutions des systèmes à travers le travail d'expertise dans les projets de l'UREC
  - Systèmes (ex. *Vista et les nouveaux apports en sécurité*)
  - Réseaux et architectures
    - IPv6
    - VoIP
    - Virtualisation
    - Objets communicants (téléphone intelligent, assistant personnel, communauté « nabaztag » ...)
  - Web et services -> étude des risques de fuite d'informations
    - Applications grand public : Google Apps & Co ... , abonnement
    - Outils d'indexation et de recherche
  - Expertise des logiciels sécurité dans le projet PLUME (ex. *Ad-Aware*)

## *Expertise / soutien (3)*

- Pour la mise en œuvre des règles d'application des principes définis dans la Politique de Sécurité des Systèmes d'Information (PSSI)
- Exemples (PSSI CNRS version 1.0 <http://www.sg.cnrs.fr/FSD/securite-systemes/doc1.htm>)
  - A3IMP : Bénéfices pour l'administration au quotidien traite : « **Effacement d'un disque dur avant mise au rebut** » est une réponse au point :
    2. Protection des données --> 2.5 Réparation, cession, mise au rebut ==> Effacer les supports
  - Site <http://www.urec.cnrs.fr/> sous l'onglet Sécurité > Base documentaire > Informations techniques  
Les documents sous **Architecture** répondent au point :
    3. Sécurisation du système d'information --> 3.9 Réseau ==> Mettre en place une architecture sécurisée

## *Expertise / soutien (4)*

- Site <http://www.urec.cnrs.fr/> sous l'onglet Sécurité > Base documentaire > Informations techniques

Les documents sous **Journaux de traces** ainsi que les thèmes traités dans la formation A3IMP répondent au point :

4. Mesure du niveau effectif de sécurité --> 4.4. Les fichiers de trace ==> Analyser les fichiers de trace

# *Le site : exemple*

- Accueil > Sécurité > Base documentaire > Informations techniques  
<https://www.urec.cnrs.fr/rubrique124.html> avec accès par certificats CNRS

*propose :*

Accès distants sécurisés

Applications Internet grand public

Architecture

Bases de données

Chiffrement

Codes malveillants (malware) et pièges

Gardes-barrière

Journaux de traces

Législation

Messagerie & certificat

Objets communicants (PDA)

Pollupostage (SPAM)

Postes clients & Clients légers

Présentations d'outils

Projets Sécurité Web

Réseaux sans Fil

Système d'exploitation

Voix sur IP

# *Exemples de documents (1)*

- Document **Recommandations de sécurité destinées aux administrateurs systèmes et réseaux du CNRS pour l'installation de réseaux locaux sans fil** (Jean-Luc Archimbaud, Catherine Grenet, Marie-Claude Quidoz)

...

*But du document* L'administrateur doit donc construire une architecture (où mettre les bornes dans son réseau ?), utiliser certaines fonctions de sécurité sur les bornes, et définir des procédures pour la connexion des stations...

...

*Mécanismes de sécurité sur les réseaux sans fil* Au fil du temps un certain nombre de mécanismes de sécurité sont apparus sur les réseaux sans fil.

- Non-annonce de l'identifiant de réseau (*Service Set Identifier* ou SSID) : cet identifiant...

## *Exemples de documents (2)*

- Document **Vulnérabilités Web sur PHP** (Gaël Beauquin)

...

Faible PHP : *include( )* La fonction PHP *include( )* est couramment utilisée lors de programmation de sites web. Elle permet d'inclure et d'exécuter un script PHP dans un autre script, ce qui permet de créer des bouts de codes qui sont réutilisables dans l'application.

...

Le paramètre étant passé via l'URL, un individu mal intentionné peut passer des paramètres arbitraires. Le comportement par défaut...

...

Faible web : *Cross Site Scripting* Il est fréquent pour un script de demander une valeur à un utilisateur, et il est non moins fréquent pour le script d'inclure la valeur entrée dans la page générée. Un exemple basique pourra être une invite du type « Entrez votre nom : »...

# Projets 2007-2008 (1)

## ▪ Ipv6

- Comment adapter ses solutions de sécurité IPv4 à l'IPv6 ?
- Les nouveautés de IPv6 à prendre en compte dans le cadre de la sécurité ?

## ▪ Web

- ANGD déposé : Aide À la Détection des Faiblesses d'un site web
- Groupe de travail en cours de mise en place (ResInfo)
  - Méthodes & outils d'analyse du code de l'application
  - Architecture à mettre en place
  - Validation & suivi des produits mis à la disposition par le CNRS (exemple Kit CNRS SPIP)
  - ...

# *Projets 2007-2008 (2)*

- Expertise des logiciels sécurité dans le projet PLUME
  - Ceux présentés lors d'A3IMP
  - Ceux de la vie courante en sécurité

# Questions ?