SÉCURITÉ de l'information
Sécurité Informatique / Numéro 2 ////// Octobre 2008

ÉDITORIAL

Un numéro spécial : « fédérations d'Identités »

PAR BERNARD RAPACCHI
Directeur de l'Unité Réseaux du CNRS (UREC)
bernard.rapacchi[aroba]urec.cnrs. fr

La Gestion des Identités et des Autorisations est bien évidemment une des bases de la Sécurité des Systèmes d'Information. Le CNRS se préoccupe de ces aspects depuis plusieurs années, notamment avec la mise en œuvre de l'Infrastructure de Gestion de Clés (IGC) du CNRS au début des années 2000, mais il faut bien admettre que les éditeurs de logiciels et les développeurs de systèmes d'exploitation n'ont pas investi, comme nous pouvions l'espérer, dans une utilisation simple et efficace des certificats. De plus, avec l'arrivée des nouvelles applications de gestion du CNRS (gestion budgétaire, gestion du personnel, comptabilité, etc.), il a fallu se rendre à l'évidence et admettre que le déploiement complet des certificats CNRS pour tous les personnels était irréaliste dans les délais fixés.

L'Unité Réseaux du CNRS a proposé, dès l'automne 2007, le développement du projet Janus[1] que Claude Gross expose dans son article « Janus : la gestion des identités au CNRS ». Janus est le complément et le prolongement de l'IGC du CNRS. En aucun cas, il n'implique la fin de celle-ci. Janus est un projet conjoint Unité Réseaux du CNRS et Direction des Systèmes d'Information du CNRS ; il a permis de mettre en synergie les diverses compétences des deux entités dans les aspects « intergiciels » d'une part, et dans les aspects « applications » d'autre part. Les technologies de fédérations d'identités utilisées par Janus sont des technologies déjà éprouvées : elles ont été, entre autres, développées dans le cadre du consortium Internet2 aux États-Unis. Elles sont largement utilisées dans d'autres pays, européens en particulier, et chez nos voisins suisses.

La refonte des applications de gestion du CNRS nous a obligés à trouver avec Janus des solutions à des problèmes spécifiques. La particularité tient en plusieurs points, par exemple la possibilité de s'authentifier par certificat électronique ou login/mot de passe. Ainsi, Janus est un des rares développements de fédérations d'identités prenant autant en compte les aspects de redondance de chacune des parties du système, tant au niveau authentification que référentiel d'usage.

Fraîchement nommé directeur de « l'Unité Réseaux du CNRS » (UREC), je fus interpelé dans une conférence sur les fédérations d'identités organisée par nos collègues du CRU[2] pour que « le

>>>> suite page 6

[1] http://www.dsi.cnrs.fr/si/catalogue-applis/detail.asp?id_appli=204

[2] http://www.cru.fr/

Janus : la gestion des identités au CNRS

Par Claude Gross
claude.gross[aroba]urec.cnrs. fr,
CNRS – UREC
http://www.urec.cnrs.fr/

La gestion des identités, en particulier pour l'accès aux applications, est un problème qui n'est pas résolu correctement aujourd'hui au CNRS. Les spécificités du CNRS, avec ses centaines d'unités disséminées géographiquement, rendent d'autant plus difficile cette gestion.

Le contexte

La mise en place d'une IGC[1] pour diffuser des certificats électroniques aux personnels des unités CNRS avait pour but de répondre à cette question. Mais le déploiement généralisé des certificats dans toutes les unités se heurte à plusieurs problèmes, en particulier :

- l'utilisation des certificats électroniques est complexe pour l'utilisateur ;
- leur diffusion, si on veut donner une certaine valeur aux certificats, nécessite l'existence d'une autorité d'enregistrement dans chacune des unités.

Par ailleurs, les certificats en eux-mêmes ne peuvent répondre qu'au problème de l'identification et de l'authentification, et non à la gestion des habilitations. Or, la question essentielle à laquelle les applications sécurisées doivent répondre est : « Qui a droit à quoi ? ». Pour répondre à cette question, il faut bien sûr pouvoir identifier et authentifier une personne, mais il faut également disposer d'informations précises sur les rôles et les droits de cette personne dans son organisation. Un chercheur, un ingénieur, un directeur ou un gestionnaire doivent chacun pouvoir s'authentifier, mais leurs privilèges suivant les applications ne seront pas les mêmes. Ce besoin existe à tous les niveaux, à celui des applications nationales mais aussi à celui des laboratoires.

Enfin, le CNRS n'est pas un organisme isolé du monde et le besoin d'outils permettant l'authentification inter-organismes existe. Nos partenaires, par exemple les universités, n'ont pas fait le choix des certificats électroniques comme méthode d'authentification.

Pour autant, la difficulté du déploiement généralisé des certificats au CNRS ne doit pas nous conduire à revenir dix ans en arrière. Pendant longtemps au CNRS, et c'est encore parfois le cas aujourd'hui, la gestion des accès aux applications était faite par identifiant/mot de passe, et ceci

[1] Infrastructure de Gestion de Clés

>>>> suite page 2

au niveau de chaque application, avec pour conséquences :

- la multiplication des identifiants/mots de passe pour les utilisateurs ;
- un système d'authentification et des interfaces de login spécifiques à chaque application ;
- une gestion des comptes des utilisateurs au niveau de chaque application ;
- un niveau de sécurité très bas (mauvaise gestion des comptes, qualité des mots de passe, comptes utilisés par plusieurs personnes...).

Le projet Janus est donc une évolution tenant compte de l'existant, permettant de résoudre les problèmes ci-dessus et de rendre possible l'interopérabilité avec nos partenaires des autres EPST et des universités.

Le projet

La technologie retenue pour ce projet est *Shibboleth*[2] développée par le consortium Internet2 et utilisée également par nos partenaires des universités dans le cadre de la fédération d'identités du CRU[3]. Cette technologie, décrite par ailleurs, ne le sera pas dans cet article.

Ce projet de gestion des identités s'articule autour de deux composants :

- un annuaire ou référentiel ;
- un service de fournisseur d'identités.

Chacun de ces composants représente un projet en soi.

Démarré fin 2007, le projet Janus comprend plusieurs phases :

- avril 2008 : mise en place d'un fournisseur d'identités CNRS. S'appuyant sur un référentiel incomplet, il sera essentiellement utilisé dans cette phase pour la gestion des accès à l'application Sirhus (application de gestion des ressources humaines) ;
- fin 2008 : mise en place du nouveau référentiel. Cette phase permettra l'ouverture du service à toutes applications CNRS ;
- courant 2009 : enrichissement du référentiel et mise en phase des outils nécessaires.

À partir de fin 2008, le service pourra donc être ouvert potentiellement à toute application CNRS (DSI, délégations régionales, laboratoires...). Cette ouverture se fera progressivement en commençant avec des applications pilotes, par exemple le portail de l'INIST comme la direction de cet institut en a exprimé le souhait.

Le référentiel

L'annuaire est la brique de base pour la gestion des identités. Utilisant le protocole standard LDAP, il doit contenir toutes les informations nécessaires à l'authentification ainsi qu'à la gestion des habilitations.

Le CNRS disposait déjà d'un annuaire LDAP dont le contenu est une extraction des bases de données du SI CNRS. C'est ce référentiel qui est utilisé depuis avril 2008 pour l'accès à l'application Sirhus. Mais l'organisation et le contenu de cet annuaire n'ont pas été conçus pour répondre aux besoins spécifiques d'un service de fournisseur d'identités. En particulier, seuls les personnels statutaires du CNRS y sont présents alors que tous les personnels, CNRS ou non, travaillant dans une unité CNRS doivent pouvoir accéder aux applications CNRS.

Un travail est donc en cours pour mettre en place un nouveau référentiel qui devra permettre :

- l'authentification de tous les personnels des unités CNRS ;
- un plus grand niveau de gestion des habilitations pour l'accès aux applications, via la propagation d'attributs, permettant de déterminer les rôles ou les droits des utilisateurs.

Son alimentation se fera :

- par extraction des données à partir d'une ou plusieurs bases de données du SI CNRS (en particulier Labintel et à terme Sirhus) ;
- via des interfaces spécifiques pour les données non présentes dans les bases de données ci-dessus (mot de passe, identifiants internes SAP...).

Ce référentiel devrait être mis en place d'ici décembre 2008. Son contenu sera complété en 2009 avec des attributs supplémentaires pour élargir les possibilités de gestion des habilitations. Grâce à la propagation d'attributs, les applications CNRS pourront utiliser ces données pour la gestion de leurs accès (sur des profils pouvant être définis sur la base des attributs présents).

Le service de fournisseur d'identités

Ce service s'appuie :

- sur un serveur CAS[4] pour le service d'authentification ;
- sur le référentiel pour la propagation d'attributs.

Le service CAS est configuré pour accepter une authentification soit par certificat CNRS, soit par identifiant/mot de passe, en s'appuyant pour cela sur l'annuaire (Bind LDAP).

L'identifiant retenu est l'adresse mail qui, dans le cas d'une authentification par certificat, est extraite de celui-ci. Le choix de cet identifiant, qui est fourni par Labintel, est pragmatique et n'est pas sans poser des problèmes. En particulier, la nécessaire unicité de cet identifiant n'est pas garantie par Labintel, ce qui oblige un traitement en aval pour l'obtenir.

La gestion des mots de passe (initialisation, modification...) est réalisée grâce à l'application Sesame (https://sesame.dsi.cnrs.fr).

La gestion des habilitations

La première phase du projet a consisté avant tout à mettre en place le service de fournisseur d'identités. Celui-ci s'est appuyé dans un premier temps sur l'annuaire issu de Sirhus (personnels statutaires CNRS). Il s'appuiera dans un second temps sur le nouveau référentiel qui sera mis en place en décembre 2009. Ce dernier contiendra des données issues du système d'informations actuelles et donc gérables immédiatement. En corollaire, le niveau de gestion des habilitations sera nécessairement limité car, par exemple, certaines fonctions existantes au CNRS sont absentes du SI actuel.

La phase suivante consistera principalement à augmenter les possibilités dans ce domaine en complétant le référentiel avec des données non gérées actuellement dans le SI. Ce travail impliquera :

- une spécification de ces données ;
- la mise en place d'un outil pour leur gestion.

Le choix de ces données complémentaires sera guidé par :

- la pertinence de leur présence dans le référentiel ;
- la faisabilité de leur gestion. Il ne sert à rien d'alimenter un annuaire avec des données qui ne seront pas correctement mises à jour.

Le but n'est pas de gérer les habilitations pour n'importe quelle application, les profils SAP par exemple sont gérés en interne dans SAP.

Ce système devra non seulement permettre la gestion décentralisée de ces données, mais également, à partir de la définition d'un ensemble de fonctions et de droits, de rendre possible la délégation.

2 https://spaces.internet2.edu/

3 http://federation.cru.fr/

4. CAS : Central Authentication Service

Sécurité du service

Certaines fonctionnalités du service comportent des risques particuliers qui sont discutés ci-après.

La disponibilité du service

Un service d'authentification centralisé est une application critique qui ne peut subir de défaillance de quelle que nature qu'elle soit. Pour essayer d'atteindre ce haut niveau de disponibilité, l'architecture mise en place est la suivante :

- le fournisseur d'identités et le service CAS sont installés sur deux serveurs en répartition de charge ;
- le futur référentiel consistera en deux serveurs LDAP, l'un maître et l'autre esclave, en répartition de charge ;
- l'accès réseau sera redondé.

L'unicité des comptes

Un des arguments présentés ci-dessus pour justifier le projet est d'éviter aux utilisateurs de gérer de multiples comptes en fonction des applications auxquelles ils sont amenés à se connecter. Mais le choix d'un compte personnel unique pour les utilisateurs a pour inconvénient majeur que la compromission d'un seul compte a des conséquences plus importantes, puisqu'il permet d'accéder à toutes les applications auxquelles a accès le propriétaire de ce compte. Pour limiter ce risque, plusieurs choses sont à considérer :

- une information doit être donnée aux utilisateurs pour leur faire prendre conscience de l'importance de la protection de leur compte ;
- toutes les connexions entrant en jeu dans le système sont chiffrées par l'utilisation systématique du protocole HTTPS.

Un autre problème actuel est la divulgation de compte, par exemple pour permettre à un collègue de se connecter à une application. Cette pratique devrait tendre largement à se réduire pour deux raisons :

- le système de délégation qui sera mis en place, via la gestion des habilitations, supprimera l'une des principales justifications de cette pratique. Par exemple, le directeur d'unité qui donne son compte à la secrétaire pour accéder à une application réservée aux directeurs d'unités n'aura plus de raisons de le faire s'il peut donner une délégation ;
- à partir du moment où les utilisateurs auront pris conscience de l'importance de leur compte personnel, ils seront beaucoup moins enclins à « prêter » celui-ci.

SSO et Logout

Le fournisseur d'identités Janus offre la fonctionnalité de SSO (*Single Sign On*). Cette technique permet, lorsqu'un utilisateur s'est authentifié pour accéder à une application, de ne pas avoir à le refaire s'il veut accéder à une autre application utilisant également ce fournisseur d'identités.

Cette fonctionnalité, en apportant un confort pour les utilisateurs, introduit également des risques. En effet, le problème de la déconnexion, difficile avec une technologie telle que Shibboleth, n'est pas actuellement traité dans les versions actuelles de Shibboleth. La seule possibilité offerte est la fermeture complète de la session en fermant le navigateur.

Pour autant, ce problème n'est pas vraiment nouveau, car actuellement lorsqu'un utilisateur s'authentifie pour accéder à une application, le navigateur conserve l'identifiant/mot de passe utilisé ou laisse l'accès au magasin de clés, dans le cas d'un certificat, pendant toute la session.

Par contre, la configuration de Shibboleth permet de mettre en place des timers de sessions et d'inactivités sur le fournisseur d'identités et sur chacune des applications fournisseurs de services, permettant de limiter le temps de vie d'une authentification.

Certificat ou identifiant/mot de passe ?

La méthode d'authentification sur le fournisseur d'identités est soit par certificat CNRS soit par identifiant/mot de passe. Ce choix, qui est possible grâce à l'existence de l'IGC CNRS, est pour l'instant uniquement du ressort de l'utilisateur.

Il n'est pas impossible d'envisager à terme de rendre obligatoire, pour l'accès à certaines applications, l'utilisation de certificats, éventuellement sur support physique. Cette possibilité, qui devrait être justifiée par le niveau de criticité des applications, permettrait d'augmenter significativement le niveau de sécurité des accès aux applications concernées.

Confidentialité

La technique de propagation d'attributs, offerte par Shibboleth, nécessite une réflexion sur les problèmes de confidentialité que son utilisation peut entraîner.

En particulier, il est hautement souhaitable qu'une application utilisant le fournisseur d'identités, puisse obtenir les attributs dont elle a besoin et uniquement ceux-là.

Les possibilités importantes de configuration du système offrent une entière liberté à ce sujet et permettent, au niveau de chaque application, de définir la liste des attributs qui lui seront délivrés. Cela permet d'aller jusqu'à rendre possible des accès anonymes à certaines ressources (l'application a la preuve que l'utilisateur a le droit d'accès mais ne connaît pas son identité).

Pour chaque application candidate à l'utilisation du fournisseur d'identités CNRS, il sera ainsi nécessaire d'indiquer les informations demandées et de les justifier.

En conclusion

Un projet de gestion d'identités comme Janus ne prétend pas régler tous les problèmes de sécurité. Il consiste avant tout à essayer d'utiliser un ensemble d'outils le mieux possible pour mettre en place les conditions nécessaires pour atteindre un meilleur niveau de sécurité.

En parallèle, il offre une plus-value aux utilisateurs par le biais de l'unicité de leur compte et de la fonction SSO. Il offre également aux administrateurs d'applications la possibilité de déléguer complètement la gestion de l'authentification au fournisseur d'identités et, grâce à la propagation d'attributs, des possibilités de gestion des droits. Si on ajoute à cela les futures possibilités offertes par la gestion des habilitations avec son système de délégation, on peut espérer à l'avenir limiter (voire supprimer ?) l'adoption par les utilisateurs de certains comportements à risques.

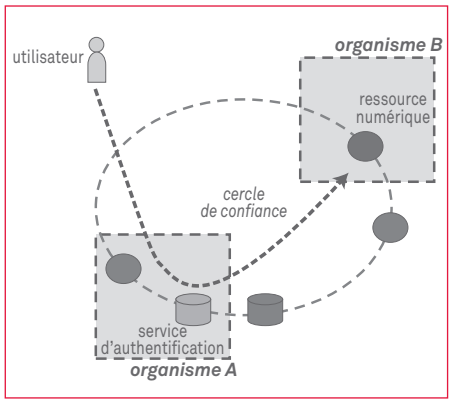
Par ailleurs, le fournisseur d'identités CNRS intégrera la fédération d'identités Renater qui démarrera à partir de février 2009. Cette fédération, qui regroupera des EPST ainsi que les universités françaises, facilitera le partage des ressources de la communauté enseignement/recherche en France.

Projet transverse par nature, un projet de gestion des identités tel que Janus entraîne avec lui tout le système d'informations. Des informations qui, jusque-là, étaient rarement à jour ou même existantes parce que non utilisées, le seront davantage, car elles seront rendues nécessaires pour accéder à certaines ressources. Or la qualité du contenu du SI est une des conditions pour obtenir un meilleur niveau de sécurité du système d'informations. ■

La fédération d'identités*

Par Olivier Salaün
salaun[aroba]cru. fr
Comité Réseaux des Universités
http://www.cru.fr/

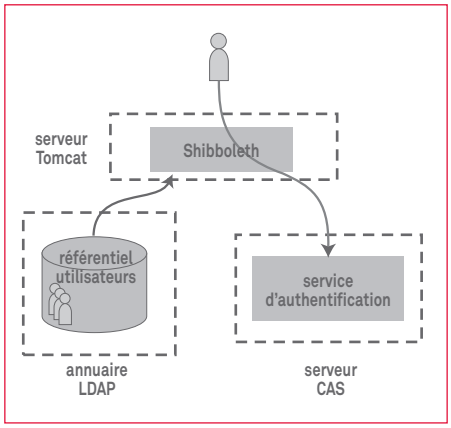
Le contrôle d'accès à certaines ressources numériques est un enjeu majeur pour les établissements d'enseignement supérieur et de recherche. En effet toutes les données publiées ne sont pas publiques ; il faut donc pouvoir authentifier les utilisateurs et contrôler l'accès à ces données ou à ces applications sans multiplier les référentiels utilisateurs. Les mécanismes de fédération d'identités permettent de transmettre un profil utilisateur à un service consommateur d'identités, en garantissant des exigences de sécurité et de protection des données personnelles. On peut dès lors généraliser de nouveaux usages : travail collaboratif, e-learning, accès nomade à la documentation électronique, distribution de logiciels commerciaux.
Le consortium Internet2 a été pionnier dans le domaine en développant le logiciel open source Shibboleth. Ce logiciel est aujourd'hui massivement utilisé dans le monde universitaire, ce qui garantit l'interopérabilité des services au niveau international.



Accès à une ressource numérique distante via la fédération d'identités.

Comment ça marche ?

L'architecture de fédération d'identités repose sur deux briques fonctionnelles : le fournisseur de services et le fournisseur d'identités. La brique Shibboleth ***fournisseur de services***, située au niveau d'une ressource numérique (cours en ligne, application), peut être considérée comme un consommateur d'identités numériques ; elle permet donc de gérer le contrôle d'accès à cette ressource. La brique Shibboleth ***fournisseur d'identités***, installée dans l'organisme de rattachement d'un utilisateur, permet de transmettre l'identité numérique de ce dernier.
Lorsqu'un utilisateur accède à la ressource numérique, il est redirigé vers le fournisseur d'identités de son organisme. Il s'authentifie auprès de son organisme, au moyen d'un identifiant et d'un mot de passe par exemple. L'utilisateur est alors renvoyé vers la ressource numérique, accompagné d'une identité numérique. La relation de confiance entre le fournisseur de services et le fournisseur d'identités garantit la confiance dans cette identité numérique. L'accès à la ressource numérique est autorisé si le profil de l'utilisateur correspond à la politique de contrôle d'accès.



Architecture d'un fournisseur d'identités Shibboleth.

Prérequis pour les organismes :

Ces mécanismes de fédération d'identités sont réalisés grâce à des briques logicielles interopérables (Shibboleth).
La brique fournisseur d'identités s'articule avec le système d'information de l'organisme. Il repose donc sur les éléments suivants :

- un référentiel utilisateur fiable (annuaire LDAP ou autre base de données) ;
- un service central d'authentification web (un serveur CAS par exemple).

L'organisme désirant mettre en place un fournisseur d'identités doit donc disposer de ces deux services.
La brique fournisseur de services s'installe aisément sur un serveur web (disponible pour Apache et pour IIS), en amont d'une application web. À moins qu'elle soit nativement compatible avec Shibboleth, l'application web devra être adaptée pour désactiver son système d'authentification natif.
Shibboleth est un mécanisme de propagation d'identités, développé par le consortium Internet2, qui regroupe 207 universités et centres de recherche. C'est une application open source, développée en Java. Elle améliore la sécurité de l'accès aux applications extérieures. De nombreuses applications supportent nativement Shibboleth.

Le service proposé par Renater

Le service de fédération sera proposé aux adhérents Renater à partir de février 2009, à l'issue d'une phase pilote. Cette phase transitoire permettra la continuité du service proposé actuellement dans le cadre de la fédération du CRU.

Documentation, formation

Renater propose des documentations techniques, en partenariat avec le CRU. Des sessions de formation seront également organisées en 2008 et en 2009, dans le cadre des formations CiRen.
La fédération Renater :
http://www.renater.fr rubrique service
Site du CRU : **http://federation.cru.fr**
Shibboleth :
http://shibboleth.internet2.edu ■

* Cet article a été publié par Renater sous l'intitulé « fiche services fédération d'identités » en septembre 2008.

Petite revue de presse

Avis de Tempest

Une étude portant sur plusieurs dizaines de claviers, en connectique filaire (USB ou PS/2), a montré qu'il était possible d'espionner les frappes d'une pièce à l'autre, grâce aux émissions électromagnétiques qu'ils émettent :

http://www.canardwifi.com/2008/10/21/pirater-les-claviers-cest-desormais-possible/

Les internautes anglophones seraient davantage victimes de vol d'identité

Et pourtant, les Français avouent transmettre sur les réseaux sociaux des données personnelles qu'ils utilisent par ailleurs comme mot de passe... et sont 61 % à avouer en changer moins d'une fois par an :

http://www.zdnet.fr/actualites/internet/0,39020774,39384348,00.htm

Sécuriser Windows XP ?

Le NIST le propose dans son guide « Guidance for Securing Microsoft Windows XP Home Edition » (en anglais) téléchargeable sur

http://csrc.nist.gov/itsec/SP800-69.pdf

Surtaxer n'est pas jouer

De plus en plus d'utilisateurs reçoivent sur leur téléphone mobile des SMS indésirables, les amenant à composer abusivement des numéros surtaxés. Pour aider à lutter contre cette malveillance, la Fédération française des télécoms met en place, en concertation avec le secrétaire d'État chargé de l'Industrie et de la Consommation, un dispositif d'alerte et de traitement permettant aux consommateurs de signaler ces SMS abusifs, via le 33700 :

http://www.minefe.gouv.fr/presse/dossiers_de_presse/081021telephonie_internet/sms_indesirables.pdf

Jack a dit Clickjacking...

Des détails concernant la faille multiplateforme surnommée « clickjacking » commencent à émerger. Une des exploitations les plus alarmantes de cette faille concerne la possibilité d'observer et d'écouter les internautes qui disposent de caméras et de micros branchés sur leurs ordinateurs :

http://www.bulletins-electroniques.com/actualites/56234.htm

http://www.zdnet.fr/actualites/informatique/0,39040745,39383973,00.htm

La diffusion des technologies de l'information dans la société française

Le baromètre du Credoc sur la diffusion des technologies de l'information dans la société française révèle, cette année, cinq évolutions majeures : une forte accélération de l'équipement des particuliers en ordinateurs personnels et en connexions à Internet haut débit ; l'explosion de la téléphonie fixe par ADSL ; le ralentissement de la diffusion du téléphone mobile ; le franc succès rencontré par l'administration électronique et les achats par Internet ; une méfiance accrue des internautes face à la protection des données personnelles sur Internet.

L'étude du Credoc est disponible sur :

http://www.arcep.fr/uploads/tx_gspublication/etude-credoc-2007.pdf

Protégez gratuitement votre PC sous Windows

De l'antivirus au pare-feu, en passant par le nettoyage ou le renforcement du système, il n'y a plus d'excuse pour ne pas se protéger :

http://www.indexel.net/1_6_4944__3_/2/12/1/Protegez_gratuitement_votre_PC_sous_Windows.htm

Quatre logiciels antispyware gratuits :

http://www.indexel.net/1_6_5297__3_/15/90/1/Quatre_logiciels_antispyware_gratuits.htm

Sept ouvrages pour améliorer la sécurité de votre SI :

http://www.indexel.net/1_6_5096__3_/2/12/1/7_ouvrages_pour_ameliorer_la_securite_de_votre_SI.htm

Cours de piratage des systèmes de vote électroniques aux États-Unis

Des étudiants de l'université Rice ont suivi un cours de sécurité informatique durant lequel ils ont dû faire de leur mieux pour altérer des machines à voter électroniques. Objectif : tester leur vulnérabilité :

http://www.atelier.fr/securite/10/09102008/vote-electronique-securite-universite-rice-37268-.html

Le premier réseau de cryptographie quantique au monde activé à Vienne

Des scientifiques ont annoncé avoir activé à Vienne le premier réseau de télécommunication au monde sécurisé au moyen de la cryptographie quantique, dans le cadre du projet européen Secoqc auquel participent plusieurs unités du CNRS (**http://www.secoqc.net/html/project/partners.html**). Des données cryptées, y compris une vidéoconférence, ont été transmises lors d'une conférence internationale entre six centres espacés de jusqu'à 85 kilomètres via des fibres optiques standard, ouvrant la voie à une application de cette technologie très complexe aux réseaux de télécommunication courants :

http://www.promethee.fr/actus/index.php?2008/10/08/337-le-premier-reseau-de-cryptographie-quantique-au-monde-active-a-vienne

Skype, un botnet ?

C'est ce que démontre Cédric Blanchet sur :

http://sid.rstack.org/pres/0606_Recon_Skype_Botnet.pdf

On peut aussi relire les supports de l'intervention de Fabrice Desclaux et Kostya Kortchinsky à la conférence RECON 2006 :

http://2006.recon.cx/en/f/vskype-part2.pdf

Effacer d'une manière sécurisée un disque dur

Un « Live CD » pour effacer d'une manière sécurisée le contenu d'un disque dur :

http://www.ultimatebootcd.com/

... mais, pour certains, la seule méthode efficace est la méthode radicale :

http://hackaday.com/2008/09/16/how-to-thermite-based-hard-drive-anti-forensic-destruction/

Un livre blanc de l'Enisa sur quelques techniques d'ingénierie sociale

L'ingénierie sociale se réfère à des techniques de manipulation qui se ramènent à convaincre quelqu'un d'effectuer de son plein gré une transgression ou une divulgation d'informations confidentielles. Ces attaques sont devenues un problème de sécurité d'autant plus important qu'il faut bien reconnaître qu'il est souvent plus facile à un pirate d'exploiter les utilisateurs que la technologie.

http://www.enisa.europa.eu/doc/pdf/publications/enisa_whitepaper_social_engineering.pdf

La vie privée et la technologie

Le magazine *Scientific American* (http://www.sciam.com/sciammag/?contents=2008-09) consacre son numéro de septembre à la vie privée et aux défis qu'elle adresse aux spécialistes de la sécurité. Lire à ce sujet l'article du webzine « Internet Actu. net » :

http://www.internetactu.net/2008/09/17/la-vie-privee-et-la-technologie/

L'iPhone d'Apple espion malgré lui ?

Pour obtenir les effets graphiques de transition entre deux applications, l'iPhone garde en mémoire les dernières données consultées par son utilisateur, selon un expert. Une technique pouvant permettre à celui-ci, mais aussi à des pirates, de retrouver des données.

http://www.businessmobile.fr/actualites/technologies/0,39044306,39383242,00.htm

Laposte.net a diffusé involontairement une publicité piégée

Mardi 2 septembre, une fausse alerte de sécurité était diffusée sur le webmail de La Poste, invitant les utilisateurs à télécharger un logiciel de sécurité contenant un spyware :

http://www.01net.com/editorial/389835/laposte.net-a-diffuse-involontairement-une-publicite-piegee/

Les « bidouilleurs » de la société de l'information

- « Y aura-t-il un scandale Sesam Vitale ? », par Jean-Marc Manach, *InternetActu*,

http://www.internetactu.net/2005/09/09/yaura-t-il-un-scandale-sesam-vitale/

- Mifare Classic : « La sécurité de millions de cartes à puce sans contact sérieusement remise en question », par David Maume, *01net*,

http://www.01net.com/editorial/387107/la-securite-de-millions-de-cartes-a-puce-sanscontact-serieusement-remise-en-question/

- Flash Eurobaromètre n° 225 : « La protection des données au sein de l'Union européenne - Les perceptions des contrôleurs de données - Perceptions des citoyens » (PDF), **http://ec.europa.eu/public_opinion/flash/fl_226_fr.pdf** et pour une analyse : « Informatique et libertés : les Français sont nuls » (J.-M.M.), *InternetActu*,

http://www.internetactu.net/2008/06/02/informatique-et-libertes-les-francais-sont-nuls/

- TV B Gone, la télécommande universelle permettant d'éteindre tous les postes de télévision auprès desquels on passe : **http://www.tvbgone.com**
- La culture *hack* du Massachusetts Institute of Technology (MIT) : **http://hacks.mit.edu**
- Hacker Space Festival : **http://www.hackerspace.net**
- Le Lab : **http://www.tmplab.org**
- TechShop : **http://techshop.ws**
- Les imprimantes 3D : **http://blog.reprap.org**
- Le Chaos Computer Club (Allemagne) : **http://www.ccc.de**, « Le Chaos Computer Club (CCC) concrétise le débat sur la biométrie et les empreintes digitales de Schäuble », par Stephan M., *Les Dessous de l'Allemagne* : **http://allemagne-et-plus.a18t.net/?p=26**
- Foebud : **http://www.foebud.org**

Informations collectées par R. L.

Avec son portail, la DCSSI rend la SSI accessible à tous

Les machines de bureau comme celles de salon, le réseau ADSL qu'on a chez soi comme celui en Ethernet 100 Mbit/s sur fibre optique de certains de nos laboratoires, les grands centres de calculs comme le petit ordinateur de secrétariat, toute cette belle technologie, suivant les besoins, doit être protégée nous dit-on ... Mais sait-on toujours très bien comment ou pourquoi ?

Le nouveau portail de la DCSSI (**http://www.securite-informatique.gouv.fr**) répond à ce besoin. Il s'annonce tant comme un outil de travail indispensable pour les professionnels que comme une mine d'informations pour les particuliers un peu sensibilisés à la SSI.

Par exemple on y trouve les dix commandements de la sécurité sur l'internet (**http://www.securite-informatique.gouv.fr/gp_rubrique34.html**), tout un jeu de fiches techniques classées par ordre alphabétique (**http://www.securite-informatique.gouv.fr/gp_mot4.html**), les principaux guides de configuration dont on peut avoir besoin (**http://www.securite-informatique.gouv.fr/gp_mot2.html**), toutes sortes de mémentos bien utiles (**http://www.securite-informatique.gouv.fr/gp_mot1.html**), ainsi que des modules d'autoformation sur divers sujets (**http://www.securite-informatique.gouv.fr/gp_mot24.html**).

On y trouve encore, dans l'actualité de la SSI, une revue des alertes de sécurité avec leur analyse (**http://www.securite-informatique.gouv.fr/gp_rubrique9.html**), les faits marquants (**http://www.securite-informatique.gouv.fr/gp_rubrique10.html**) et enfin des analyses techniques (**http://www.securite-informatique.gouv.fr/gp_rubrique69.html**).

Et puisque ce numéro spécial traite de la fédération d'identités, il est naturel de vous inviter à vous reporter au module autoformation sur l'authentification (**http://www.securite-informatique.gouv.fr/gp_article261.html**), vous vous rendrez compte ainsi de la grande qualité du portail de la DCSSI... et vous pourrez évaluer votre compréhension des articles de ce bulletin.

»» suite de l'Éditorial, page 1

CNRS ne fasse pas cavalier seul ». C'est effectivement dans un esprit de partage des compétences et de mutualisation des solutions que l'Urec[3] collabore étroitement avec le CRU et la DSI[4] de l'Inria[5], en particulier dans divers groupes de travail Renater[6] et des manifestations autour des JRES[7]. Patrick Lagadec, Directeur de Recherche du CNRS à l'École Polytechnique, montre bien la nécessité de ces petits groupes réactifs, composés de personnes de formations et d'expériences différentes, d'approches complémentaires, pour répondre aux crises « hors cadre ». Les fédérations d'identités sont, à cet égard, des projets typiques de synergie des acteurs. Ainsi, Janus s'intégrera naturellement dans la fédération Renater qu'Olivier Salaün présente dans son article.

Si on se réfère à Wikipédia ou à l'Encyclopedia Universalis, Janus est une divinité romaine veillant sur le seuil de la maison, protégeant le passage de l'intérieur vers l'extérieur (et inversement), assurant finalement le passage du monde des hommes à celui des dieux et, à ce titre, toujours invoqué au début de toute prière rituelle. En ce sens, le nom de Janus exprime parfaitement ce que tant le Comité d'Évaluation des Systèmes d'Information que l'Inist[8] et, au-delà, les unités de recherche, attendent de ce projet : être le moyen d'authentification unique pour toutes les applications. À cette fin, nous proposerons en 2009 des formations de sensibilisation pour montrer comment les applications de recherche peuvent s'intégrer à Janus et quel intérêt les utilisateurs y trouveront.

[3] http://www.urec.fr/
[4] Direction des Systèmes d'Information
[5] http://www.inria.fr/
[6] http://www.renater.fr/
[7] http://www.jres.org/
[8] http://www.inist.fr/

SÉCURITÉ DE L'INFORMATION
Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
Joseph Illand
Fonctionnaire de Sécurité de Défense
Centre national de la recherche scientifique
3, rue Michel-Ange, 75794 Paris cedex 16
Tél. : 01 44 96 41 88
Courriel : joseph.illand[aroba]cnrs-dir. fr
http://www.sg.cnrs.fr/fsd

Rédacteur en chef :
Robert Longeon
Chargé de mission SSI du CNRS
Courriel : robert.longeon[aroba]cnrs-dir. fr

Impression : Bialec, Nancy (France) - D.L. n° 70381

ISSN 1257-8819