

Bruno BONFILS

<bbonfils@opencsi.com>

Ingénieur systèmes, réseaux et sécurité

Compétences fonctionnelles

- Chef de projet
- Consultant IAM / PKI

Compétences techniques

<i>Systèmes d'exploitation</i>	Solaris, Linux, Windows 2000/2003/2008
<i>Réseaux</i>	IPv4, notions d'IPv6, VPN (SSL, IPSec)
<i>Serveur d'applications</i>	JBoss, Glassfish, Tomcat, WebLogic
<i>Scripting</i>	Python, Shells
<i>Sécurité</i>	PKI (X509v3, horodatage, signature, workflow), XadES, RBAC, Radius, SAMLv2
<i>Annuaire</i>	Administration et architecture LDAP (OpenLDAP, Sun One Directory Server), OpenDJ
<i>Conception</i>	UML, Merise
<i>SSO</i>	CAS (Central Authentication Service), OpenAM, Microsoft ADFS

État civil

<i>Né le</i>	24 Mai 1980 à Troyes (10)
<i>Nationalité</i>	Française
<i>Situation familiale</i>	Célibataire
<i>Divers</i>	Permis de conduire

Expériences professionnelles

04/2011 à ce jour	SAS OpenCSI Fondateur
-------------------	--------------------------

SER2S : Administrateur système

Gestion de la plateforme de développement composé de plusieurs clusters de virtualisation Proxmox. Administration et supervision des clusters, des machines virtuelles, des services associés. Gestion des habilitation (LDAP, SSO). Gestion de la politique de sauvegarde (bacula).

Participation à des projets liés aux nouveaux moyens de paiements.

Environnement : EJBCA, HSM SafeNet, WebSphere

Euler Hermes France : Conseil sécurité

En renfort de l'équipe RSSI du groupe Euler Hermes, je suis amené à intervenir sur différents sujets de fond, notamment la refonte réseau et les problématiques d'isolations, les différents accès utilisateurs (internes, externes, invités), le durcissement sécuritaire dans les développements d'applications, et d'autres sujets comme le renforcement de l'authentification/autorisation entre WebServices (architecture SOA).

Euler Hermes France : Conseil PKI

En charge de la mise en place d'une PKI destinée à délivrer des certificats aux clients de la société. Accompagnement, suivi et tests fonctionnels de la RA développé par les équipes du client. Support aux clients d'Euler Hermes pour la mise en œuvre de l'authentification par certificat.

Environnement : EJBCA, HSM SafeNet, WebSphere

SER2S : Conseil PKI

Conseil technique et fonctionnel sur la mise en œuvre d'une PKI destiné à délivrer plusieurs types de certificats :

- Certificats utilisateurs internes, pour authentification par carte à puces sur poste Windows
- Certificats clients, utilisés pour accéder à des applications critiques

Environnement : EJBCA, HSM nCipher

SACEM : Cartographie du Système d'Information

Accompagnement technique et fonctionnel sur la mise en place d'un outil permettant la cartographie complète du système d'information du client pour permettre l'analyse de dépendances d'impact à partir de n'importe quelle composant technique du SI, ou composant fonctionnel (Business Process).

Environnement : iTop, ITIL

SACEM : Migration SSO

Première phase : étude des besoins et l'existant du client pour remplacer leur solution de SSO existante basée sur Oracle SSO : rédaction d'une proposition d'architecture.

Seconde phase : implémentation technique de la solution proposée.

Environnement : OpenAM

04/2009 à 04/2011

RTL

Responsable système et réseau

Refonte de l'infrastructure Web hébergeant les différents sites du groupe (notamment www.rtl.fr) en collaboration avec les équipes en charge du développement des différentes applications ainsi que du responsable de l'équipe éditoriale.

Refonte du stockage de l'ensemble du groupe.

Mise en place d'une solution de déploiement continu pour faciliter la montée de version des applications (solution présentée lors d'une conférence devops à Paris).

Environnement : Solaris, Linux, Windows. Hitachi AMS 2500

09/2006 à 11/2008

Groupe LINAGORA, SA, Paris. Société de services en logiciels libres

Chef de projet de l'équipe sécurité

Société Générale (projet de mai 2008 à sept. 2008), Chef de projet (projet CRYPTO)

Contexte : La société générale souhaite délivrer des certificats de chiffrement de manière très simple à l'ensemble de ses collaborateurs (internes et prestataires).

En charge du suivi du projet de développement d'une RA (Registration Authority) fonctionnelle basé sur un framework de workflow (JBPM) permettant aux administrateurs de modifier le comportement de l'application. Rédaction des spécifications techniques et fonctionnelles. Suivi de l'assurance qualité sur l'ensemble des livrables.

Environnement: Redhat 4 x86, EJBCA 3.6, SafeNet HSM

Région Wallone (janvier 2008 à avril 2008), Chef de projet (signature numérique)

Contexte : Les citoyens belges disposent d'une carte d'identité électronique contenant des certificats. La région de la Wallonie dispose d'une suite d'application Web et d'une applet de signature permettant aux citoyens de remplir des formulaires administratifs et de les signer en utilisant leur certificat contenu dans leur carte d'identité.

Évolution d'une applet existante pour y ajouter des nouvelles fonctionnalités (XAdES 1.3.2, co/contre signature). Rédaction de spécifications fonctionnelles, techniques, suivi des développements.

Environnement: XAdES

CertEurope (projet de sept. 2007 à déc. 2007) Chef de projet : Projet de SSO

Mise en place d'une solution de SSO (basé sur CAS) permettant une authentification unique (multi-domaines) entre plusieurs applications hébergées par différentes entités. Recherche de solution technique. Rédaction des spécifications fonctionnelles et techniques (notamment en UML). Développement d'un module Apache permettant l'authentification des utilisateurs auprès du serveur CAS, la simulation d'une authentification par certificat, et la gestion des habilitations (URL par URL) des utilisateurs au sein de l'application protégée par le module.

- Patch du binding Perl Crypt::OpenSSL::X509

- Patch de mod_ssl
- Patch openssl

Environnement: Redhat 4 x86, CAS, Apache 2, Perl, mod_perl 2

GIE Cartes bancaires (projet d'août 2007 à oct. 2007), Chef de projet : PKI

Intégration d'une PKI pour le service RMA (Risk Management et Audit) du GIE Cartes bancaires. Suivi du développement spécifique, recette, documentation, installation, formation du personnel à l'utilisation d'un HSM et du logiciel EJBCA. Aide à la rédaction et participation à la cérémonie des clés officielle.

Environnement: Redhat 4 x86, EJBCA 3.5, nCipher HSM

GIE Cartes bancaires (depuis mars 2007) régime de 2 jours par semaine) : Administration système

Administration des serveurs (principalement Solaris 10) de la partie extranet du GIE Cartes bancaires, aussi bien au niveau système qu'au niveau des applications, composé de serveurs LDAP Sun, Java Enterprise System 5, des serveurs d'applications Glassfish, PostgreSQL, etc. Utilisation massive des zones Solaris 10 pour la segmentation des applications et des droits dans différents conteneurs, mise en place de la gestion des ressources CPU.

Aide à la mise en production de la PKI au sein de nombreux acteurs comme un annuaire LDAP, un HSM nCipher, le logiciel d'émission des cartes à puces BlueX d'AET, un domaine Active Directory pour l'authentification par cartes à puces, et les nombreux services (notamment Access Manager pour le SSO) utilisant les certificats pour l'authentification.

Environnement logiciel : EJBCA, Solaris 10, Redhat Linux 4 ; Sun One Directory Server 5.x, 6.x ; Sun Application Server 7 ; Glassfish v2 ; PostgreSQL

Environnement matériel : Sun T2000, Sun Fire x4200, Sun v40z, Sun Blade 6000, Sun Blade 8000, nCipher netHSM.

Assemblée Nationale Française (de mars 2007 à juillet 2007), chef de projet technique : création d'un poste de travail Linux

Contexte : suite à une décision (en novembre 2006) des questeurs de l'assemblée nationale, cette dernière à émis un appel d'offre en janvier 2007 concernant la réalisation (et le support) d'un poste de travail basé sur le système d'exploitation libre Linux, pour une mise en production en juin.

Aide à la rédaction de la réponse à l'appel d'offre, notamment sur les aspects de sécurité (authentification 802.1x avec mise à jour du mot de passe local permettant l'utilisation d'un poste en mode déconnecté).

Recherche des problèmes légaux, notamment ceux liés à l'utilisation de logiciels libres pour la lecture des fichiers multimédias.

Gestion des parties techniques du projet, attribution et suivi des tâches. Rédaction des documentations. Architecture et installation des serveurs et des outils nécessaire à une gestion de parc centralisée.

Environnement : KUbuntu, FAI (Full Automated Installation), Freeradius avec authentification par LDAP, 802.1x (spécification d'un module PAM)

Conseil général des bouches du Rhône (de novembre 2006 à décembre 2006), chef de projet : migration des services Internes

Migration des services DNS, DHCP, et authentification VPN vers Linux. Spécifications des scripts permettant la conversion des données provenant du SI du CG13 au format des logiciels Bind9, DHCPd et Freeradius. Planification et réalisation de la migration vers les nouveaux serveurs sans interruption de service. Formation des administrateurs CG13 à freeradius.

Environnement : Fedora Core, ISC Bind 9, ISC DHCP, Python, Freeradius, Syslog-ng

GIE Cartes Bancaires (septembre 2006 à février 2007), administrateur système : PKI

Intégration de la PKI EJBCA au sein de l'intranet du GIE Cartes Bancaires. Suivi des développements, recette, documentation. Aide à la rédaction de la cérémonie des clés.

Environnement : Solaris 10, NetHSM de nCipher, EJBCA

Recherche

Au sein de l'équipe réseau du premier opérateur normé ISO 9001 2000, ma tâche consista à rechercher, tester différents matériels réseaux nécessaire pour assurer la croissance et l'évolution de l'infrastructure. La normalisation ISO impose une rigueur au niveau des documentations (installation, configuration, maintenance, exploitation).

- Réseaux
 - Recherche, étude, documentation de la solution VPN SSL (Firepass) avec utilisation d'un annuaire LDAP pour le mapping des utilisateurs et des profils. Isolation totale des différents clients à l'aide de multiple tables de routages et l'utilisation du 802.1q
 - Test de QoS (entre CPE et équipement de collecte Redback)
 - Mise en place d'une architecture complète de tests xDSL (modem, DSLAM, L2TP)
 - Développement (en ruby et Perl) de webservices permettant l'automatisation du provisionning

Environnement : Juniper M7i, NetScreen 500, Redback, Avilinks, FirePass, BigIP

Refonte de l'architecture systèmes et réseaux

Tout en assurant la maintenance des 50 serveurs (composés de Windows NT4 à 2003, HP-UX 11, AIX, Solaris 8 à 10) et l'interopérabilité, mon travail consistait à la refonte totale de l'architecture réseaux, nécessaire à la croissance de la société (de 50 à 150, avec des partenaires étrangers).

- Réseaux
 - Segmentation du réseau (VLAN)
 - Sécurisation de la partie publique (DMZ à deux niveaux protégée par des ponts filtrants)
 - QoS (niveaux 2 et 3, principalement sur IOS)
 - Supervision (installation d'un collecteur NetFlow, développement de scripts, notamment pour superviser la QoS)
 - Externalisation (interne -> Colt) de la salle serveur (recherche de prestataire, planification et suivi de la migration) avec seulement 48h d'indisponibilité
 - Interconnexions multiples avec fournisseurs et prestataires via IPSec (LAN 2 LAN)
- Systèmes
 - Installation d'un serveur Solaris Jumpstart (pour les versions 9 et 10) permettant l'installation automatique des serveurs
 - Centralisation des informations des comptes externes dans un annuaire LDAP (Sun One Directory Server 5.x)
 - Supervision des serveurs
 - Remise au propre de toute la partie backup (recherche de nouveau matériel, réécriture des politiques de sauvegarde)
 - Mise en production de Solaris 10 (utilisation massive des zones, écriture de manifest SMF, utilisation des gestions de ressources permettant la segmentation CPU des différentes zones)
- Sécurité
 - Sécurisation des serveurs publics (durcissement noyau à l'aide du patch GRSec)
 - Installation de la PKI EJBCA permettant la gestion des certificats serveurs
 - Nombreuses politiques de filtrage IP (iptables, ipf)
 - R&D sur le support du SSO dans les applications de l'entreprise (Kerberos, JAAS)

Environnement : Cisco 3550, 3560, 2610, 3005 ; OSPF ; Solaris ; AIX ; HP-UX ; Linux ; Windows ; Dell PowerVault 136T, Veritas Backup Exec

Mise en production d'une infrastructure tolérante à la panne

En parallèle du support client (tous niveaux), et après une analyse de l'existant et des nouveaux besoins, j'ai centralisé l'ensemble des informations systèmes (comptes Unix / mails, alias mails, domaines, etc.) vers un annuaire LDAP (OpenLDAP). J'ai ensuite déployé un dispositif permettant d'assurer une répartition de charge des services HTTP et une haute disponibilité des services annexes (OpenLDAP, base de données), en réduisant au maximum les points de défaillance unique (SPOF).

- Systèmes
 - Centralisation des données systèmes dans un annuaire LDAP (script de migration, d'administration, de supervision)
 - Recherche et mise en production d'une solution de répartition de charge et de haute disponibilité (LVS, Heartbeat)
 - Supervision (Nagios et Cacti)
- Réseaux
 - Mise en production de LVS (Linux Virtual Server)
 - Filtrage (iptables et ipf)
- Développement
 - Développement d'une bibliothèque Perl permettant la configuration des hôtes virtuels HTTP dans IIS à l'aide des interfaces COM, permettant l'automatisation du provisionning des sites hébergés sous Windows
 - Développement d'une interface d'administration client orienté utilisateurs finaux

Environnement : Debian GNU/Linux, Windows 2000, FreeBSD

Formation professionnelles

- Veritas Backup Exec (Janvier 2005)

Formations scolaire

- 2001 à 2003 : BTS Informatique de gestion (ARLE) en alternance, AMGE (Strasbourg)
- 2000 : Première année DEUG MIAS
- 1999 : Bac S

Langues

- Anglais : Courant
- Français : Langue maternelle

Implication dans le milieu OpenSource

- 1998 : Publication d'un article sur GTK dans Linux Magazine n°2
- 2000 : Fondateur du site communautaire debian-fr.org (rédaction de 34 articles)
- 2002 : Publication d'un article sur Caudium dans Linux Magazine n°33
- 2003 : Conférence aux JDLL (Journée des logiciels libres) à Lyon sur les solutions de haute disponibilité sur Linux
- 2006 : Membre fondateur de l'association 1901 GUSES (Groupe d'utilisateur du système d'exploitation (Open)Solaris)
- 2006 : Conférences sur la PKI : Lyon, Maubeuges, Strasbourg, Calais (université)
- 2007 : Conférence aux RMLL (Rencontre Mondiales des Logiciels Libres) à Amiens, sur le fonctionnement de zfs et des zones OpenSolaris
- 2007 : Fondateur du site communautaire <http://sysadmin.asyd.net/>
- 2008 : Conférence sur OpenSolaris aux RMLL
- 2008 : Conférence sur la signature numérique aux RMLL