Jeudi 30 septembre 2010

TELECOM ParisTech (ENST)
de 9H à 18H

Amphi Thévenin
46, rue Barrault - 75013 Paris

ARCSI 2010

Cryptologie et SSI de demain

en partenariat avec TELECOM PARISTECH.

Demain*, un monde virtuel plus sûr ?

ARCSI 2008 avait été l'occasion de mesurer le chemin parcouru depuis l'origine des temps et de décrire l'état de l'art atteint en matière de sécurité de l'information. ARCSI 2010 a l'ambition d'éclairer l'avenir.

La marche vers la dématérialisation de l'information est inexorable. En devenant numérique pour être plus efficace, celle-ci est, en contre partie, soumise à tous les risques d'altération, de corruption et d'usurpation du monde virtuel, bien supérieurs à ce qu'ils sont dans le monde réel. Certes, les interceptions et les vols de documents ont toujours existé, comme les faux en écriture, les falsifications de preuves ou encore la fausse monnaie. L'arrivée de l'électricité puis de l'électronique avait déjà révolutionné les transmissions et par voie de conséquence les modes d'action des prédateurs. Mais aujourd'hui les technologies de l'information offrent des possibilités d'actions malveillantes d'une toute autre ampleur et d'une très grande variété. Ainsi, au-delà des systèmes d'information traditionnellement visés (télécommunications, messageries, systèmes de paiement, etc.) se sont ajoutés tous les systèmes automatisés assurant des fonctions critiques pour le bon fonctionnement des infrastructures vitales de notre pays.

Face à ces nouvelles menaces des parades ont été développées mais :

- A-t-on pris la juste mesure des risques à venir ?
- Les techniques de protection mises en œuvre ou envisagées sont-elles à la hauteur des enjeux ?
- La cryptologie, pilier historique de la SSI continuera-t-elle à jouer un rôle majeur ?
- L'Internet du futur restera-t-il cet espace de liberté si cher à ses promoteurs ?
- Ou, face aux dérives qu'il autorise, sera-t-il soumis à un contrôle plus rigoureux des Etats ?

A toutes ces questions, ARCSI 2010 tentera d'apporter des réponses d'ordre technique, juridique et éthique à travers les interventions d'éminents spécialistes comme de hauts responsables de l'administration.

* Hier, en 1650, La Rochefoucauld écrivait : **« Celui à qui vous dites votre secret devient maître de votre liberté. »**

ENTREE GRATUITE POUR TOUS.

Possibilité de déjeuner sur place au restaurant de TELECOM ParisTech. Ticket repas à 20€ délivré à l'accueil de l'Amphi Thévenin. Le repas sera gratuit pour les adhérents de l'ARCSI et les étudiants, sur présentation de leur carte.

Inscription obligatoire en ligne sur le site :
http://www.arcsi.fr/

PROGRAMME DU 6ème COLLOQUE
ARCSI 2010

Cryptologie et SSI de demain

- 08h15 : Accueil

- 09h00 : **Général (2s) Jean-Louis DESVIGNES** - Président de l'ARCSI.
Allocution d'ouverture

- 09h30 : **Bernard BARBIER** - Directeur technique de la DGSE.

Exposé : Internet, défis et enjeux pour la cryptographie et le renseignement technique.

En 2010 plus de 5 milliards de systèmes (PC, téléphones) se connectent à l'INTERNET: quels sont les défis et les enjeux pour la cryptographie et le renseignement technique.

- 10h15 : **Jean-Jacques QUISQUATER** - Professeur de cryptologie à l'Université catholique de Louvain-la-Neuve, Belgique

En plus d'avoir publié environ deux cents papiers et 20 brevets dans le domaine de la cryptologie, Jean-Jacques Quisquater a aussi travaillé en théorie des graphes. Il a élargi récemment son domaine de recherches en étudiant les cordes à nœuds, khipus, des Incas. Il a un doctorat d'Etat de l'Université d'Orsay et a enseigné, avec Jacques Stern, la cryptologie à l'ENS entre 1991 et 2002. C'est aujourd'hui son dernier jour de travail à temps plein ...

Exposé : Le RSA sera-t-il notre Titanic ? Le futur de la cryptologie.

Partons du principe de Kerkhoffs (1883), aussi formulé comme la maxime de Shannon : la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef. Mais sur quoi doit reposer la sécurité d'un système globalement ? La cryptographie quantique nous prévient gentiment à l'avance que certains cryptosystèmes pourraient vite céder et que la longueur des clés doit au minimum doubler. Il serait intéressant de voir toutes les hypothèses sous-jacentes mais nous allons nous concentrer sur le fait que certaines optimisations d'attaques ont pu passées inaperçues mais pas à tout le monde. Comment concevoir des systèmes qui résistent aux cassages des cryptosystèmes ? A quand le Titanic (14 avril 1912) de la cryptographie, que sera l'iceberg et avons-nous assez de canots de sauvetage ?

- **11H00** : ***Pause***

- 11h30 : **Henri GILBERT** - Responsable du laboratoire de cryptologie de l'ANSSI**.**

Exposé : Fonctions de hachage - la compétition SHA-3.

Dans la boîte à outils des algorithmes cryptographiques sur lesquels repose la sécurité des systèmes d'information, les fonctions de hachage disputent aux primitives de chiffrement la place du couteau suisse. Cependant, la solidité des fonctions de hachage actuellement les plus utilisées (MD5 et SHA-1, conçues dans les années 90) est insuffisante pour assurer une protection durable de ces systèmes : les progrès de la cryptanalyse au début des années 2000 ont en effet conduit à un effondrement de la sécurité pratique offerte par MD5 et à une remise en question de la sécurité offerte à moyen terme par SHA-1. Cette situation est à l'origine de l'initiative du National Institute of Standards and Technology américain (NIST) d'organiser une compétition internationale d'une durée de quatre ans qui doit aboutir en 2012 à la sélection d'une nouvelle fonction de hachage normalisée, SHA-3. Plusieurs équipes françaises participent à cette compétition.

- 12h15 : **Michel RIGUIDEL** - Professeur émérite à Télécom ParisTech (ENST).

Professeur émérite au Département Informatique et Réseaux à Telecom ParisTech, et précédemment directeur de ce département jusqu'en 2009. Il enseigne la sécurité numérique et les réseaux de nouvelle génération. Il dirige des recherches sur la sécurité de l'Internet du Futur et sur la protection des infrastructures critiques.
Il est expert à l'ANR, membre du Conseil d'Evaluation du métier Télécommunications à la DGA, et expert à la Commission Européenne. Dans le FP7 européen, il coordonne les projets de feuille de route de recherche en sécurité : sécurité du futur Internet, recherche européenne en sécurité en coopération avec les Etats-Unis.
Aujourd'hui en position de retraité, il est devenu auto-entrepreneur : Conseil en informatique, réseau et sécurité.

Exposé : Des fissures dans l'édifice cryptologique ? Les perspectives en sécurité numérique.

- **13H00** : ***Déjeuner***

- 14H30 : Garance **MATHIAS et Marc BLANCHARD**

Garance MATHIAS :

De formation universitaire orientée en droit des contrats (mémoire sur la sécurité du paiement électronique), en droit des Ressources Humaines et a été récemment complétée par la formation IERSE (L'Institut d'Etudes et de Recherche pour la Sécurité des Entreprises - au sein de la gendarmerie nationale), après quelques années au sein des cabinets internationaux - département NTIC (Deloitte&Touch, Denton,etc.), Garance Mathias a décidé de créer une structure, en 2003, dédiée à l'activité des entreprises et plus particulièrement aux problématiques de sécurité informatique, de contrats tant en Conseil qu'en Contentieux.

Marc BLANCHARD - Epidémiologiste, Virus Docteur

Directeur des Laboratoires de Recherches Technologiques & Scientifiques, Editions Profil / BitDefender - 2009
Ancien Directeur des TechLabs Doctor Web France - 2008
Ancien Directeur de L'ESAC European Scientific Antivirus Centre Kaspersky - 2003
Ancien Directeur du Centre de Recherches Trend Micro - 1996
Ancien Virus Docteur Central Point Software – 1991
Membre actif du RECIF Recherches en Criminalité Informatiques

Les recherches de Marc Blanchard ont une particularité originale : elles sont orientées sur l'épidémiologie et les prédictions futures. Il a ainsi développé et mis au point un système taxinomique, permettant un rapprochement des techniques et technologies utilisées par les codes malicieux. En fonction des technologies, le système permet d'établir des calques permettant de définir des probabilités de propagations sur des futurs proches, non encore existantes. C'est la raison pour laquelle de nombreuses prédictions telles que l'arrivée des codes malveillants comme loveletter, l'utilisation des ports TCP/IP, des infections actives, des codes modulaires, etc., avaient été prédites en collèges scientifiques entre experts ces dernières années avant même leurs apparitions.
Aujourd'hui, ces recherches sont orientées essentiellement sur les Ghostnets, réseaux parallèles ayant pour mission de déstabiliser les gouvernements/ministères et grandes industries françaises de productions et de gestion de l'eau, d'électricité, etc.

Exposé : Ghostnets - Des attaques d'aujourd'hui vers les attaques du futur - Réaction juridique.

Notre présentation permet de mieux cerner, notamment à l'aide de démonstrations, les codes malveillants de dernières générations et leurs évolutions, l'évolution des attaques afin de mieux tenter d'appréhender leurs conséquences sur les postes des utilisateurs, serveurs d'entreprises (déni de service, ...), y compris sur le plan juridique.
L'aspect juridique dressera un état des lieux tant de la réglementation que de la jurisprudence ainsi que les éventuelles évolutions....

- 15H30 : **Philippe PAINCHAULT** - Responsable des solutions SSI chez Thalès – spécialiste du Quantique.

De formation X-ENST, Expert cryptologue à THALES depuis 15 ans, ce qui inclut la réalisation d'études cryptographiques fondamentales, notamment pour l'administration française, mais aussi la définition d'algorithmes ou de protocoles de sécurité pour les différents équipements THALES.

Exposé : Cryptographie quantique : sécurité et applications.

La cryptographie quantique est un outil permettant potentiellement d'obtenir une sécurité importante, mais son implantation comporte des restrictions pouvant affecter cette sécurité. Les principes sont ici rappelés, ce qui permet ensuite d'expliciter précisément les apports de sécurité d'une telle solution, selon le type de réalisation choisie. Enfin, le projet européen Secoqc est décrit brièvement, afin d'illustrer ce que peut offrir un système quantique aujourd'hui.

- **16H15** : ***Pause***

- 16H40: **Philippe WOLF -** Conseiller du Directeur général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Ancien élève de l'École Polytechnique (1978), docteur en Informatique (1985) de l'Université Pierre et Marie Curie, Paris 6ème et ingénieur général de l'Armement, M. Philippe WOLF fut responsable du département « sécurité électronique et informatique » du Centre d'Électronique de l'Armement (CELAr) à Bruz (1985-1995). Il fut Directeur des études de l'École Polytechnique à Palaiseau (1995-2000). En octobre 2000, il a été nommé Directeur du Centre de formation à la sécurité des systèmes d'information (CFSSI) puis Sous-directeur « Télécommunications et Réseaux Sécurisés » au Secrétariat général de la défense nationale (2005-2008).
M. Philippe WOLF enseigne l'« Intelligence économique, Société de l'information et Société de la désinformation » à l'École Polytechnique, la « Connaissance des réseaux et sécurité », dans le Master « Droit de l'internet public

(administration – entreprises) », Université Paris 1 Panthéon-Sorbonne. Il donne des cours et conférences à l'École des Mines-ParisTech, à l'École Nationale d'Administration et à l'Institut des hautes études de défense nationale. Il publie régulièrement des articles sur la sécurité dans le cyberespace.
Chevalier de la Légion d'honneur et officier de l'ordre national du mérite, il est ancien auditeur de la 44ème session du centre des hautes études de l'armement.

Exposé : Le futur de la SSI : défense passive ou défense active ?

- 17H15 : **Sébastien LEONNET** - Administrateur Principal au Secrétariat Général du Conseil de l'UE

Ancien Officier supérieur de l'Armée de l'Air française. Diplômé de l'Enseignement Militaire Supérieur Scientifique et Technique. Chef de l'Unité « Sécurité des Systèmes d'Information et de Communication Sensibles » au Secrétariat Général de l'UE. Membre de l'ARCSI.

Exposé : Union européenne et SSI: les défis de demain

- Le nouveau règlement de sécurité du Conseil de l'UE: une avancée majeure. Vers un règlement commun aux Institutions ?
- Mise en place d'une capacité en défense des réseaux au Secrétariat Général du Conseil de l'UE. Vers une capacité globale aux Institutions ?
- Interopérabilité entre les Institutions, les Etats membres et les pays tiers.

- 18H00 : Clôture par **Patrick PAILLOUX** - Directeur général de l'Agence nationale de la sécurité des systèmes d'information.

Le monde de la SSI : bilan, prospective, stratégie.

EN PARALLELE, SE TIENDRA UNE EXPOSITION DES INDUSTRIELS PARTENAIRES DE L'ARCSI PERMETTANT D'APPRECIER LEURS DERNIERES SOLUTIONS DE SECURITE.

Partenaires de l'ARCSI