Programme détaillé des 11es Rencontres de l'ARCSI

Paris – 7 novembre 2017

Messageries et systèmes de confiance

Quel monde numérique allons-nous laisser à nos enfants ?

La cybersécurité est-elle un combat perdu pour la quasi-totalité de l'humanité ?
Vos manières de vivre peuvent-elles s'adapter dans un monde sans sécurité numérique ?
Un jour l'Internet peut-il tomber ? Sommes-nous bien armés ?
Faut-il reconstruire un nouvel Internet de confiance ?

Les débats sont animés par le Président de l'ARCSI
Questions/réponses possibles après chaque intervention

08 h 30 ***Accueil***

09 h 00 **Général (2s) Jean-Louis DESVIGNES** [M] – *ARCSI*

- Jean-Louis DESVIGNES est le Président de l'ARCSI.

• ***Allocution d'ouverture.***

09 h 20 **M. Renaud LIFCHITZ** [M] – *Digital Security*

- Renaud LIFCHITZ est un expert en sécurité informatique français. Consultant, formateur et chercheur, ses principaux centres d'intérêt sont la sécurité protocolaire, le développement sécurisé, la cryptographie et la théorie des nombres. Il travaille aujourd'hui essentiellement sur l'IoT et les protocoles sans fil et intervient régulièrement dans les principales conférences de sécurité internationales. Quelques-uns de ses sujets d'études significatifs : cartes bancaires sans contact, géolocalisation GSM, blockchain, signatures RSA, ZigBee, Sigfox, LoRaWAN, Vigik et calcul quantique.

• ***État de l'art de la sécurité des messageries.***
Bien que pour l'essentiel les protocoles de messagerie sécurisés sont en pratique cryptographiquement inviolables, il reste plusieurs voies royales pour compromettre toute la sécurité d'un échange sécurisé. Dans un état de l'art que nous souhaitons le plus complet possible, nous passerons en revue les axes de vulnérabilités des messageries instantanées sécurisées et soulèverons les problématiques des modèles existants, tout en formulant des recommandations pour en faire un usage serein.

10 h 00 **- M. Bernard BARBIER** [M] – *CAPGEMINI*

- Bernard BARBIER est responsable, depuis janvier 2014, de la Cyber Sécurité Interne du Groupe CAPGEMINI/SOGETI. Il est membre de l'Académie des Technologies. Il a été : Directeur Technique de la DGSE de 2006 à 2013 ; Directeur du laboratoire de recherche dans les nanotechnologies : le LETI à Grenoble, de 2003 à 2006 ; Directeur des Systèmes d'Information, DSI, du CEA : Commissariat à l'Énergie Atomique, de 2000 à 2003.

• ***Chiffrement et confiance***
Comment rétablir la confiance dans le Numérique et l'Internet. La confiance est globale : toute la chaîne du numérique doit être de confiance : les composants, les logiciels systèmes (BIOS), les OS, les applications et l'utilisateur final… Comment la cryptographie et le chiffrement peuvent rétablir la confiance ?

10 h 40 ***Pause***

11 h 10 **M. Philippe WOLF** [M] – *IRT-SystemX*

- Philippe WOLF, ingénieur général de l'Armement (2s), a rejoint l'IRT-SystemX en avril 2015 après avoir servi la SSI de l'État pendant 30 ans. Il y dirige un projet de recherche finalisée intitulé EIC (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité). Ce projet vise à mettre en œuvre une plateforme expérimentale et technique qui permet d'évaluer le couplage de technologies de cybersécurité à travers des cas d'usage innovants dans le domaine des Territoires Intelligents, de l'Usine 4.0, du Transport Connecté et Autonome et des nouveaux services de l'Internet des Objets. EIC mène également une recherche concertée et cohérente dans les domaines économiques et juridiques. Il s'agit, par exemple, de quantifier les coûts d'une cyber-attaque, d'anticiper les ergonomies acceptées des fonctions de sécurité dans les nouveaux systèmes dits intelligents ou de mener une analyse juridique prospective sur la protection des données et de l'information.

• Pourrons-nous bâtir des systèmes de confiance demain ?

Cette conférence s'appuie sur les 15 prédictions d'Adi Shamir pour les 15 prochaines années exposées le 24 février 2016. Elles ouvrent, pour nous tous, des éléments de réflexion qui alimenteront nos prochaines rencontres.

11 h 50 **M. Jon D. PAUL** [A] – *Crypto-Museum* et *Scientific Conversion*

- Jon D. PAUL est un inventeur et homme d'affaires de Manhattan, il est ingénieur en électronique. Il est diplômé du *City College of New York* (CCNY) : BSEE en 1968 et MSEE en 1971. En 1968, il a conçu les analyseurs de spectre temps réel *NSA* et *US Marine Underwater Sound laboratoires*. Depuis 1971, il s'intéresse aux télécommunications et à l'ingénierie de brevet. En 1972, il a conçu les premiers processeurs de son, le studio numérique. En 1983, il est consultant en électronique de puissance et en audio numérique. En 1986, il travaille aux *Dolby Laboratories* et chez *THX/LucasFilm*. Jon est l'inventeur du brevet n° 5 051 799 de 1989 qui décrit le premier microphone numérique, il a été acheté et utilisé par 160 compagnies de téléphonie mobile.

Depuis les années 1980, Jon est un chercheur internationalement reconnu, écrivain et conférencier sur les machines de chiffrement, le chiffrement de la voix et leurs liens avec la technologie numérique moderne. Ses conférences ont été présentées lors de réunions au : *Bletchley Park*, Musée de l'Armée, ENST, Musée des Transmissions, NAB et SMPTE. La *Paul Foundation*, à but non lucratif, soutient la recherche avancée sur la maladie de Parkinson. Jon partage son temps entre la Californie et la France ; il apprend le français et est un photographe passionné.

• Les origines de notre monde numérique

ou l'histoire du téléphone mobile, de l'audio et de la vidéo numérique, techniques toutes issues de la transformée de Fourier, du VOCODER de Dudley et du système de cryptophonie SIGSALY.

On connaît peu en effet le rôle central de la cryptologie et de la science de la parole dans le développement des médias numériques modernes. Informatique, compression numérique, DSP et chiffrement sont étroitement liés. Les médias numériques doivent beaucoup aux mathématiques (Fourier), à la cryptologie (Vernam), à la synthèse vocale (Dudley), la théorie de l'information (Shannon), ainsi qu'aux inventions nées dans l'urgence de la Seconde Guerre mondiale.

Ainsi, le VOCODER d'Homer Dudley inventé en 1938, permettant la compression audio dans un facteur 10 est vite mis à contribution quand les Alliés mettent une priorité absolue à la sécurisation des conversations transocéaniques. En six mois, Bell Telephone Laboratories (BTL) développe le système SIGSALY utilisant ce VOCODER ainsi qu'une dizaine d'autres innovations fondamentales telles que la modulation par impulsion codée (PCM), la conversion rapide Analogique/Numérique ou l'étalement de spectre.

Nous présenterons donc le VOCODER de Dudley et le système SIGSALY, une reconstitution du premier codeur/décodeur (codec) PCM de SIGSALY utilisant des lampes d'origine. Nous n'oublierons pas de mentionner une contribution surprenante de l'actrice Hedy Lamarr à la technique du saut de fréquence. La présentation comprend des photos rares, de la musique d'époque, la première compression VOCODER et un document audio exceptionnel : une conversation SIGSALY.

12 h 30 ***Cocktail déjeunatoire***

14 h 00 **M^me^ Solange GHERNAOUTI** [M] – *Professeur de l'Université de Lausanne*

- Prof. S. Ghernaouti, Dir. Swiss Cybersecurity Advisory & Research Group. Université de Lausanne.

• Hyperconnectivité & dépendances numériques : utopies et réalités de la confiance.

L'urbanisation numérique du vivant et de la société structure et influe notre manière d'être au monde. Tous dépendants au numérique, et à ses fournisseurs de service, nous sommes tous concernés par les opportunités et les risques générés par l'hyperconnectivité. Entre promesses de bonheurs et peurs, la technocivilisation de la société et le cyberespace que nous allons laisser en héritage aux générations futures, nous invitent à revisiter sous l'angle de la confiance, les valeurs fondamentales de notre humanité.

14 h 40 **M. Herbert GROSCOT** [M]

- Actuaire indépendant, membre certifié de l'Institut des Actuaires, participant au Groupe de Travail Cyber de l'Institut ; Enseignant à l'EPITA sur la Majeure d'Intelligence Artificielle, la Mineure Finance et les Mathématiques de la Sécurité.

• Cyber Risque et Assurance.

Par cyber risque, nous entendons « Tout ce qui touche à l'atteinte, la violation ou la perte de données, ainsi qu'à des intrusions de réseau ou à la détérioration d'actifs aussi bien matériels qu'immatériels ».

Les sinistres cyber ont des spécificités qui, en dehors de leur nouveauté les rendent difficiles à appréhender, parmi lesquelles on peut citer :

- *Le caractère « invisible » et latent de la cause d'un sinistre cyber (p. ex. temps « d'incubation » d'un virus ou d'un vers, délai nécessaire avant l'évaluation de l'amplitude d'une attaque) ;*
- *La distance géographique entre le lieu du délit et le lieu du sinistre*
- *Le caractère contagieux d'une attaque*
- *La dimension technologique, avec ce qu'elle entraîne en termes de prévention et de détection, d'autant plus que les technologies évoluent en permanence ;*
- *La difficulté à évaluer l'origine et les coûts des dommages matériels ainsi qu'immatériels.*

Dans ce contexte, nous commençons par présenter le besoin de couverture du risque cyber en fonction des types d'attaques rencontrées - cibles, victimes, et type de pertes subies.

Suit une présentation d'une cartographie des risques cyber en cohérence avec une typologie de sinistres couramment rencontrée en IARD – dommage, responsabilité civile, immatériel et autre.

Le risque cyber ayant une forte composante technologique, et un fort impact juridique pour une entreprise, nous abordons les sujets suivants :

- *L'impact du Règlement Général sur la Protection des Données qui entre en vigueur en mai 2018,*
- *L'importance du distinguo entre bonnes pratiques en cyber sécurité, normes, et clauses d'exclusion de contrat,*
- *L'importance, pour une entreprise de connaître le coût potentiel de ses dommages, à travers un process de gestion de risque impliquant les décisionnaires de l'entreprise.*

Nous concluons avec un aperçu de l'offre en matière de cyber assurance.

15 h 20 ***Pause***

15 h 50 **M. Jérôme NOTIN** – *ANSSI*

- Directeur général du Service cybermalveillance.
Jérôme NOTIN a rejoint l'ANSSI en mai 2016 en qualité de préfigurateur du dispositif. Il est impliqué dans la SSI depuis de nombreuses années et dispose d'expériences dans la création et la direction d'entreprises. Il a été nommé en mars 2017 Directeur général du GIP ACYMA qui porte le dispositif national d'assistance aux victimes d'actes de cybermalveillance.

• Dispositif d'assistance aux victimes d'actes de cybermalveillance.
Cybermalveillance : objectifs et premiers retours suite au lancement national d'octobre 2017.
- Se protéger des cyber risques n'est plus une option pour les entreprises, quelle que soit leur taille. L'enjeu économies est vital : il s'agit pour elles de préserver leurs savoir-faire, leurs compétences, leurs données sensibles. En un mot, leur compétitivité.
- Les enjeux économiques, stratégiques et d'image relevant de votre responsabilité de dirigeant d'entreprise ne peuvent ignorer la sécurité des systèmes d'information.

16 h 30 **MM. Émile GABRIÉ & Gaston GAUTRENEAU** – *CNIL*

- Émile GABRIÉ travaille à la CNIL depuis 2008. Juriste initialement en charge des fichiers de police au sein du service des affaires juridiques, il a été chef adjoint de ce service de 2012 à 2014. Depuis avril 2014, il dirige le service des affaires régaliennes et des collectivités territoriales, qui a pour missions principales le conseil des autorités publiques et le contrôle a priori des activités de traitement qu'elles mettent en œuvre dans les domaines régaliens, et notamment de la justice, de la police, du renseignement et des libertés publiques.

- Gaston GAUTRENEAU appartient aujourd'hui au service de l'expertise technologique de la CNIL qu'il a rejoint il y a trois ans. Il intervient notamment sur les sujets de la cybersécurité, des nouveaux moyens de paiements et de la gestion de la fraude. En tant que consultant, spécialiste de la sécurité des systèmes d'information, il est intervenu durant 12 ans chez différents clients, principalement du secteur bancaire. Il a pu notamment travailler sur les domaines des risques opérationnels bancaires, de la gouvernance en sécurité des systèmes d'information, de la sensibilisation à la sécurité et des obligations légales et réglementaires sur ces sujets. Gaston GAUTRENEAU a une formation d'ingénieur télécom acquise à l'EPITA en 2002. Il a suivi en 2012 les cours du DU Analyse des Menaces Criminelles Contemporaines de l'Université Panthéon Assas.

• Le chiffrement : un élément vital de la sécurité des données.
La question de l'équilibre entre protection des données personnelles, innovation technologique et surveillance est au centre de nombreuses préoccupations, dans un contexte marqué par des cyberattaques de grande envergure comme par les révélations d'Edward Snowden sur la surveillance de masse. Or, le chiffrement contribue à la résilience de nos sociétés numériques et de notre patrimoine informationnel. Alors que la loi pour une République numérique a confié à la CNIL le soin d'assurer la promotion des technologies de chiffrement, la CNIL a pris position sur les enjeux du chiffrement et d'éventuelles « portes dérobées ». La mise en place de tels dispositifs ou de clés maîtres fragiliserait l'avenir de l'écosystème du numérique et la protection des données personnelles des individus, alors même que les autorités disposent par ailleurs de nombreux autres moyens permettant d'accéder aux données nécessaires aux enquêtes relatives aux faits graves, et de les analyser.

17 h 30 ***Fin***