TELECOM ParisTech

Institut Mines-Télécom

Les 9es Entretiens de Télécom ParisTech

TELECOM ParisTech ALUMNI

CYBERSÉCURITÉ

QUELS ENJEUX TECHNIQUES ET SOCIÉTAUX ?

Partenaires

11 et 12 mars 2015 à Télécom ParisTech

#CYBSC

Tutoriel technique
mercredi 11 mars 2015

Séminaire
jeudi 12 mars 2015

Télécom ParisTech
46, rue Barrault - Paris 13e

Informations actualisées sur : **www.telecom-paristech.fr/cybersecurite**

CYBERSÉCURITÉ
QUELS ENJEUX TECHNIQUES ET SOCIÉTAUX ?

CONTEXTE

La sécurité numérique vit un changement d'échelle, au fil de la métamorphose numérique et de son omniprésence dans nos activités professionnelles, sociales ou ludiques.

En parallèle, l'état des lieux révèle une insécurité diffuse, ancrée parfois jusque dans nos dispositifs eux-mêmes. Elle contourne des barrières dont le principe est fragilisé par les usages mobiles et le tout-connecté ; la gestion de nos données, de nos logiciels ou de nos identités est assurée par des tiers, en des lieux indéfinis et sous des juridictions indéterminées.

À l'insécurité s'ajoute la perte de confiance. Avec pour nécessité d'être à la fois réparateur des dysfonctionnements et refondateur de nos systèmes d'information.

Quelles protections demain ? Pour quels modèles éthiques et sociétaux et en fonction de quelles évolutions technologiques ?

La cyber vulnérabilité touche les entreprises, les États et collectivités locales, l'individu. Elle atteint les liens sociaux, nos dispositifs de santé autant que d'échange de monnaie.

L'intégration grandissante du numérique et de l'humain fait naître de nouveaux enjeux sociétaux et technologiques en termes de sécurité.

Une révolution pointe qui ne se contente plus d'apposer des rustines de sécurité sur des systèmes d'information et de communication existants, mais qui refonde entièrement le noyau de sécurité autour duquel réarticuler ces systèmes.

D'autres ruptures sont envisageables : technologiques, comme la cryptographie quantique, ou en évolution culturelle, comme le renoncement au tout-logiciel. À quels horizons seront-elles déployables ? Selon quelles modalités ?

Réunissant des industriels, des représentants publics, des chercheurs et des juristes, les Entretiens de Télécom ParisTech sur la Cybersécurité du 12 mars 2015 ont pour objectif d'établir un dialogue entre acteurs, et un diagnostic lucide du temps disponible pour initier des solutions.

Ce séminaire sera précédé, le 11 mars 2015, d'une journée dédiée au tutoriel abordant certaines problématiques scientifiques et techniques de la cybersécurité.

Comité scientifique

Romain ALLÉAUME,
Enseignant-chercheur à Télécom ParisTech

Thierry BARITAUD,
Coordinateur Sécurité Globale Produits et Services à Groupe Orange

Jean-Luc DANGER,
Enseignant-chercheur à Télécom ParisTech

Jean-Pierre DARDAYROL,
Membre du Conseil général de l'économie

Patrick DUVAUT,
Directeur de la Recherche à Télécom ParisTech

David FAYON,
Administrateur des postes et télécoms

Colonel Éric FREYSSINET,
Chef du Centre de lutte Contre les Criminalités Numériques (C3N), Gendarmerie nationale

Philippe LAURIER,
Enseignant, économiste

Gwendal LE GRAND,
Chef du service de l'Expertise Informatique à la CNIL

Michel LEVY,
Délégué aux Relations Internationales et Industrielles à Télécom ParisTech

Gérard MEMMI,
Responsable du département Informatique et Réseaux à Télécom ParisTech

Gérard PELIKS,
Réserve citoyenne Cyberdéfense et Président de l'atelier sécurité de Forum Atena

Alain RIESEN,
Directeur de la Formation Continue à Télécom ParisTech

Ahmed SERHROUCHNI,
Enseignant-chercheur à Télécom ParisTech

CYBERSÉCURITÉ
QUELS ENJEUX TECHNIQUES ET SOCIÉTAUX ?

SÉMINAIRE *#CYBSC*

jeudi 12 mars 2015

8 h ACCUEIL ET PETIT DÉJEUNER

8 h 30 **Ouverture de la journée**
Yves POILANE, *Directeur de Télécom ParisTech* et **Dominique JEAN,** *Président de Télécom ParisTech alumni*

8 h 45 **Cybersécurité : Menaces et Opportunités**
Guillaume POUPARD, *Directeur général de l'ANSSI*

9 h 15 **Cybersécurité dans les entreprises**
Alain BOUILLÉ, *Président du CESIN*

9 h 45 **Les Risques du Quantified Self et de l'Internet des Objets**
Vincent TRELY, *Président - Fondateur de l'APSSIS*

10 h 15 **Gouvernance et politique de sécurité**
Sébastien HÉON, *Directeur des relations institutionnelles, Airbus Defence and Space*

10 h 45 PAUSE

11 h TABLE RONDE
« Réponses techniques, scientifiques, sociétales et régaliennes »
animée par **le Colonel Éric FREYSSINET,** *Chef du Centre de lutte Contre les Criminalités Numériques (C3N), Gendarmerie nationale,*
avec la participation de :
Général (2s) Jean-Louis DESVIGNES, *Président de l'ARCSI*
Thierry FLORIANI, *Responsable de la Sécurité des Systèmes d'Information, Numergy*
Ismet GERI, *Directeur Europe du sud, Proofpoint*
Frank GREVERIE, *Vice-Président Corporate Cybersecurité, Capgemini*
Armen KHATCHATOUROV, *Chercheur à Télécom École de Management*
Claire LEVALLOIS-BARTH, *Coordinatrice de la Chaire "Valeurs et politiques des informations personnelles"*

12 h 15 PAUSE DÉJEUNER

13 h 45 **Aspects éthiques de la Cybersécurité en entreprise**
Michel Van DEN BERGHE, *Directeur Orange Cyberdéfense*

14 h 15 **La protection des données du Quantified Self et de l'IoT**
Dr Florent FREDERIX, *Principal Administrator, Trust and Security unit, Commission européenne*

14 h 45 **Protection des identités, Nouvelles monnaies**
Didier GRAS, *Responsable Sécurité des Systèmes d'Information, Groupe BNP Paribas*

15 h 15 **Bouleversements juridiques inhérents à la Cybersécurité**
Maître Isabelle LANDREAU, *Avocat au Barreau de Paris, médiateur en nouvelles technologies*

15 h 45 PAUSE

16 h TABLE RONDE
« Techniques en rupture et perspectives »
animée par le **Lieutenant-colonel Gérard PELIKS**, *Réserve citoyenne Cyberdéfense (RCC)*,
avec la participation de :
Gilles GRAVIER, *Director Product Management, ID Quantique SA*
Jean-Jacques QUISQUATER, *Université catholique de Louvain*
Nicolas RUFF, *Ingénieur sécurité, Google*
Olivier THONNARD, *Architecte Sécurité, Amadeus IT Group*
Hassan TRIQUI, *Président, Secure-IC SAS*

17 h 15 **Conférence de clôture des Entretiens**
Alain FIOCCO, *Sr Director CTO, CISCO*

Ce programme est susceptible d'être légèrement modifié

Partenaires

Réserve Citoyenne Cyberdéfense

Association des Réservistes du Chiffre et de la Sécurité de l'Information

Informations actualisées sur : www.telecom-paristech.fr/cybersecurite

CYBERSÉCURITÉ
QUELS ENJEUX TECHNIQUES ET SOCIÉTAUX ?

TUTORIEL mercredi 11 mars 2015

Sécurité des échanges TLS et SSL : état et perspectives

Ahmed SERHROUCHNI, enseignant-chercheur au département Informatique et Réseaux de Télécom Paristech

Le protocole TLS&SSL est le protocole de sécurité des échanges le plus déployé. Ceci est dû notamment à sa situation au niveau applicatif et aussi à son intégration aux browsers. Les services de sécurité assurés par TLS atténuent d'une manière conséquente les problèmes de sécurité dans les échanges. Son usage est actuellement quasi admis et implicite pour le grand nombre.

Dans ce tutoriel le protocole TLS sera présenté et analysé sous les angles : des services fournis, des différentes extensions qui lui ont été ajoutées, des mécanismes cryptographiques sur lesquels il se base, de ses faiblesses et des attaques qu'il peut subir. Un poids sera mis sur les problématiques des certificats notamment pour les réseaux véhiculaires.

Peut-on concevoir un système embarqué robuste aux cyberattaques ?

Jean-Luc DANGER et Sylvain GUILLEY, enseignants-chercheurs au département Comelec de Télécom Paristech

Les cyberattaques sont avant tout des attaques logicielles permettant d'observer, prendre le contrôle ou perturber à distance un système. Pour arriver à leurs fins, elles exploitent des vulnérabilités logicielles du système, ou utilisent des «portes dérobées». Les attaques logicielles fonctionnent généralement en deux phases : déclenchement d'une vulnérabilité (généralement «latente» dans le logiciel) et puis exploitation par exécution d'une charge utile. Il existe des moyens de protection essentiellement de nature logicielle pour lutter contre ces menaces. Les machines virtuelles, les logiciels anti-virus, l'offuscation de code, etc., font partie de l'arsenal de protection, mais ils ne permettent de garantir que partiellement la sécurité face aux menaces cyber, et peuvent eux-mêmes être sujets à attaques ou bugs. Le matériel est un moyen plus efficace de protection du fait qu'il n'est pas modifiable. Quelques processeurs actuels embarquent des moyens de protections, comme le bit NX (Intel/AMD/ARM) qui tente d'empêcher le processeur d'exécuter des données injectées de l'extérieur, ou l'unité de gestion de mémoire (MMU). Mais ces protections restent impuissantes face à certaines vulnérabilités ou erreurs de programmation, notamment les mauvaises indirections.

Nous présentons dans ce tutoriel les principes des attaques logicielles. Puis sont abordées les techniques de protection, logicielles et matérielles, et les méthodes de conception pour ajouter des fonctionnalités à un processeur, le rendant ainsi plus robuste face aux cyberattaques.

Traitement quantique de l'information et applications en cryptographie

Romain ALLÉAUME, enseignant-chercheur au département Informatique et Réseaux de Télécom Paristech

En utilisant la spécificité de la logique quantique pour transmettre et manipuler l'information, on ouvre des possibilités radicalement nouvelles, que ce soit pour le traitement de l'information (calcul) ou la sécurisation des communications, voire la génération de nombres aléatoires parfaitement sûrs.

Expériences de pensée du temps d'Einstein, on est désormais capable de produire, modifier et mesurer des systèmes quantiques (atomes, photons) avec des performances qui ouvrent la voie au traitement quantique de l'information. Ces progrès ont entrainé une explosion de la recherche au cours des 30 dernières années mais aussi la naissance d'entreprises commercialisant des systèmes des technologies quantiques, notamment pour la distribution de clés secrètes, depuis plus de 10 ans. Plus récemment, des investissements significatifs ont été effectués par des entreprises comme Google, IBM ou Microsoft dans le domaine du calcul quantique, dont les promesses (simulation, data-mining, machine learning, cryptanalyse...) sont au moins aussi considérables que les difficultés qui restent à résoudre afin de fabriquer des ordinateurs quantiques de grande taille.

Nous présentons dans ce tutoriel certaines idées fondamentales en information quantique, et notamment le concept d'intrication, qui désigne une propriété des objets quantique permettant d'observer des corrélations impossible à obtenir avec des objets répondant à la logique classique.

Nous abordons ensuite les grandes familles d'application de l'information quantique dans le domaine de la cryptographie : distribution quantique de clé, génération d'aléa, ainsi qu'ordinateurs quantiques, dont on sait la capacité à casser efficacement la plupart des algorithmes à clé publique existant actuellement (notamment RSA). Nous discuterons également de l'État d'avancement de ces technologies ainsi que de leurs interactions et de leur impact dans le domaine de la cryptographie et de la sécurité.

Ce programme est susceptible d'être légèrement modifié

INFOS PRATIQUES

Tarifs

Tutoriel du 11 mars 2015
Tarif [1] (net de taxes) : **490€**

Séminaire du 12 mars 2015
Tarif[1] (net de taxes) : **200€**

Tutoriel + Séminaire
Tarif[1] (net de taxes) : **600€**

(1) Ces frais sont imputables au plan de formation de l'entreprise.

Tarif Séminaire du 12 mars pour les membres cotisants de Télécom ParisTech alumni
(si inscription à titre individuel) : **140€**

Ces tarifs comprennent le déjeuner et les pauses-café

Inscription

www.telecom-paristech.fr/cybersecurite

Contacts

Mél : entretiens-cybersecurite@telecom-paristech.fr
Tél. : +33 (0)1 45 81 77 20 - Fax : +33 (0)1 45 81 71 23

alumni
Mél : cybersecurite@telecom-paristech.org
Tél. : +33 (0)1 45 81 80 48

Accès

Télécom ParisTech
46, rue Barrault - 75013 Paris, France

Métro : ligne 6, station Corvisart
RER : ligne B, gare Cité Universitaire (15 min à pied)
ou Denfert-Rochereau puis métro ligne 6
Bus : lignes 62 (Vergniaud), 21 (Daviel) ou 67 (Bobillot)

TELECOM ParisTech
TELECOM ParisTech ALUMNI
université PARIS-SACLAY