SEMINAIRE TECHNIQUE en partenariat avec

Jeudi 18 février 2016 de 9h00 – 17h00

Cybersécurité - IoT et systèmes embarqués

Enjeux et solutions pour la transformation numérique

L'arrivée massive des objets connectés dans le quotidien du citoyen mais aussi dans celui des entreprises a commencé, l'interdépendance des systèmes, la multitude de protocoles et la connexion à internet sont autant de failles possibles dans ces produits.

Les objets connectés sont des systèmes matériels communicants qui supportent un logiciel applicatif embarqué qui sont fortement concernés par les problématiques de sécurité logicielles et matérielles :

- Le système doit garantir la disponibilité, l'intégrité et la confidentialité des données qu'il manipule et qu'il échange,
- Le système (logiciel et matériel) doit être protégé contre la copie et le "reverse engineering" dans le cadre de la lutte contre l'espionnage industriel,
- Le système doit être protégé contre les attaques intérieures et extérieures qui visent à le détourner de sa fonction et/ou à en prendre le contrôle.

Pour répondre à ces problématiques il est indispensable d'avoir une culture de la gestion du risque, de la protection des données (sécurité offensive, sécurité défensive), de la protection des logiciels et des systèmes (développement, test et validation, contrôle permanent en fonctionnement).

Objectif : Sensibiliser les participants aux enjeux liés à la sécurité, présenter quelques bonnes pratiques à intégrer dans la conception d'un objet connecté « secure by design », présenter des exemples de mise en œuvre des dernières technologies de réseau bas débit (Sigfox, LoRa), proposer des pistes de sécurisation, évoquer les opportunités liées à la mise en œuvre de bonnes pratiques et technologies en sécurité des systèmes d'information, éclairer les participants sur les enjeux actuels et à venir.

Personnes concernées : Vous êtes une entreprise qui conçoit déjà des systèmes embarqués ou connectés via des réseaux classiques ou des réseaux bas débit comme Sigfox et LoRa, ce séminaire s'adresse à vous : dirigeants d'entreprise, ingénieurs commerciaux, ingénieurs et techniciens qui conçoivent, mettent en œuvre, valident ou simplement utilisent des produits connectés, ingénieurs en charge du test et validation en sécurité de ces objets.

PROGRAMME

8h30 Accueil des participants

9h00 Introduction à la journée par Sébastien SALAS, CAP'TRONIC et Jean François BAILLETTE, G-ECHO

→ Mythes et réalités du marché des objets connectés par Olivier EZRATTY, Consultant

Où en sont les objets connectés ? Comment le marché est-il en train de se structurer, où sont les segments les plus porteurs et créateurs de valeur ? Quels sont les différents modèles économiques et leur viabilité ? A quoi ressembleront les plateformes qui consolideront la valeur ? Est-ce que les standards ouverts pourront éviter cette captation par quelques entreprises ? Quel sera le rôle des réseaux M2M dans cette chaine de valeur ?

Bio de l'intervenant :
Olivier Ezratty conseille les entreprises pour l'élaboration de leurs stratégies d'innovation (veille technologique, stratégies produits, création d'écosystèmes) et en particulier dans le domaine des objets connectés. Il est aussi très actif dans l'écosystème des startups qu'il accompagne comme board member, consultant, conférencier et auteur. Il publie notamment le "Guide des Startups" sur son blog Opinions Libres ainsi que le "Rapport du CES de Las Vegas" tous les ans depuis 2006. Il est aussi le co-auteur de l'initiative « Quelques Femmes du Numérique ! » (http://www.qfdn.net). Ingénieur de l'Ecole Centrale, il a par ailleurs une double expérience dans le développement logiciel (chez Sogitec) ainsi que dans le marketing (chez Microsoft France dont il a notamment été le Directeur Marketing).

→ IoT et sécurité Sigfox par Renaud LIFCHITZ, expert sécurité chez Digital Security

Lors du développement et de l'intégration IoT, de nombreuses questions se posent sur la fiabilité et la sécurité des transmissions sans fil. Après avoir expliqué le fonctionnement de la technologie Sigfox, nous aborderons en détails les

forces et faiblesses de Sigfox concernant la sécurité des données transmises. Des recommandations seront données aux intégrateurs et développeurs utilisant le protocole pour durcir la sécurité.

- Présentation de Digital Security, du CERT-UBIK
- Problématiques de sécurité courantes des communications sans fil
- Présentation de la technologie Sigfox et caractéristiques physiques des transmissions Sigfox
- Fonctions de sécurité de Sigfox : redondance, authentification, chiffrement, mécanisme anti-rejeu
- Vulnérabilités résiduelles
- Recommandations de développement et d'intégration

Bio de l'intervenant :
Expert français reconnu en sécurité informatique ayant une expérience de 10 ans en tant qu'auditeur et formateur, principalement dans le secteur bancaire. Il s'intéresse tout particulièrement au développement sécurisé, aux protocoles de communication sans fil et à la cryptographie. Il a été intervenant dans de nombreuses conférences internationales : CCC 2010 (Allemagne), Hackito Ergo Sum 2010 & 2012 (Paris), DeepSec 2012 (Autriche), Shakacon 2012 (Etats-Unis), 8dot8 2013 (Chili) et a formé plus de 1800 personnes.

→ **Etude de la sécurité LoRa par Philippe COLA, BOUYGUES Telecom (sous réserve)**

→ **Attaques de systèmes embarqués communicants, par Aviram JENNIK de Beyond Security**

→ **La sécurité à l'ère des objets connectés par Yann ALLAIN d'Opale Security**

Comment s'y prendre quand on est une PME, retour d'expérience Opale Security

- Après plus d'une centaine d'audits de sécurité IoT, que faut-il retenir ?
- Points de vigilance, bonnes pratiques et outils de sécurisation disponibles pour les équipes R&D
- Comment mettre en place une conception sécurisée des IoT dans votre entreprise (sans alourdir les budgets, ni les délais !)

Bio de l'intervenant :
Yann ALLAIN, expert en sécurité et Ingénieur en électronique et en informatique, est le fondateur et actuel dirigeant de la société Opale Security. Seule société en Europe ayant une expérience significative en sécurisation des objets connectés (IoT) et en SSI. Ancien responsable de la sécurité applicative d'un groupe international (ACCOR), Security Researcher, BlackHat Speaker. Yann possède plus de 20 ans d'expérience, dont 16, dédiés à la sécurité des SI et des systèmes embarqués.

Présentation des exposants du mini salon :

Alliantech : Solutions sans fil pour le test et la validation des applications de mesure via SIGFOX.

Digital Security : Protéger les Systèmes d'Information et les écosystèmes des objets connectés.

HSC by Deloitte Expertise, conseil, audit en sécurité des systèmes d'information.

Isit : Outils et plateformes de développement / validation, en sureté et sécurité de fonctionnement d'applications temps réel embarqué.

Neotech Assurances pour l'Entreprise et couverture de la cybersécurité.

12h50 à 14h00 Repas - buffet

→ **Présentation des actions du pôle AESE sur la sécurité, retour sur l'action collective, par Franck Lepecq**

→ **Présentation de la commission sécurité de Digital place, Mathieu Sacrispeyre**

→ **Présentation de la Mêlée Numérique et de la commission sécurité, Caroline Duhailler**

SEMINAIRE TECHNIQUE en partenariat avec

Jeudi 18 février 2016 de 9h00 – 17h00

→ L'open source et la sécurité par Fabien Lahoudère de OPEN WIDE

La sécurité est un sujet de plus en plus présent lors de la conception d'un système embarqué. Les systèmes basés sur GNU/Linux et autres technologies open source étant de plus en plus utilisés dans l'embarqué, ils n'échappent pas à la règle. Un architecte peut se poser de nombreuses questions sur les facultés des logiciels open source face à l'enjeu de la sécurité.

Sécurité et open source sont-ils compatible ? Linux est-il un noyau sur ? Comment évaluer la sécurité de mon système GNU/Linux ? Quels sont les outils disponibles ?

Bio de l'intervenant :
Fabien Lahoudère est consultant chez Open Wide et travaille en tant que développeur et intégrateur de solutions pour des systèmes GNU/Linux embarqué. Il intervient dans différents secteurs d'activités telles que la radionavigation, l'automotive, le multimédia et le réseau. Il a notamment intégré le support de netmap pour le projet open source Haka security et a l'élaboration du projet Twavox.

→ Plateforme EIC (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité) par Philippe WOLF, IRT-SystemX

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.

Bio de l'intervenant :
Philippe WOLF - SystemX, ingénieur général de l'Armement, 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).

→ La recherche en sécurité au LAAS-CNRS par Eric ALATA et Vincent NICOMETTE

Sécurité sur les systèmes embarqués et les objets connectés: Panorama

La généralisation rapide de l'usage de l'informatique dans les systèmes grands public ainsi que dans l'internet des objets nécessite de rapidement se soucier de la sécurité. Certains des verrous mis en évidence par ces nouvelles applications peuvent être traités par les méthodes classiques de sécurité, mais d'autres nécessitent des mesures spécifiques. Dans ce sens, cet exposé présente des exemples de travaux menés par le LAAS dans le domaine de lasécurité des ystèmes embarqués et conclut avec un panorama des enjeux traités par l'équipe dans un avenir proche.

Bio de l'intervenant :
Eric Alata est chercheur au LAAS-CNRS au sein de l'équipe « Tolérance aux fautes et Sûreté de Fonctionnement informatique (TSF) » et enseignant à l'INSA de Toulouse. Ses domaines de recherche concernent la sécurité dans les systèmes embarqués et sur Internet, en traitant aussi bien la sécurité dans les couches basses des systèmes que dans les couches applicatives.

→ Intelligence économique Vs Intelligence collective : un défi 4.0. Se former en continu par Thierry ROUX, Great-X

Et l'homme dans tout ça ? Comment en mettant en œuvre les préceptes de l'intelligence économique et stratégique, on peut mieux renforcer et valoriser sa compétitivité et son innovation. Avec un principe de base : se former (veiller) en continu et transformer son expertise en valeur.

Tout en rappelant le champ de vision de l'intelligence économique et les interactions des réseaux, nous balayerons ensemble les fondamentaux du CODEX de l'information à l'action, où l'information est le minerai de la connaissance et la connaissance la source de toute innovation.

→ Quelles garanties des cyber-risques pour votre entreprise par Nicolas HELENON, NeoTech assurances

Date et lieu : 18/02/16 de 9h00 à 17h00 – Salle de conférence du LAAS-CNRS,

7 av. du colonel Roche 31031 TOULOUSE

SEMINAIRE TECHNIQUE en partenariat avec

Jeudi 18 février 2016 de 9h00 – 17h00

Prix : participation aux frais de la journée, 30 € TTC

Pour vous inscrire cliquer ici

Contact : Sébastien SALAS – 06 87 83 32 32 –- salas@captronic.fr

Nos intervenants :

Nos partenaires :

Nos sponsors :