2022 Embedded-SEC

24 mars 2022
Conférence
4ème édition - PARIS

Programme de la conférence Embedded-SEC 2022

Une conférence à suivre en “présentiel” ou en “distanciel”
de 9 H à 17 H 30

Jeudi 24 mars

Toutes les présentations et les documents proposés par les intervenants seront accessibles le jour même de la conférence

2022 Embedded-SEC 24 mars 2022 Conférence - 4ème édition - PARIS

PROGRAMME COMPLET

9 H 00 – 9 H 25 Accueil des participants

9 H 25 Introduction de la journée par François Gauthier, directeur de publication de L'Embarqué

9 H 30 - 10 H 15 (dont 5 mn Q&A) **Keynote**

Speaker : Sylvain Guilley

Cofondateur et CTO

Société/Organisme : Secure-IC

Titre : **Securyzr integrated Security Services Platform (iSSP) :**
Protection des IoT tout au long de leur cycle de vie

Résumé : Comme les deux lames d'une épée à double tranchant, la connectivité des objets connectés offre donc à la fois inconvénients et avantages. Pour intégrer ces considérations dans une politique de sécurité globale, il s'agit d'une part, de définir clairement les services déployés et leur protection, et d'autre part, de les faire valider dans le cadre d'une démarche de certification.
La gestion des services de sécurité des IoT connectés fait appel à différentes fonctions. La première est la "programmation initiale", à savoir l'injection des premières clés et logiciels, dans le respect de leur confidentialité et leur authenticité. Cette première étape "instancie" véritablement l'IoT comme racine de confiance. Sur cette base, peuvent se déployer essentiellement deux services. Le premier est la descente d'information et/ou de mises à jour depuis une plateforme "cloud" débarquée, qui rend possible le maintien, voire même le renforcement de la sécurité. Le second est la remontée d'incidents de sécurité, permettant, du côté "cloud", d'assurer une veille active de sécurité. Ces deux services peuvent être rendus pour la plateforme IoT ou pour les applications qu'elle héberge.
Concernant la certification, les schémas se mettent en place pour permettre une évaluation ouverte. Mentionnons la norme EN ETSI 303 645 (Cyber Security for Consumer Internet of Things) en Europe ou la norme NIST SP 800 193 (Firmware Resiliency) aux États-Unis. En termes de marchés verticaux, les considérations de gestion distante sont explicitées dans la clause 13 du standard ISO/SAE 21434 pour les véhicules, dans l'IEC 62443-4-2 pour les applications de type "industrial IoT".
Aujourd'hui, Secure-IC propose "integrated Security Services Platform" (iSSP), une solution qui permet de configurer, de déployer et de gérer une flotte d'iSE depuis le cloud, sous forme de SaaS ou d'une application logicielle à installer sur les infrastructures du client.

10 H 15– 10 H 45 (dont 5 mn Q&A)

Speaker : Abdoul Niazi

Senior Functional Safety Application Engineer

Société/Organisme : Ansys

Titre : **Une approche basée modèles combinant les analyses de risque dysfonctionnelles et la cybersécurité**

Résumé : La cybersécurité est devenue une composante majeure des analyses de risques pour les systèmes embarqués, notamment dans les transports, la défense, l'énergie. Elle s'associe à d'autres analyses de risque, notamment les analyses dysfonctionnelles.
L'ensemble de ces analyses peuvent être réalisées à partir de modèles d'architecture conçus par les ingénieurs systèmes s'appuyant sur des outils basés modèles.
Ansys, avec la solution medini, présentera comment réaliser ces analyses dans une plateforme unique, en support des normes ISO26262, IEC 61508, ARP4761 et ISO21434, D0 356.

10 H 45 – 11H 15 (dont 5 mn de Q&A)

Speaker : Benjamin Mouchard

Marketing Manager

Société/Organisme : Prove & Run

Titre : **Delivering IoT security on ARM Cortex-M33 micro-controllers**

Résumé : The presentation will focus on the security services, the security levels and certifications adapted to the a vast majority of IoT products and systems.

Modern ARM Cortex-M33 architectures offer efficient and robust isolation, delivering optimized integration of « out-of-the-box » security services and offering a cost-effective alternative to using Security Elements for delivering Root-of-Trust services.

The ARM PSA initiative is one of the emerging standards in IoT, with the objective to drive the ecosystem towards a common security baseline. We will introduce ARM PSA security objectives, the security services and and how to achieve the security assurance level according to the threats and the security evaluation methodologies available.

Finally, we will introduce ProvenCore-M, ProvenRun's solution that leverages Arm's Cortex-M33 security capabilities and fulfill ARM PSA requirements (and beyond) to achieve highest system-wide security objectives.

11 H 15 – 11 H 30 PAUSE CAFE

11 H 30 -12 H 00 (dont 5 mn Q&A)

Speaker : Frédéric Maraval

Products Manager

Société/Organisme : ISIT

Titre : **Allier Sûreté de Fonctionnement & Cybersécurité : une solution par l'architecture et la séparation des domaines**

Résumé : L'avènement de la connectivité fait qu'aujourd'hui des mondes séparés tels que l'IT et l'OT se retrouvent entremêlés et que par conséquent des systèmes critiques autrefois isolés se retrouvent sous la menace d'attaques extérieures. Sûreté de fonctionnement et cybersécurité sont aujourd'hui indissociables lorsqu'on doit concevoir un équipement. Mais comment répondre aux exigences, parfois antagonistes, de ces deux domaines surtout lorsque l'écosystème dans lequel va évoluer le système que l'on doit concevoir n'est pas entièrement maitrisé ? Une solution est la séparation et l'isolation des applicatifs au sein de l'équipement. Dans cette présentation seront couverts :

- Origine et principe de la séparation
- La notion de « least privilege »
- Virtualisation matérielle et séparation de noyaux
- Hyperviseur monolithique vs Séparateur de noyaux
- Principes du séparateur LynxSecure
- Avantages et bénéfices des séparateurs de noyaux

12 H 00 – 12 H 30 (dont Q&A 5 mn)

Speaker : Peter Nielsen

EMEA & APAC Channel Director

Société/Organisme : White Source

Titre : **DevSecOps solutions and strategies to protect your open source**

Résumé : Open source components comprise between 60% and 80% of the codebase in modern applications and the number of open source projects is expected to grow. With this growth comes an increase of security risks as the attack surface expands. So, what can be done to protect your applications? What are the most effective DevSecOps tools and practices to fix vulnerabilities in open source?

12 H 30 – 13 H 45 PAUSE DEJEUNER

13 H 45 – 14 H 15 (dont Q&A 5 mn)

Speaker : Eric Sema

Senior Business Development Manager

Société/Organisme : Vector

Titre : **How to improve cybersecurity robustness with intrusion detection system in automotivehe IoT Satellite Connectivity**

Résumé : La cybersécurité est un élément important qui ouvre la voie à la connectivité des véhicules. Par le passé, l'industrie automobile a déployé des efforts considérables pour doter les architectures E/E des véhicules de mécanismes de sécurité. Par exemple, les mises à jour logicielles signées, le démarrage des calculateurs sécurisé et la communication embarquée (inter-ECU) sécurisée sont de plus en plus répandus. Aujourd'hui, les systèmes de détection d'intrusion (IDS) attirent l'attention des constructeurs et des équipementiers automobiles en tant que mécanisme de sécurité supplémentaire. Bien que la détection d'intrusion soit un mécanisme de sécurité connu et couramment utilisé depuis longtemps dans les systèmes informatiques classiques, ces mécanismes n'ont pas fait l'objet d'un déploiement massif dans le monde automobile jusqu'à maintenant.

14 H 15 - 14 H 45 (Q&A 5 mn)

Speaker : Martin Becker

Field application engineer for verification and validation workflows

Société/Organisme : MathWorks

Titre : **The holy grail of cybersecurity engineering: Traceability, Certainty, and Efficiency**

Résumé : Cybersecurity has become a significant concern for the broad public, with a growing number of attacks reported on various devices across all industries. Embedded systems are no exception : The damage from cybercrime on embedded devices is estimated to exceed $50B by 2023, and security is becoming the leading barrier for adoption of connected devices. To counteract these concerns and help embedded designers cope with these new conditions, various regulations and standards (EN 303 645, IEC-62443, ISO/SAE 21434) have been released in recent years. They are providing guidance around governance, risk management, and engineering methods. Unfortunately, the standards remain silent about concrete, reliable processes. Engineering teams are thus left with the burden of connecting the dots to make systems more secure. Common challenges are: How can we trace and validate security goals, artifacts, and meta-information from paper to code? How can we handle updates efficiently and meanwhile ensure consistency of processes and artifacts? And how can we move from basic evidence to solid confidence in our security solution, to minimize oversight and the need for updates ?

In this talk, we demonstrate how engineers can design and maintain more secure embedded systems with the help of model-based design. And only when three aspects are covered – tracability, certainty and efficiency – can engineers reliably build secure systems, and keep them secure in today's fast-changing threat landscape.

14 H 45 – 15 H 15 (Q&A 5 mn)

Speaker : Samuele Falcomer avec Giovanni Solito

Principal Product Manager (u-blox Cellular) et Senior Product Manager (u-blox Services)

Société/Organisme : u-blox

Titre : **Protecting business critical data from silicon-to-cloud**

Résumé : We live in an age when the internet continually connects more and more physical objects, which makes it more important than ever to be able to fully trust and control your IoT device. Data is the main asset of your business. Encrypting and transferring data in IoT settings requires complex and expensive solutions that involve millions of devices. u-blox innovative IoT security solution makes it extremely simple to protect your data, both on device and from device to cloud. We implement a true end-to-end concept where data are protected from the device to the end-user and are not visible by the intermediate nodes/platforms nor by the service provider. Out-of-the box on-boarding to IoT cloud platforms provides total control of the device certificate lifecycle, enabling mass market scale.

Through the symmetric key management system, engineers have a streamlined and scalable alternative to the conventional public key infrastructure or pre-shared key arrangements. Keys can be triggered from either the module side or the server/cloud side, with significant savings realized in terms of system cost, operational complexity and in power consumption.

15 H 15-15 H 30 PAUSE CAFÉ

15 H 30 – 16 H 00 (Q&A 5 mn)

Speaker : Yannick Gaudin

Security Architect

Société/Organisme : Lacroix

Titre : **Harmonisation mondiale des attentes de sécurité pour les systèmes industriels avec l'IEC 62443**

Résumé :
Depuis maintenant plusieurs années, la cybersécurité des systèmes industriels n'est plus une option. L'ensemble des acteurs de la chaine de fourniture, du fabricant à l'opérateur en passant par l'intégrateur, ont conscience de l'importance et de l'étendue du sujet. Les menaces évoluent rapidement, le profil des attaquants se diversifie et les campagnes d'attaques deviennent de plus en plus sophistiquées. Si ce tableau est globalement connu et admis aujourd'hui, il convient de coordonner les stratégies afin d'offrir une réponse efficace aux menaces courantes et à venir. La plupart des normes de sécurité se concentrent sur le produit lui–même : c'est le point d'attention obligatoire pour adresser le sujet de la cybersécurité d'un système industriel et il est porté majoritairement

par le fabricant. Malheureusement, cela ne suffit plus face aux menaces actuelles: l'intégration de multiples produits impliquent des communications qui doivent être intégrées dans le modèle de cyber défense. Aussi, l'opération de ces systèmes doit se faire dans des conditions établies afin de ne pas dégrader les niveaux de protection en place sur les équipements déployés. Comment assurer une défense en profondeur des systèmes industriels en intégrant l'ensemble des acteurs (fabricant, intégrateur, opérateur) ?
L'IEC 62443 adresse cette problématique, tout en offrant de la flexibilité sur les niveaux de sécurités visés.

16 H 00 – 16 H 30 (Q&A 5 mn)

Speaker : Michael Fuhrmann

Senior Field Application Engineer

Société/Organisme : IAR Systems

Titre : **Enforcing security legislation compliance in IoT application**

Résumé : Let's face it: good security is hard, but the new legislation for IoT security and privacy rapidly being introduced globally will force you implement security. You probably already know that governments in Europe, UK and US are at the forefront of IoT device security and have many requirements that devices must meet in order to be sold. You may think that injecting security into an existing product can be costly and hard, but there are practical ways to improve security throughout your product's lifecycle. We will show you how to jump-start your road to developing secure devices by introducing you to the 13 Best Practices of IoT security and how they can be easily implemented in your application.

The 13 best practices include no default passwords, a secure update mechanism, end-of-life policies clearly communicated to customers, and more. While the legislation globally is evolving, we know that it will include steps similar to the 13 best practices. Once you have these implemented, it is easily possible to adapt to whatever additional requirements that may be imposed by European EN 303645 and the evolving US Cybersecurity Improvement Act (NISTIR 8259).

16 H 30 – 17H 00 (Q&A 5 mn)

Speaker : Manuel Capel

CTO et cofondateur

Société/Organisme : Parcoor

Titre : **Détection de malwares et d'attaques réseau sur appareil**

Résumé **:** Les appareils IoT sont attaqués typiquement 5 minutes après être connectés sur Internet (source : NETSCOUT Threat Intelligence Report). Les cyberattaques sur l'IoT ont progressé de 300% par an entre 2018 et 2020. À présent, environ 30% des cyberattaques visent l'IoT (source : Forbes). En 2019, 2.9

milliards d'appareils IoT étaient infectés par des malwares dans le monde (source : Forbes). En l'état, la protection des appareils IoT est déléguée à des systèmes tiers, avec des capacités importantes (SIEM, SOC…) pour superviser la détection de menaces. La solution de Parcoor est de réaliser la détection de malware fondée sur l'extraction d'une empreinte des binaires exécutés. Une sélection d'empreintes discriminantes grâce à un algorithme incrémental, développé en interne, permet une classification de nouveaux binaires avec un nombre limité de comparaisons. Ces solutions de première ligne de défense ne nécessitent pas de connexion Internet, ce qui est important pour des systèmes subissant des communications intermittentes (trains, avions…) ou qui auraient été isolés de façon malveillante. Elles peuvent être installées en complément de systèmes de protection centrale.

17 H 00 – 17H 30 (Q&A 5 mn)

Speaker : Sean Evoy

Senior Product Manager

Société/Organisme : GrammaTech

Titre : **Deliver Secure, Embedded Solutions with DevSecOps and Static Code Analysis**

Résumé : Embedded software powers critical functions in products that support applications such as industrial, manufacturing, medical, automotive, aerospace, military and defense. In these cases, device failure from software defects is not an option. Ensuring quality, security and safety of these systems, devices and controls must start and span the entire software development lifecycle (SDLC). Establishing a DevSecOps process that integrates and automates static application security testing (SAST) into the SDLC is an effective and efficient strategy.
In this session, you will learn best practices for :

- Implementing quality, safety and security testing at every step of the SDLC
- Integrating SAST into CI/CD pipelines to achieve DevSecOps success
- Applying industry standards for critical safety and security (i.e. AUTOSAR, MISRA, ISO, IEC, BSA, FDA, JPL, etc.) at every step of the way
- Accelerating development projects by analyzing code and fixing defects early

17 H 30 – 18 H 30 COCKTAIL DE CLOTURE