

L'OFFRE CEA TECH POUR LA CYBER SÉCURITÉ

Nos compétences technologiques en réponse aux enjeux de la cyber sécurité :



Systèmes industriels, « Supervisory Control And Data Aquisition » (SCADA)

Protection des réseaux (eau, électricité), des infrastructures (transport, finance, internet, etc.), des sites de production, résilience des systèmes



Vie privée, données personnelles

Confidentialité des données (santé, communication, etc.), Internet des objets, cloud, niveau de sécurité adapté aux besoins des utilisateurs



technologique

Caractérisation

Logiciels sécurisés

Traitement de données

Communication et protocoles

Évaluation en vue d'une certification

Implémentation sécurisée sur le matériel

Composants et systèmes embarqués

Architecture de circuits intégrés

Cryptographie



Évaluation

Respect de la réglementation, évaluation de composants et systèmes électroniques, architecture par assemblage de composants certifiés, logiciels



Safe by design

« E to E security », protection contre les attaques, analyse des failles de sécurité et fiabilité (matériel et logiciel), sans contact



Sécurité de l'information, protection

Lutte contre l'espionnage, détection de cyber-attaque, analyse de données de sécurité et de comportement, protection des données publiques



Cryptographie

Protocoles, implémentation sécurisée, adaptation aux contraintes applicatives (performance, coût, sécurité)



L'expertise CEA Tech s'adresse :

- Aux fabricants de composants et systèmes
- Aux développeurs de logiciels et opérateurs de service de sécurité
- Aux constructeurs et opérateurs d'infrastructures critiques
- Aux industriels du transport, de l'aéronautique, etc.
- Aux organismes publics





Conseil, expertise et intelligence économique

Audits des systèmes et solutions de sécurisation : adéquation entre le niveau de sécurité et le besoin industriel, stratégie d'implémentation, caractérisation des menaces, attaques

Sécurité des logiciels

Fiabilité et sécurité des logiciels, recherche de vulnérabilité, outils de conception, analyse de risques

Architectures systèmes pour la sécurité

Architectures intrinsèquement sûres, circuits intégrés sécurisés (numérique, RF et proche capteurs) y compris en technologies avancées (FDSOI, 3D), logiciels sur puce, virtualisation, plates-formes embarquées sécurisées

Évaluation sécuritaire de composants et systèmes

Multiples accréditations notamment dans le domaine bancaire (Critères Communs, EMVCo, VISACARD, MASTERCARD)

Caractérisation

Évaluation de la résistance des composants et systèmes aux attaques physiques (consommation, électro-magnétique, laser, glitches, etc.), cryptanalyse matérielle

Cryptographie

Mise en oeuvre sécurisée et performante de protocoles cryptographiques, cryptologie avancée (crypto-homomorphe, pairing)

Communication et protocoles sécurisés

Solutions sans contact, communication sans fil (RFID, Wifi, Ultra Wide Band, Zigbee), infrastructures de réseaux, authentification forte, protocoles sécurisés pour réseaux de capteurs

Big Data et analyse de données, analyse de comportement, fouille de données

Détection d'alertes précoces à partir d'événements (ex : cyber-attaque), intelligence économique

Systèmes et intégration de capteurs (capacitif, pression, etc.)

Biométrie (empreinte digitale, rétine, iris), reconnaissance vocale

Nanoélectronique (PCRAM, OxRAM, CBRAM, MRAM)

Fiabilité et robustesse des composants « mémoire », caractérisation sécuritaire des technologies émergentes (FDSOI)
