CYBERSECURITE

Responsable : Chantal CAUDRON DE COQUEREAUMONT

chantal.caudron-de-coquereaumont@intradef.gouv.fr

Tél : 02 99 42 92 53 ou 02 21 07 12 35

La thématique « Cybersécurité » couvre un large spectre d'expertises aussi variées que la spécification d'algorithmes cryptographiques, la conception de composants électroniques et de produits de protection et défense, le développement logiciel sécurisé, l'architecture de sécurité des systèmes, la détection d'attaques, l'évaluation matérielle et logicielle, etc. L'objectif est de maintenir une dynamique d'innovation permettant :

- d'anticiper l'évolution de la menace, qui est en constante évolution ;
- de répondre aux enjeux opérationnels associés à la SSI des programmes actuels et futurs, dans un contexte d'évolution rapide des technologies.

La problématique de cybersécurité résulte de la confrontation entre défenseur et attaquant dont les enjeux sont la maîtrise des services numériques et la disponibilité opérationnelle. Cette dualité se retrouve dans les axes d'expertises à adresser, entre connaissance des menaces et ingénierie de la sécurité d'une part et évaluation dans la posture d'un attaquant d'autre part.

Les sous-thèmes de la thématique cybersécurité à adresser en priorité sont les suivants (notamment les sujets en gras), à noter que tout sujet disruptif sera regardé :

SOUS-THEME 1 : CRYPTOGRAPHIE

- **Cryptographie post-quantique, en particulier à base de codes et de réseaux**
- **Preuve de sécurité automatiques et semi-automatiques des protocoles cryptographiques, sécurité des implémentations cryptographiques**
- Nouveaux services cryptographiques tels que chiffrement à base d'attributs, signature de groupe, diffusion (broadcast)
- Formalisation de la vérification de la bonne gestion et utilisation des algorithmes, paramètres et clés cryptographiques dans un produit ou système
- Modélisation de sources connues d'aléa, évaluation de la qualité d'un aléa

SOUS-THEME 2 : SECURITE MATERIELLE ET LOGICIELLE DES COMPOSANTS, PRODUITS ET SYSTEMES

- **Mécanismes de sécurisation des OS ou des mécanismes de virtualisation**
- **Interactions Matériel/Logiciel : exploitation logicielle de mécanismes matériels pour la sécurisation globale du produit ou système, impact de la microarchitecture sur la sécurité logicielle et prise en compte dans les modèles**
- **Techniques d'évaluation de la robustesse des composants face à des attaques par canaux auxiliaires ou injection de fautes**
- **Techniques d'analyse de code statiques ou dynamiques, de recherche de vulnérabilités**
- **Analyse massive automatisée de code à base d'IA**
- Techniques de sécurisation des composants

- Spécification, formalisation et vérification de conception sécurisée d'architectures matérielles et logicielles
- Contrôle et réduction de la surface d'attaque de produits sur étagère (COTS) matériels et logiciels
- Processeurs sécurisés et chiffrement mémoire à la volée
- Techniques de compilation permettant la mitigation de vulnérabilité (ajout de mécanismes d'intégrité du flot de contrôle par exemple)
- Cloisonnements (entre processus, mémoire)
- Résilience, tolérance aux fautes et sécurité en dysfonctionnement (fail-secure)
- Convergence sûreté de fonctionnement (SdF) et sécurité : technologique (langage, développement, compilation safe & secure), méthodologique (par exemple, unification des méthodologies d'arbres d'attaques et d'arbres de défaillances), prise en compte des contraintes de SdF dans les mécanismes de sécurité
- Sécurité des systèmes de contrôle industriel et sécurité des objets connectés
- Contrôles de conformité des composants par rapport à leur description (GDS2)
- Résistance aux attaques par injection de fautes
- Génération de tests basés sur des modèles qui permettent de s'assurer de l'adéquation des programmes avec leurs spécifications

SOUS-THEME 3 : SECURITE DES RESEAUX

- **Supervision adaptative de la sécurité des SDN (software defined network), sécurité du plan de contrôle**.
- Cadre (framework) formel pour la vérification des protocoles de routage, voir plus généralement de réseaux

SOUS-THEME 4 : CONNAISSANCE DE LA MENACE

- **Analyse automatisée de binaires en particulier détection de similarités**
- L'étude des similarités des techniques d'attaques et mode opératoire
- Analyse de malwares
- Traitements de données massives pour l'analyse des modes opératoires d'attaque et plus globalement le renseignement d'intérêt cyber

SOUS-THEME 5 : LUTTE INFORMATIQUE DEFENSIVE

- **Détection des malwares et des attaques avancées,**
- **Traitement de donnée massives pour détecter des comportements anormaux et des signaux faibles d'attaque**
- **Techniques de leurrage et d'appât pour tromper ou détourner l'attaquant**
- Supervision adaptative à la virtualisation des systèmes,
- Techniques de visualisation pour la supervision et pour l'analyse des données et évènements de sécurité
- Evaluation des solutions de détection