STRATEGIE NATIONALE CYBERSECURITE

PROGRAMME ET EQUIPEMENTS PRIORITAIRES DE RECHERCHE CYBERSECURITE

Webinaire Appel à Projets PEPR Cybersécurité

13 juillet 2022

https://anr.fr/PEPR-Cyber-AAP

Date limite de soumission : 30/09/22

STRATEGIE NATIONALE CYBERSECURITE

PROGRAMME ET EQUIPEMENTS PRIORITAIRES DE RECHERCHE CYBERSECURITE

Agenda

- Contexte et périmètre de l'appel
- Soumission et sélection
- Réponses aux questions

Stratégie nationale d'accélération pour la cybersécurité

- Inscrite dans le plan France 2030, elle s'articule autour de quatre axes principaux :
  - Développer des solutions souveraines de cybersécurité ;
  - Renforcer les liens et les synergies entre acteurs de la filière ;
  - Soutenir la demande (individus, entreprises, collectivités et État), notamment en la sensibilisant mieux tout en faisant la promotion des offres nationales ;
  - Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre.

STRATEGIE NATIONALE CYBERSECURITE

PROGRAMME ET EQUIPEMENTS PRIORITAIRES DE RECHERCHE CYBERSECURITE

Programme et Équipements Prioritaires de Recherche (PEPR) Cybersécurité

- Vocation de soutenir des activités stratégiques de recherche fondamentale, au plus haut niveau mondial, en support aux industriels de la filière et répondant aux priorités définies dans le cadre de la stratégie nationale.

- Pilotage du CEA, du CNRS et d'Inria

- Plusieurs outils ouverts à toute la communauté scientifique :
  - Projets ciblés
  - Appels à projets

STRATEGIE NATIONALE CYBERSECURITE

PROGRAMME ET EQUIPEMENTS PRIORITAIRES DE RECHERCHE CYBERSECURITE

Projets ciblés du PEPR Cybersécurité

- P1 – Protection des données personnelles, Vincent Roca
- P2 – Sécurité des calculs, David Pointcheval
- P3 – Vérification de Protocoles de Sécurité, Stéphanie Delaune
- P5 – Défense contre les programmes Malveillants, Jean-Yves Marion
- P6 – Supervision et orchestration de la sécurité, Ludovic Mé et Hervé Debar
- P7 – Architectures Sécurisées pour le Numérique Embarqué, Jacques Fournier
- P8 – Améliorer l'évaluation de la sécurité des systèmes logiciels, Florent Kirchner

STRATEGIE NATIONALE CYBERSECURITE

PROGRAMME ET EQUIPEMENTS PRIORITAIRES DE RECHERCHE CYBERSECURITE

Appel à projets du PEPR Cybersécurité

- Financer des projets de recherche à des niveaux de TRL 1 à 4, destinés à apporter des éléments de connaissance indispensables aux développements des technologies de cybersécurité et favoriser l'émergence de ces outils et solutions avant leur transfert vers le secteur industriel.
- Budget de 15 M€ pour trois axes thématiques :
  - Axe 1. Protection des données multimédias.
  - Axe 2. Recherche et techniques d'exploitation de vulnérabilités.
  - Axe 3. Cryptanalyse de primitives cryptographiques.
- Un seul projet sera retenu par axe thématique.

Axe 1. Protection des données multimédias

Contexte

L'information par l'image, le texte et le son, et plus généralement à travers le multimédia, s'est particulièrement accentuée avec le développement des réseaux sociaux et, plus récemment, des activités de télétravail liées à la crise sanitaire.

Il est urgent de protéger les informations multimédias et détecter leur falsification. Cette problématique s'étend à la sécurité des IA (confidentialité, intégrité, disponibilité) qui peuvent être compromises. Le sujet est d'importance dans plusieurs domaines critiques (*manufacturing*, santé, mobilité) et à fort enjeu économique.

STRATEGIE NATIONALE CYBERSECURITE

PROGRAMME ET EQUIPEMENTS PRIORITAIRES DE RECHERCHE CYBERSECURITE

Axe 1. Protection des données multimédias

Sujets abordés
• Tatouage d'images, de sons et de vidéos • Traçage de traites • Détection de manipulations d'images et de son (incluant la voix), hypertrucage (*deepfake*) • Caractérisation d'attaques et développement de protections d'algorithmes de *machine learning* • Biométrie et reconnaissance faciale, biométrie comportementale, à des fins d'authentification • Détection d'usurpation de voix et contre-mesure.

Axe 1. Protection des données multimédias

Mots clés associés

- Tatouage d'images, de sons et de vidéos (watermarking) ;
- Traçage de traites ;
- Détection de manipulations d'informations, hypertrucage (deepfake);
- Attaques et protections d’algorithmes de machine learning de classification d’images,
- Biométrie et reconnaissance faciale;
- Biométrie comportementale à des fins d’authentification

Axe 2. Recherche et techniques d'exploitation de vulnérabilités.

Contexte

La recherche et l'exploitation de vulnérabilités dans les systèmes numériques nécessitent de nouveaux outils de criminalistiques (matériels, logiciels) pour identifier les vulnérabilités, notamment les portes dérobées, afin de combler le retard de la France dans ce domaine.
Plusieurs verrous scientifiques sont à lever afin de mieux comprendre les vulnérabilités des systèmes et améliorer les techniques de recherche de vulnérabilités, en particulier les techniques automatisées.
Ce pour faire face à des usages criminels qui se développent. Notons enfin que dans le cadre des cas d'usages criminalistiques, les « preuves » récupérées, que ce soit sur la valeur de la preuve elle-même et sur la manière dont elle a été récupérée, doivent être acceptables d'un point de vue juridique. Dans cette optique, les impacts légaux des techniques développées doivent être pris en compte.

Axe 2. Recherche et techniques d'exploitation de vulnérabilités.

Sujets abordés

- Recherche de vulnérabilités et de portes dérobées (fuzzing de binaires en environnements sécurisés de confiance, canaux auxiliaires) sur des systèmes déployés ;
- Recherche de failles dans les noyaux de systèmes d'exploitation;
- Analyse et désassemblage de codes machines exécutés non extractibles (racine de confiance par canaux auxiliaires) ;
- Vulnérabilités spécifiques au web ;
- Développement d'exploits sur systèmes sécurisés ;
- Méthodologies d'attaques utilisant de l'apprentissage machine ;
- Automatisation de la recherche de vulnérabilités et d'exploitation ;
- Investigation de failles matérielles pouvant être exploitées par logiciel;
- Analyse forensique d'images systèmes et de mémoires de systèmes embarqués ;
- Menace persistante avancée ;
- Sécurité des téléphones mobiles ;
- Outils et méthodologies d'analyses sur dispositifs physiques ;
- Impact/évolution du cadre légal associé aux techniques criminalistiques étudiées.

Axe 2. Recherche et techniques d'exploitation de vulnérabilités.

Mots-clés associés

- Recherche de vulnérabilités et de portes dérobées ;
- Développement d'exploits ;
- Méthodologies d'attaques ;
- Apprentissage machine ;
- Automatisation ;
- Investigation numérique ;
- Analyse forensique,
- Outils et méthodologies d'analyses sur dispositifs physiques.

Axe 3. Cryptanalyse de primitives cryptographiques.

Contexte

La cryptanalyse est une branche de la cryptologie qui consiste à étudier la sécurité des primitives cryptographiques.

Elle vise aussi bien à prouver la sécurité qu'à montrer que la sécurité visée n'est pas atteinte, ce qui peut se faire par le biais d'une analyse théorique ou de l'exploitation d'une faille dans des conditions réelles ou de laboratoire.

La communauté scientifique française se situe, dans le domaine de la cryptanalyse, au tout premier plan sur la scène internationale.

L'objectif de cet axe « Cryptanalyse de primitives cryptographiques » et de renforcer ce positionnement, d'essaimer les compétences au niveau national et de les transférer vers les acteurs privés et étatiques de la filière

Axe 3. Cryptanalyse de primitives cryptographiques.

Sujets abordés

L'axe thématique porte sur les deux volets suivants, qui devront être tous les deux couverts par le projet retenu

- **Cryptographie à clef symétrique**. cryptanalyse d'algorithmes de chiffrement (par bloc ou par flot), de chiffrement authentifié, de modes de chiffrement, de fonctions de hachage, de MAC et de générateurs pseudo-aléatoires. Les travaux viseront à la fois la proposition de nouvelles techniques de cryptanalyse, l'amélioration de techniques existantes, et la cryptanalyse de primitives existantes.
- **Cryptographie à clef asymétrique**. cryptanalyse d'algorithmes de chiffrement, de schémas de signature, et de générateurs pseudo-aléatoires, reposant sur la difficulté de la factorisation et du logarithme discret (et plus généralement sur les problèmes mathématiques qui ne sont pas étudiés dans le cadre du PEPR Technologies Quantiques), ainsi que sur la cryptanalyse de primitives cryptographiques reposant sur des courbes algébriques ou des couplages.

Axe 3. Cryptanalyse de primitives cryptographiques.

Mots-clés associés

- Cryptanalyse ;
- Clef symétrique ;
- Clef asymétrique ;
- Schéma de signature ;
- Algorithme de chiffrement ;
- Chiffrement authentifié ;
- Mode de chiffrement ;
- Fonction de hachage ;
- MAC ;
- Factorisation ;
- Logarithme discret ;
- Courbes algébriques;
- Couplages.

Caractéristiques de l'appel

- Le projet devra impliquer entre 4 et 8 unités de recherche.
- La durée maximale des projets est de 5 ans.
- Chaque projet doit choisir un seul axe thématique.
- Un seul projet sera retenu par axe thématique.
- L'aide minimale demandée des projets devra être de 3,5M€ en regard des objectifs des thématiques.

Critères d'évaluation (cf. 3.3 texte de l'appel)

1) Excellence et ambition scientifique

- Clarté des objectifs et des hypothèses de recherche ; Caractère novateur, ambition, originalité ; Pertinence de la méthodologie.

2) Qualité du consortium, moyens mobilisés et gouvernance

- Compétence et implication du responsable scientifique du projet ; Qualité et complémentarité du consortium scientifique ; Adéquation entre les moyens demandés et les objectifs ; ...

3) Impact et retombées du projet

- Capacité du projet à répondre aux enjeux de recherche de l'axe thématique choisi ; Impacts économiques et sociétaux, contribution au développement de solutions en réponse aux enjeux des domaines prioritaires de la stratégie d'accélération nationale ; Stratégie de diffusion et de valorisation des résultats ; ...

Soumission

Le dossier de soumission complet est constitué de deux documents intégralement renseignés :

- Le **« document scientifique »,** d'une longueur maximum de 20 pages, rédigé en français, comprenant une description du projet envisagé, selon le format fourni.
- Le **« document administratif et financier »,** qui comprend la description administrative et budgétaire du projet.

Les documents à remplir seront accessibles à partir de la page web de publication de l'AAP : https://anr.fr/PEPR-Cyber-AAP

Annexe financière

- **Un onglet par établissement**
- Les bénéficiaires des aides sont des **établissements d'enseignement supérieur et/ou de recherche** (…) Les entreprises pourront avoir le statut d'Établissement partenaire dans les projets mais ne bénéficieront pas de financement.
- **Financement des personnels statutaires à hauteur maximale de 40%** du total des dépenses éligibles hors frais généraux.
  - Le taux des 40% sont appréciés au niveau de chaque Établissement.
  - Pas de limitation pour les contractuels.
- **Frais généraux portés à 20%** : Ces frais ont un caractère forfaitaire et sont plafonnés à 20 % des dépenses éligibles réalisées dans la limite de l'aide accordée, hors frais généraux.

Procédure de sélection

- Evaluation par un **comité de sélection** indépendant (à dimension internationale).
- Les directeurs de programme proposeront au Secrétariat Général Pour l'Investissement (**SGPI**) la désignation des projets qui pourraient être financés et le montant d'aide qui pourrait leur être définitivement attribué.
- Le **Premier ministre**, après avis du SGPI, arrêtera la décision concernant les bénéficiaires et les montants accordés.
- Chaque projet fera l'objet d'un contrat entre l'ANR et l'établissement coordinateur du projet, détaillant les obligations réciproques des parties.

Modalités de suivi

- **Reporting annuel** : rapport d'avancement, indicateurs de suivi, relevés de dépenses.

- **Réunions annuelles de suivi** avec le responsable du projet, représentants établissements partenaires, direction de programme du PEPR Cyber, ANR