À propos de C&ESAR

Depuis 1997, le ministère français des armées organise chaque année un colloque dédié à la cybersécurité réunissant les acteurs gouvernementaux, industriels et académiques. Cet événement vise un double objectif, scientifique et opérationnel, en rassemblant durant trois jours experts, chercheurs, praticiens et décideurs, pour un tour d'horizon sur un sujet particulier. Le thème choisi est abordé dans une perspective opérationnelle aussi bien que théorique, avec une dimension didactique prononcée pour aider les professionnels de secteurs différents à partager une compréhension commune de problématiques souvent complexes. Cette approche interdisciplinaire de la cybersécurité permet aux utilisateurs de terrain d'étudier et d'anticiper les avancées théoriques ou techniques, et aux industriels ou aux scientifiques de confronter la recherche et le développement des produits aux réalités opérationnelles.

Intelligence Artificielle et Cybersécurité

Les récentes avancées en intelligence artificielle (IA) et en particulier en apprentissage (Machine Learning) promettent de révolutionner de nombreux domaines. La cybersécurité au sens large (logiciel, matériel, réseaux, …) profite déjà de ces avancées que ce soit dans les phases de conception ou d'analyse, ou pour défendre un système déployé.

Ces systèmes intelligents peuvent être la cible de nouvelles classes d'attaques qui visent à les tromper ou influencer leur comportement. On peut citer par exemple le chatbot Tay de Microsoft.

Par ailleurs le manque fréquent d'explicabilité des prises de décision, et la difficulté à analyser leur comportement, peuvent présenter un risque pour les systèmes qui les intègrent et freiner leur adoption.

L'édition 2018 de la conférence C&ESAR s'intéresse à ces deux volets: les apports de l'intelligence artificielle pour la cybersécurité, et les risques de sécurité propres aux intelligences artificielles.

Le comité de programme attend des propositions de communication sur l'intelligence artificielle pour les thèmes suivants :

- *l'analyse* de risque automatisée dans les systèmes sécurisés,
- *la protection* de systèmes sécurisés par des IA,
- *les attaques* visant l'IA,
- *la qualification et la certification* d'algorithmes ou de systèmes à base d'IA.

Les contributions attendues porteront donc sur l'apport de l'IA pour la sécurité des systèmes dans ses différentes composantes (logiciels, matériels et réseaux), sans omettre la place de l'humain. Concernant l'IA, le comité de programme privilégie les méthodes d'apprentissage, mais les autres formes d'intelligence artificielle seront également considérées.

Le comité de programme appréciera des soumissions sur les cas d'usage suivants :

- la configuration automatique de réseau sous l'angle sécurité, l'entrainement contre la menace cyber,…
- l'analyse d'images, l'analyse de signaux électroniques, l'analyse des alarmes réseau,…
- la threat Intelligence,
- les responsabilités de la prise de décision avec une IA dans la boucle, et la place de l'humain dans la boucle
- la détection de fraudes, la tentative d'influence, les attaques par empoisonnement, la prévention des biais en apprentissage,…
- l'analyse automatisée de logiciel, la désobfuscation de code, l'évaluation de robustesse de la sécurité (mots de passe…), la correction automatique de failles de sécurité,…

- les limitations de l'IA pour la cybersécurité, IA et respect de la vie privée, acquisition des données d'apprentissage, détection des signaux faibles
- des retours d'expérience sur l'usage actuel de l'IA pour la cyber
- l'usage de l'IA en contexte contraint (limitations en ressources, en temps, en données)

Modalités de soumission

- *Première étape :* les propositions de communication (3 à 6 pages) sont à soumettre au plus tard le ~~29 juin 2018~~ **6 juillet 2018 (nouvelle date)**
  via https://www.easychair.org/conferences/?conf=cesar2018 au format PDF. Doivent y figurer le titre de la communication, sa catégorie (analyse ; protection; attaque ; qualification-certification), les noms et prénoms des auteurs ainsi que leur affiliation, l'adresse électronique de l'auteur principal, un résumé (10 lignes max.) et une liste de mots clés. Les auteurs seront prévenus de l'acceptation ou du rejet le **5 septembre 2018**.
- *Seconde étape :* les auteurs envoient au plus tard le **2 octobre 2018** une version définitive de la communication (de 8 à 16 pages) à contact@cesar-conference.org, copie à benoit-f.martin@intradef.gouv.fr. Les auteurs s'engagent dans cette version définitive à prendre en compte les remarques des relecteurs transmises lors de la notification de la décision.
- *Instructions pour la version définitive de l'article* : document PDF au format A4 sans les numéros de page, suivant le modèle Springer Lecture Notes in Computer Science
  (modèle LaTeX : ftp://ftp.springernature.com/cs-proceeding/llncs/llncs2e.zip;
  modèle Word : ftp://ftp.springernature.com/cs-proceeding/llncs/word/splnproc1703.zip.).
- *Langues et critères de sélection :* les communications peuvent être rédigées en français ou en anglais. Les critères de sélection seront principalement le respect du thème de la conférence et de l'appel à communications, la clarté et l'effort pédagogique. Les exposés techniques seront considérés dans la mesure où ils présentent aussi un état de l'art d'un domaine et non uniquement un résultat particulier. Les communications ne doivent pas être à vocation commerciale. Les communications acceptées seront publiées dans les actes du colloque.

Dates importantes

- Soumission des propositions de communications (entre 3 et 6 pages) : **6 juillet 2018** (nouvelle date)
- Notification aux auteurs : **5 septembre 2018**.
- Version finale (entre 8 et 16 pages) : **2 octobre 2018**
- Conférence : **du 19 au 21 novembre 2018**

Comité de programme

José ARAUJO (ANSSI)
Christophe BIDAN (CentraleSupélec)
Frédéric CUPPENS (IMT - Atlantique)
Ivan FONTARENSKY (THALES)
Guillaume DUVEAU (DGNUM, MINARM)
Guillaume MEIER (AIRBUS)
Eric WIATROWSKI (ORANGE)
Boris BALACHEFF (HP)
Yves CORREC (ARCSI)
Herve DEBAR (Télécom SudParis)
Patrick HEBRARD (NAVAL Group)
Benoît MARTIN (DGA-MI, MINARM)
Ludovic PIETRE-CAMBACEDES (EDF)

Partenaires