Defence-related Research Action - DEFRA

ACRONYME: AMC3

Titre: Automated Methodology for Common Criteria Certification

Durée du projet: 01/02/2024 - 31/07/2027

Mots-clés: cybersécurité, certification

Budget: 1.673.000 €

dont contribution IRSD: 1.590.634 €

DESCRIPTION DU PROJET

La Défense Belge s'appuie de plus en plus sur des logiciels, tant applicatifs que sous forme de systèmes cyber-physiques. Lorsque ces logiciels présentent des défauts, des vulnérabilités et des faiblesses, des attaquants peuvent exploiter leurs faiblesses et altérer des systèmes critiques ou exfiltrer des informations sensibles. Afin d'atténuer ce risque et de garantir que les logiciels sont fiables et dignes de confiance, les activités de certification et d'accréditation ont traditionnellement été intégrées dans le cycle de vie des logiciels. L'assurance logicielle par la certification et l'accréditation souffre de processus extrêmement consommateurs de ressources et de temps. Il faut une approche structurée et, dans une large mesure, automatisée/agile, qui tienne compte des mises à jour des logiciels. L'initiative ARCOS montre que la défense US évolue vers des niveaux plus élevés de maturité en cybersécurité, ce qui implique une évaluation plus approfondie de tous les logiciels et systèmes approuvés pour l'un des réseaux militaires classifiés ou non.

AMC3 vise à concrétiser cette vision et de l'appliquer au secteur belge de la défense. Les objectifs d'AMC3 sont (1) de moderniser les processus de certification de la cybersécurité de la Défense, et (2) d'automatiser le processus et de réduire drastiquement la charge humaine. Etant donné le nombre toujours croissant de systèmes IT et OT utilisés par la Défense belge, et la complexité croissante de ces systèmes, une gestion du risque de cybersécurité exige que le processus d'accréditation interne soit basé sur l'automatisation de parties majeures du processus. Pour ce faire, AMC3 offre une vérification basée sur de la simulation automatique (formelle) et une surveillance qui produisent des preuves tout en préservant la traçabilité pour construire automatiquement l'argumentation des cas d'assurance. Étant donné qu'une grande partie de la contribution au processus d'accréditation doit être fournie par le fabricant du logiciel/système, il est important d'impliquer l'industrie de la défense ainsi que la défense elle-même dans ses développements internes. Le système MASFAD développé en interne servira d'étude de cas pour l'expérimentation et la validation tout au long du projet. L'objectif est de valider la méthodologie AMC3, et en particulier l'interaction/collaboration entre l'équipe de développement et la cellule d'accréditation militaire. L'objectif de ce projet est précisément de développer une méthodologie de certification et d'accréditation automatisée, d'assembler un ensemble d'outils qui soutiennent cette méthodologie et la valider sur deux cas d'utilisation typiques liés à la défense. Le premier cas d'utilisation est un outil de détection des menaces persistantes

avancées (APT) développé en interne pour protéger les réseaux gouvernementaux et militaires, tandis que le second est un logiciel de système d'arme.

Les trois phases AMC3 sont: (1) développement d'une méthodologie pour la certification automatique avec techniques de validation efficaces, (2) prise en compte de l'incrémentalité de la certification pour les mises à jour, (3) automatisation du contrôle de la certification à l'exécution, et analyse technique/coût. Deux études de cas seront utilisées. La première, MASFAD, provient de l'ERM et est un IDS qui est déployé comme un jumeau numérique sur une représentation simulée mais pertinente du réseau de la défense. Il sera principalement utilisé au cours des phases 1 et 2. Le second, FNH SAM, est proposé par FN Herstal pour la phase 3. Il s'agit d'un logiciel en production de gestion d'armement. Ces deux études de cas permettront respectivement de développer la méthodologie et de réaliser une analyse technico-économique afin d'estimer le coût-bénéfice de l'implémentation de la méthodologie dans une solution industrielle.

Les enseignements tirés du cas d'utilisation MASFAD auront un impact direct sur les processus de certification et d'accréditation au sein de la Défense belge et renforceront la cyber-résilience des réseaux militaires classifiés et non classifiés. Le cas d'utilisation en collaboration avec FNH applique la méthodologie AMC3 à FN® SAM avec un impact potentiel direct sur la Défense belge puisque FN® SAM a été évalué avec une preuve de concept en 2021 et fait l'objet d'un pré-déploiement en 2023. Un déploiement complet plus tard est prévu pour gérer l'ensemble de la flotte d'armes de la Défense belge. Les résultats de AMC3 seront déployés progressivement dans la solution opérationnelle de FN® SAM afin de renforcer la sécurité de l'ensemble de la solution. Pour permettre l'adoption de la méthodologie AMC3, une analyse coûts/bénéfices sera réalisée.

Les résultats de AMC3 seront une méthodologie et sa plateforme prototype, validée en termes d'évolutivité et de rentabilité sur deux études de cas industrielles. Ces innovations permettent l'adoption de méthodologies plus agiles et suffisamment rigoureuses pour certifier les logiciels nouvellement développés ou mis à jour. Les bénéficiaires de cette nouvelle méthodologie sont les acteurs de la Défense (directs ou chaîne d'approvisionnement) et leurs fournisseurs, ainsi que l'ensemble du tissu socio-économique confronté à la certification automatique. Pour un impact maximal, les résultats seront diffusés auprès des organismes de certification belges (CCB) et internationaux, y compris les projets Horizon Europe travaillant sur le thème de la certification automatique.

COORDONNEES

Coordinateur
Axel Legay
UCLOUVAIN/ Pôle en ingénierie informatique
e-mail: axel.legay@uclouvain.be

Partenaires
Philippe Massonet
CETIC/ Positionnement Entreprises-Recherche
e-mail: philippe.massonet@cetic.be

Wim Mees
ERM/ Communications, Systèmes d'Information et Senseurs (CISS)

e-mail: Wim.Mees@mil.be

Yves Roskam
FN Herstal S.A./ FN Herstal Business Development
e-mail: Yves.Roskam@fnherstal.com

LIEN(S) DU PROJET

Lien temporaire : https://www.cetic.be/AIDE-en