SEC202

2024-2025

SESSION 1

Devoir final

La session 1 du cours SEC202 – SACE Sécurité des Architectures Complexes et Émergentes la cybersécurité pour la promotion SEC202 -2024-2025 Semestre 1 du Centre de Paris se déroulera sous forme d'un projet final comportant une partie individuelle (livrable 1) et une partie en trinôme (livrables 234) à remettre au plus tard le 8 février 2025 dans Moodle.

Votre trinôme

Votre trinôme travaillera en complète autonomie, cependant l'enseignant désigné comme responsable du sujet vous suivra.

Votre binôme et le sujet attribué figurent dans l'espace moodle, votre sujet est également disponible par votre enseignant désigné

Document

Vous trouverez ce document* dans scholar https://scholar.google.com/

* Les ressources IEEE, Elsevier, ou autres sont accessibles depuis l'ENF. *https://bibliotheques.cnam.fr/opac/.do?sysb=ep*
* En cas de difficulté seulement vous me contacterez : Véronique Legrand.

Chaque membre du binôme adressera en son nom propre ses livrables dans l'espace devoir de Moodle.
https://par.moodle.lecnam.net/mod/assign/view.php?id=674605

Rappel des objectifs du devoir

Au travers d'un article scientifique de base, vous devrez comprendre et réimplémenter un modèle d'attaque avec un outil de « threat modelling ».

L'évaluation porte sur le travail de réimplémentation du threat model de l'attaque, le code doit être fonctionnel ou expliquer pourquoi il ne l'est pas le cas échéant.

Un rapport est demandé, il porte en premier sur un travail de compréhension et de restitution de l'article qui peut intégrer les questions en annexe, la seconde partie du rapport porte sur votre travail de réimplémentation de préférence en python ou dans le langage de modélisation que vous choisirez, le code, vos choix de librairie, sont laisses à votre appréciation, etc. et seront des éléments pris en compte.

En plus de la modélisation de l'attaque, une simulation sur un environnement virtualisé peut être proposé, ce sera un plus.

Livrables

livrable 1 : Rapport
format docx dans moodle pour l'antiplagiat

- Forme
  - Individuel
  - Synthèse
  - format word – max 2 pages avec schéma.
  - À déposer dans le devoir « moodle »
  - Nommage du fichier :
    - *SEC202S1S2-Livrable1-Synthèse-NomEnseignant-NomAuditeurX.docx*
  - Cartouche de votre devoir :
    - Nom de l'article :
    - Nom de l'enseignant :
    - Auteur du résumé : (auditeur)
- Contenu
  - Chaque auditeur rédige individuellement une synthèse structurée autour des questions génériques ci-dessous que nous vous conseillons de traiter de cette façon pour structurer votre démarche. En effet, tout article scientifique amène à se poser ces 4 questions, il est donc important que votre synthèse aborde ces 4 questions.
    - Quel est à votre avis les contexte et problématique de l'approche proposée par les auteurs ?
    - Quel est le principe, le formalisme, l'architecture et/ou le modèle adopté par les auteurs ? En quoi cette modélisation est-elle appropriée dans le contexte ?
    - Les auteurs ont procédé à une expérimentation, que vous avez réimplémentée avec votre trinôme, cependant, vous décrirez l'avancée que constituent les résultats obtenus, quelle a été votre contribution dans le travail du groupe.
    - Vous établissez le lien avec les cours SEC202, à quelles notions du cours cet article fait-il appel et à quelles notions ne fait-il pas appel ?
- Remarques :

- Chaque auditeur devra rédiger sa propre vision de l'article en suivant cette trame, avec ses propres mots, en remettant sa rédaction sur Moodle individuellement.
- Le recours à une IA est autorisé à condition de citer ses sources, dans le cas contraire, le travail est considéré comme du plagiat.

livrable 2 : Réimplémentation
format zip dans moodle.

- Forme
  - Groupe
  - format word – max 4 pages.
  - À déposer dans le devoir « moodle » pour le groupe
  - Nommage du fichier : SEC202S1S2-Livrable2-Rapport-NomEnseignant-NomAuditeur1- NomAuditeur2- NomAuditeur3.docx
  - Cartouche de votre Rapport :
    - Nom de l'article :
    - Nom de l'enseignant :
    - 3 Auteurs du rapport : (auditeur 1-3)
- Contenu
  - Contenu : votre travail de réimplémentation
  - L'objectif est de reproduire, réimplémenter, le modèle d'attaque que les auteurs proposent dans l'article afin d'obtenir les résultats qu'ils indiquent.
  - Il s'agit généralement d'un fichier JSON, ou en python, vos enseignants pourront vous proposer un langage de description d'attaque qui vous permettra d'automatiser la constitution de ce travail dans la mesure du possible.

- Remarque :
  - Vous expliquez chaque étape de la constitution de votre threat modelling.

Livrable 3 : Video
format zip dans moodle.

- Forme
  - Groupe
  - Visibilité des auditeurs via la caméra/son pendant toute la durée de la video
  - Video 10 mn max.
  - À déposer dans le devoir « moodle »
  - Nommage du fichier : SEC202S1S2-Livrable3-Video-NomEnseignant-NomAuditeur1- NomAuditeur2- NomAuditeur3.docx
  - Cartouche de votre video :
    - Nom de l'article :
    - Nom de l'enseignant :

- 3 Auteurs: (auditeur 1-3)

- Contenu
  - Avec votre binôme, vous présentez les résultats de votre réimplémentation.
  - Vous partagez votre écran pour présenter vos slides, on doit vous voir et vous entendre, caméra allumée tout au long de l'exposé.
  -

Livrable 4 présentation en pptx
Dans moodele

Consignes

les livrables envoyés par mail ne sont pas acceptés.
Le travail ne devra pas provenir de copié-collé (hors citation des sources),
le plagiat est un motif d'annulation du devoir, le travail est exclusivement produit par le binôme.
Les enseignants pourront en cas de besoin demander un complément d'information par oral ou par écrit.
Le recours à GPT est possible sous réserve que vous citiez vos sources et modes d'interactions avec l'IA.

Synthèse individuelle : livrable 1 : L'auteur est indiqué sous le titre de la partie rédigée :

Description du modèle
Auteur : Jean Durand

Visio : livrable 3 :

Tout livrable avec une caméra/son non fonctionnels ne sera pas accepté.
Le livrable est obligatoirement déposé dans l'espace devoir de Moodle,

Rappel des compétences visées à partir du devoir

- Comprendre une architecture de sécurité « by design » ou non, sur des systèmes à architecture 3/3, en émergence, ainsi que le processus et le flux de traitement échangés,
- Modéliser un système de vie, d'attaque, de défense ou de monitoring de l'activité en sécurité de l'information pour repérer les événements et les incidents de sécurité, afin de les traiter,
- Introduire différentes méthodes de "Threat modelling" et TTP dans des architectures complexes et émergentes,
- Modéliser la surface d'attaque de systèmes complexe et émergents également en lien avec le service de Cyber Threat Intelligence, à partir de diverses sources (OSINT, etc…),

- Développer de nouveaux uses cases autour de la sécurité des systèmes complexes et émergents, plus performants au quotidien,
- Savoir « imaginer / concevoir » de nouvelles menaces et les solutions de sécurité émergentes (SOAR / MISP).

Annexe : consignes pour le rapport – livrable 1

Rappel du titre de l'article : "Protocole pour la cybersécurité des IoT"

Auteur : Madame X

Livrable 1

Le contexte et la problématique de l'approche proposée par les auteurs portent sur les modes d'interactions de l'IoT dont la multiplicité des protocoles de communications soulève de nombreuses questions, etc.
Le modèle adopté par les auteurs de cet article a été déjà proposé dans un article précédent. Il repose sur un principe en plusieurs étapes.
…..
Dans le cadre de l'évaluation des travaux des auteurs, j'ai contribué particulièrement sur la partie « threat modelling » et l'automatisation de l'attaque en langage SDL.

J'ai pu comprendre grâce à ce travail les modes d'évaluation d'une atteinte à l'intégrité d'un IoT présentant des vulnérabilités dans son protocole.

Cependant, nous avons observé que cette technique de modélisation n'est pas la seule, elle a été comparée avec une autre peu explicitée dans l'article, qui fait référence à un article précédent que nous avons utilisé.

Le lien avec le cours est précisément la partie etc....

Annexe : consignes pour le rapport – livrable 2

Partie II – Notre expérimentation

Auteur : Madame X., Monsieur Y., Madame Z.

La ré implémentation de l’attaque etc.....

Conclusion