Vulnérabilités Logicielles

Composante
École Nationale Supérieure d'Électrotechnique d'Électronique d'Informatique d'Hydraulique et des Télécommunications

En bref

Code: N9EN25A

Présentation

Objectifs

Apprentissage des concepts suivants :

- Vulnérabilités logicielles diverses
  - BOF diverses (piles, tas, BSS)
  - chaînes de format
  - integer overflow
  - programme SUID
  - return oriented programming
- Analyse statique undefined behavior
- Contre-mesures (Control Flow integrity, etc.)
- OpenBSD

Description

L'objectif de ce cours est de présenter aux étudiants différents types de vulnérabilités logicielles que l'on rencontre fréquemment, en particulier dans les programmes écrits en langage C, langage qui sera le support pour ce cours. Les contre-mesures usuelles protections mémoires permettant de se protéger de ce type de vulnérabilités sont également proposées.

A l'issue de cet enseignement, l'étudiant saura analyser un programme et juger de son niveau de sécurité en considérant les vulnérabilités logicielles présentées dans cet enseignement. Il sera capable d'identifier les tests à réaliser pour mettre en évidence l'existence d'une vulnérabilité logicielle. Il sera également capable de comparer différentes contre-mesures, d'identifier le plus adapté pour corriger une vulnérabilité et de le mettre en œuvre.

Enfin, on expose les bonnes pratiques de développement pour la sécurité. À l'aide du cas d'étude OpenBSD, les étudiants apprennent par exemple les bon choix architecturaux et fonctions de la bibliothèque standard C à utiliser ou éviter.