Discipline(s) : Infomatique et télécommunications

SOFTWARE VULNERABILITIES

Nature	UE

RESPONSABLES

Sandrine Blaz

OBJECTIFS

Comprendre les vulnérabilités qui peuvent affecter les programmes développés dans des langages où la gestion de la mémoire est effectuée directement par le programmeur (par exemple C, C++).
S'intéresser aux mécanismes (au niveau du système d'exploitation, du compilateur) permettant de détecter ces vulnérabilités, voire d'en empêcher le déclenchement à l'exécution.
Connaître les contre-mesures couramment employées pour se protéger contre ces vulnérabilités.

Ce cours est un cours de tronc commun du parcours securité du master informatique. Il comprend de nombreux TPs et son nombre d'heures est plus élevé que les autres cours du parcours Science Informatique

MOTS-CLÉS

vulnérabilité logicielle, corruption mémoire, shellcode, rétro-ingéniérie de code binaire, obfuscation de code

PRÉREQUIS

Langage C, connaître un langage assembleur, connaissances de base en système d'exploitation (gestion mémoire) et en compilation

CONTENU

Débordement mémoire
Mise en œuvre au moyen de shellcode
Rétro-ingéniérie de code
Obfuscation de code
Autres mesures préventives
Analyse statique, analyse dynamique de code

COMPÉTENCES ACQUISES

À l'issue de cette UE, les étudiants maîtriseront les techniques d'analyse de code binaire, de découverte de vulnérabilités de type débordement de mémoire et de protection associées.

APPARTIENT À

Master 2 informatique parcours Science Informatique

Mise à jour le 17 juillet 2017

CONTACT(S)

Département Informatique et télécommunications
École normale supérieure de RennesCampus de Ker LannAvenue Robert Schuman
35170 BRUZ
Tél. : 02 99 05 52 43
E-mail
Site Internet