Avviso di seminario

Dipartimento di Matematica e Fisica

Università degli Studi della Campania “Luigi Vanvitelli”

Giovedì 23 Settembre 2021 – Aula H, h. 15.00

RICARDO J. RODRIGUEZ

Universidad de Zaragoza,

Departamento de Informática e Ingeniería de sistemas (DIIS)

Catching Malware in Memory: Challenges and Issues

Abstract: Memory forensics is one of the steps of computer forensics, related to the analysis of digital evidence collected from the memory of the system under analysis after a computer incident. Memory forensics can be useful for recovering encryption keys, fileless malware, or (some) packaged samples. This seminar will cover the malware analysis process applied to memory forensic science and the current problems and open challenges faced during this process, presenting the latest advances made by my research group in this area. In particular, I will show how the memory acquisition and analysis process is performed on a memory dump, ending with the extraction of a suspicious artifact for malware analysis, and how the tools we have developed can help you during the analysis process.

Per motivi organizzativi, gli studenti interessati a partecipare sono pregati di contattare il prof. Stefano Marrone.

Il proponente,

Stefano Marrone