Descrizione progetto di ricerca
Sviluppo di un framework REST per Threat Attribution

Tutor: Prof. Mirko Viroli

9 aprile 2021

Abstract

L'assegno si inquadra nel contesto di attività di ricerca e sviluppo avviata in collaborazione con YOROI s.r.l., volta all'utilizzo di tecniche di analisi statica dei programmi per realizzare Threat Attribution, ossia attribuire a una organizzazione o gruppo un attacco informatico sulla base dell'analisi del codice malware.

Collocazione e attività di ricerca

Questa proposta è relativa ad un assegno di natura *commerciale*, e si colloca nelle attività di ricerca relative alla seguente collaborazione del DISI con una azienda del territorio:

- DISI - YOROI 2020/2021: Prototipo di Framework Software per Threat Attribution

Questa attività sottende la linea di ricerca che studia tecniche avanzate per l'ingegnerizzazione di sistemi software basate sul rapporto fra il linguaggio di programmazione o specifica, e i suoi tool (di analisi ed esecuzione). In particolare, lo scopo principale dell'assegno è quello di contribuire a sviluppare le tecniche, la metodologia, il design e l'implementazione necessari a definire un framework estendibile, e basato su REST API, per gestire il ciclo di vita della Threat Attribution.

Piano di Formazione

Alla luce del contesto delineato sopra, il progetto di ricerca sarà organizzato secondo le seguenti fasi:

1. studio e analisi del funzionamento di Malware e della loro Attribuzione
2. design architetturale di un framework REST per Threat Attribution;
3. implementazione prototipale;
4. sviluppo incrementale di meccanismi avanzati di attribuzione, basati su analisi statica di programmi e machine learning.

Ci si aspetta che le competenze acquisite in questa attività di ricerca consentano l'individuazione di contributi innovativi nell'intersezioni possibili fra gli ambiti di Software Engineering, Cybersecurity, e Machine Learning.