MAECO-Lite

A UFO-Grounded Modular Ontology for Dynamic Malware Analysis

Introduction

- **Heterogeneous representations:** Malware analysis relies on diverse models, standards, and tools to describe samples, runtime behaviours, and analysis results.
- **Semantic inconsistencies:** Differences in terminology and conceptualization hinder the integration, interpretation, and reuse of malware analysis knowledge.

Research Question

How can knowledge derived from dynamic malware analysis be represented in a semantically precise and coherent way?

Research Objectives

1. **Ontological analysis:** Analyse MAEC and selected STIX Cyber-Observable Objects (SCOs) using UFO to identify conceptual ambiguities and clarify their semantics.
2. **Ontology development:** Develop MAECO-Lite, a lightweight, modular ontology for dynamic malware analysis, aligned with UFO and incorporating relevant MAEC, STIX, and MITRE ATT&CK concepts.

The UFO-based analysis distinguishes enduring entities from event-like entities, thereby providing a principled foundation for MAECO-Lite.

MAEC and STIX

- **MAEC:** Provides a structured vocabulary for describing malware characteristics, behaviours, and analysis results.
- **STIX:** Represents and exchanges structured cyber threat intelligence, including malware-related information and relationships.

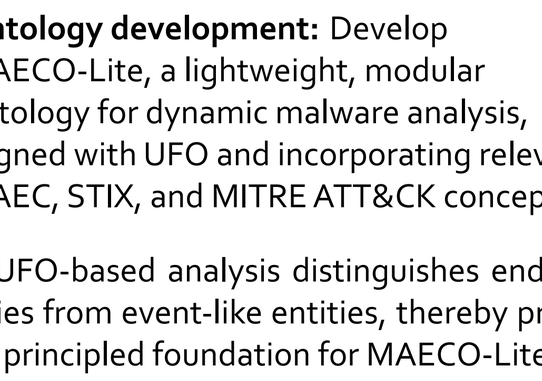


Figure 1-1. MAEC Overview

Unified Foundational Ontology (UFO)

- **Endurants:** Entities that persist through time, such as malware samples, files, and processes.
- **Perdurants:** Events and processes that unfold over time, such as runtime actions and behaviours.
- **Dispositions:** Intrinsic potentialities of entities to bring about certain events, such as malware capabilities.

UFO-Based Ontological Analysis of MAEC and STIX

The analysis examines selected MAEC constructs using UFO to identify their ontological categories and modelling inconsistencies.

- **Malware Instance:** A role played by a File during analysis, not a distinct entity type.
- **Action and Behavior:** Confuses dispositions (potentialities) with events (perdurants).
- **Process Tree Node:** Combines processual roles with temporal relations.
- **Observable Object:** A role mixin incorrectly specialized by kinds.

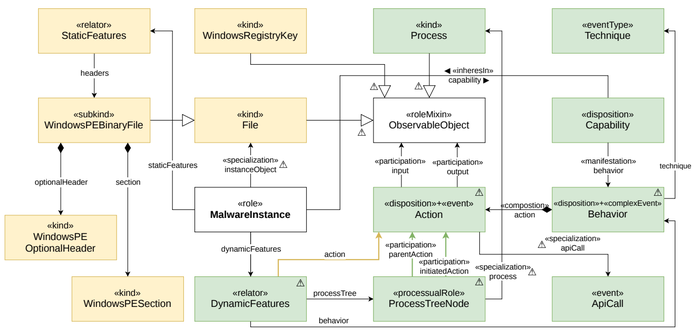


Figure 1. Ontological ambiguities and category conflicts identified in MAEC through UFO-based analysis.

MAECO-Lite Design

The ontology design was guided by five objectives:

1. **Behavioural representation:** Capture interpretable malware behaviours observed during sandbox execution.
2. **Simplicity:** Maintain a lightweight and computationally manageable structure.
3. **Standards alignment:** Reuse relevant concepts from MAEC, STIX, and MITRE ATT&CK.
4. **Ontological grounding:** Apply UFO to ensure conceptual clarity and semantic consistency.
5. **Modularity:** Organize concepts into coherent, feature-based modules.

MAECO-Lite Structure

MAECO-Lite is organized into five modules:

- **Core:** Consists of the main classes: Sample, Process, Action, File, WindowsRegistryKey, and Technique.
- **Actions:** Contains 146 action (API-call) classes, organized under 17 higher-level action categories.
- **Files** and **Registry:** Capture file-system and Windows registry interactions through specialized classes and relations.
- **Techniques:** Represents 691 MITRE ATT&CK techniques and 14 higher-level tactic-based categories.

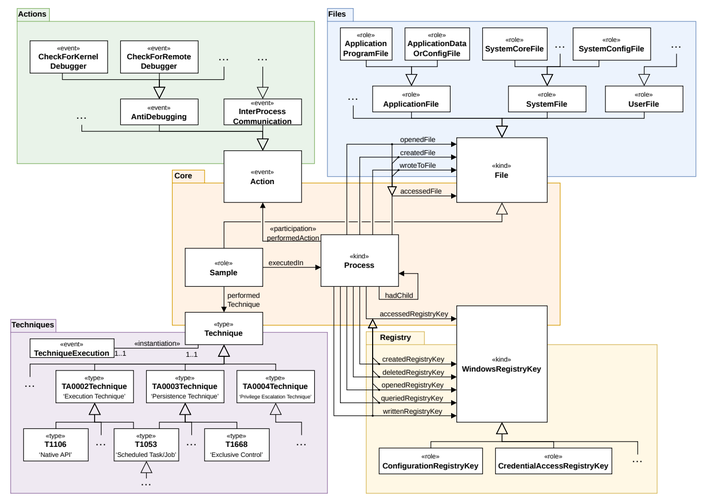


Figure 2. Overview of the five MAECO-Lite modules and their relationships.

Evaluation

Table 1. Results from baseline MAEC ontology.

Algorithm	Accuracy	Precision	Recall	FP Rate	F1
OCEL	0.49 ± 0.00	0.49 ± 0.00	1.00 ± 0.00	1.00 ± 0.00	0.66 ± 0.00
CELOE	0.49 ± 0.00	0.49 ± 0.00	1.00 ± 0.00	1.00 ± 0.00	0.66 ± 0.00
PARCEL	0.50 ± 0.00	0.00 ± 0.00	0.00 ± 0.00	0.00 ± 0.00	0.00 ± 0.00
SPACEL	0.50 ± 0.00	0.00 ± 0.00	0.00 ± 0.00	0.00 ± 0.00	0.00 ± 0.00

Table 2. Results from MAECO-Lite ontology.

Algorithm	Accuracy	Precision	Recall	FP Rate	F1
OCEL	0.79 ± 0.03	0.77 ± 0.03	0.83 ± 0.03	0.18 ± 0.03	0.80 ± 0.03
CELOE	0.74 ± 0.01	0.68 ± 0.01	0.89 ± 0.01	0.41 ± 0.03	0.77 ± 0.01
PARCEL	0.80 ± 0.01	0.86 ± 0.02	0.73 ± 0.01	0.11 ± 0.02	0.79 ± 0.01
SPACEL	0.71 ± 0.03	0.90 ± 0.02	0.48 ± 0.06	0.05 ± 0.01	0.62 ± 0.06

Learned Rules

Rule 1:

$\exists \text{executedIn}.\exists \text{performedAction}.\top$
$\sqcap \geqslant 2\ \text{performedTechnique}.\text{Defense Evasion Technique}$

Rule 2:

$\exists \text{performedTechnique}.\text{Process Hollowing}$
$\sqcap \exists \text{performedTechnique}.\text{Inter-Process Communication}$

COMENIUS UNIVERSITY BRATISLAVA

MATFYZ CONNECTIONS November 25, 2026 Bratislava, Slovakia

Zekeri Adams · Peter Švec · Ján Kľuka
Martin Homola · Roderik Ploszek
Monday Onoja · Štefan Balogh