Digital Forensics Investigation Research Group

Towards Automated Forensic Event Reconstruction of Malicious Code

Ahmed F.Shosha
Ahmed.Shosha@ucdconnect.ie

Joshua I.James
Joshua.James@ucd.ie

Chen-Ching Liu
Liu@ucd.ie

Pavel Gladyshev
Pavel.Gladyshev@ucd.ie

Digital Forensics Investigation Research Group, School of Computer Science and Informatics, University College Dublin, Ireland

Motivation

- Digital forensic investigation is based on investigators' practical experience; It lacks formal theories to support it.
- Formal investigative methods for digital forensics are needed.
- The need to extend the applications of **Event Reconstruction Theory** to malicious software digital forensic investigation.

The Problem

- **Formally** prove that an evidence trace object is a results of an execution of specific malware.
- **Identify** which execution path in malware code has contributed in the creation of the evidence trace.
- **Inferring** further malicious evidence traces.
- **Investigation** of Anti-Forensic techniques.

Formal Malware Forensic Investigation and Event Reconstruction Method

Modelling Malware Code → **Formalising Evidence and Observations** → **Model-Check Observed Evidence** → **Reconstruct Malicious Events**

Malicious code CFG is modelled as $\mathcal{M}$ using FSA.

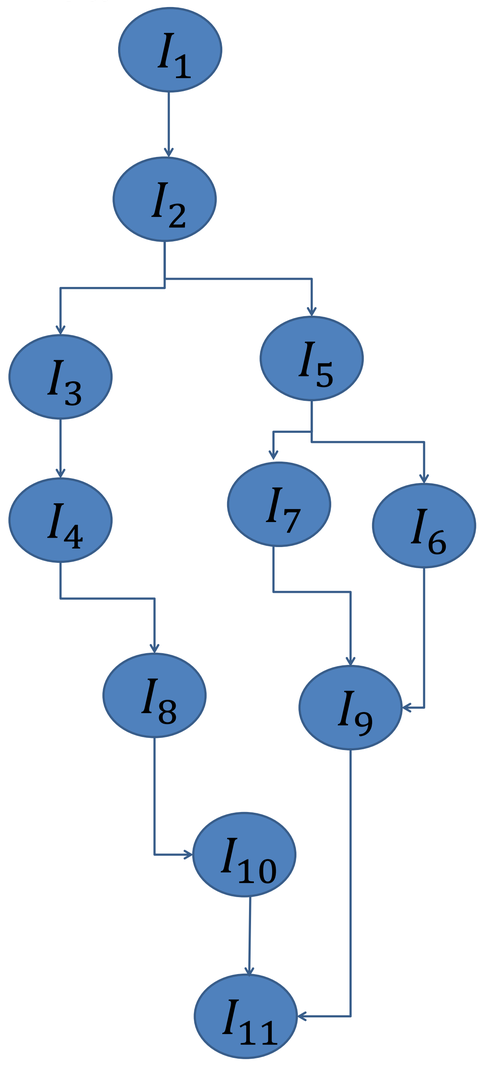
Evidence object is described in Comp. Tree Logic (CTL) formula, $\Gamma = \varphi_1 \ldots \vee \varphi_n$.

Evidence objects are checked in $\mathcal{M}$ using model checking algorithm.
$\mathcal{M}$ (CFG) $\vDash \Gamma$(Evidence).

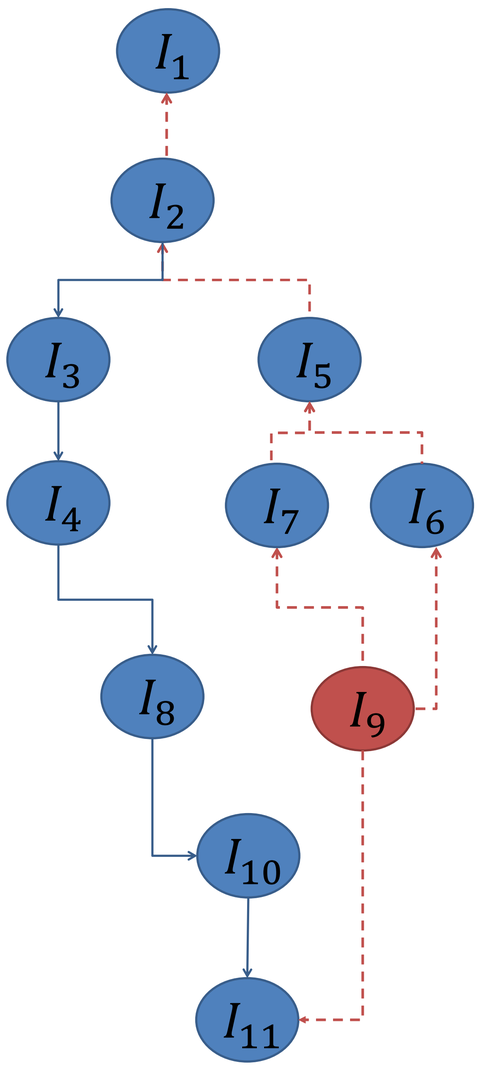
Further evidence traces are reconstructed using event reconstruction algorithm. $\psi^{-1}(\mathcal{M})$.

Evidence Trace Model Checking

$\varphi_x = \mathbf{EF}\langle \text{Evidnce} \rangle \wedge \mathbf{AF}[\![(\text{ Evidnce Property})]\!]$



Model CFG Automton.



Reconstructed Model.

Anti-Forensic Investigation

Formalising Anti-Forensic logic in CTL → **Model-Check the technique logic in $\mathcal{M}$**

- Anti-Forensic methods are described in CTL φ.
- φ (Anti-Forensic) is model-checked in $\mathcal{M}$.
- Evidence traces bounded to Anti-Forensic formula φ are identified.
- reverse-engineering the impact of Anti-Forensic techniques.

This research is supported by EU FP7 project, "A Framework for Electrical Power Systems Vulnerability Identification, Defence and Restoration (AFTER)."