Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

SECURITY ASSURANCE ACROSS SYSTEM LAYERS

From Credentials to Learning Systems to Executables

Antreas Dionysiou,
Marie Skłodowska-Curie Postdoctoral Fellow
A.Dionysiou@tudelft.nl

RESEARCH VISION

To design security mechanisms that detect compromise, leakage, and tampering across three critical layers of modern computing systems.

MODERN SYSTEMS

- **TRUST IN AUTHENTICATION** — Detecting Credential Compromise *(Honeywords, Deception)*
- **TRUST IN LEARNED MODELS** — Privacy & Integrity of ML Systems *(Inference, Inversion)*
- **TRUST IN EXECUTABLES** — Post-Compilation Binary Tampering *(Memory-Safety Validation)*

CREDENTIAL LAYER

Problem

Credential database breaches remain undetected for months or even years.

Approach

Leverage honeywords credentials to detect misuse of leaked credential databases during authentication.

Key Insight

Credential theft becomes detectable at the moment of exploitation.

Representative Work

- *Dionysiou et al.*, HoneyGen (AsiaCCS 2021)
- *Dionysiou et al.*, Lethe (EuroS&P 2022)

ML SYSTEMS

Problem

ML models can leak sensitive information or misbehave in response to crafted inputs.

Approach

Estimate the feasibility of security & privacy ML attacks under practical black-box threat models.

Key Insight

Many state-of-the-art attacks fail in real-world settings — but some leaks persist.

Representative Work

- *Dionysiou et al.*, SoK on MIAs (PETS 2023)
- *Dionysiou et al.*, Deep-BMI (PETS 2023)
- *Dionysiou et al.*, EvilText (AISEC 2021)

EXECUTION LAYER

Problem

Memory-safe binaries can lose safety guarantees after compilation due to tampering.

Approach

Pre-execution validation of compiled binaries to ensure safety checks remain intact.

Key Insight

Memory safety must be verified at load-time, not assumed.

Representative Work

- *Louka et al.*, Memory safety in Rust (EuroSec 2024)
- *Moreno et al.*, System call interposition (Middleware 2025)
- VALIDATE (MSCA-PF, ongoing)

TAKE-HOME MESSAGE

Protecting modern systems requires a multilayered approach — from detecting credential database breaches, to securing ML models, to validating executables.

Scan for Publications & Contact