RIVERSIDE RESEARCH

UC-PACT

Universal Composability for Preventing Adversarial Composition Techniques

Riverside Research, a leader in open architecture security solutions with a proven track record in the defense and intelligence communities, has received a multi-year award from DARPA.

Along with teammates, Boston University and High Peaks Cyber, Riverside Research is conducting research under DARPA's Hardening Development Toolchains Against Emergent Execution Engines (HARDEN) program.

The HARDEN program aims to develop practical tools that will prevent exploitation of integrated computing systems by disrupting robust patterns of reliable exploits used by attackers, and depriving the attackers of emergent execution engines.

Riverside Research is helping achieve DARPA's goal through the automatic translation of emergent vulnerabilities and system software into Universal Composability for Preventing Adversarial Composition Techniques (UC-PACT) Domain-Specific Language (DSL) as well as the translation of Sensor Open Systems Architecture (SOSA™) specifications to UC-PACT DSL.

> *"This effort is significant because it enables us to develop technology that will have a broad security impact on DoD Open Architectures."*

Dr. Mike Clark, Associate Director
Secure and Resilient Systems Group
Riverside Research

This material is based upon work supported by the Defense Advanced Research Projects Agency (DARPA) and Naval Information Warfare Center Pacific (NIWC Pacific) under N66001-22-C-4020.

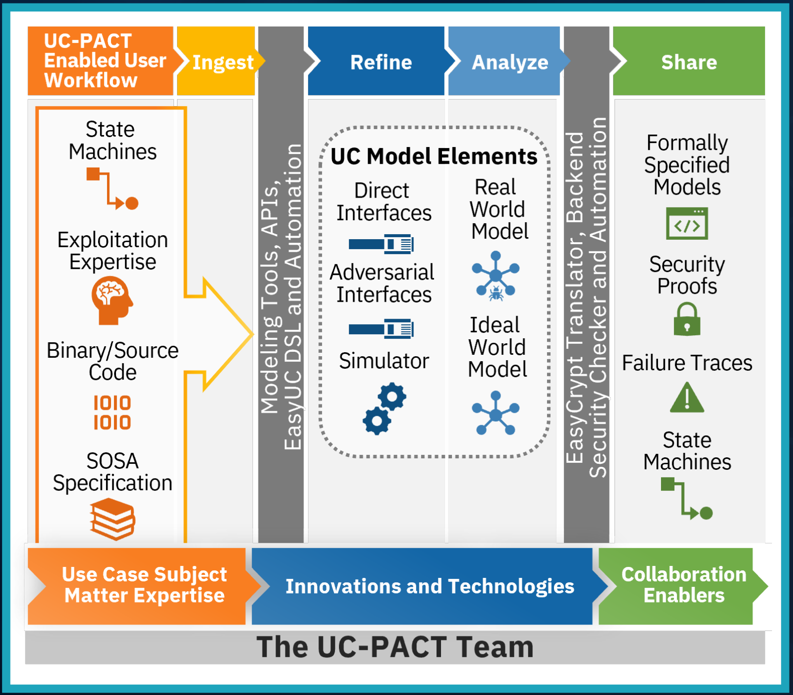
Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the DARPA and NIWC Pacific.

Distribution A: Approved for Public Release

Riverside Research is an independent nonprofit focused on our nation's security. Our nonprofit structure allows us to design solutions that follow where the science leads, and our collaborative innovation model produces accelerated results. Our independent research and development is in the public interest and for the benefit and furtherance of the U.S. government's mission-related work.

RIVERSIDERESEARCH.ORG
MCLARK@RIVERSIDERESEARCH.ORG

UC-PACT WORKFLOW IS DESIGNED FOR NON-FORMAL METHOD EXPERTS



UC-PACT Enabled User Workflow

Ingest

Refine

Analyze

Share

State Machines

Exploitation Expertise

Binary/Source Code

1010
1010

SOSA Specification

Modeling Tools, APIs, EasyUC DSL and Automation

UC Model Elements

Direct Interfaces

Adversarial Interfaces

Simulator

Real World Model

Ideal World Model

EasyCrypt Translator, Backend Security Checker and Automation

Formally Specified Models

Security Proofs

Failure Traces

State Machines

Use Case Subject Matter Expertise

Innovations and Technologies

Collaboration Enablers

The UC-PACT Team

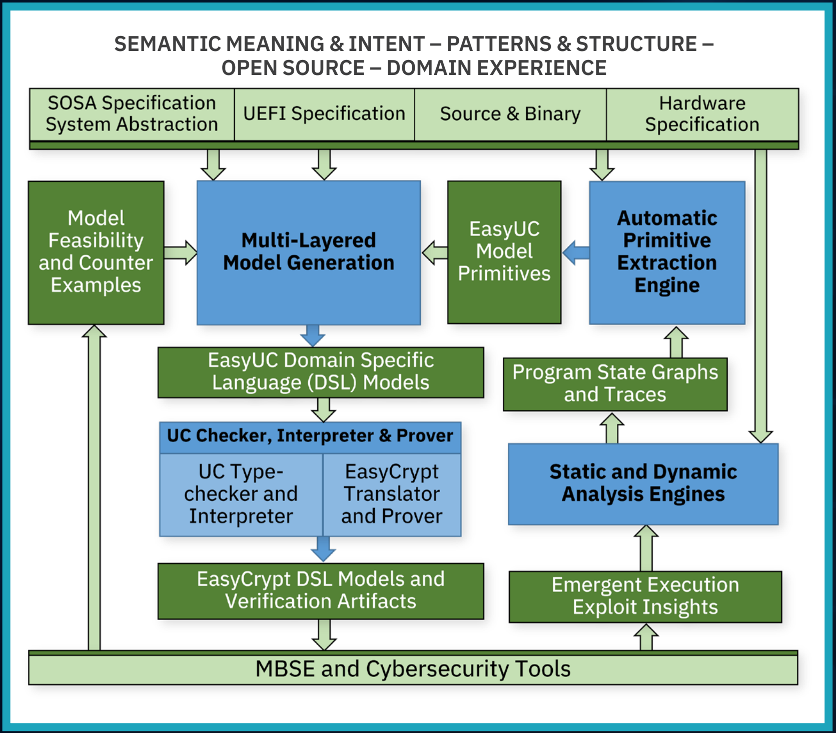
Interactive modeling tool capturing system interfaces and behaviors for formal security assessment

Cross-layer reasoning about and mitigation of emergent execution engines

Model-based System Security Engineering for SOSA security needs, including trusted-sensor startup

Automating model generation using specification artifacts, adversarial model categorizations, and code state graphs from static and dynamic analyses

HOW WE WILL PROVIDE THE WORKFLOW



SEMANTIC MEANING & INTENT – PATTERNS & STRUCTURE – OPEN SOURCE – DOMAIN EXPERIENCE

SOSA Specification System Abstraction

UEFI Specification

Source & Binary

Hardware Specification

Model Feasibility and Counter Examples

Multi-Layered Model Generation

EasyUC Model Primitives

Automatic Primitive Extraction Engine

EasyUC Domain Specific Language (DSL) Models

Program State Graphs and Traces

UC Checker, Interpreter & Prover

UC Type-checker and Interpreter

EasyCrypt Translator and Prover

Static and Dynamic Analysis Engines

EasyCrypt DSL Models and Verification Artifacts

Emergent Execution Exploit Insights

MBSE and Cybersecurity Tools

MULTI-LAYERED MODEL GENERATION: Encode traditional exploits, classes of Common Weakness Enumerations (CWEs), and difficult to capture emergent execution

EASYCRYPT TRANSLATOR AND PROVER: Provide semi-automatic synthesis of UC DSL models, and improve both the EasyCrypt proof assistant and EasyUC DSL

STATIC AND DYNAMIC ANALYSIS ENGINES: Leverage Ghidra and Unicorn to extract program state graphs and traces to enable automatic synthesis of UC model elements (e.g., real functionalities)

AUTOMATIC PRIMITIVE EXTRACTION ENGINE: Automatically generate intended and adversarial interfaces to surface emergent execution engines within our UC models

RIVERSIDE RESEARCH

RIVERSIDERESEARCH.ORG
MCLARK@RIVERSIDERESEARCH.ORG