

Opportunity Title: Improving Program Understanding with Fine-Grained

Execution Traces Fellowship

Opportunity Reference Code: ICPD-2024-52

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2024-52

How to Apply **Create and release your Profile on Zintellect** – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 3 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: <https://orise.orau.gov/icpostdoc/index.html>.

If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

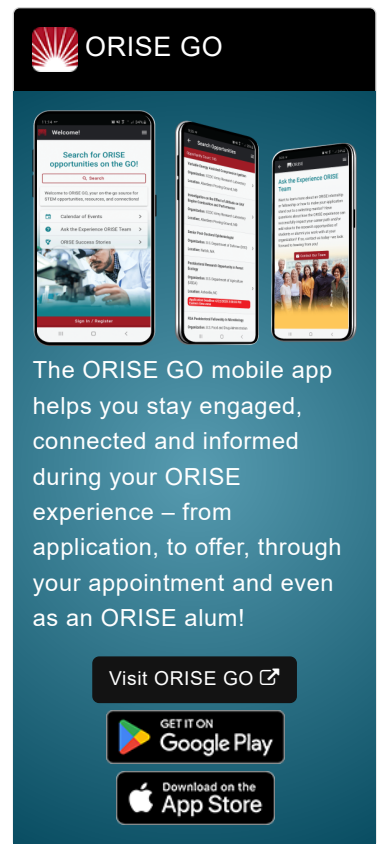
Application Deadline 2/28/2024 6:00:00 PM Eastern Time Zone

Description **Research Topic Description, including Problem Statement:**

How can detailed program execution traces be leveraged to improve and accelerate software reverse engineering and software testing tasks? Software reverse engineering, specifically decompilation, is predominately a static analysis task and tends to run up against undecidability early. Current dynamic analyses are coarse-grained (e.g. dynamic taint tracking) or do not provide any feedback to static analysis tools. Leveraging fine-grained program execution traces (e.g. changes to program state including registers and memory on a per-instruction basis) may allow software reverse engineering tools to improve their outputs by providing concrete information in locations where they would normally fallback on heuristics.


Example Approaches:


There is previous research into performing type inference on program traces (<https://doi.org/10.1145/2896499>) which could serve as a basis for improving decompilation in software reverse engineering tools. Common software reverse engineering platforms rely heavily on type information to provide human-readable decompilation, but types can be impossible to infer from local context (within a function) and prohibitively expensive to infer across a whole program. Utilizing type inference across a series of program execution traces, it should be possible to provide additional context to a decompiler, especially for values on the heap. Alternatively, there are tools for dynamically inferring likely invariants from a program execution trace (<https://doi.org/10.1016/j.scico.2007.01.015>). These invariants tend to be difficult for humans to reason about, particularly when source code is unavailable for the software under test. Type information inferred by static analyses in software reverse engineering platforms could provide the scaffolding to reason about invariants generated by these tools at the proper level of abstraction for program understanding (e.g. these are the likely invariants a type must uphold between member variables vs. these




ORISE GO

The ORISE GO mobile app helps you stay engaged, connected and informed during your ORISE experience – from application, to offer, through your appointment and even as an ORISE alum!

Visit ORISE GO 

GET IT ON
 Google Play

Download on the
 App Store

Opportunity Title: Improving Program Understanding with Fine-Grained

Execution Traces Fellowship

Opportunity Reference Code: ICPD-2024-52

are the invariants upheld by these regions of memory at these PCs).

Relevance to the Intelligence Community:

- Develop/enhance near-real-time cyber forensics.
- Develop/enhance capabilities for document and media analysis.

Key Words: Software Reverse Engineering, Software Testing, Static Analysis, Dynamic Analysis

Qualifications Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the appointment start date
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
 - **Chemistry and Materials Sciences** ([12](#))
 - **Communications and Graphics Design** ([3](#))
 - **Computer, Information, and Data Sciences** ([17](#))
 - **Earth and Geosciences** ([21](#))
 - **Engineering** ([27](#))
 - **Environmental and Marine Sciences** ([14](#))
 - **Life Health and Medical Sciences** ([45](#))
 - **Mathematics and Statistics** ([11](#))
 - **Other Non-Science & Engineering** ([2](#))
 - **Physics** ([16](#))
 - **Science & Engineering-related** ([1](#))
 - **Social and Behavioral Sciences** ([30](#))