

Opportunity Title: Strengthening Container Security Through Cyber Forensics and Zero Trust Fellowship

Opportunity Reference Code: ICPD-2024-11

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2024-11

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.

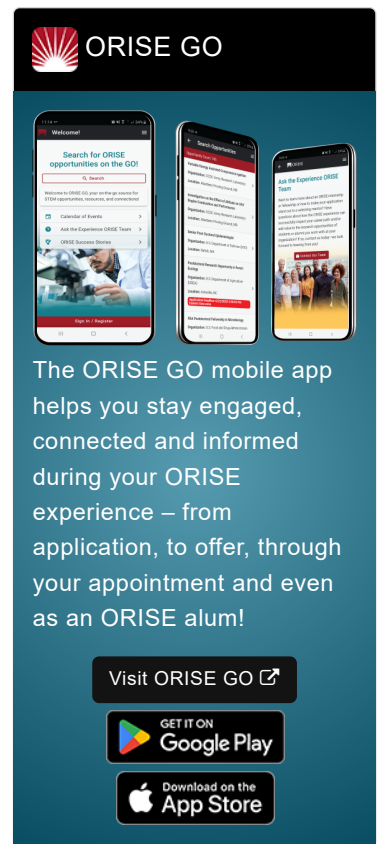
Application Deadline 2/28/2024 6:00:00 PM Eastern Time Zone

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

Widespread malware attacks on container repositories can impact on data integrity in national security applications. Third party access has been identified as a major contributor to the problem. The plan is to employ a new cyber forensic tool in a zero-trust security environment to mitigate and reduce the ability of cyber intrusions that can alter and steal valuable data.


Successful mission operations depend on the ability of an organization to collect, manage, analyze, and secure its data. Traditional network frameworks have become less appealing because they rely on a “trust but verify” paradigm that does not stand up well against the advanced tools and techniques of modern cyber attackers. The Zero Trust Framework has emerged as a logical replacement because it represents a paradigm shift to a “high-level strategy that assumes that individuals, devices, and services cannot automatically be trusted.” It is essential that the IC be able to trust the data that it depends, which is often stored in data repositories, arguably, the most prominent means for data sharing around the globe. Hence, the repositories must be trustworthy and secure. Unfortunately, widespread malware attacks on data repositories have recently been reported, in some cases, impacting data critical to national security. Third-party apps, a staple of how we interact with data and services in both cloud and mobile-driven environments have shown a number of potential risks and breaches that signal a growing and troubling trend.


Most of the recently recorded attacks on data repositories have largely been accomplished through “access” tokens that authorize the sharing of specific user account information. The latest attacks on data repositories seem to have a common thread, i.e., they come primarily through third party access provided by ()Auth, the open standard for token-based authentication and authorization.




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: Strengthening Container Security Through Cyber Forensics and Zero Trust Fellowship

Opportunity Reference Code: ICPD-2024-11

Through ()Auth, request links, recipients can be deceived into illicit grants, e.g. consent phishing emails that can enable access to attackers via API resources. In these cases, targeted users unknowingly grant permissions that allow attackers to make API calls on their behalf through attacker-controlled apps. Unfortunately, access to cloud SaaS environments is obtained with relative ease due to end user-granted permissions occurring without much scrutiny. Permissions can be granted by end users simply via a permissions request submitted from the third-party app. Similar problems can also occur through browser extensions via application performance interfaces (APIs). These clear cases that remind us of the dangers of pushing for greater access without a parallel focus on security.

As a result, the focus of this proposal is to develop a new framework based on advanced cyber forensics and the zero trust security model to improve container security in applications critical in select NATO operations.

- The objective is to examine the performance of a new cyber forensic tool, currently used in law enforcement, and if it can be extended to NATO-related applications through the use of a zero trust security model.
- In this study, the emphasis is placed on an advanced forensic based cyber security framework aligned with a zero trust security model that relies more on data lineage, end-to-end metadata, and the use of machine learning tools and methodologies. Most of the current computer forensic software have weaknesses that by themselves make them ill-suited for certain types of analyses. Such shortcomings require cross-validation of findings, wherein machine learning tools and techniques can play an important role.

The results of this research are expected to provide mitigation strategies and insight into adversary efforts to compromise or steal valuable data in NATO operations. The study will serve as a foundation for future endeavors that identify cyber vulnerabilities and exploits used, as well as ways to counter and protect critical data from intrusions.

Example Approaches:

Intrusion Detection and Prevention, Cyber Forensics, SIEM

Relevance to the Intelligence Community:

- Develop/enhance near real-time cyber forensics.

Key Words: Zero Trust Framework, Cyber forensics, Machine Learning, Data Repositories, Containers

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

Opportunity Title: Strengthening Container Security Through Cyber Forensics and Zero Trust Fellowship

Opportunity Reference Code: ICPD-2024-11

- 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** ([6](#))
 - **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](#))