Opportunity Title: Protocol-Agnostic Device Identification and Authentication in Smart Cities Fellowship
Opportunity Reference Code: ICPD-2024-30

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2024-30

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:**

Smart cities are physically distributed and typically uncontrolled environments within which a wide range of devices are deployed. To ensure the security of their environments, system integrators and maintainers of smart cities need to have comprehensive awareness of devices within their smart city networks, and confidence that those devices are not being impersonated. While some of this functionality may be provided by network protocols used in a smart city, the heterogeneity of current smart city networks does not present a clear mechanism for system-wide device identification and authentication.

This project would be expected to:

- Determine classes of devices and associated communications protocols likely to be used in an Australian smart city. Explicate existing methods for device identification and authentication applicable to these device classes and protocols.
- Review both current and conceptual future flaws in the secure authentication of smart city devices. This would include techniques that allow for the impersonation of devices at the time of provisioning or at a later date due to a practical physical or online attack.
- Devise a device and communications protocol-independent architecture which facilitates the identification and secure authentication of all devices connected in a smart city environment.
- Deploy the architecture, using a variety of case study devices deployed in representative networks, within a laboratory environment to validate its effectiveness against the identified flaws.

Example Approaches:

Suggested approaches would include:

- Literature review, public vendor documentation analysis and open-source intelligence scan to determine:
  - The types of devices and communications protocols commonly used in Australian smart cities.
  - Current methods for smart city device and network identification and authentication.
  - Current flaws in the secure authentication of smart city devices.
- Analysis and laboratory research to determine:
  - The validity of any published flaws and potential attacks on the identification and authentication of smart city devices.
  - A device and communications protocol-independent architecture which facilitates smart city device identification and secure authentication.
  - The validity of the architecture against identified attacks and flaws using a variety of case study devices deployed in representative networks.

Relevance to the Intelligence Community:

Smart Cities and similar initiatives are large-scale deployments of interconnected systems and devices that observe, analyse and act upon data to provide a service or function to the public. The union of discrete technology stacks at a large scale is what provides the utility of a smart city. Technologies deployed at such a scale promise to improve the lives of citizens, efficiently deliver essential and ancillary services, and increase economic productivity with minimal user interaction.

The highly connected nature of a smart city creates a unique risk profile that must be considered. Increased scale and complexity create novel risks and amplify those already known. Identifying and authenticating devices in this environment is a critical first step in helping risk owners appropriately manage and secure their systems.

Information relevant to the intelligence community could be prioritized as follows:

- Mechanisms to detect unknown devices in complex systems.
- Authentication mechanisms that protect against impersonation of devices at time of provisioning in large complex systems.
- Architectures that validate the detection of all devices across a network with little to no performance depreciation.
- Active and passive authentication mechanisms in complex systems.

Understanding how to identify and authenticate complex protocol agnostic devices will lay a foundation to provide incident responders and cyber uplift analysts with the necessary information to address the risks associated with the field in terms of national security.

Reference:

L. Xia, D.T. Semirumi, R. Rezaei, (2023), ‘A thorough examination of smart city applications: Exploring challenges and solutions throughout the life

cycle with emphasis on safeguarding citizen privacy', Sustainable Cities and Society, Volume 98, https://doi.org/10.1016/j.scs.2023.10477.

Key Words: Complex Systems, Architecture, Device Discovery, Smart Cities, IoT, IIoT, Cyber Security, Data Verification, Authentication, Identification.

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)