PREP Research Associate

This position is part of the National Institute of Standards (NIST) Professional Research Experience (PREP) program. NIST recognizes that its research staff may wish to collaborate with researchers at academic institutions on specific projects of mutual interest, thus requires that such institutions must be the recipient of a PREP award. The PREP program requires staff from a wide range of backgrounds to work on scientific research in many areas. Employees in this position will perform technical work that underpins the scientific research of the collaboration.

Research Title:
Evaluating and Advancing Measurement of Real-Time Deepfake Detection and Digital Injection Prevention for Digital Identity Services

U.S. Citizen Preferred

The work will entail:
The increased availability of generative AI technology has given rise to fear of these tools being used to disrupt any number of cybersecurity safeguards implemented by US Government and commercial systems. Most notably, identity systems used to enable remote proof of identity and online access have found themselves in the crosshairs of attackers [1,2,3]. Many of these use real-time deepfake technology to defeat biometrics and human-supported identity verification systems. They use technical measures to insert (known as injection) modified or forged media (images or videos) into communication channels to defeat matching algorithms, presentation attack detection, or human reviewers. Protections against these attacks focus on two areas: defending against the injection and detecting the deepfakes. The project will focus on providing controls for the first and measurement for tools used in detection. No organization should rely on just one of these methods as it should be assumed that attackers will be able to achieve an injection. This makes accurate detection imperative, while at the same time, all efforts need to be made to deter injections since detection algorithms are nascent and will likely miss well-crafted deepfakes. Some products currently support detection capabilities, yet there are no well-established metrics, tests, or standards to measure the effectiveness of these technologies in combating real-world threats.

This project will address this gap by evaluating risks posed by emerging injection techniques and real-time deepfakes and establishing a framework for measuring the efficacy of available controls. It will give NIST the foundation for a measurement-based approach to support federal government guidelines and future technology assessments. Ideally this research will set the framework for an ongoing technical evaluation capability like those established by the Face Recognition Technology Evaluation and Face Analysis Technology Evaluation programs.

Key responsibilities will include but are not limited to:

- Generating deepfake artifacts,
- proposing a scientific framework for evaluation of different detection and prevention tools
- recommending performance metrics for detection systems

- Presenting results at internal meetings, and occasional meetings with external stakeholders.
- Ensuring that results, protocols, software, and documentation have been archived or otherwise transmitted to the larger organization
- assisting in the development of research papers or guidelines

Qualifications

- A Doctorate or in a Doctoral program with a focus on Computer Science, Engineering, or Cybersecurity
- 5-8 years of relevant experience.
- Expertise in biometric systems and biometric system threats
- Ability to work with leading software and hardware to replicate deepfake threats and evaluate detection system performance
- Familiarity with multiple scripting languages.
- Ability to develop deepfake artifacts for testing.
- Strong oral and written communication skills.

Privacy Act Statement

Authority: 15 U.S.C. § 278g-1(e)(1) and (e)(3) and 15 U.S.C. § 272(b) and (c)

Purpose: The National Institute for Standards and Technology (NIST) hosts the Professional Research Experience Program (PREP) which is designed to provide valuable laboratory experience and financial assistance to undergraduates, post-bachelor's degree holders, graduate students, master's degree holders, postdocs, and faculty.

PREP is a 5-year cooperative agreement between NIST laboratories and participating PREP Universities to establish a collaborative research relationship between NIST and U.S. institutions of higher education in the following disciplines including (but may not be limited to) biochemistry, biological sciences, chemistry, computer science, engineering, electronics, materials science, mathematics, nanoscale science, neutron science, physical science, physics, and statistics. This collection of information is needed to facilitate administrative functions of the PREP Program.

Routine Uses: NIST will use the information collected to perform the requisite reviews of the applications to determine eligibility, and to meet programmatic requirements. Disclosure of this information is also subject to all the published routine uses as identified in the Privacy Act System of Records Notices: NIST-1: NIST Associates.

Disclosure: Furnishing this information is voluntary. When you submit the form, you are indicating your voluntary consent for NIST to use of the information you submit for the purpose stated.