SIVANA HAMER

Ph.D. Student in Computer Science | Researching Software Supply Chain Security

@ sahamer@ncsu.edu   🌐 sivanahamer.github.io   in sivanahamer   ⌂ sivanahamer   ✦ Sivana Hamer

Second-year Computer Science Ph.D. Student at North Carolina State University. Currently, I am researching the **state of software supply chain security** as a community **to help improve the security posture of industry and open-source projects**. I look forward to opportunities to conduct software supply chain security research.

EXPERIENCE

Graduate Research Assistant
North Carolina State University

📅 Aug 2023–Present

Researcher and Interim Instructor
Universidad de Costa Rica

📅 2020-2023

Student Visitor Research Internship
Carnegie Mellon University

📅 Jan 2022–March 2022

FEATURED RESEARCH PROJECTS

How not to be Solarwinds, Log4j, or XZ Utils

- Analyzing how major software supply chain attacks (SolarWinds, Log4j, XZ Utils) occurred and what are safeguards against attacks to guide companies in adopting related software supply chain safeguards and frameworks. Collaboration with **Yahoo**.
- **Methods:** Qualitative Analysis, Incident Analysis, LLM.
- **Tools:** MITRE ATT&CK, Threat Modeling, P-SSCRM.
- **Publication:** Work in progress planning to submit Q1 2025.

Reputation Measures to Review Dependencies

- Investigated if network centrality measures, proxying contributor reputation, can be used as a signal to inform developers of dependency changes that require additional examination.
- **Methods:** Mixed-Methods, Statistical Models, Social Networks.
- **Results:** Network centrality measures are a significant factor in explaining how developers review dependencies in Rust.
- **Tools:** Python, R, SQL, GitHub API.
- **Publication:** Major Revision in Transactions of Software Engineering.

Comparing Vulnerabilities ChatGPT and StackOverflow

- Compared the vulnerabilities of ChatGPT and StackOverflow to help raise software developers' awareness of the security implications when selecting code snippet platforms.
- **Method:** Quantitative Analysis, Statistical Methods.
- **Results:** ChatGPT generated less vulnerable code. Yet, insecure code propagation can happen in both platforms.
- **Tools:** Python, R, ChatGPT API, StackOverflow API, CodeQL.
- **Publication:** In IEEE Security and Privacy Workshops 2024.

RESEARCH INTERESTS

Software Supply Chain Security • Software Security • Empirical Software Engineering • Software Measurement

EDUCATION

Ph.D. Computer Science
North Carolina State University

📅 Aug 2023 – Expected 2028

Advisor: Dr. Laurie Williams

M.Sc. Computer Science
Universidad de Costa Rica

📅 2023

Thesis: Mining software repositories to automatically measure developer code contributions. *Advisor:* Dr. Christian Quesada-López

B.Sc. Computer Science
Universidad de Costa Rica

📅 2020

AWARDS

- *Goodnight Doctoral Fellowship (2023-2027).*
- *RSA Conference Security Scholar (2024).*
- *North Carolina State University Provost's Doctoral Fellowship (2023).*
- *Best Postgraduate Grade Universidad de Costa Rica* (2020).

SKILLS

- *Languages:* English, Spanish.
- *Programming languages:* Python, Java, R, C#, JavaScript, Bash, SQL.
- *Software tools:* Git, Jenkins, JIRA, Visual Studio Code, CodeQL, SonarQube, LLM.
- *Frameworks and libraries:* ASP.NET, Flask, Bootstrap, jQuery, React, Unity.
- *Research methods:* Quantitative, Qualitative, Mining Software Repositories, Machine Learning, Statistical Models.