SIVANA HAMER

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

sahamer@ncsu.edu sivanahamer.github.io sivanahamer sivanahamer Sivana Hamer

Third-year Computer Science Ph.D. Student at North Carolina State University. I am currently researching the **state of software supply chain security** as a community **to help improve the security posture of industry and open-source projects**. I have published in top software engineering venues such as ICSE, TSE, FSE, and TOSEM. I am also a Google and Goodnight PhD fellow. I look forward to opportunities to conduct software supply chain security research.

RESEARCH INTERESTS

Software Supply Chain Security • Software Security • Empirical Software Engineering • Software Measurement • Software Security • Mining software repositories

FEATURED RESEARCH PROJECTS

Reduce your risk of being Solarwinds, Log4j, or XZ Utils

- Analyzing the attack techniques in SolarWinds, Log4j, and XZ Utils to systematically synthesize software supply chain framework tasks to provide software organizations with a recommended starter kit of tasks. Collaboration with **Yahoo**.
- **Methods:** Qualitative Analysis, Incident Analysis, Meta Synthesis.
- **Results:** Frameworks are missing tasks; hence, even if all tasks were adopted, organizations would still be vulnerable to attacks.
- **Tools:** MITRE ATT&CK, Threat Modeling, P-SSCRM, LLMs.
- **Publication:** In International Conference on Software Engineering 2026.

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:** In IEEE Transactions on Software Engineering 2025.

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.

AWARDS

- *Google PhD Fellowship (2025-2027).*
- *Goodnight Doctoral Fellowship (2023-2027).*
- *International Conference on Software Engineering Distinguished Shadow Reviewer (2026).*
- *RSA Conference Security Scholar (2024).*
- *North Carolina State University Provost's Doctoral Fellowship (2023).*
- *Best Postgraduate Grade Universidad de Costa Rica* (2020).

EDUCATION

Ph.D. Computer Science — Aug 2023 – Expected 2027
North Carolina State University
Advisors: Dr. Laurie Williams and Dr. William Enck

M.Sc. Computer Science — 2023
Universidad de Costa Rica
Thesis: Mining software repositories to automatically measure developer code contributions.
Advisor: Dr. Christian Quesada-López

B.Sc. Computer Science — 2020
Universidad de Costa Rica

EXPERIENCE

Graduate Research Assistant — Aug 2023–Present
North Carolina State University

Security Research Intern — May 2025–Aug 2025
Phoenix Security

Researcher and Interim Instructor — 2020-2023
Universidad de Costa Rica

Student Visitor Research Intern — Jan 2022–Mar 2022
Carnegie Mellon University

PUBLICATIONS

Conferences & Workshops

- **Hamer, Sivana**, "Towards a Software Supply Chain Security Barometer: A Model to Assess and Guide Community Efforts," in *International Conference on Software Engineering - Doctoral Sympossium (ICSE-DS)*, 2026.
- **Hamer, Sivana**, J. Bowen, M. N. Haque, R. Hines, C. Madden, and L. Williams, "Closing the Chain: How to reduce your risk of being SolarWinds, Log4j, or XZ Utils," in *International Conference on Software Engineering (ICSE)*, 2026.
- L. Williams, **Hamer, Sivana**, and N. Zahan, "Can the rising tide of software supply chain attacks raise all software engineering boats?" In *Companion Proceedings of International Conference on the Foundations of Software Engineering (FSE Keynote)*, ACM, 2025.
- **Hamer, Sivana**, M. d'Amorim, and L. Williams, "Just another copy and paste? comparing the security vulnerabilities of chatgpt generated code and stackoverflow answers," in *Deep Learning Security and Privacy Workshop*, IEEE Security and Privacy Workshops (SPW), 2024.
- C. Quesada-López, **Hamer, Sivana**, and M. Jenkins, "Exploring students' behaviors and perceptions in continuous measurement of software projects," in *Latin American Computing Conference (CLEI)*, IEEE, 2024.
- **Hamer, Sivana**, C. Quesada-López, and M. Jenkins, "Students' perceptions of integrating a contribution measurement tool in software engineering projects," in *IEEE International Conference on Software Engineering Education and Training*, 2023.
- E. Kuhlmann, **Hamer, Sivana**, and C. Quesada-López, "Visualización de software como ciudad: Un análisis de percepciones y experiencias de estudiantes," in *Latin American Computing Conference (CLEI)*, IEEE, 2023.
- **Hamer, Sivana**, C. Quesada-López, and M. Jenkins, "Automatically recovering students' missing trace links between commits and user stories," en, in *Conferencia Iberoamericana de Software Engineering (CIbSE)*, 2021.
- **Hamer, Sivana**, C. Quesada-López, and M. Jenkins, "Students projects' source code changes impact on software quality through static analysis," in *Quality of Information and Communications Technology*, Springer International Publishing, 2021.

- **Hamer, Sivana**, C. Quesada-López, A. Martínez, and M. Jenkins, "Measuring Students' Source Code Quality in Software Development Projects Through Commit-Impact Analysis," in *International Conference on Information Technology & Systems*, Springer International Publishing, 2021, pp. 100–109.
- **Hamer, Sivana**, C. Quesada-López, A. Martínez, and M. Jenkins, "Measuring students' contributions in software development projects using Git metrics," in *2020 XLVI Latin American Computing Conference (CLEI)*, IEEE, 2020.

Journals

- **Hamer, Sivana**, N. Imtiaz, M. Tamanna, P. Shabrina, and L. Williams, "Trusting code in the wild: Exploring contributor reputation measures to review dependencies in the rust ecosystem," *IEEE Transactions on Software Engineering*, 2025.
- L. Williams, G. Benedetti, **Hamer, Sivana**, *et al.*, "Research directions in software supply chain security," *ACM Transactions on Software Engineering and Methodology*, 2025.
- **Hamer, Sivana**, C. Quesada-López, A. Martınez, and M. Jenkins, "Using git metrics to measure students' and teams' code contributions in software development projects," en, *CLEI Electronic Journal*, 2021.

PRESS RELEASES

- **ConversingLabs (November, 2025).** Can Frameworks Stop Supply Chain Attacks?
- **College of Engineering, North Carolina State University (October, 2025).** Sivana Hamer Receives Google PhD Fellowship
- **Resilient Cyber (October, 2025).** Resilient Cyber Newsletter #70.
- **The Register (March, 2025).** Too many software supply chain defense bibles? Boffins distill advice.
- **InfoWorld (March, 2025).** Developers: apply these 10 mitigations first to prevent supply chain attacks.

INDUSTRY PRESENTATIONS

- **S3C2 Software Supply Chain Community Day (November, 2025).** What are we automatically attesting to?
- **DHS Protecting the Hardware and Software Supply Chain (September, 2025).** Prioritizing Framework Tasks by Analyzing Cyber Threat Intelligence.
- **MITRE SSCA (September, 2025).** Prioritizing Framework Tasks by Analyzing Cyber Threat Intelligence.
- **DAFITC (August, 2025).** Prioritizing Framework Tasks by Analyzing Cyber Threat Intelligence.
- **NC Pace (April, 2025).** Closing the Chain: How to reduce your risk of being SolarWinds, Log4j, and XZ Utils.
- **S3C2 Software Supply Chain Community Day (November, 2024).** Closing the Chain: How not to be Solarwinds, Log4j, or XZ utils.

POLICY

- **MITRE ATT&CK (2025).** Improvements to MITRE ATT&CK techniques being revised and scheduled to be released in a new version.
- **P-SSCRM (2025).** Improvements to software supply chain frameworks tasks scheduled to be released in a new version.

MENTORSHIP

- Archismita Ghosh (MS Student). Current North Carolina State University student.
- Jacob Bowen (MS Student). Now at the Department of Defense (DoD).

SERVICE

- Reviewer: Transactions of Software Engineering (2024).
- Shadow Reviewer: International Conference on the Foundations of Software Engineering (2025), International Conference on Software Engineering (2026), International Workshop on Methodological Issues with Empirical Studies in Software Engineering (2026).
- Student Officer in the WSPR laboratory.
- Student Officer at LA/CSC (Computer Science Organization for Latin American students).

- Computer Science Doctoral Recruiting Event Student Volunteer for North Carolina State University (2024, 2025).
- Student Volunteer Hackpack Capture the Flag (2024, 2025).
- Maintainer of the se-deadline web page to keep track of the deadlines of software engineering research venues.

TEACHING

Interim Instructor
Escuela de Ciencias de la Computación e Informática, Universidad de Costa Rica

- Software Design (CI-0136)
- Databases (CI-0127)
- Software Engineering and Database Integrator Project (CI-0128)
- Programming 1 (CI-0112)
- Computer principles (CI-0202)

Undergraduate Teaching Assistant
Escuela de Ciencias de la Computación e Informática, Universidad de Costa Rica

- Integrated project of software engineering and databases (CI-0128).
- Software engineering (CI-0126).
- Probability and statistics (CI-0115).

SKILLS

- *Languages:* English, Spanish.
- *Programming languages:* Python, Java, R, C#, JavaScript, Bash, SQL.
- *Software tools:* Git, Jenkins, JIRA, Visual Studio Code, CodeQL, SonarQube, LLMs.
- *Frameworks and libraries:* ASP.NET, Flask, Bootstrap, jQuery, React, Unity, n8n.
- *Research methods:* Quantitative, Qualitative, Mining Software Repositories, Machine Learning, Statistical Models.

REFERENCES

- *Dr. Laurie Williams*
  Goodnight Distinguished Professor, Computer Science Department
  North Carolina State University
  Email: lawilli3@ncsu.edu
  Relationship: Thesis Advisor
- *Dr. William Enck*
  Goodnight Distinguished Professor, Computer Science Department
  North Carolina State University
  Email: whenck@ncsu.edu
  Relationship: Thesis Advisor