



VICEROY NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH



CySER Virtual Seminar

Dr. Basavesh Ammanaghatta Shivakumar

Assistant Professor, Washington State University

Information Flow Control: From Classical Security to Agentic AI

Oct. 21, 2026, 11:10 AM – 12 PM Pacific

Team Link: [Click here to join the meeting](#)

Meeting ID: 278 795 403 235 905 | Passcode: SS9dK9zU

Abstract:

Information flow control is a way to reason about where data comes from, where it is allowed to go, and how it can influence a system. These ideas have been used for many years in security to prevent information leaks, enforce confidentiality and integrity, and reason about attacks that exploit unintended flows of information.

In this talk, I will give an overview of information flow control and show how it has been used in different security settings, including software security and cryptographic implementations. I will then discuss why these ideas are becoming important again for AI agents. Modern agents can read untrusted content, access private data, call external tools, and take actions on behalf of users. As these systems become more capable, it becomes harder to understand and control how information moves through them.

I will discuss how information flow control can help address problems such as prompt injection, data leakage, and unsafe use of tools by tracking how trusted, untrusted, and sensitive information moves across an agentic workflow. I will also present examples from recent work on information-flow based security for AI agents and discuss open problems in building agentic systems that are both useful and secure.

Bio:

Basavesh Ammanaghatta Shivakumar is an Assistant Professor in the School of Electrical Engineering and Computer Science at Washington State University. His research focuses on systems and software security, program analysis, fuzzing, agentic AI security, and applications of formal methods in security. His work has been published at top-tier security and programming languages conferences, including IEEE Symposium on Security and Privacy, ACM CCS, and PLDI. Before joining WSU, he was a Postdoctoral Associate at Virginia Tech. He received his Ph.D. from Radboud University, with his doctoral research conducted at the Max Planck Institute for Security and Privacy in Germany. He also holds an M.S. from Purdue University and a bachelor's degree in Computer Engineering from NITK Surathkal.



cyser.wsu.edu

