Software Target-Focused Flow Analysis
Harsha Deshmukh & Daniel Sokoler, Purdue University

Research Question
Given a set of source code written in the C programming language and a program point with known vulnerability, how can we derive flows to the vulnerable target from start point of the program?

Introduction
Existing parsers parse the C code to generate an AST of the complete source code, this prevents the user from specifying any determined program point (vulnerability) of interest to be analyzed for its reachability from the starting point of program. Thus, our tool will utilize the AST to backtrack all the paths from the vulnerable point. This assists in visualizing the reachability of a target point from a code-security viewpoint.

Approach
Our approach is a bottom-up one. Identify the vulnerable point by its line number and continually trace upwards to a function definition. When there are no more functions to trace, the flows have been identified.

Discussion & Results
Our tool can currently identify flows at the function level. As seen in the below sample code, we are expecting two flows:
- Main → foo → foobar → vulnerable point
- Main → bar → foobar → vulnerable point

The Control Flow Graph on the right is the current automated output of our tool.

<table>
<thead>
<tr>
<th>References</th>
</tr>
</thead>
</table>

Conclusion
Thus, we working towards developing a control flow analyzer to enumerate the flows that reach the vulnerability.

This research is a part of the Information Security Research and Education (INSuRE) project. INSuRE is a partnership between successful and mature Centers of Academic Excellence in Information Assurance Research (CAE-R) and the National Security Agency (NSA), the Department of Homeland Security and other federal and state agencies and laboratories to design, develop and test a cybersecurity research network. INSuRE is a self-organizing, cooperative, multi-disciplinary, multi-institutional, and multi-level collaborative research project that can include both unclassified and classified research problems in cybersecurity.