SAND2016-6900C

The Center for Cyber Defenders

Expanding computer security knowledge

StarScream: RE and VA with IDA Pro

Urmit Patel, Georgia Institute of Technology;
Eric Buedel, Purdue University

Project Mentors: Josh Templin, Org. 5638; Josh Eads, Org. 5631

Problem Statement:

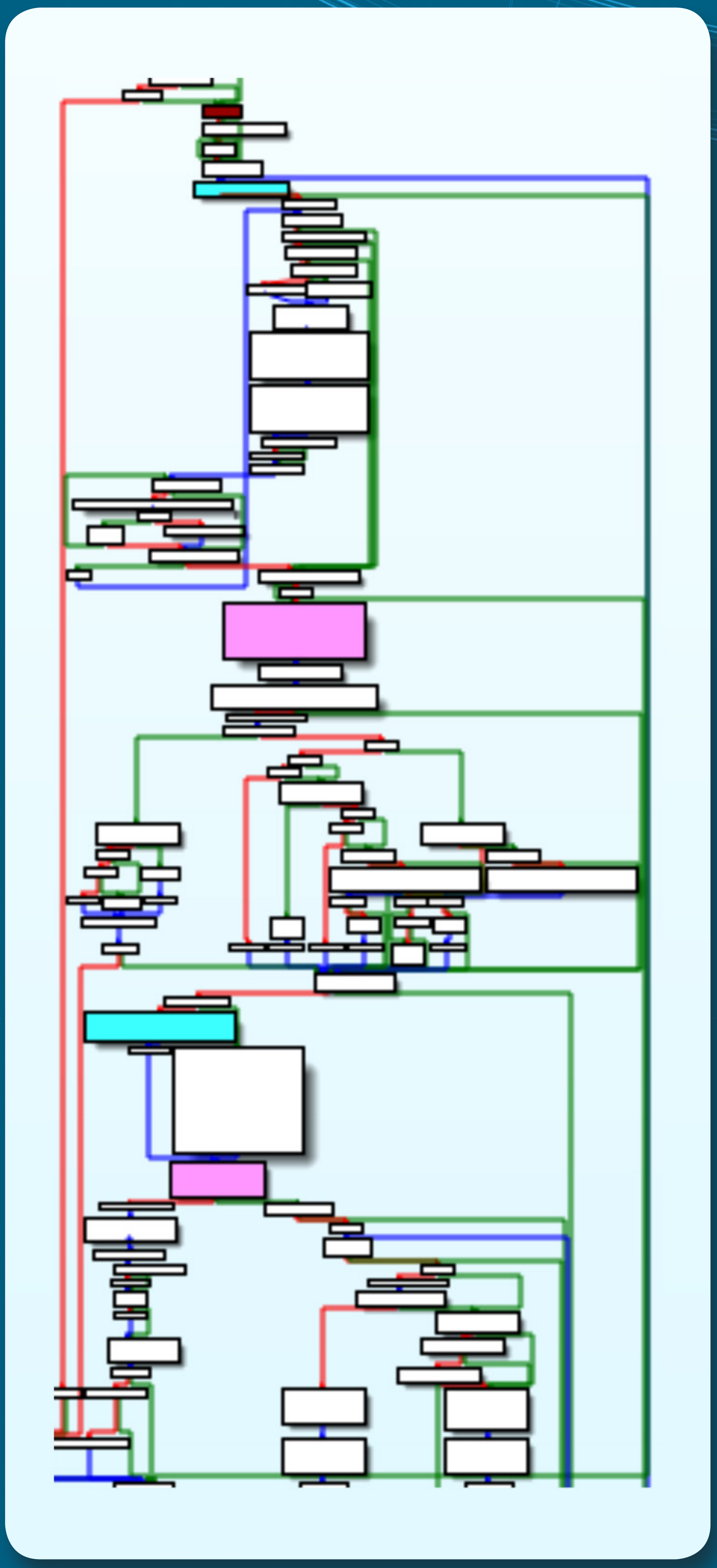
- Investigate vulnerabilities in source code extracted from an embedded system

Objectives:

- Reverse engineer binary code using IDA Pro
- Perform a vulnerability assessment to locate and categorize any weaknesses

Approach:

- Disassemble binary code using IDA Pro
- Develop familiarity with code based on previous annotations
- Explore and annotate smaller functions
- Conglomerate understanding of smaller functions to develop high-level understanding of code



Graph view of essential function

Results:

- Determined significance of different control flow paths
- Ruled out code previously thought to be vulnerable

Impact and Benefits:

- Highlight the importance of secure code in embedded systems

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-84AL8500. SAND2016-XXXXC.