

The Summer Undergraduate Research Fellowship (SURF) Symposium  
4 August 2016  
Purdue University, West Lafayette, Indiana, USA

# Benchmark for Security Testing on Embedded Systems

Khaled Saab, Abraham Clements, and Saurabh Bagchi  
Department of Electrical and Computer Engineering, Purdue University

## ABSTRACT

With the growing popularity of the Internet of Things (IoT), embedded devices continue to integrate more into our daily lives. For this reason, security for embedded devices is a vital issue to address. Attacks such as stack smashing, code injection, data corruption and Return Oriented Programming (ROP) are still a threat to embedded systems. As new methods are developed to defend embedded systems against such attacks, a benchmark to compare these methods is not present. In this work, a benchmark is presented that is aimed at testing the security of new techniques that defend against these common attacks. Two programs are developed that carry three key values needed for a benchmark: realistic embedded application, complex control flow, and being deterministic. The first application is a pin lock system and the second is a compression data logger. A complexity evaluation of the two applications revealed that the pin lock system contained 171 functions and 190 nodes with 252 edges in the control-flow graph, and the compression data logger contained 192 functions and 1,357 nodes with 2,123 edges in the control-flow graph. The current benchmark will be improved in the future by adding more applications with a wider range of complexity.

## KEYWORDS

Embedded Systems, Cybersecurity, Benchmark