Lane Gramling
EECS 700
Reading 15

Summary - Using Program Analysis to Synthesize Sensor Spoofing Attacks

This paper's primary point of focus is on sensor input spoofing attacks, and how co-opting concepts of program analysis, chiefly symbolic execution, leads to a particularly effective way of discovering new vectors for these attacks to exploit. As a proof of concept, the authors develop a study around a simple gesture recognition system driven by a basic microcontroller linking some sensor inputs, and develop a symbolic execution framework to generate adversarial input signatures that spoof the gestures the assembly is designed to recognize.

Contributions

To lay the groundwork for their major contributions, the authors first clarify their threat model and approach to solving the problem. Their threat model specifies that the focus of their attack will be on spoofing gestures to their recognition system by using program analysis techniques to extract what forms of input signals drive the desired outcome. To to this, their described approach is to devise a framework for symbolic execution specialized to signal input patterns.

This framework, which the authors named DrE, is the primary contribution of the paper. DrE'sj purpose is to analyse embedded firmware by using a directed form of symbolic execution that uses a desired control action as the target for which to manipulate, spoofing input signals as its form of input. To allow for this, the authors implemented a number of novel techniques to circumvent issues typical of traditional targets of symbolic execution, such as path explosion. These techniques include its use of biased state selection and control flow graph analysis.

The authors also provide a number of metrics detailing the performance of DrE, which I personally view as high enough to be convincing of its value in future exploration. In the study, DrE was capable of successfully spoofing all 8 tested inputs at least some of the time.

Limitations

Despite the success rate, there are some limitations to the experiments that were carried out. Firstly, the input signal was quite simple in the gesture recognition system used for study, consisting of a one-dimensional magnitude-vs-time analysis. Additionally, as pointed out by the authors, their study focuses on a situation where control logic is implemented in the software, as well as the fact that many sensors produce binary or numeric values, in which case physical spoofing becomes more important.

Future Work

Given the success rate of the test under examination, and despite the discussed limitations, this paper provides a proof-of-concept that sensor input spoofing attacks can be developed through symbolic execution techniques given certain circumstances, which opens the door for further exploration into more complicated types of sensors and signals. An interesting way to proceed would be to do some more inquiry into what types of signal inputs can be efficiently spoofed using symbolic execution techniques.