Using Program Analysis to Synthesize Sensor Spoofing Attacks
Paper Summary

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

Sensors are an important part of the embedded systems, in which system behavior is solely based on the sensor signal input. In the sensor spoofing attack, the attackers change physical state of the device or the system to force this system into an unintended behavior, they use software as well as physical approach (the paper shows how an attacker can attack the system by analyzing the source code and finding the correct sensor inputs), tough the paper focuses on the software approach. "This paper initiates research on software analysis tools that can help discover and exploit sensor spoofing vulnerabilities in embedded software". The paper introduces 'directed, compositional symbolic execution framework' targeting MSP 430 micro-controller software. They focus on a simple system with a micro-controller attached to one or more sensors. Their primary goal is to discover malicious sensor readings which drives the code into unintended state. The paper introduces DrE, which uses modular approach taking advantage of directed and compositional symbolic execution. "It uses combination of call graph and control flow graph analysis with compositional symbolic execution", to mitigate the path explosion. It starts from programs entry point, finding the possible call chains to the function having the target, by symbolically executing target function and proceeding backwards through the call chain. They applied DrE to a gesture recognition system AllSee, demonstrating a spoofing attack against AllSee.

2 Contribution

Paper introduces DrE, which uses modular approach, taking advantage of directed and compositional symbolic execution. They showed that the spoofing attack against gesture recognition systems such as Allsee are possible when run with emulated sensor hardware. Their results question the security of the gesture control systems.

3 Strengths

Using software defined radio to generate the spoofing attacks, the authors were successful in claiming all the gestures. I liked that they provided actual code snippets (algorithms) which are very simple to understand (Although not completely, but I was able to understand based on the usage of simple function names, e.g. ConstructInnerCall()).

4 Limitations

As the authors mentioned, their techniques will become more challenging when used with other types of sensors (wireless signals used by Allsee is a simple case). I feel that it must implemented and tested on different firmwares (than MSP430), after looking at the limitations they mentioned (e.g. global pointers problem).

5 Future Work

As the authors suggested, as a future work, they believe that their techniques will be generalized to other sensor based systems, which may include light, sound, etc.