Summary:

* This paper discusses a system to identify and block malicious network activity toward a smart device. It uses machine learning to isolate unusual traffic indicative of intrusion. The modular design allows it to be deployable in many settings and home environments
* Much of the paper is focused on the implementation and case study conducted by the authors on an example network. This case study showed that the implementation helped but it included a large number of erroneous classifications.

Contributions:

* The main contribution this paper makes is proposing a framework to detect attacks on smart devices.
* A prototype was created to solve an experimental test case using Philips Hue, a smart lighting system.
* When the system detects an attack it raises an alert and attempts to block or isolate the attack using OpenFlow, a standard managed by the Open Networking Foundation that allows controllers to modify the network behavior of devices on the network.

Assumptions

* I believe a system like this could be a significant step toward securing computer systems in the future.
* The theoretical ability to be attached to any network and protect the devices on it simply through monitoring normal traffic and identifying irregular connections could be a great step in the future security, especially in networks with large numbers of smart devices.

SWOT Analysis

|  |  |
| --- | --- |
| Strengths:   * The system’s ability to identify attacks conducted with data it was not trained on shows good promise for detection. * The modular approach should allow this system to work under many different environments. * The system does not require end users to work with the system after initial startup. | Weakness:   * The focus on only one set of tests, while promising, does mean that the authors have not roven this works in a general case. * The tests they used were based on single types of devices, not on a normal environment with many different devices communicating. * Smart devices are not discovered automatically, and have to be manually entered into the system. |
| Opportunities:   * The security benefits are immediately visible. This system, or one like it, could be attached to any network with smart devices and allows for a good degree of security, without requiring the end user to monitor traffic. | Threat:   * The system does still produce a large number of false results that could encourage users to override the system on a regular basis. * The test environment was not representative of a normal home or business. |