**Title**: Vulnerability Assessment of Skybell HD Doorbell

Abstract:

IoT devices are littered with misconfigurations, open services, and a multitude of other vulnerabilities. Most of these are overlooked by manufacturers so that they can be first to market and reap the rewards, however, this leaves customer’s privacy and security at risk. Devising a methodology to consistently discover vulnerabilities in IoT devices would allow manufacturers to better test their products before putting them into the hands of customers.

This paper attempts to define steps to identify vulnerabilities in the Skybell HD Doorbell, which acts as a stepping-stone to conducting similar assessments on IoT devices. Through the stages of device footprinting, enumeration, and scanning, attacks are found that can be carried out. Beyond just generalities of these stages, this paper provides specific commands, protocols, and services to look for to fully assess a device.

By walking through the aforementioned stages, it was found the Skybell HD Doorbell has a stronger security posture than other IoT products. Network traffic was encrypted, the mobile application is obfuscated, and no services allowed remote access. Generic attacks that were successful included a WPA/WPA2 deauthentication attack, enumerating usernames through an API, resetting the owner through physical access, or blocking the camera physically. This shows the success of Skybell’s security mindset and also the steps to assess the device presented in this paper.