

By 2020, the number of smart home appliances, security devices, and energy monitoring systems will be in the millions. These devices are manufactured by diverse companies at different scales, many of whom do not have software development or security expertise. Furthermore, these devices often have limited computation capabilities, making it difficult for them to rely on standard security protocols; they may also be difficult to patch, given that the manufacturers may not have the resources or incentives to maintain device security. In this work, we survey the security practices of several state-of-the-art popular smart home devices by passively monitoring their network traffic in a controlled smart-home lab environment. Our initial investigation has revealed some troubling patterns and trends: for example, we have found that many home IoT devices communicate with online servers in clear text. Our initial analysis suggests that privacy and security problems are rampant across a wide range of devices; we believe that, due to the nature of the software development ecosystem and provider incentives, it is imperative to pursue defense in depth, through a combination of intelligent network anomaly detection and, where possible, more robust testing and software development ecosystems for the devices themselves.