A taxonomy of cyber-physical threats and impact in the smart home

Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny R.J. Fontaine, Avgoustinos Filippoupolitis, Etienne Roesch

PII: S0167-4048(18)30487-5
DOI: https://doi.org/10.1016/j.cose.2018.07.011
Reference: COSE 1373

To appear in: *Computers & Security*

Received date: 9 May 2018
Revised date: 21 July 2018
Accepted date: 25 July 2018

A taxonomy of cyber-physical threats and impact in the smart home

Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny R. J. Fontaine, Avgoustinos Filippoupolitis, Etienne Roesch

Computing and Information Systems
University of Greenwich, UK
E: r.j.heartfield@gre.ac.uk

Abstract

In the past, home automation was a small market for technology enthusiasts. Interconnectivity between devices was down to the owner's technical skills and creativity, while security was non-existent or primitive, because cyber threats were also largely non-existent or primitive. This is not the case any more. The adoption of Internet of Things technologies, cloud computing, artificial intelligence and an increasingly wide range of sensing and actuation capabilities has led to smart homes that are more practical, but also genuinely attractive targets for cyber attacks. Here, we classify applicable cyber threats according to a novel taxonomy, focusing not only on the attack vectors that can be used, but also the potential impact on the systems and ultimately on the occupants and their domestic life. Utilising the taxonomy, we classify twenty five different smart home attacks, providing further examples of legitimate, yet vulnerable smart home configurations which can lead to second-order attack vectors. We then review existing smart home defence mechanisms and discuss open research problems.

1. Introduction

As homes adopt Internet of Things (IoT) technologies and become increasingly smart by utilising networked sensing and actuation, cloud computing and artificial intelligence, they naturally become more vulnerable to threats in cyber space. Some of these threats are entirely new. The majority are not, but applying them in a domestic context generates second-order threats to the physical and emotional safety of the occupants to an extent not previously experienced. Here, we present a taxonomy of cyber threats to smart homes already observed in the wild or in controlled experiments, as well as potential future vulnerabilities exposed by specific smart home configurations and technology adoption.

Smart home cyber security is usually addressed as an extension of the smart grid, looking almost exclusively at energy-related attacks [1]. This has begun to change. Indicatively, Lin and Bergmann [2] have taken a holistic perspective on smart home privacy and security, identifying the combination and convergence of heterogeneous technologies, with lack of specialised security knowledge, as two key challenges exacerbating the cyber threat to smart home environments. Here, we look more deeply at the technical building blocks of cyber threats to smart homes, identifying key classification criteria that help to shape the attack landscape. We do not claim that this taxonomy can be exhaustive. However, in identifying and characterising existing and potential future cyber threats to the smart home, we are able to highlight motivations, resources, vulnerabilities and crucially their impact, so as to help establish the problem space for defence measures that would address them.

2. Related Work

The smart home is not a fundamentally new technological paradigm. So, although there has not been a taxonomy of cyber threats for smart homes before, it is meaningful to contrast against related work that is more general for IoT or previously established areas, such as wireless sensor networks and networked embedded systems. In 2010, Babar et al. [3] were the first to propose a taxonomy of IoT cyber threats, but only provided a high-level overview of security requirements and types of threats in terms of communication, identity management, storage management, embedded security, physical threats and dynamic binding. More recent work by Jing et al. [4] has looked at IoT security from the perspective of security needs at the application layer, the transportation layer and what they refer to as the perception layer, which is where the data collection occurs. The resulting architecture is effectively a taxonomy of the types of threats at each layer, which, interestingly, includes smart home security as one of the requirements at the application layer, but does not elaborate further. Another area of interest is privacy in IoT, where Ziegerldorf et al. [5] have classified the impact of an IoT privacy breach as relating to identification, tracking, profiling, privacy-violating interaction, lifecycle transitions, inventory attacks and linkage. This is a well thought-out taxonomy, but is naturally limited to privacy and does