Smart Locks: Evaluating the Roles of Security, Trust, and Perceived Risk on Consumer Adoption

TREO Talk Paper

David M. Bourrie
University of South Alabama
dbourrie@southalabama.edu

Abstract

The Internet of Things (IoT) can be briefly defined as a network of sensors and objects that can communicate directly with one another without human intervention. As consumers move toward smarter homes with home automation products (i.e., dishwasher, fridge, lighting, thermostat, and vacuum), one of the first layers of defense for consumers to protect their homes and assets are the locks on their doors. Smart locks are electromagnetic locks designed to perform locking and unlocking operations after receiving instructions from an authorized device using a wireless protocol and a cryptographic key to execute the authorization process. Many smart locks offer additional enhanced features like cameras and motion sensors.

The global smart lock market is expected to reach over $2.5 billion US by 2023, at a compound annual growth rate over 13% between 2017 and 2023. Oversees, the adoption of smart locks has been promoted to improve the lives of people with physical and visual disabilities by using facial recognition on a smartphone rather than having to use a physical key. The consumer adoption of smart locks has motivated the retail sector towards more convenient shopping experiences. Products like Amazon Key and Walmart’s Deliv service now permit the ability to deliver groceries and packages inside consumers’ homes and even allow the possibility of putting away your cold and frozen groceries, if needed.

Much of the growth rate for smart locks leverages consumers growing fear, safety, and security concerns regarding where they live. Consumer adoption of smart locks can be deterred by the risk of cyberattacks through smart devices or IoT-enabled devices and is the largest challenge facing smart lock manufactures. Older generation smart locks were more susceptible to cyberattacks and privacy concerns due to short battery life, lightweight computational abilities, and older wireless protocols.

This study aims to investigate the antecedents of smart lock adoption by extending protection motivation theory (PMT). PMT has been used to explain individual’s behavior in response to threats and their propensity to engage in voluntary security behaviors. This research will increase our understanding of consumers’ grasp of the protection motivation construct and the influence of fear, trust, and perceived risk.