Politecnico di Torino

ScuDo
Scuola di Dottorato ~ Doctoral School
WHAT YOU ARE, TAKES YOU FAR

Doctoral Dissertation
Doctoral Program in Computer and Control Engineering (36^{th}cycle)

Securing IoT Gateways in Smart Home Environments

By

Luca Mannella

******

Supervisor(s):
Prof. Fulvio Corno, Supervisor
Prof. Antonio Lioy, Co-Supervisor

Doctoral Examination Committee:
Prof. Claudio Ettore Casetti, Politecnico di Torino
Prof. Davide Ferraris, University of Malaga
Prof. Giorgio Giacinto, Referee, University of Cagliari
Prof. Luigi Patrono, Referee, University of Salento
Dr. Andrea Vesco, LINKS Foundation

Politecnico di Torino
2024

Abstract

The Internet of Things (IoT) has seen increasing adoption in residential settings, leading to a proliferation of IoT devices within homes. While offering enhanced functionality and convenience, IoT devices also introduced challenges in terms of management and security. Indeed, managing a large set of IoT devices individually can be cumbersome for users, especially considering the diverse nature of this class of devices.

To help users handle their devices, Smart Home Gateways (SHGs) have been introduced. An SHG serves as a central point for managing and coordinating IoT devices, simplifying the users' tasks. SHGs can also provide an additional layer of security by acting as a buffer between the IoT devices and the Internet, thereby protecting the devices from direct exposure to potential threats online. Moreover, SHGs can be equipped with additional security mechanisms, following the security-in-depth approach.

To encourage the adoption of those solutions and to allow manufacturers and developers to easily include their devices, SHGs are often designed in an extensible way, allowing anyone to produce their own plug-ins. However, the extensibility of SHGs, which allows developers to add their own code, can potentially introduce new security issues. This makes the design and management of SHGs (and their plug-ins) a critical aspect of IoT security in residential settings.

Against this backdrop, the goal of this thesis is to analyze the sources of security issues in plug-in-based SHGs through the definition of an ad-hoc threat model aimed at identifying the main risky behaviors from the point of view of plug-in developers. After validating the model through proof-of-concept implementations, expert assessments, and user surveys, the model served as a foundation for the subsequent development of mitigation solutions based on existing industry standards founded on code integrity, network access control, and outsourcing security functionalities from resource-constrained IoT devices to the Smart Home Gateway. To validate these mitigation solutions, a series of experiments were conducted through a laboratory setup. The achieved results demonstrated their effectiveness in enhancing the security posture of the protected network.

In conclusion, by enhancing the security of plug-in-based Smart Home Gateways, this thesis offers a framework for bolstering the security of smart home environments.