Smart Home Privacy Protection Methods against a Passive Wireless Snooping Side-Channel Attack

Authors Mohammad Ali Nassiri Abrishamchi, Anazida Zainal, Fuad A. Ghaleb, Sultan Noman Qasem and Abdullah M. Albarrak 2ORCID

Publication Year 2022
Grant Number RG-21-07-04
DOI link https://doi.org/10.3390/s22218564

Abstract: Smart home technologies have attracted more users in recent years due to significant advancements in their underlying enabler components, such as sensors, actuators, and processors, which are spreading in various domains and have become more affordable. However, these IoT-based solutions are prone to data leakage; this privacy issue has motivated researchers to seek a secure solution to overcome this challenge. In this regard, wireless signal eavesdropping is one of the most severe threats that enables attackers to obtain residents' sensitive information. Even if the system encrypts all communications, some cyber attacks can still steal information by interpreting the contextual data related to the transmitted signals. For example, a "fingerprint and timing-based snooping (FATS)" attack is a side-channel attack (SCA) developed to infer in-home activities passively from a remote location near the targeted house. An SCA is a sort of cyber attack that extracts valuable information from smart systems without accessing the content of data packets. This paper reviews the SCAs associated with cyber–physical systems, focusing on the proposed solutions to protect the privacy of smart homes against FATS attacks in detail. Moreover, this work clarifies shortcomings and future opportunities by analyzing the existing gaps in the reviewed methods.