Title: Detecting rogue attacks on commercial wireless insteon home automation systems

Author: Christopher M. Talbot, Michael A. Temple, Timothy J. Carbino, J. Addison Betances

PII: S0167-4048(17)30205-5
DOI: https://doi.org/doi:10.1016/j.cose.2017.10.001
Reference: COSE 1212

To appear in: *Computers & Security*

Title: Detecting Rogue Attacks on Commercial Wireless Insteon Home Automation Systems

Christopher M. Talbot, Michael A. Temple, Timothy J. Carbino, and J. Addison Betances
Department of Electrical and Computer Engineering
Air Force Institute of Technology
Wright-Patterson AFB, USA
[christopher.talbot, michael.temple*,timothy.carbino, joan.betancesjorge]@afit.edu
*Corresponding Author

Abstract: The Internet of Things (IoT) supporting commercial wireless home automation applications is expanding as technical capability evolves and implementation costs continue to decrease. However, many home automation devices lack robust security and are vulnerable to a multitude of bit-level attacks. This was highlighted during the first successful Insteon network intrusion demonstration that occurred at DEF CON 23 using a Software Defined Radio (SDR) with YARD Stick One devices. In response, Radio Frequency Distinct Native Attribute (RF-DNA) Fingerprinting is introduced here as a counter-hacking approach for augmenting network bit-level Identity (ID) authentication using Physical Layer (PHY) waveform features. An RF-DNA Fingerprinting process is adopted here and applied to wireless Insteon home automation devices. Rogue device detection is addressed using a Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) ID verification process. Rogue assessments include attacks by like-model Insteon Switch (IS) devices and YARD Stick One SDR devices programmed to present actual (false) bit-level credentials for authorized Insteon devices while functionally controlling the state of an unprotected (no RF-DNA discrimination) targeted end point device. Device classification and Rogue Rejection Rate (*RRR*) performance is assessed using Time Domain (TD) and Slope-Based Frequency Shift Keyed (SB-FSK) Fingerprinting with features extracted from a variant (data dependent) signal response region. The Rogue Rejection Rate (*RRR*) for SB-FSK Fingerprinting was superior to TD Fingerprinting and included *RRR* ≈ 95% for 25 like-model IS attacks and *RRR* ≈ 100% for 36 YARD Stick One SDR attacks. SB-FSK Fingerprinting is more computationally efficient (70% fewer features) than TD Fingerprinting and provides an added benefit of being implementable using features extracted from variant data dependent FSK signal response regions.

Keywords: Insteon, IoT, SDR, RF-DNA, Multi-Factor Authentication, Home Automation

1.0 Introduction

The Internet of Things (IoT) for commercial wireless home automation is expanding as technical capability evolves and implementation costs decrease. Unfortunately, system security evolution is lagging and systems remain vulnerable to a multitude of attacks that are easily implemented using a basic laptop computer and receiver front-end costing less than $100 [Shi1,Shi2]. In one case, IoT vulnerabilities were left unchecked and an individual gained unauthorized control of several million IoT devices and conducted a wide spread network attack that crippled the World Wide Web in various parts of the US [Sim1]. While generally hesitant in terms of acknowledging the inherent vulnerabilities, commercial home automation device manufacturers strive to assure consumers that their products are secure. This is the case for SmartLabs Inc. who developed the Insteon family of commercial devices and aim to comfort consumers by suggesting their devices provide optional encryption support (but not a standard encryption cipher), data integrity via Cyclic Redundancy Check (CRC) encoding, and device identification (ID) authentication using 3-byte plaintext addressing [Ins1-Ins3].

Home automation cyberattack risk can be minimized by using more robust methods for authenticating network device bit-level IDs. The lack of reliable authentication mechanisms that cannot be easily bypassed is one of the top 10 security design flaws that designers must avoid [Arc1]. The method proposed here for improving wireless home automation security includes augmenting typical bit-level ID authentication mechanisms with device Physical (PHY) layer features through Radio Frequency (RF) air monitoring. Specifically, the use of PHY-based RF Distinct Native Attribute (RF-DNA) Fingerprinting which not only supports network access control objectives (authorized device acceptance and rogue device rejection) but also provides an indication of device health (good, degraded, or malfunctioning) [Dan2]. Of particular relevance to work here are cyberattack demonstrations involving Insteon devices and a Software Defined Radio (SDR) using a YARD Stick One receiver front-end. YARD Stick One devices are inexpensive and readily available commercial SDR devices [Yar1] that can be used to support cyber defensive and offensive objectives. The primary motivation for work here includes a DEF CON 23 [Shi1,Shi2] demonstration representing the first (known) successful Insteon network intrusion attack using a YARD Stick One SDR. In this case, the protection provided by "something you have" (hardware interface device) and "something you know" (Insteon bit-level IDs) Multi-Factor Authentication (MFA) factors [Pci1] was effectively mitigated. Results here suggest that if a third "something you are" (PHY-based RF fingerprint) MFA factor [Pci1] were in place for targeted Insteon devices during DEF CON 23, there is near 100% certainty that the network intrusion attack would have been thwarted.