ISSN 0167-4048
ELSEVIER
Computers & Security
The International Source of Innovation for the Information Security and IT Audit Professional
ifip

A Two-Factor Authentication Scheme Against FDM Attack in IFTTT based Smart Home System

Barnana Baruah, Subhasish Dhal

PII: S0167-4048(18)30240-2
DOI: 10.1016/j.cose.2018.03.004
Reference: COSE 1310

To appear in: *Computers & Security*

Received date: 7 November 2017
Revised date: 14 February 2018
Accepted date: 17 March 2018

Please cite this article as: Barnana Baruah, Subhasish Dhal, A Two-Factor Authentication Scheme Against FDM Attack in IFTTT based Smart Home System, *Computers & Security* (2018), doi: 10.1016/j.cose.2018.03.004

A Two-Factor Authentication Scheme Against FDM Attack in IFTTT based Smart Home System

Barnana Baruah[*], Subhasish Dhal

Indian Institute of Information Technology Guwahati, India

Abstract

Smart Home is an emerging key-element of the advantages of Internet of Things (IoT), which facilitates an individual to have control over the smart devices of his house through the Internet. However, its control should be confined to the legitimate user only, which can refrain from malicious activities. Internet services like IFTTT (If This Then That) integrate heterogeneous Smart Home devices and allow the user to customize Smart Home configurations via IFTTT recipes. Earlier researches have suggested an attack scenario based on Feature-Distributed Malware (FDM), where the malware can compromise the victim's IFTTT account and as a result the attacker can manipulate the recipes from his own device. This paper proposes a secure IFTTT-based Smart Home framework by incorporating suitable captcha-based One Time Password (OTP) authentication scheme and Physical Unclonable Function (PUF). A suitable adversarial model has been used to evaluate the security of the framework.

Keywords: IFTTT, IoT, Malware, Recipes, Smart Home

1. Introduction

IoT is one of the fastest growing technology and enters almost all verticals of the World Economy [1]. Smart Home is one of the applicable fields of IoT [2]. It facilitates the users to remotely control the heterogeneous Smart Home devices for various aspects such as safety, security, comfort, healthcare,

[*] Corresponding author

Email addresses: barnanabaruah12.13@gmail.com (Barnana Baruah), subhasis@iiitg.ac.in (Subhasish Dhal)