# Security Analysis and Exploitation of Arduino Devices in the Internet of Things



| | |
|---|---|
| Title | Security Analysis and Exploitation of Arduino Devices in the Internet of Things |
| Publication Type | Conference Paper |
| Year of Publication | 2016 |
| Authors | Alberca, Carlos, Pastrana, Sergio, Suarez-Tangil, Guillermo, Palmieri, Paolo |
| Conference Name | Proceedings of the ACM International Conference on Computing Frontiers |
| Publisher | ACM |
| Conference Location | New York, NY, USA |
| ISBN Number | 978-1-4503-4128-8 |
| Keywords | Human Behavior, Pervasive computing, pubcrawl, Resiliency, Scalability |

Abstract

The pervasive presence of interconnected objects enables new communication paradigms where devices can easily reach each other while interacting within their environment. The so-called Internet of Things (IoT) represents the integration of several computing and communications systems aiming at facilitating the interaction between these devices. Arduino is one of the most popular platforms used to prototype new IoT devices due to its open, flexible and easy-to-use architecture. Ardunio Yun is a dual board microcontroller that supports a Linux distribution and it is currently one of the most versatile and powerful Arduino systems. This feature positions Arduino Yun as a popular platform for developers, but it also introduces unique infection vectors from the security viewpoint. In this work, we present a security analysis of Arduino Yun. We show that Arduino Yun is vulnerable to a number of attacks and we implement a proof of concept capable of exploiting some of them.

| | |
|---|---|
| URL | http://doi.acm.org/10.1145/2903150.2911708 |
| DOI | 10.1145/2903150.2911708 |
| Citation Key | alberca_security_2016 |