Lumos: Identifying and Localizing Diverse Hidden IoT Devices in an Unfamiliar Environment

Rahul Anand Sharma, Elahe Soltanaghaei, Anthony Rowe, Vyas Sekar

Carnegie Mellon University

Abstract

Hidden IoT devices are increasingly being used to snoop on users in hotel rooms or AirBnBs. We envision empowering users entering such unfamiliar environments to *identify and locate* (e.g., hidden camera behind plants) *diverse* hidden devices (e.g., cameras, microphones, speakers) using only their personal handhelds.

What makes this challenging is the limited network visibility and physical access that a user has in such unfamiliar environments, coupled with the lack of specialized equipment.

This paper presents Lumos, a system that runs on commodity user devices (e.g., phone, laptop) and enables users to identify and locate WiFi-connected hidden IoT devices and visualize their presence using an augmented reality interface. Lumos addresses key challenges in: (1) identifying diverse devices using only coarse-grained wireless layer features, without IP/DNS layer information and without knowledge of the WiFi channel assignments of the hidden devices; and (2) locating the identified IoT devices with respect to the user using only phone sensors and wireless signal strength measurements. We evaluated Lumos across 44 different IoT devices spanning various types, models, and brands across six different environments. Our results show that Lumos can identify hidden devices with 95% accuracy and locate them with a median error of 1.5m within 30 minutes in a two-bedroom, 1000 sq. ft. apartment.

1 Introduction

Imagine a user walking into an unfamiliar environment such as a hotel room or Airbnb. Nowadays, the user has to be wary of wireless Internet-of-Things (IoT) devices being used to spy on them. These devices could be installed by the owner or by a previous guest. This threat is not just hypothetical; there are numerous reported incidents where IoT surveillance devices were used in Airbnbs [1–3, 5, 9, 11, 16], cruise ships [6], and motels [10]. A 2019 survey of 2,000 American travelers revealed that 58% were worried that their host had installed hidden surveillance equipment, and 11% of respondents had actually found a hidden camera in some past rental [13].

Ideally, we want to empower users so that as they enter an unfamiliar space, they can run an app on their personal handheld (e.g., phone or tablet). This app would report a list of *detected* and *identified* devices and their corresponding locations. "Detect," here, means knowing that there is some device (i.e., binary notification), "identify" entails knowing what type of device it is (e.g., type=camera), and "localize" entails knowing the device's location in the physical space (e.g., behind the plants). While cameras in particular are imminent privacy threats, in general we want to detect/identify and localize *diverse* hidden IoT devices, as these could also be potential threats for tracking users (e.g., [21, 25, 33, 66]).

This problem is challenging due to two practical factors. First, users have limited visibility and control inside such an unfamiliar environment with their little knowledge of the devices and their wireless configurations; e.g., they cannot tap into network interfaces at wireless access points or instrument the environment. Second, users typically only have personal (commodity) handhelds and do not carry expensive hardware or specialized sensing equipment [15, 41]. Given our requirements and these constraints, existing methods are not sufficient for our context (see Table 1). For example, today's "spy-tech" solutions rely on manual and thorough scanning of the environment [4, 7, 8, 15, 18]. Other efforts focus exclusively on camera-specific effects (e.g., motion or light triggering) and do not generalize to other, more diverse hidden IoT devices [26, 51]. Similarly, network-based device fingerprinting solutions [45, 48, 53] rely on privileged access to the host network and fail in the presence of limited network visibility. Finally, many of these solutions cannot localize devices, and/or would need separate instrumentation of the environment [37, 59].

This paper presents Lumos, a system that enables a user to identify and locate IoT devices in an unfamiliar environment using a commodity personal device. As a starting point, we focus on 802.11 WiFi connected devices, which represent a significant fraction of the IoT device market today [58]. At a high level, Lumos sniffs and collects encrypted wireless packets over the air (aka 802.11) to detect and identify the hidden devices. It then predicts the location of each identified device with respect to the user as they walk around the perimeter of the space. Our design makes three contributions: