Computer Science and Application 计算机科学与应用, 2020, 10(3), 464-470
Published Online March 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.103048

Hans汉斯

Research and Practice of "Device-Device" Security Attack and Defense Based on IoT + AI

Feng Liu[1,2*], Yuchuan Yang[1], Yuying Lu[1], Yucong Li[1], Ce Sun[1], Yu Sun[1]

[1]Binjiang College, Nanjing University of Information Science and Technology, Wuxi Jiangsu
[2]Institute of Artificial Intelligence and Change Management, Shanghai University of International Business and Economics, Shanghai
Email: *lsttoy@163.com

Received: Feb. 24th, 2020; accepted: Mar. 9th, 2020; published: Mar. 16th, 2020

Abstract

Thanks to the rapid development of artificial intelligence, people's lifestyles have become more intelligent and convenient. However, with the rapid development of smart devices, security issues, privacy issues, and the personal safety of property have brought great potential threats. This article takes a smart light bulb that can be controlled through Wi-Fi as a representative, and studies the communication principle between smart devices and clients and how to write script programs to forge permissions and gain control of smart devices. The experiment mainly uses the penetration test method. Simulate hacking to remotely control the robot to approach the user's smart light network Wi-Fi source, and then simulate the smart device's smart device and successfully override the power. The smart light can be controlled without the user's authorization, which proves certain questions of the safety of the smart device. At the same time, it also emphasized the issues of security and privacy protection of the device.

Keywords

Smart Home, Network Security, Penetration Testing, Network Attack and Defense

基于IoT+AI的"物–物"安全攻防的研究与实践

刘　峰[1,2*]，杨雨川[1]，陆瑜莹[1]，李远聪[1]，孙　策[1]，孙　钰[1]

[1]南京信息工程大学滨江学院，江苏　无锡
[2]上海对外经贸大学人工智能与变革管理研究院，上海
Email: *lsttoy@163.com

收稿日期：2020年2月24日；录用日期：2020年3月9日；发布日期：2020年3月16日

*通讯作者。

文章引用: 刘峰, 杨雨川, 陆瑜莹, 李远聪, 孙策, 孙钰. 基于 IoT+AI 的"物–物"安全攻防的研究与实践[J]. 计算机科学与应用, 2020, 10(3): 464-470. DOI: 10.12677/csa.2020.103048

摘 要

得益于人工智能的高速发展，人们的生活方式也变得更加智能而便捷，但在智能设备猛烈发展的同时，安全问题、隐私问题乃至财产人身安全都带来了极大的潜在威胁。本文以一个可通过Wi-Fi控制的智能灯泡为代表，研究了智能设备与客户端之间的通信原理及如何编写脚本程序去伪造权限并取得智能设备的控制权，实验主要采取了渗透测试的方法，模拟黑客行为远程操控机器人去接近用户的智能电灯网络Wi-Fi源，进而对其智能设备进行模拟攻击，并成功越权，得以在没有用户授权的情况下控制智能电灯的开关，证明了智能设备的安全存在一定的问题。同时也是侧面强调了使用设备的安全性和隐私保护等问题。

关键词

智能家居，网络安全，渗透测试，网络攻防

1. 文献综述及研究背景

2004 年前智能家居安防产业刚刚在我国兴起，因此相关的标准数目比较少；2005 年后，随着智能家居安防产业的发展壮大，新制定的标准数目呈现明显的上升趋势。但是，在进入 2015 年后，新制定的标准又出现了大幅度回落，这说明了经过近 10 年的快速发展，智能家居安防产业又迎来了新的发展瓶颈。在全球范围内，智能家居安防专利申请量排名前五的申请人分别是报知机株式会社、海尔集团、Panasonic、矢崎和东京瓦斯，可见中日韩和美国企业是该领域的重要申请人。虽然中国企业对该领域的研究起步晚，但其投入的力度却越来越大[1]。

目前智能产品发展迅速，包括格力，美的，海尔等老牌家居巨头在内的各大厂商，以及谷歌，百度，小米等知名科技公司都在智能家居的研发上花费了大量的精力与财力，通过家居智能化，人们可以通过网络轻松控制家里的各个设备，如热水器，空调，照明设备等，而据统计，人的一生超过 70%的时间是在家里度过的[2]，如此的接触比例更加说明了智能家居等智能设备的安全性是极其重要的，而一些潜在的危害都可能带来或大或小的安全及隐私问题。

小的方面，如果黑客入侵了用户家中的智能设备网络，那么黑客可接管智能设备的控制权，对家中的智能设备实施可能带来安全隐患的操作，如使婴儿房的空调制冷，开关防盗门等，甚至可以随意开关家庭监控造成隐私安全问题。西班牙黑客 Jesus Molina 某酒店住宿期间，发现了房屋内的多个操控系统漏洞，利用这些漏洞，能够实现对酒店 250 多个房间里的灯光、温控器、百叶窗、电视以及门外的请勿打扰电子灯的控制。另外，由于酒店对客人的 iPad 缺少安全认证，黑客也可利用笔记本电脑控制其他房间的设备。更为严重的是，黑客甚至还可以在其 iPad 等设备中安装木马程序，实现远程控制[3]。

大的方面，假设某 A 地医生通过远程手术给一个 B 地病人实施手术，黑客通过入侵其医疗设备，恶意更改设备设置参数，则有可能对病人造成生命威胁。黑客巴纳拜 • 杰克就曾计划在 2013 年的黑客大会上，展示通过入侵心脏起搏器，发出一系列 830 V 的高压电击，除此之外，智能化生产也在发展之中，

黑客同样会对大型工厂的正常工作带来影响。

因此本文主要是基于在一个逐渐智能化，物联网设备爆炸性增长的未来场景下进行网络安全的主动防御检测，通过模拟攻击物联网设备，突破安全防护的检测方式，来给予未来我们日常生活中所需要进行网络安全予以警示和经验的学习。

2. 攻击系统及环境的硬件设计方案

赵俊和任姣姣在文章中主要通过重放攻击实现接入内网，但其过度依赖于现有软件，只简单叙述了现有软件的使用流程，且文章进度截至到接入内网，没有实现接管控制权限。杨丽，冯娟，卢秀丽，刘强[4]仅对智能设备本身的硬件安全做出了研究，讨论了安防，如火灾一类的安全，没有对安全隐私等网络安全方面做出研究讨论。刘发贵，彭妙霞[5]的研究是对网关流量进行分析，形成病毒防护系统，而本文的渗透测试基于内网环境，无需通过内网即可对智能设备发起攻击。

2.1. 实验环境的设计

用智能灯泡为代表来设计智能场景，切断线路使灯泡的线路与 esp-01/01s 继电器相连接(如图 1)，在 python 环境下，用 pip 指令安装 esptool，usb 插入 esp8266 给 esp8266 刷入固件，在网页端内网对其进行设置，并使其接入智能设备所在 Wi-Fi 网络中，自此，可以实现通过手机电脑或其他在该网络下的电子设备去控制这个灯的开关闭合，以该智能灯作为智能设备代表。

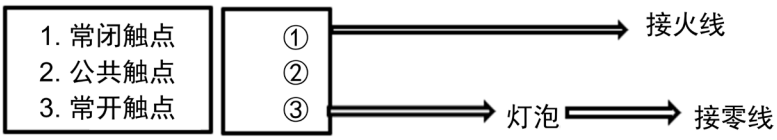

Figure 1. Schematic diagram of relay connection
图 1. 继电器接法示意图

2.2. 移动攻击设备设计

采用树莓派 3B 作为控制核心，以电源，电机驱动模块等硬件作为载体，制作了一个可移动的微型计算机，该设备可被远程操控实现移动，带有 Wi-Fi 模块，可接入无线网络。

GPIO 口指通用输入输出口，通过 GPIO 口可将树莓派与其他硬件连接起来，树莓派有 40 个 GPIO 口可用来拓展其他的外部设备，可使用 BCM 的方式来对引脚进行定义、编号。之后对管脚的类型进行设置和初始化，通过 python 的 bottle 框架和 python 代码即可实现该攻击设备的网页端控制(如表 1)。

3. 攻击系统脚本设计方案

3.1. 内网攻击脚本的设计

在所有的安全事件中，有超过 70%的安全事件是发生在内网上的，并且随着网络的庞大化和复杂化，这一比例仍有增长的趋势[6]。脚本引用了 python 的 pyWi-Fi，time 模块，pyWi-Fi 模块用于主要的 Wi-Fi 网络破译，time 模块则提供了各种的时间参数。实验首先获取周围存在的 Wi-Fi 列表，获取这些 Wi-Fi 的 ssid 值，选择智能设备网络源 Wi-Fi，目标智能设备(本实验中的智能电灯)附近所有 Wi-Fi 的 SSID 值和 Wi-Fi 相关信息并形成列表，我们选择目标智能电灯所在的 Wi-Fi 内网，之后脚本程序将利用内置的全球 top 1000 弱口令密匙字典对所选择的 Wi-Fi 进行密匙破译，在破译完成之后，我们的攻击设备将自动连接 Wi-Fi 并执行权限伪造脚本程序(如图 2)。

Table 1. GPIO control trolley bus design
表 1. GPIO 控制小车总线设计图

	序号	地	电源	.BCM GPIO	.BOARD GPIO	FUNC	.BCM GPIO	BOARD GPIO	FUNC
IIC	17	GND	5V	GPIO 2	3	SDA	GPIO 3	5	SCL
UART	16	GND	5V	GPIO 14	8	TXD	GPIO 15	10	RXD
超声波	15	GND	5V	GPIO 4	7	ECHO	GPIO 17	11	TRIG
红外	14	GND	5V	GPIO 18	1	IR_R IP_L IR_M IRF_R IRF_L	电源板插针及功能引脚分配表		
	13	GND	5V	GPIO 27	13				
	12	GND	5V	GPIO 22	15				
	11	GND	5V	GPIO 23	16				
	10	GND	5V	GPIO 24	18				
LED	9	GND	5V	GPIO 10	19	LED0 LED1 LED2			
	8	GND	5V	GPIO 9	21				
	7	GND	5V	GPIO 25	22				
预留 io	6	GND	5V	GPIO 11	23				
	5	GND	5V	GPIO 8	24				
	4	GND	5V	GPIO 7	26				
	3	GND	5V	GPIO 5	29				
	2	GND	5V	GPIO 6	31				
	1	GND	5V	GPIO 12	32				
电机驱动				GPIO 19	35	IN1			
				GPIO 13	33	ENA			
				GPIO 16	36	IN2			
				GPIO 21	40	IN3			
				GPIO 20	38	ENB			
				GPIO 26	37	IN4			
ID EEPROM				ID_SD	27	ID_SD			
				ID_SC	28	ID_SC			

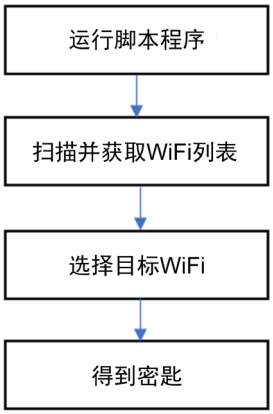

Figure 2. Decoding script control flowchart
图 2. 破译脚本控制流程图

通过以上流程，我们可以执行上述流程，并通过脚本来实现 Wi-Fi 源的获取并进行攻击。

1) 首先调用程序获取 Wi-Fi 列表如图 3 所示。

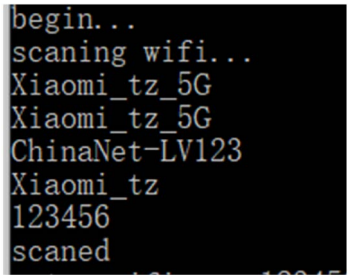

Figure 3. Scripts to obtain a list of Wi-Fi
图 3. 脚本程序获取 Wi-Fi 列表

2) 选择需要破译的 Wi-Fi 进行破译工作如图 4 所示。

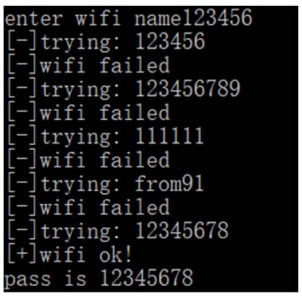

Figure 4. Flowchart of script cracking Wi-Fi key
图 4. 脚本程序破译 Wi-Fi 密匙流程图

3.2. 智能设备控制流程设计

通过在用户控制智能灯处抓包分析可知，用户通过点击不同的功能按钮去实现不同的控制效果，每个不同的按钮对应不同的服务端，在发起请求时，客户端会向服务端以 GET 方式发送请求报文，在收到请求报文后，服务端会处理请求报文，并向客户端返回响应报文。继电器因此而得到控制，来改变电平的高低进而控制电路电流达到开关智能灯的效果(如图 5)。

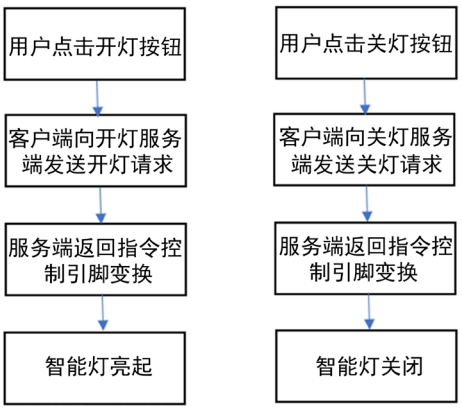

Figure 5. Smart light control flowchart
图 5. 智能灯控制流程图

3.3. 权限伪造脚本程序的设计

基于 3.2 所示智能设备控制原理，使用 python 编写脚本程序来模拟请求过程，从而取得无用户授权情况下的控制权。脚本首先调用 python 的 requests 库，requests 是使用 Apache2 licensed 许可证的 HTTP 库，支持 HTTP 连接保持和使用 cookie 保持会话，自动实现持久连接 keep-alive，还可自动响应内容的编码，支持国际化的 URL 和 POST 数据自动编码。使用 Requests 可以轻而易举的完成浏览器可有的任何操作。

之后脚本程序会根据渗透测试人员的需求来发送不同的 GET 方式请求报文。根据不同的控制需求，脚本程序会向不同的服务端发送请求报文，我们假设服务端 A/B 分别处理智能电灯的开/关请求，则当渗透测试人员想要开启智能电灯时，脚本程序就向服务端地址 A 发送 GET 请求报文并附上开启信号，同理则向服务端地址 B 发送请求报文。python 脚本代码流程如下图 6：

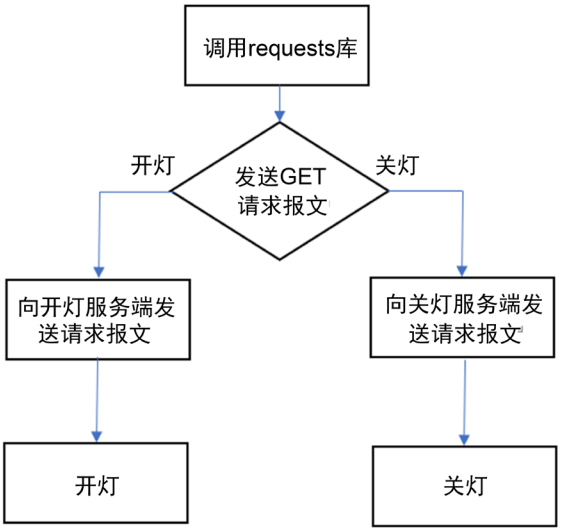

Figure 6. Flow chart of code control principle
图 6. 代码控制原理流程图

4. 实验结果与防护分析

4.1. 实验结果

实验中，我们的设备成功连上了被破译 Wi-Fi，证明成功破解了智能设备所在的网络接入其内网，在对智能灯进行开关操作过程中，脚本程序均返回状态码 200，智能灯也成功被远程操作实现了开关。实验证明了智能设备存在安全隐患且极有可能带来潜在的对人身，财产的安全威胁，而这种威胁在智能设备发展高峰期尤为突出。

4.2. IoT 智能设备安全解决方案

综上我们可以形成以下的 IoT 智能设备的方案如下：

增大智能设备所在无线网络的密码安全性：1) 增加密码位数；2) 同时包含数字，大小写字母，特殊符号；3) 避免信息弱口令，如生日，门牌号等；4) 定期更换密码。增大越权控制难度：1) 以 POST 方式发送请求报文；2) 请求报文参数加密；3) 设置白名单：仅白名单用户可向服务端发送请求报文。

同时，为防止攻击使设备出现暂停服务或者直接损坏，也要求智能家电具备周全的异常处理机制[7]。对智能设备厂家来说，入侵检测是通过对主机和网络上的各种数据进行收集整理之后应用固定的模式对

信息进行匹配分析经过分析发现是否存在系统恶意入侵行为并进行相应的报警和记录。入侵检测与报警系统提供了对智能家居内部攻击外部攻击和误操作的实时保护是保证网络安全的重要途径[8]。

4.3. 创新性和研究价值分析

本论文创新性在于通过 IoT 有别于被动扫描累的网络安全检测手段，而采取主动攻击的方式来进行网络安全防护检测并有效的模拟了此次攻击行为，意味着未来在 IoT 时代不仅仅只是类似于黑客的方式进行物理攻击，而有可能通过物－物之间实施大规模入侵行为。故本文在探究在未来物联网时代大规模物－物攻击的思考方式和攻击手段上有一定的参考价值。

5. 小结与展望

本文基于网络控制继电器的原理设计了可网络控制的智能灯作为当前智能设备的代表，运用渗透测试和编写脚本程序对整个智能系统进行了安全测试与评估，得出了当前智能设备存在的安全问题和潜在威胁，并分析了其产生原因，提出了解决办法。虽然目前的智能设备仍存在很多的问题，但随着网络安全越来越被普通人、企业、国家所重视，所投入的资金越来越多，相信未来的智能设备安全问题将会得到改善，恶意的黑客行为也将越来越难以下手。同时 IoT 智能设备的密码安全性增强方案也能够给广大用户带来安全性的提升。同时下一步的研究是基于未来的 IoT 时代下海量智能设备透过物－物自动化大规模攻击的预警与阻断。

基金项目

本项目受上海对外经贸大学人工智能变革与管理研究院区块链技术与应用研究中心资助。项目号：SUIBE-ABC-2020-3。

参考文献

[1] 张永刚. 我国智能家居现状与问题[J]. 智能建筑与城市信息, 2012(12): 26.

[2] 陈灿. 智能家居安防标准体系浅析[J]. 中国管理信息化, 2017, 20(9): 171-173.

[3] 刘冀鹏, 张洪沛. 智能家居安防技术专利分析[J]. 软件, 2018, 39(1): 165-168.

[4] 杨丽, 冯娟, 卢秀丽, 刘强. 基于物联网智能家居安全监控系统设计[J]. 现代电子技术, 2019, 42(8): 63-66.

[5] 刘发贵, 彭妙霞. 一种智能家居安全网关的安全防护方法[P]. 中国专利, CN108809970A. 2018-11-13.

[6] 物联网之弊: 黑客发现酒店安全漏洞[EB/OL]. http://www.ifanr.com/434444, 2014-7-21.

[7] 王春莲. 内网网络安全解决方案研究[J]. 硅谷, 2011(4): 89.

[8] 刘东, 常清雪, 雷敏. 智能家居安全隐患及其应对策略[J]. 中国信息安全, 2016(10): 71-73.