1.SoK Security Evaluation of Home-Based IoT Deployments

基于家庭的物联网部署的安全评估

目录

摘要 2
一、引言 2
二、方法论 2
A.抽象模型概述 2
B.安全性 3
C.系统化方法 3
D.评估范围和攻击模型 3
三、系统化知识 3
A.设备 3
B.安全性 5
C.云端点 6
D.通信 6
四、评价 8
A.实验设置 8
B.数据 8
C.挑战 8
D.设备 8
E.移动应用 9
F.云端点 9
G.通信 10
H.缓解措施 10
五、提案 10
A.利益相关者 10
B.建议 11
六、结论 11
七、致谢 11

摘要

基于家庭的物联网设备在其安全实践方面享有惨淡的声誉。从表面上看，物联网设备的不安全性似乎是由集成问题引起的，可以通过简单的措施来解决，但这项工作发现这是一个幼稚的假设。事实是，物联网部署的核心是利用传统的计算系统，例如嵌入式，移动和网络。这些组件有许多未开发的挑战，例如，过于特权的移动应用程序对嵌入式设备的影响。

我们的工作提出了一种方法，研究人员和从业人员可以使用该方法来分析基于家庭的物联网设备的安全性。我们使用此方法将基于家庭的物联网的文献系统化，以了解攻击技术，缓解措施和利益相关方。此外，我们评估了 45 种设备用来扩充系统化的文献，来发现被忽视的研究领域。为了使该分析透明并易于被社区采用，我们提供了一个公共门户网站来共享我们的评估数据，并邀请社区做出自己的独立发现。

（简单提出当前物联网的安全状况，并说明自己的研究成果——一种可以分析物联网设备安全性的方法。）

一、引言

涉及物联网（IoT）的安全问题继续导致严重的操作问题，包括最常见的攻击[1]，设备的大量利用[2]和有关“异国”设备黑客攻击的引人注目的标题[3]。对物联网设备的需求，尤其是在数十亿美元的住宅市场[4]中，已引起了当今的淘金热。新兴公司正在争夺物联网市场。由于上市时间和生产成本要比审慎的安全做法优先，因此人们对受损的物联网设备的熟悉程度已经越来越高。研究人员和供应商正在追赶以解决物联网不安全问题，但是其中许多工作是模糊不清的和临时的。

一些工作组和市场领导者已经提出了针对物联网设备的标准化[5] – [12]，但是不幸的是，他们尚未就解决方案达成共识。此外，基于家庭的物联网设备的异构性加剧了这些不安全因素，因为尽管核心功能相似，但基于设备类型的具体功能却可能大不相同。例如，物联网吸尘器和家庭助理设备可能使用嵌入式 Linux 操作系统，但设备上运行的服务将有所不同。这些差异使得难以分析各种基于家庭的物联网产品。

国家支持的敌手非常了解这些困境，他们已经利用这些优势进行了复杂的网络操作[1]。更糟的是，一些供应商将服务后门留在其设备中，后来被僵尸网络发现并加以利用[13]。甚至不成熟的犯罪集团也利用猖獗的不安全因素来进行分布式拒绝服务（DDoS）攻击[2]。不幸的是，清理工作和漏洞修补远远不够完美，随着其他设备的联机，针对它们的威胁变得多种多样，这使它们得以进一步传播[14]。为了系统地解决这些安全问题，研究人员需要通过进行度量和深入研究来对漏洞进行分类和解决，以了解情况。对于基于家庭的物联网安全性有很多研究工作，但是它们是分散的。我们的社区需要了解当前的文献，对安全漏洞进行洞察和识别。这些见解将使研究界可以正式确定哪些不安全因素会长期存在，拟议的缓解措施是什么以及利益相关者应承担的责任。此外，这些深入的研究和文献分类可以指导社区帮助他们确定工作的轻重缓急。（提出现在需要做的工作。）

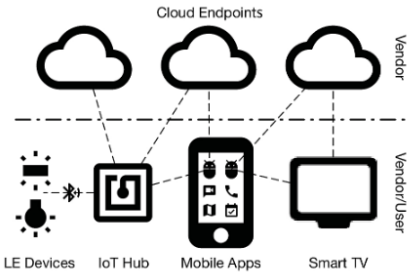
在这项工作中，我们提出了一种建模方法，用于研究基于家庭的 IoT 设备并基于组件分析评估其安全状态，这些组件分析包括：IoT 设备，配套的移动应用程序，云端点和关联的通信渠道。利用我们的方法，我们将基于家庭的物联网设备的研究文献系统化，以了解攻击技术，建议的缓解措施和利益相关者的责任。我们利用这些知识得出见解并为我们的社区确定研究机会。此外，我们评估了当今市场上可用的 45 种基于家庭的 IoT 设备，并概述了其在 IoT 组件中的安全性。

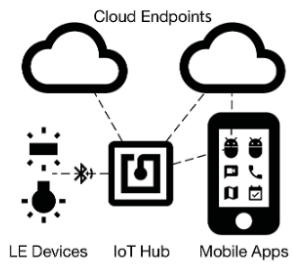
在系统化和评估的基础上，我们比较了两种方法之间的共同点和差异，这些见解表明了它们的共性和差异。我们提供了每个组成部分的缓解措施列表，并为不同的利益相关者提出了解决所发现问题的策略。最重要的是，我们建立了一个门户网站，邀请同行的研究人员，供应商和超级用户来进行新设备评估，并使用已发布的数据集和建议的方法来改进我们的结果。

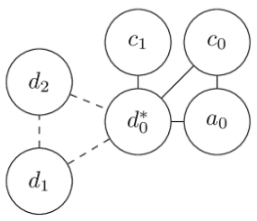
（本文提出了一种建模方法，用于研究基于家庭的 IoT 设备，并基于组件分析评估其安全状态，第二，建立了一个门户网站，邀请同行的研究人员，供应商和超级用户来进行新设备评估，并使用已发布的数据集和建议的方法来改进我们的结果）

1 可通过以下网址在线访问评估门户：https：//yourthings.info。

图 1：典型的家庭式 IoT 设置。图 2：单一 IoT 部署。图 3：物联网图模型







（low-energy (LE)）

二、方法论

我们的工作有两个方面，文献的系统化和基于家庭的物联网设备的评估。这项工作依赖于将物联网部署细分为组件的抽象模型，我们将其统一应用于研究文献和设备评估。

A.抽象模型概述

我们提出了一个抽象模型来表示物联网部署及其拓扑。图 1 是具有多个设备的物联网家庭连接示例。该方法涉及将每个设备分成各自的拓扑，如图 2 所示。形式上，我们将物联网部署定义为一组顶点 V 和边 E，如图 3 所示。总体而言，我们的抽象模型具有四个主要组件：一组设备（D），一组云端点（C），一组移动应用程序（A）和一组通信通道（E）。

$$\text{where:} \quad A, C, D \subset V; \quad D : \{d_i, i \in \mathbb{Z}\}; \quad C : \{c_j, j \in \mathbb{Z}\}; \quad A : \{a_k, k \in \mathbb{Z}\}; \quad E : \{e_l, l \in \mathbb{Z}\}$$

对于每个设备部署，我们构造一个代表性的图并检查每个组件的安全性属性。

（公式化模型）

B.安全性

安全属性分为三类：攻击载体，应对措施和利益相关者。攻击媒介是用于规避物联网系统安全性的方法。应对措施定义应采取哪些措施来解决攻击媒介。最后，利益相关者代表负责缓解的一方。

攻击载体。

设备具有三种攻击类别：漏洞服务，弱身份认证和默认配置，其定义如下：

•漏洞服务是指正在运行的服务中的漏洞。

•弱认证是指弱或可猜测的凭据。

•默认配置是指使用不安全的出厂设置运行的设备。

移动应用程序具有以下三种攻击类别，权限，编程和数据保护：

•权限是指移动应用程序拥有过多特权。

•编程是指包含易受攻击的实现的移动应用程序，包括不正确使用加密协议。

•数据保护是指移动应用程序对敏感信息进行硬编码。

（硬编码：硬编码是将数据直接嵌入到程序或其他可执行对象的源代码中的软件开发实践，与从外部获取数据或在运行时生成数据不同。 硬编码数据通常只能通过编辑源代码和重新编译可执行文件来修改。如果对隐私信息进行硬编码，很容易就会被敌手通过源码获取到。）

组件的通信具有两种攻击类别，即加密和中间人（MITM），其定义如下：

•加密是指缺乏加密或支持弱加密协议。

•MITM 表示容易受到中间人攻击。

云端点与设备和通信边缘都具有以下攻击类别：漏洞服务，身份验证弱和加密，如上所述。

应对措施。应对措施的类别，补丁和框架涵盖了所有四个组成部分。补丁是指通过供应商更新或用户关注度修补组件来减少攻击载体。框架类别缓解了需要新方法的基本问题。

利益相关者。利益相关者类别，供应商和最终用户涵盖了所有四个组成部分。这些类别指示哪个利益相关者负责处理。图 1 将 IoT 部署分为供应商和用户控制的网络。云端点由供应商控制和处理，而家庭网络中的组件可能会公开配置参数，因此用户可以禁用易受攻击的功能。例如，如果设备具有已知的默认密码，并且供应商允许用户更改默认密码，则用户可以更改密码以保护设备安全。

（物联网中的安全方面）

C.系统化方法

系统化使用建议的抽象模型，该模型在前面讨论的类别中统一显示了文献，确定了攻击技术，建议的应对措施和利益相关者的责任。每个工作都可以适用于一个或多个 IoT 组件。基于以下标准选择系统化的文献：

•优点：这项工作是独特的，是探索当前安全问题的工作之一。

•范围：这项工作侧重于基于家庭的物联网系统的安全性（进攻性和防御性）。

•影响：根据被引用的次数，这项工作被认为是重要的。

•创新：工作揭示了社区当前正在调查的新领域。

D.评估范围和攻击模型

评价范围。我们的第二个贡献是使用抽象模型评估安全属性，从而评估了基于家庭的物联网设备。我们将范围限制在基于家庭的 IoT 设备上，因为它们与系统化工作相关，并且随时可用，并且可以轻松复制实验设置。

攻击模型。为了进行评估，我们将攻击模型简化为 Internet 协议（IP）网络攻击者。我们认识到，有更强大的对手可以攻击基于低能耗（LE）的设备[15]，但是它们需要专用的资源，而这些资源在许多家庭网络中是不可用的。由于 hub 和低能耗设备之间存在信任会话，因此我们认为对 hub 设备（低能耗和 IP 之间的通信桥）的利用等同于对所有连接的低能耗设备的利用。我们排除了对低能耗设备的直接评估，但考虑了其平台中心 hub 的评估。最后，我们认为家庭网络是不受信任的网络，我们不对具有完全可见性的移动应用程序，调制解调器/路由器或 Web 浏览器的安全状态做出任何假设（[16]）。

（评估范围限制在基于家庭的 IoT 设备,提出观点——家庭网络是不受信任的网络）

三、系统化知识

本节介绍了基于抽象图模型的基于家庭的物联网研究的系统化（参见图 3）。表 I 概述了系统化工作及其相应的小节，在此我们将详细讨论文献。组件分类突出了工作的重点，而攻击媒介，缓解措施和利益相关者则确定了方法。系统化突出了代表工作；因此，它没有为所有相关工作提供全面的参考。

A.设备

大多数基于家庭的物联网研究都集中在设备上，因为设备组件是物联网部署的基石。

1）攻击媒介：几篇著作（[17]–[20]）探讨了物联网设备配置的不安全性。Barnes [17]，基于 Clinton 等人的发现。 [18]，演示了设备上裸露的硬件引脚如何使他获得特权访问权并监视最终用户。如 Chapman [21]和 Rodrigues [22]所示，不安全的配置加上认证不力或缺乏认证会加剧该问题。正在运行的服务中的身份验证不充分或缺乏身份验证，是造成几种已记录攻击的关键原因[23]-[26]。这些攻击表明设备的设置和配置是供应商必须考虑并评估安全漏洞的重要过程。供应商应强制执行严格的身份验证策略，并要求最终用户在允许设备运行之前对其进行配置。

Max [23]评估了 August 智能锁的安全性，发现弱身份认证和不安全的默认配置破坏了锁的安全性。他发现了硬编码的凭据和调试配置，可以对锁进行修改和自省。奥伯迈耶等人的工作。 [25]在基于云的摄像机上发现，尽管该设备的密码看似很强（36 个字母数字和符号），但密码是反向的摄像机的 MAC 地址，并经过 Base64 编码。Kavalaris 等。 [26]显示 Sonos 设备在高端口上运行未经证明和未经身份验证的服务，从而使 LAN 客户端可以完全控制该设备。由于缺少身份验证，Sonos 设备容易受到未经授权的设备配对的影响。SmartAuth [24]发现，身份验证问题也通过过度特权的应用程序在物联网应用程序平台中显现出来。设备配对会在客户端与其设备之间建立可信通道。此外，IoT 中心将 LE 设备桥接到 IP 网络，IP 网络具有预先建立的信任关系，如图 3 所示。攻击者将利用此特定过程来规避设备或将其用作支点。

物联网应用程序平台公开了基于权限的模型，以允许第三方应用程序运行。费尔南德斯等。 [27]–[29]显示了对第三方应用程序的隐式信任如何对设备的安全性产生重大影响。设备平台内有许多子组件，这些子组件可能会使设备的固定变得困难。许多供应商都有良好的做法来确保安全的身份验证和安全的默认配置（如 O'Flynn [30]所示），但是核心设备服务可能会遭受旁信道信息泄漏的困扰。Ronen 等。 [15]表明，尽管 Philips

Hue 设备相当安全，但他们能够通过边信道攻击提取主加密密钥，并将其与通信协议中发现的漏洞相结合，从而导致可蠕虫利用。

固件中的缺陷使攻击者能够窃取 WiFi 凭证[31]，将智能恒温器转变为间谍小工具[32]，勒索它们[33]，在智能电视上运行任意命令[34]以及暗中控制家庭辅助设备[35]。Costin 等。 [36]对固件分析进行了大规模研究，发现了一系列法则。文献表明，设备安全性需要采取防御性方法来保护旁通道，固件和硬件。用于软件和硬件开发的工具链具有供应商必须使用的定义完善的安全开发流程。

（进行调研，阐述当前已发现的问题，个人认为非常好，调研充分，为下文做了很好的准备）

2）应对措施：为解决易受攻击的服务，配置错误和身份验证不可靠的问题，供应商通过设备更新进行修补，而物联网平台中固有的设计缺陷则通过新框架得以缓解。Wang 等。 [37]提出了一种基于源的框架，该框架可在整个部署中聚合设备活动，以检测错误和恶意活动。

表 I：使用基于组件的分析对当前文献进行系统化。每个部分对应于方法学中讨论的图形组成部分，涵盖攻击载体，应对措施和利益相关者。这意味着攻击，措施或利益相关者的类别适用于所讨论的文献。

Component	Ref	Attack Vector			Mitigations		Stakeholders	
		Vuln. Services	Weak Auth	Default Config	Patching	Framework	Vendor	End User
Device Section III-A	Ur13 [19]			✓	✓		✓	
	Costi14 [36]	✓			✓		✓	
	Chapm14 [21]		✓	✓	✓		✓	
	Kaval14 [26]	✓	✓	✓	✓		✓	✓
	Wuess15 [20]			✓	✓		✓	
	Rodri15 [22]		✓	✓	✓		✓	
	Lodge16 [31]	✓			✓		✓	
	Ike16 [18]			✓	✓		✓	
	Franc16 [33]	✓			✓		✓	
	O'Fly16 [30]	- -	- -	- -	- -	- -	- -	- -
	Ferna16 [27]	✓			✓		✓	
	Max16 [23]	✓	✓	✓	✓		✓	
	FlowF16 [28]	✓		✓	✓	✓	✓	
	Oberm16 [25]	✓	✓	✓	✓		✓	
	Barne17 [17]			✓	✓		✓	
	Herna17[32]	✓			✓		✓	
	Morge17 [34]	✓			✓		✓	
	Ferna17 [29]	✓		✓	✓		✓	
	Ronen17 [15]	✓			✓		✓	
	Dolph17 [35]	✓			✓		✓	
	Tian17 [24]	✓	✓		✓	✓	✓	✓
	Wang18 [37]	- -	- -	- -		✓	✓	
		Permissions	Programming	Data Protection				
Mobile Application Section III-B	Barre10 [38]	✓			✓		✓	
	Au12 [39]	✓			- -	- -	✓	✓
	Egele13 [40]		✓	✓		✓	✓	
	Vienn14 [41]		✓	✓	- -	- -	- -	- -
	Max16 [23]		✓	✓	✓		✓	
	Sivar16 [16]	✓		✓		✓	✓	✓
	Demet17 [42]	✓		✓		✓		✓
	IoTFu18 [43]		✓		- -	- -		✓
		Vuln. Services	Weak Auth	Encryption				
Cloud Endpoint Section III-C	Max16 [23]	✓	✓		✓		✓	
	Oberm16 [25]		✓	✓	✓		✓	
	Nandi16 [44]	✓				✓		✓
	Blaic16 [45]	✓	✓	✓	✓		✓	
	Wilso17 [46]			✓		✓	✓	✓
	Surba17 [47]	✓			- -	- -	✓	✓
	DTAP18 [48]	✓	✓	✓		✓	✓	✓
		Encryption	MITM					
Communication Section III-D	BEAST11 [49]	✓			✓		✓	
	Garci11 [50]	✓	✓		✓	✓	✓	
	LUCKY13 [51]	✓			✓		✓	
	Ryan13 [52]	✓	✓		- -	- -	- -	- -
	Foula13 [53]	✓	✓		- -	- -	- -	- -
	Alfar13 [54]	✓			✓		✓	
	Selvi14 [55]	✓			✓		✓	
	POODL14 [56]		✓		✓		✓	
	FREAK15 [57]	✓			✓		✓	
	CRIME15 [58]		✓		✓		✓	
	SMACK15[59]	✓	✓		✓		✓	
	Adria15 [60]	✓	✓		✓		✓	
	Zilln15 [61]	✓	✓		- -	- -	- -	- -
	DROWN16 [62]	✓	✓		✓		✓	
	Jasek16 [63]		✓		✓		✓	
	Kinti16 [64]	- -	- -		✓			✓
	Aptho17 [65]	✓			✓			✓
	Wood17 [66]	✓				✓		✓

SmartAuth [24]是一个框架，可识别在 SmartThings 和 Apple Home 等平台上运行的 IoT 应用程序所需的权限。FlowFence [28]是一个框架，可将应用程序代码拆分为敏感和非敏感模块，并通过不透明的处理程序来协调执行。这种方法给开发人员造成了负担，因为他们必须注意对敏感和不敏感数据执行什么代码。此外，研究人员可以采用在移动应用程序框架中发现的技术来解决物联网平台的不安全问题。

3）利益相关者：表一显示主要利益相关者是卖方。供应商负责修补和更新易受攻击的设备，但可以通过配置将某些职责委托给用户。例如，用户可以通过禁用设备上有问题的服务来减轻不安全感。SmartAuth [24]为设备上的应用程序提供了派生的身份验证方法，但是实施必须由供应商来完成。用户可以通过选择授权第三方应用程序的权限来获得控制权。Kavalaris 等。 [26]显示了 Sonos 设备公开的服务如何造成安全风险。用户可以通过网络分段来减轻这种风险，但是它需要一些技术专长。

没有多少设备允许用户完全配置正在运行的服务，甚至禁用它们，除非他们具有特权访问权限。基于所有建议的应对措施，最终用户可以管理驻留在家庭划分方的配置或网络分段，如图 1 所示。最终用户没有太多控制权，并且通常会获得一个简约的界面，这限制了易受攻击的服务的应对。另一方面，供应商有责任使设备保持最新状态。

4）拿走：文献讨论了设备安全性的某些方面。设备具有许多有助于整体安全的组件，例如平台权限，未经身份验证的服务，不安全的配置以及软件和硬件错误。此外，它们在组合时会被放大。设备安全性不仅仅存在于软件中，而且存在于硬件和旁通道中的漏洞。在许多设备中都发现了嵌入式 Linux，但没有安全的开放式 IoT 平台，该平台可以合并社区新提出的框架[24]，[28]，[37]。系统修补程序解决了大多数漏洞。修补过程并不完美[32]，可以通过在其他计算领域中实施的良好实践来改进[67]。最终用户几乎无法控制或查看设备的运行情况。安全地提供健康遥测和细粒度的配置参数可以使用户减轻即时风险。用户可以通过多种方式部署设备，这超出了供应商允许的假设，因此，在制定安全措施时，供应商应假定设备面向互联网。

（为了应对物联网设备中的安全问题，供应商采取了很多措施，打补丁、改进框架，但这些还不够，用户掌控着太少的功能，应该进一步加强用户的权限）

通用计算系统面临着类似的问题，这些通用计算系统可公开访问并运行易受攻击的服务或使用弱认证（SSH 和可猜测的密码）。从安全平台和操作系统改编技术将改善许多。

IoT devices.

Device: Vulnerabilities in IoT systems manifest themselves in hardware, software, and side-channels and they are exacerbated when combined. There are efforts to address the security problems in IoT platforms, but common vulnerabilities across different products need a systematic analysis. Mitigating vulnerabilities relies heavily on vendors, but vendors should provide a way for users to control, inspect, and evaluate their devices. Adapting mature technology to manage IoT devices can significantly improve the security of IoT.

（iot 系统中的漏洞表现在硬件、软件、信道中，当他们连接在一起时，安全问题会加剧，针对 iot 平台上安全问题有很多尝试，但跨不同产品的漏洞需要一个系统化的分析，应对措施大部分依靠供应商，但是供应商应该位用户提供一个能够控制、检查和评估他们设备的方式，应用成熟的技术去管理 iot 设备能够很好的改进 iot 的安全）

B.安全性

移动应用程序。许多基于家庭的 IoT 设备都有一个配套的移动应用程序来控制，配置和与设备交互。我们在抽象模型中将移动应用程序表示为一个顶点（请参见图 3）。可以利用移动应用程序作为对物联网部署的攻击面。

1）攻击载体：Acar 等。 [68]确定了 Android 移动应用程序问题的五个不同领域，即权限演变，权限革命，网络化，编程引起的泄漏和软件分发。我们采用了 Acar 的方法，并确定了影响物联网设备的三大主要不安全因素：过特权（权限[38]，[39]），编程错误（编程[40]）和硬编码的敏感信息（数据保护[41]]）。Max [23]显示了编程错误如何泄漏有关设备和云端点的敏感信息。Max 使用敏感信息来转储凭据，提升特权并规避 August Smart Lock 的安全性。除了 Max 的工作之外，没有直接的攻击利用移动应用程序来绕过 IoT 设备。

Chen 等。 [43]提出了 IoTFuzzer，它可以在 IoT 部署中对移动应用程序进行检测以发现 IoT 设备上的错误。Chen 的方法是独特的，并利用了供应商在应用程序中编程的语义。尽管没有关于在野外使用此技术的报道，但是从理论上讲，攻击者可以使用相同的方法来升级 IoT 设备上的特权。Sivaraman 等。 [16]展示了如何在本地网络上使用移动应用程序来收集有关可用家用设备的信息，然后重新配置路由器/调制解调器防火墙规则以使设备面向互联网。Hanguard [42]展示了供应商关于 LAN 的宽松安全假设如何可以暴露 IoT 设备。随行移动应用程序是设备的切入点，供应商通常会认为部署网络是可信且安全的。这些假设可能会对设备的安全性产生严重影响，尤其是当设备依赖未经身份验证的服务或未经加密的通信时。

2）应对措施：Hanguard [42]提出了一个用户空间移动应用程序，该应用程序与路由器接口以通过基于角色的访问控制（RBAC）控制访问。Hanguard 的方法将阻止 Sivaraman 等人讨论的攻击。 [16]但无法阻止来自已损坏的伴随应用程序的攻击。通过遵循 Pscout [39]中讨论的最佳实践来保护移动应用程序的安全，Barrera 等人。 [38]，Egele 等。 [40]，和 Viennot 等。 [41]，减少了攻击面。不幸的是，正如 Viennot 等。 [41]显示，Google Play 商店中的大部分应用程序都包含与权限，编程错误和信息泄漏有关的问题。移动应用程序平台已经成熟，并且具有内置的安全设施以推广良好做法。开发人员和供应商应遵守最佳做法，并定期审核其移动应用程序。

3）利益相关者：移动应用程序组件依赖于用户和供应商。部分原因是大多数移动平台提供给最终用户的权限模型。Hanguard [42]为用户提供了一个系统，该系统可以通过路由规则（用户划分，图 1）在本地网络内部进行部署，而这不涉及供应商。Sivaraman 等。 [16]建议用户在网络上运行移动应用程序时应保持警惕，并且仅使用授权商店（Google Play，Apple App Store 等）。供应商必须解决编程错误并通过更新来保护信息存储。供应商必须熟悉移动平台才能部署安全的应用程序，或使用信誉良好的第三方开发人员来提供安全的开发专业知识。

4）带走：Acar 等人的工作。 [68]显示了移动应用安全领域的成熟度。内在的信任被赋予了移动应用程序，移动应用程序在许多情况下控制着 IoT 设备或云服务的核心组件。Max [23]和 IoTFuzzer [43]演示了如何滥用移动应用程序与 IoT 设备或云服务之间的隐式信任。物联网供应商和开发人员应遵守平台开发指南，并利用安全功能来确保正确部署。通过细粒度控制来限制移动应用程序对设备的访问是一个有希望的方向，它可以减少攻击的影响。最后，应进一步研究 Hanguard 的[42]方法，以为最终用户提供控制以减轻风险。

（移动应用程序：移动应用程序受到物联网设备的信任，攻击者已利用这种信任作为攻击点。供应商应该对信任关系做出保守的假设，并限制与核心服务的交互。移动应用程序仍然遭受过度特权，编程错误和硬编码敏感数据的困扰。在移动平台上遵守既定的安全开发准则将改善 IoT 安全性。）

Mobile Application: Mobile applications are trusted by IoT devices and attackers have leveraged that trust as an attack point. Vendors should make conservative assumptions about the trust relationship and limit the interactions with core services. Mobile applications still suffer from over-privileged permissions, programming errors, and hard-coded sensitive data. Adhering to established secure development guidelines in mobile platforms will improve IoT security.

C.云端点

云端点是物联网部署的互联网组件，从某种意义上说，它们定义了物联网是什么。他们提供核心服务，例如远程管理，警报和数字内容。物联网设备及其移动应用程序信任这些云终结点，这为攻击者提供了额外的攻击点。我们在抽象图形模型中将云端点建模为顶点（请参见图 3）。

1）攻击媒介：Max [23]的攻击是一个很好的例子，涉及物联网生态系统的所有组件。该攻击在八月智能锁的云终结点上发现了不安全的应用程序接口（API），从而将来宾帐户升级为管理员帐户。Blaich [45]审核了 Wifi Barbie 娃娃的各种漏洞，发现云端点未对固件下载进行身份验证，具有多个跨站点脚本漏洞，允许用户名枚举，没有蛮力限制并且发布了永不过期的 cookie。Obermaier 等。 [25]对监控摄像头的云端点进行了审计，结果表明攻击者可以注入镜头，触发虚假警报以及对摄像头系统进行拒绝服务攻击。这些攻击之所以可能是由于基础结构配置中引入的漏洞，易受攻击的服务以及不安全的 API。Zuo 等。 [69]利用客户端到云的信任来实现 AutoForge，该伪造将来自移动应用程序的请求伪造到云端点，从而实现密码暴力破解，密码探测和安全访问令牌劫持。物联网组件之间的隐式信任非常敏感，供应商必须在允许端点不受限制的访问之前验证端点。

IoT 集成平台，例如 IFTTT [70]，automate.io [71]和 CloudWork [72]，都是第三方云端点。他们使用 OAuth 令牌连接多个 IoT 设备以执行用户编程的任务。Surbatovich 等。 [47]研究了使用配方 2 时对隐私和完整性的安全隐患，并表明某些配方可以使攻击者分发恶意软件并进行拒绝服务攻击。南迪等。 [44]通过触发动作编程（TAP）报告了类似类型的用户引发的编程错误，这导致了错误的事件触发或缺少事件触发。费尔南德斯等。 [48]指出，云集成平台可能会遭到破坏，这可能会公开暴露用户的 OAuth 令牌。这些情况很可能基于 Equifax [73]和 Orbitz [74]等最近的平台妥协而发生。威尔逊等人的工作。 [46]并未确定物联网生态系统上的攻击媒介，但它研究了用户对物联网供应商的隐私和信任。这些攻击表明云集成服务缺乏细粒度的控制，并且泄漏了可能导致漏洞的私人和敏感信息。

2）应对措施：为缓解这些攻击，Max [23]，Obermaier 等人。 [25]和 Blaich [45]建议适当的配置和安全的身份验证机制。Surbatovich 等。 [47]提供了一个框架来分析云平台的配方，这激发了以后的工作。南迪等。 [44]提出了一种自动触发器生成系统，该系统可以分析用户定义的触发器中的错误，并通过重写触发器来纠正它们。费尔南德斯等。 [48]提出将分散式框架用于称为 DTAP 的触发动作可编程平台。DTAP 平台是 IoT 云平台与用户本地网络之间的隔离片，并且代理基于转移令牌访问 IoT 设备（XTokens）。缓解技术包括保护云端点，提供工具来分析第三方集成服务，帮助开发人员为其应用程序生成正确的触发器，以及为寿命短的令牌提供对设备功能的受限访问。

一些相关，威尔逊等。 [46]着眼于赋予物联网用户以信任他们的私有数据的能力。该技术称为 TLS 旋转和释放（TLS-RaR），该技术要求审核员实体收集 TLS 数据包，以要求供应商提供会话密钥以解密通信。然后，卖方旋转 TLS 会话密钥，并向审核员披露先前的密钥，以解密收集到的 TLS 数据包。审核系统必须部署在最终用户边界上，并收集他们希望审核的设备的流量。

3）利益相关者：供应商控制云端点（参见图 1），而用户则无法检查或控制其设备向云端点发送的内容[66]，[75]。此外，第三方云提供商为物联网部署提供基础架构即服务（IaaS）和平台即服务（PaaS）。许多物联网设备依靠基于云的基础架构来运行其服务。计划外中断[76]，基础设施受损[77]和故意攻击[78]影响了云端点的部署。当涉及到云基础架构配置和 API 实施（[23]，[25]，[45]）时，供应商应负责处理漏洞。

较新的 IoT 设备正在利用托管的 IoT 平台，该平台承担了公共云提供商的许多安全责任。另一方面，大多数提议的框架（[44]，[46]，[48]）都是以用户为中心的，并以有限的方式赋予最终用户可见性和控制力。费尔南德斯等人的工作。 [48]和威尔逊等。 [46]是一种混合方法，可以由供应商和用户或受信任的第三方联合部署。对于云提供商，供应商可以通过多样化和过度订阅不同的云提供商来减轻风险。

4）取得成功：物联网云终端通过配置和 API 实施展现了不安全的云部署，但是可以使用易于使用的云安全工具来解决这些漏洞。需要进行其他度量以进一步了解云部署中这些错误配置的程度。Censys 项目[79]是有价值的数据源，可以使研究人员从历史上分析物联网基础设施。此外，物联网云集成平台还引入了新挑战，这些挑战模仿了分散式信任管理[80]等经典工作。集成云平台为用户提供了一种方法，可以根据事件将多个 IoT 设备链接在一起以执行任务，并且它们遭受特权过高和隐私隐患的困扰，这在 Surbatovic 等人的工作中得到了证明。 [47]。

费尔南德斯等。 [48]通过将信任管理系统和令牌认证协议应用于物联网平台，将先有技术用于物联网云平台。供应商正在调整托管的物联网云平台，这将安全责任转移到了云供应商，例如 Amazon IoT Core [81]，Azure IoT Hub [82]和 Google Cloud IoT [83]。物联网云终端更多地依赖第三方基础架构来部署和运行其服务，这意味着供应商应考虑针对意外停机和基础架构受损的应急计划。需要进行其他研究来了解托管的物联网云平台以及存在哪些可能的弱点。

（云端点：云端点存在配置错误和易受攻击的服务，可以使用行业标准适当地保护它们。第三方云提供商通过提供供应商适应的安全管理的物联网平台，发挥了重要作用。通过集成平台开发，分析和部署第三方应用程序的工具链需要特别注意。）

Cloud Endpoint: The cloud endpoints suffer from misconfiguration and vulnerable services that can be properly secured using industry standards. Third-party cloud providers play an important role by offering securely managed IoT platforms, which vendors are adapting. Toolchains for developing, analyzing, and deploying third-party applications via integration platforms require additional attention.

D.通信

物联网部署中的通信边缘（参见图 3）分为两类协议，互联网协议（IP）和低能耗（LE）协议。两种通信都可以存在于网络的用户边界上（参见图 1），但是只有 IP 通信可以通过 Internet 进行。工业界和学术界的研究人员都因为其在其他领域的适用性而对网络通信的安全性进行了大量投资。

大多数基于家庭的物联网系统实现四种通信协议：IP，Zigbee，Z-Wave 和 BluetoothLE（BLE）。（Zigbee，Z-Wave 和 BluetoothLE（BLE）都有安全问题）物联网设备选择使用 IP 套件进行通信，这是因为其可靠性和可靠的能力来传输不可思议的全球网络流量。IP 协议是无状态的，不提供安全性，但是可以使用 TCP 和 TLS / SSL 协议来补充 IP 协议，以提供所需的安全性功能。根据文献，我们确定了家庭物联网设备使用的五个流行的应用层协议，即：DNS，HTTP，UPnP，NTP 和自定义实现。（全部都有安全方面问题）

1）攻击媒介：DNS 协议是 Internet 服务所依赖的轻量级协议，但是基于递归和客户端配置无意中泄漏了私人信息。Kintis 等。 [64]发现启用 EDNS 客户端子网功能（ECS）[84]（嵌入客户端 IP 地址的截短部分）的开放式递归 DNS 会对隐私产生影响。Selvi [55]演示了如何使用对 NTP 的 MITM 攻击绕过 HTTP 严格传输安全性（HSTS）。HTTP 协议提供了更可靠的传输方式，但是像 DNS 和 NTP 一样，它不提供任何保密性或完整性。Bellissimo 等。 [85]和塞缪尔等。 [67]演示了像 HTTP 这样的不安全协议如何使攻击者进入 MITM 并后门系统软件更新过程。

物联网设备广泛依赖 UPnP 协议来提供易于配置和控制。UPnP 使用 HTTP 协议，因此继承了相同的法则[86]。Garcia [50]展示了攻击者如何滥用 UPnP，因为它缺少身份验证，验证和日志记录。GNUcitizen [87]演示了启用 UPnP 的设备如何容易受到跨站点脚本（XSS）漏洞的影响，而 HD Moore [88]则介绍了有关 Internet 上启用 UPnP 的设备的统计数据和度量。他们的工作表明，未经身份验证和未加密的应用层协议使用使攻击者能

够大规模利用设备，从而导致其他攻击。TLS / SSL 会话提供了保密性和完整性，有助于解决这些通信协议中的固有缺陷。

研究人员已经彻底检查了 TLS / SSL 协议，并发现了严重的漏洞。从 2011 年开始，BEAST [49]公开了 TLS 1.0 中的初始化向量（IV）漏洞，使攻击者可以预测流中下一条消息的 IV。2012 年，CRIME [58]展示了允许压缩的 TLS 会话（例如 Google 的 SPDY 协议）如何容易受到会话劫持。2013 年，AlFardan 等人。 [51]在 MAC 验证中使用格式错误的数据包来推断时间延迟（一种侧信道攻击），以从密文中统计推断明文。AlFardan 等。 [54]还展示了 RC4 流密码如何削弱 TLS 会话的安全性。POODLE [56]暴露了 SSL 3.0 中的降级漏洞，该漏洞允许两方之间进行不安全的通信。Beurdouche 等。 [59]在允许 MITM 攻击的 TLS / SSL 库的几种客户端和服务器实现中发现了漏洞，包括 FREAK [57]漏洞。

Adrian 等人披露的其他攻击。 [60]和 DROWN [62]说明了实现安全通信协议的困难。由于许多 IoT 通信支持较旧版本的 TLS / SSL 协议，因此容易受到 MITM 攻击。TLS / SSL 还广泛用于托管 IoT 平台中以保护通信通道。诸如 AWS IoT Core [81]，Azure IoT Hub [82]和 Google Cloud IoT [83]之类的新兴托管 IoT 平台实现了利用证书和 TLS / SSL 的自定义协议。这些协议和平台的文档很少，但是依靠经过时间检验的技术来实现安全的端到端通信。

BLE [89]，Zigbee [90]和 Z-Wave [91]协议存在许多安全问题。Ryan [52]显示了蓝牙密钥交换协议中的一个严重缺陷，它使攻击者能够被动地恢复会话密钥。Jasek [63]演示了攻击者如何被动和主动滥用蓝牙网络堆栈中 GATT 层中的通用属性配置文件。Zillner 等。 [61]显示了 Zigbee 联盟[90]定义的默认信任中心链接密钥在所有设备上如何相同。Fouladi 等。 [53]展示了如何使用 Z-Wave 固件中的硬编码常量来导出会话密钥，该密钥最终被公开。LE 协议的旧版本具有关键的安全漏洞，许多家用物联网设备在硬件中实现了这些漏洞。因此限制了它们的缓解选择。

除了固有的法律之外，LE 协议还提供了一种接近功能，身份验证系统依靠此功能来识别地理存在。Ho 等。 [92]展示了如何通过序列化 LE 数据包并通过 IP 中继它们来对 LE 协议进行中继攻击。研究人员表明，针对 LE 协议的 MITM 中继攻击是可行的，并且可以打破身份验证系统所依赖的地理邻近性。如 Apthorpe 等人所述，这些通信渠道可能会涉及隐私问题。 [65]和伍德等。 [66]。

2）应对措施：对于 HTTP，UPnP，DNS 和 NTP 协议，建议的应对措施包括禁用 DNS 中的 ECS 功能，使用 NTP 协议的更新版本（NTPv4）以及将 TLS / SSL 与不安全的协议（HTTPS）一起使用。对于 TLS / SSL 实施方法，将服务器端和客户端库升级到最新版本应该可以解决该漏洞。此外，禁用弱或易受攻击的 TLS / SSL 版本可减少暴露，但会失去向后兼容性。对于基于 LE 的通信，第一代 Zigbee 和 Z-Wave 协议具有关键缺陷，并且缓解选项有限。供应商可以以兼容性为代价来禁用这些协议的不安全部分[93]。

研究人员最近的一个方向是 Apthorpe 等人的工作。 [65]和伍德等。 [66]。伍德等。 [66]提出了一种监控家庭网络并通知用户物联网设备发送的敏感数据的系统。Apthorpe 等。 [65]证明了家庭网络上的流量整形如何能够防止侧信道监听。研究的这一方向需要进一步关注，以增强消费者保护其网络和隐私的能力。

选择使用 Z-Wave 的设备现在必须选择 Z-Wave Plus，它具有改进的安全性[94]和空中（OTA）更新功能。同样，Zigbee 添加了新的安全模型以允许称为“信任中心（TC）”的安全密钥分发[95]。TC 是 Zigbee 网络中的一个受信任实体，有权将密钥分发给 Zigbee 客户端设备。TC 为每个 Zigbee 连接的设备提供了唯一的加密密钥，这与传统密钥分发模式不同。为了减轻 LE 协议中的中继攻击，Ho 等人。 [92]介绍了一种基于接触的意图通信方法，该方法使用身体区域网络（BAN）进行信号传播。

3）利益相关者：由于实施是在设备，云端点或移动应用程序中的，因此最终用户无法解决通信问题。此外，由于某些漏洞需要硬件升级，因此厂商在解决通信漏洞方面的选择有限，但是在某些情况下他们可以将其禁用[93]。供应商可以修补设备，移动应用程序和云端点上的易受攻击的库。

互联网服务提供商（ISP）可以了解基于 IP 的协议的使用情况，但它们不直接负责任何应对措施。为了使 ISP 参与进来，他们必须提供定义其角色的网络和法律政策。对于 LE 协议，供应商可以通过禁用易受攻击的配对来缓解旧设备。如果存在这样的选项，用户可以使用其他方法将 LE 设备与 IoT 集线器配对。用户可以购买提供下一代安全 LE 协议的更新设备，例如 Z-Wave Plus 和 Zigbee。

4）带走：通信通道为基于家庭的物联网提供必要的功能。基于家庭的物联网设备已经适应了 IP 和 LE 协议的行业标准，但是它们受遗留库的困扰，在某些情况下无法修复。

供应商有责任解决通信渠道中的漏洞。此外，供应商可以直接更新云端点和移动应用程序，但是供应商必须主动并告知影响其软件的漏洞。物联网设备继续依赖于不安全的协议（如 UPnP），并且正如我们接下来将要展示的那样，它很少在 LAN 上加密其通信。最终用户不知道他们的设备或移动应用程序是否容易受到弱加密或 MITM 攻击，除非他们分析和测试通信流量。明智的高级用户可以将其本地网络划分为受信任和不受信任区域，以限制暴露。

TLS / SSL 解决了容易受到 MITM 攻击的不安全协议，但是它们在其实现和部署中也存在缺陷。克拉克等人的工作。 [96]提供了有关 SSL 和 HTTPS 的其他分析。ISP 可以提供概述最佳网络实践的报告以及有关设备和协议利用率的统计信息。托管云 IoT 平台使用依赖于公钥基础结构（PKI）和 TLS / SSL 协议的自定义通信协议。需要进一步研究以调查托管云物联网平台使用的协议。这些新平台尚未得到充分研究，并警告您进行进一步调查以发现任何弱点。

（通信：物联网设备依赖于不安全的协议，这些协议不提供保密性或完整性，而是通过使用 TLS / SSL 协议来增强它们的安全性。许多设备在 LAN 上缺乏加密，这使它们容易受到 MITM 攻击。TLS / SSL 协议在实施和部署方面存在缺陷，并要求供应商保持警惕。托管云物联网平台使用自定义协议，这需要进一步审核。ISP 具有大量信息，可以指导供应商进行安全部署。）

（云托管是基于云计算技术的标准化产品，定位于网络应用型企业，适合绝大多数数据中心托管用户，服务于广大的企事业单位、公司及网站用户。虚拟专用服务器，也称为 VPS，虚拟专用服务器 VDS。定义：一台物理服务器，分为几个较小的服务器片，每个服务器片充当自己的虚拟服务器环境。根据所使用的虚拟化方法，VPS 只能提供一个操作系统。但使用云主机，可以自由选择任何您想要的操作系统。可以安装或更换一系列可用操作系统中的任何操作系统。云主机比较小巧轻便，基于几个不同的服务器，而且共享云主机价格并不比 VPS 高多少，而且还有很大的优势。）

Communication: IoT devices rely on insecure protocols that do not offer confidentiality or integrity but mitigate them by using TLS/SSL protocols. Many devices lack encryption on the LAN, which leave them susceptible to MITM attacks. The TLS/SSL protocols exhibit flaws in implementation and deployment and require vendors to be vigilant. Managed cloud IoT platforms use custom protocols, which require further auditing. ISPs have a wealth of information that can guide vendors to secure deployments.

四、评价

我们评估了 45 种设备，涵盖了设备，相机，家庭助理，家庭自动化，媒体和网络设备等类别。有关设备的完整概述，请参见附录 A 表 III。我们使用了商业和开源工具的组合来进行评估；所有的商业工具都有开源的对应工具。我们的方法论和评估需要最少的技术专业知识来复制，并且经过精心设计，以吸引广泛的技术受众，使他们能够为这项工作做出贡献。我们的评估结果总结在表 II 中，评估的其他细节在附录 A 表 IV 中找到。特定的设备评估案例可在附录 B 中找到。

A.实验设置

我们的网络设置包含三个主要组件：IoT 子网，自定义 Linux 网关和评估机。评估机运行我们所有的评估工具，并与 IoT 设备位于同一子网中。我们的网关是 Debian Jessie Linux 机器，它管理网络服务（DHCP，DNS 等），并将 IoT 子网连接到 Internet。此外，我们的网关全包可捕获源自 IoT 子网的所有 IP 流量。我们使用 24 端口交换机通过以太网连接有线 IoT 设备，并为需要 802.11 WLAN 的设备使用无线接入点。根据其 MAC 地址为所有 IoT 设备分配一个静态 IP。

B.数据

我们检查通过分析设备，移动应用程序，云端点和网络流量生成的不同类型的数据。这些组件之间的交互产生了网络流量（节点之间通过边进行交互，请参阅 II-A 节），我们将其捕获，提取并分类为应用程序级协议，以建立附录 A 表 VII 中的评估表。我们基于评估设备和云端点上正在运行的服务的安全审核工具生成扫描数据，然后在附录 A 表 V 和表 VI 中提供评估报告。我们使用移动应用程序审核工具来查找与第 II-B 节中定义的安全属性相关的问题。审核报告提供了过度特权的应用程序，嵌入式敏感数据和编程错误的摘要。我们使用此数据摘要为附录 A 表 IV 中的每个移动应用程序生成评估报告。

C.挑战

我们在评估 IoT 部署时面临若干挑战，包括但不限于自动化设备更新，云端点分类，无线网络分析和 iOS 应用程序解密。自动更新偏向于我们的设备评估，因为应用更新时设备状态会发生变化，我们必须在可配置的设备上禁用它。由于增加了内容交付网络（CDN）的使用，因此涉及云端点分类并需要进行手动分析以确保较高的准确性。无线访问点使用 WPA2 配置，这限制了我们从 IoT 环境的出口（网关）点收集的数据对无线到无线设备通信的可见性。我们运行了两个不同的访问点，这些访问点迫使流量穿越网关，以便获得可见性。Apple iOS 应用程序在 App Store 中已加密，并且需要越狱的 iOS 设备才能在本地下载，解密和复制 iOS 应用程序。拥有 iOS 应用程序的副本后，我们将使用各种开源和商业工具对其进行审核。

D.设备

我们使用 Nessus 扫描仪[97]扫描设备以进行服务发现，服务配置和漏洞评估。Nessus 扫描程序会用正在运行的服务的版本注释 CVE [98]信息，并提供其安全状态的摘要。Nessus 扫描仪使用 CVSS [99]评分系统对发现的漏洞的严重性进行评分（从 1 到 10），并将其分为低，中，高和严重。

表 II：该表总结了图 3 中每个图形组件的每个评估设备。有四个组件，分别是：设备（D），移动应用程序（A），云端点（C）和通信通道（E）。评估使用 Nessus 扫描仪评估设备和云端点； Kryptowire，MobSF 和 Qark 评估了移动应用程序； Nessus Monitor，ntopng，sslsplit 和 Wireshark 可以评估通信协议。设备部分总结了正在运行的服务数量和发现的问题。移动应用程序汇总了过多的权限，敏感数据或对加密协议的错误使用。通信类别将对 MITM 攻击和通信通道状态的敏感性概括为完全加密（），部分加密（）或未加密（）。有关更多详细信息，请参见附录 A。我们认为 CVSS 评分系统对高或严重类别的任何分类都是有问题的，并在表 II 中加以说明。

Device	Device Services Appendix A Table VI		Mobile Application Appendix A Table IV			Cloud Endpoints Appendix A Table V		Communication Appendix A Table VII	
	Running Services	Security Issues	Over-priviliged	Sensitive Data	Crypto Issues	SSL Issues	Service Issues	MITM	Encryption
Amazon Echo	1	0	✓	✓		✓			●
Amazon Fire TV	1	0	✓	✓			✓		◐
Apple HomePod	4	0	—	—	—	✓			●
Apple TV (4th Gen)	3	0	—	—	—	✓			●
August Doorbell	1	0	✓	✓		✓	✓	✓	◐
Belkin Netcam	1	1		✓		✓	✓	✓	◐
Belkin WeMo Crockpot	0	0		✓		✓	✓	✓	◐
Belkin WeMo Link	1	1		✓			✓	✓	◐
Belkin WeMo Motion	1	1		✓		—	—	✓	◐
Belkin WeMo Switch	1	1		✓		✓	✓	✓	◐
Bose SoundTouch 10	4	1	✓	✓	✓	✓	✓	✓	◐
Canary	0	0	—	—	—	✓			●
Caseta Wireless	2	0	✓			—	—	✓	◐
Chamberlain myQ Garage Opener	1	0			✓	✓			●
Chinese Webcam	4	1	—	—	—		✓	✓	○
D-Link DCS5009L	3	2	✓		✓	✓		✓	○
Google Home	5	2	✓		✓	—	—	✓	◐
Google Home Mini	5	2	✓		✓	—	—	✓	◐
Google OnHub	1	0	✓		✓	—	—		◐
Harmon Kardon Invoke	5	1		✓		✓	✓		●
Insteon Hub	4	6	✓	✓		✓	✓	✓	○
Koogeek Lightbulb	2	0	✓		✓	—	—		●
LIFX Virtual Bulb	0	0	✓		✓	✓		✓	◐
Logi Circle	0	0	✓			✓	✓		●
Logitech Harmony	2	1	✓			—	—		◐
MiCasaVerde VeraLite	4	6	—	—	—	✓	✓	✓	◐
Nest Cam IQ	0	0	✓	✓	✓	✓			●
Nest Camera	0	0	✓	✓	✓	✓			●
Nest Guard	0	0	✓	✓	✓	✓	✓		●
Netgear Arlo	0	0	✓	✓	✓		✓		●
nVidia Shield	2	3	—	—	—	—	—		◐
Philips HUE	2	0	✓	✓		—	—	✓	◐
Piper NV	3	0	—	—	—	✓	✓		●
Ring Doorbell	0	0	✓		✓				●
Roku 4	2	0	✓		✓	✓	✓	✓	◐
Roku TV	2	0	✓		✓	✓	✓	✓	◐
Roomba	1	0	✓	✓	✓	—	—		◐
Samsung SmartThings	1	1	✓	✓	✓	✓			●
Samsung SmartTV	4	1			✓	—	—	✓	◐
Securifi Almond	2	1	✓		✓	—	—		◐
Sonos	3	3		✓		—	—	✓	◐
TP-Link WiFi Bulb	1	0	✓		✓	—	—		●
TP-Link WiFi Plug	0	0	✓		✓	—	—		●
Wink 2 Hub	4	4	✓	✓	✓	—	—	✓	◐
Withings Home	1	0	✓				✓		●

我们评估了 45 种设备，发现总共 84 项正在运行的服务以及与这些正在运行的服务有关的 39 个问题。我们发现具有运行服务的设备，例如 SSH，UPnP，HTTP Web 服务器，DNS，Telnet，RTSP 和自定义服务。许多设备为他们的服务配置 TLS / SSL，但是它们的配置有几个问题。例如，证书是自签名的，支持弱密码到中密码，使用短 TLS / SSL 密钥，允许使用易受攻击的 SSL 版本（v2，v3 和 CBC 模式），并且证书已过期。此外，某些设备运行过时且易受攻击的服务，这些服务允许远程执行代码，泄漏敏感信息以及运行未经身份验证的服务。

例如，Insteon 集线器在端口 443 上运行带有 TLS 的 Web 服务器，并在端口 22 上侦听 SSH 连接。用于 TLS 连接的证书已过期并已自签名，而 TLS 服务则允许使用弱密码（如 RC4）和不安全的协议（如 SSLv3）。同样，Wink 2，Sonos Speakers，nVidia Shield，Google Home，Samsung SmartTV 和 Samsung Sm artThings 的证书或 TLS / SSL 配置都有问题。Wink 2 和 Sonos 都使用了 1024 位大小的短 SSL 密钥。其他设备（例如 D-Link DCS5009L，Bose SoundTouch 10，中文网络摄像头和 Securi？Almond）缺乏用于服务身份验证的加密功能，这使得 LAN 上的任何设备都可以监听。

运行 UPnP 服务的设备没有内置的身份验证或安全性，默认情况下是不安全的。MiCasaVerda VeraLite，Wink 2，Sonos，Bose SoundTouch 10，Samsung SmartTV，Logitech Harmony 和 Roku 等设备都运行 UPnP 服务，允许 LAN 上的任何人控制该设备。具体来说，MiCasaVerda VeraLite 使用具有公共漏洞的 UPnP 服务库的易受攻击版本，例如 libupnp 1.6.18（CVE-2012-5965），dropbear 2016.72（CVE-2012-0920）和 UPnP RunLua（CVE-2013- 4863）。附录 B 表 VIII 中列出了 CVSS 评分为高和严重的 CVE 的完整列表。

我们找到了 16 台运行服务没有问题的设备，还有 10 台未公开运行服务的设备。例如，Nest 摄像机使用推/拉客户端方法，这限制了正在运行的服务的公开范围。

发现。设备评估发现与设备设置，软件更新和服务配置有关的问题。附录 A 表 VI 中提供了每种器件的其他评估结果。

E.移动应用

我们使用 MobSF [100], Qark [101]和来自 Kryptowire [102]的服务来静态和动态地评估 IoT 设备的每个移动应用程序。我们同时查看了 Android 和 iOS 应用程序，并在表 II 中列出了两个 3 中的弱点。有 42 个具有配套移动应用程序的设备。我们总共分析了 83 个移动应用程序，其中 41 个是 Android，42 个是 iOS。我们发现 39 个设备存在一个或多个与权限，敏感数据或密码使用不正确有关的问题。我们观察到 24 个过度特权的移动应用程序，它们请求在移动设备上获得应用程序代码未使用的权限。

对于敏感数据，我们发现 15 个移动应用程序具有硬编码的敏感数据，例如 Google 地理编码，Google Maps，fabric.io，HockyApp，Localytics，Microsoft Virtual Earth，Umeng 的 API 密钥以及云和设备服务的其他凭据。我们发现了 17 个移动应用程序，它们没有安全地实现加密协议，或者具有硬编码的静态密钥和初始化向量（IV）。加密实现分别依赖于较旧的或损坏的算法，例如 AES-128 和 MD5 哈希。其他应用程序未强制执行 SSL，并允许通过未经验证的连接进行通信。

发现。评估确定了系统化工作忽略了移动应用程序和设备之间固有信任的问题。表 II 中提供了我们的移动应用程序评估的摘要，附录 A 表 IV 中提供了更多详细信息。

F.云端点

我们使用 Nessus Scanner 来发现，配置和评估在云端点上运行的服务。在物联网网络上，我们在 45 个设备上观察了 4,000 多个云端点域。我们将每个域分为以下四类之一：第一方，第三方，混合和未知。第一方是指在供应商的基础架构上运行的基于云的服务，第三方是指诸如内容

交付网络（CDN）之类的订阅服务，混合是指诸如 Amazon AWS 或 Microsoft Azure 之类的基于云的基础架构（IaaS），托管物联网云服务，并且由于含糊不清，“未知”指未分类的基础架构。我们将 950 个域划分为第一方，将 1287 个域划分为第三方，将 630 个域划分为混合域，将 1288 个域划分为未知域。未知类别包括设备的不可归属域。例如，在智能电视上运行的 Hulu 应用程序使用一个 AWS CloudFront 域，该域不会属于 Hulu 或智能电视，因此我们无法指示该域。

对于每个云端点，我们评估了正在运行的服务和 TLS / SSL 配置（如果适用）。我们发现有 18 台设备使用过时的服务，泄露了敏感信息，缺少用于身份验证的加密或运行了易受攻击的服务。我们发现八台使用易受攻击且具有公共漏洞的云终端设备。此外，七个设备均以明文形式通过云端点进行了身份验证。我们发现有 26 个使用云端点的设备存在 TLS / SSL 配置问题，例如自签名证书，域名不匹配以及对易受攻击的 TLS / SSL 协议版本的支持。

我们发现有十个使用配置不正确的云端点的设备，这些设备允许泄露敏感信息，例如文件路径和服务器上正在运行的进程。我们看到有四台设备使用的云终结点运行了过期的操作系统，并且厂商支持已过期（Ubuntu 10 和 Ubuntu 12）。

发现。评估发现部署不受支持的旧版操作系统和敏感信息泄露方面的问题。我们在表 II 中总结了我们的发现，并在附录 A 表 V 中提供了更多详细信息。

G.通信

我们使用 Nessus 网络监视器[97]，ntop-ng [103]，Wireshark [104]和 sslsplit [105]为每个设备配置通信边缘。我们手动检查了流量，并使用 sslsplit 对它们进行了 MITM 攻击测试。物联网设备使用基于 IP 的通道与其组件连接，在模型图中以边缘表示（请参见图 3）。我们将连接分为三种类型：设备到云（D-C），移动应用到设备（A-D）和移动应用到云（A-C）。我们观察到 43 个连接到云端点（D-C）的设备，35 个连接到云端点（A-C）的移动应用程序和 27 个通过局域网（LAN）（A-D）连接到设备的移动应用程序。

我们将这些连接分为五个应用程序协议，即：DNS，HTTP，UPnP，NTP 和自定义。定制类别是指特定于设备的应用程序协议。智能设备使用许多协议，但是在我们的实验室中，我们仅观察到上面列出的五个。我们发现 41 台设备使用了 DNS 协议，其中有 6 台不遵守网络配置的 DNS 递归服务器，而是使用了 Google 或 OpenDNS 的服务器。我们发现 38 个设备使用 HTTP 协议，其中 34 个使用 TLS / SSL 会话（HTTPS）。我们发现 21 个使用 UPnP 协议的设备通过发送多播 SSDP 请求或响应 SSDP 请求而使用。此外，我们看到 25 个使用 NTP 协议进行时间同步的设备。我们观察到 28 个使用特定于设备的自定义协议的设备。例如，Google 产品（OnHub，Home 和 Home mini）都使用端口 5228 和 5223 上的自定义协议将流量发送到 Google 的服务器。

大多数设备使用 Internet（D-C）加密。我们找到了 25 个加密所有通信的设备，15 个部分加密了通信的设备以及两个未加密到云端点的通信的设备。对于移动应用程序（A-C），有 24 个加密了它们的所有通信，有十个加密了部分通信，有一个没有加密与云端点的通信。在 LAN（A-D）上，我们观察到有五个对通信进行加密的设备，两个对通信进行部分加密的设备和 20 个未对通信进行加密的设备。很少有设备（如中文网络摄像头）没有配套的移动应用程序，而是提供了 HTTP 接口，该接口允许 LAN 上的任何设备进行身份验证并与之交互。

除了进行通讯分析外，我们还积极地对每个通讯边缘进行攻击，以测试其易感性。我们发现总共 20 台设备的一个或多个通信边缘易受 MITM 攻击。我们发现了四处易受攻击的设备到云（D-C）通信，两处易受攻击的移动应用程序到云（A-C）通信和 20 处易受攻击的应用程序到设备（A-D）通信。

发现。评估发现并非所有的通信通道都是安全的，并且缺乏端点验证。我们发现通过强制使用第三方递归 DNS 服务器来泄漏使用信息的设备。表 II 总结了设备加密和 MITM 攻击，其他详细信息请参见附录 A 表 VII。

H.应对措施

设备。受影响的设备应通过安全通道打补丁，以确保更新的完整性。供应商可以限制在 IoT 设备上运行的服务，并遵循客户端方法，即使用推/拉请求通过云端点管理设备。可以使用可配置的方法来修复设备配置，如果没有适当的配置和设置，设备将无法激活。许多设备都遵循先配置后可操作的方法，并且应由行业标准强制执行。最后，端点（云或移动）验证可确保只有经过身份验证的各方才能与设备进行交互。供应商可以将交互限制在沙盒环境中，并为所需的资源分配时间细粒度的访问控制。受信任的端点不应以不受限制的访问方式运行，并且设备应为所有各方强制执行验证超时。现代的基于家庭的物联网设备配备了足够的计算能力（[106]，[107]），可以应用许多建议的缓解措施，这与人们普遍认为它们的动力不足和能耗受限的设备相反。

app。特权过多的应用程序可能会对用户的活动产生隐私问题。移动平台应实施一个系统，以基于应用程序的功能分析来获取权限，并在运行时临时授予权限。此外，当应用程序安装在移动设备上并存储在加密的密钥存储区中时，应导出敏感信息，例如 API 密钥。密码协议很难正确实现，因此开发人员应依赖具有适当实现的成熟库。最后，开发人员应遵守这些库随附的建议准则。

云。托管平台和配置管理工具可以缓解云端点上的漏洞服务。供应商应利用由经验丰富的专业人员管理的商业平台。同样，通过 API 集成自动实现云端点配置可以减少配置错误的机会。例如，“加密” [108]可以自动为服务器续订证书。云端点不应支持不安全的协议，而应同时验证端点设备和移动应用程序。

通讯。所有物联网组件之间的网络通信应遵循相同的安全标准（LAN 或 Internet）。供应商必须使用最新的安全协议，提供有限的功能以实现向后兼容性，强制执行协议升级要求并验证端点。端点验证将确保 MITM 攻击不会成功，并保护通信的完整性。如果端点不可验证，供应商应默认为失败状态。此外，供应商可以提供一个选项来在 IoT 部署中安装自定义证书，以提高透明度。

五、提案

A.利益相关者

供应商。供应商必须针对每个级别的每个组件获得正确的安全性要求，包括物联网系统的设计，实施和部署。我们的评估表明，许多供应商都在为设备安全性而努力，但往往由于尽职调查而失败。实际上，许多供应商并不具备开发，管理和部署这些异构技术的全部专业知识。在特定领域缺乏专业知识的供应商可以外包给专门的第三方来开发其产品。

终端用户。基于家庭的物联网部署将简单的基于家庭的网络转换为复杂的类似企业的网络。最终用户可以通过配置设备以使用加密，禁用远程管理功能以及对其网络进行分段来遵循良好的安全性惯例。最重要的是，消费者可以通过购买具有隐私意识的安全设备来影响供应商。我们的门户旨在对物联网设备进行客观的安全评估，并允许消费者做出明智的决定。

其他缔约方。互联网服务提供商（ISP）并不是直接的利益相关者，但是基于家庭的物联网设备的普遍存在会影响其网络的运行。ISP 看到的大部分流量都将被加密，但是 ISP 可以通过目的地，服务端口和通信频率来识别设备。ISP 可能会实施技术补救措施来阻止某些端口，但需要法律政策进行干预。由于物联网的全球性和国际判例，这些决策可能会引发政策和合规性争议[4]。ISP 可以提供其在运行和运营住宅互联网网络方面的专业知识，可以帮助您确定基于家庭的 IoT 部署的含义。

云提供商为许多物联网供应商提供基础架构即服务，并在开发，运行和保护云基础架构和平台方面拥有多年的经验。他们的产品对供应商而言既经济又实用，但偶尔也会遭受停运的困扰[76]。云提供商在保护物联网部署中发挥着重要作用，并应继续提供量身定制的云服务，以减轻供应商的安全责任。

B.建议

测量。我们建议对设备间通信，移动应用程序到设备交互以及 IoT 组件之间的信任关系进行其他度量。局域网内对设备间通信（设备到设备和移动应用程序到设备）的研究不多。许多物联网系统（例如家庭辅助设备）会在未经用户同意的情况下自动发现局域网中的其他设备并与之交互，这需要进一步调查以了解这些通信对安全和隐私的影响。此外，进行纵向研究可以揭露潜在的缺陷，如果不进行时间分析，很难观察到。

最佳做法。物联网组件的最佳做法和指南很容易获得，但利用率较低。一些经过评估的设备具有其他供应商可以借鉴的非常好的实践，包括移动应用程序实施，云服务配置，设备配置以及组件的安全部署和交互。这些设计和实施模式应进行深入评估，以了解其对供应商的成本/收益。政府立法可以鼓励经济或基于政策的激励措施来影响供应商采用最佳做法。

标准。许多成熟的供应商已经提出了物联网系统的标准，但是社区之间没有达成共识。供应商和研究人员应结合他们的专业知识，共同起草行业标准，以提供解决家庭物联网系统中常见错误的技术。一些基于家庭的物联网系统具有网络物理组件，例如相连的烤箱，冰箱和热水器。这些类别的物联网系统必须受到安全法规和代码标准的监管，以确保不会因滥用或组件故障而造成物理伤害。政府必须在这些标准的制定中发挥积极作用，以保护消费者的安全和隐私。

六、结论

这项工作通过一个抽象模型将家庭物联网设备的现有文献系统化，从而使我们能够得出见解。我们使用相同的方法评估了 45 种 IoT 设备，发现当今物联网系统中存在许多文献中讨论的相同问题。我们在门户网站上提供结果和评估数据集，并邀请研究人员做出贡献并复制我们的工作。我们设想，这项工作将成为评估基于家庭的 IoT 设备，为研究人员提供数据以及与供应商合作的中心支柱。

七、致谢

我们感谢匿名审稿人和 Jan Werner 的深刻见解和建议。我们感谢 Kryptowire 团队提供了自动化的移动应用程序安全分析平台。本资料基于美国商务部授予的部分资助的工作。国家科学基金会（NSF）的 2106DEK 和 2106DZD 批准号为 2106DGX 和空军研究实验室/国防高级研究计划局授予 2106DTX 和 2106EHP。本材料中表达的任何观点，发现，结论或建议均为作者的观点，并不一定反映美国商务部，美国国家科学基金会，空军研究实验室或国防高级研究计划局的观点。

附录 A 评估表

TABLE IV: Mobile Application Evaluation.

Device	Mobile Application			Over-privileged	Sensitive Data	Crypto Issues
	Name	Platform	Version			
Securifi Almond	com.securifi .almond	iOS	3.5.6	✓		✓
LIFX Virtual Bulb	com.lifx .lifx	iOS	3.8.6	✓		✓
Ring Doorbell	com.ring	iOS	4.1.13	✓		✓
Roku TV Roku 4	com.roku. ios.roku	iOS	4.2.3	✓		✓
Netgear Arlo Camera	com.netgear .arlo	iOS	2.4.8	✓	✓	✓
TP-Link WiFi Plug TP-Link WiFi Bulb	com.tplink .kasa-ios	iOS	1.11.1	✓		✓
Chamberlain myQ Garage Opener	com.chambe-rlain .myq.chambe-rlain	iOS	6216.0.0			✓
Google Home Mini Google Home	com.google .Chromecast	iOS	1.28.508	✓		✓
Apple HomePod	—	iOS	—	—	—	—
Wink 2	com.quirky .wink	iOS	6.8.0	✓		✓
Google OnHub	com.google .android.apps .access.wifi .consumer	Android	jetstream BV10127	✓		✓
Samsung SmartThings	com.smart-things .android	Android	2.13.0	✓	✓	✓
Philips HUE	com.philips .lighting.hue2	Android	2.19.0	✓	✓	
Insteon Hub	com.insteon .insteon3	Android	1.9.8	✓	✓	
Sonos	com.sonos .acr	Android	8.3.1		✓	
Nest Camera Nest Cam IQ Nest Guard	com.nest .android	Android	5.17.0.31	✓	✓	✓
Belkin WeMo Motion Belkin WeMo Switch Belkin WeMo Link Belkin WeMo Crockpot	com.belkin .wemoandroid	Android	1.19.0		✓	
Amazon Echo	com.amazon .dee.app	Android	2.2.1615.0	✓	✓	
Belkin Netcam	com.belkin .android. android belkinnetcam	Android	2.0.4		✓	
Amazon Fire TV	com.amazon. storm.lightning. client.aosp	Android	1.0.13.18	✓	✓	
D-Link DCS5009L	com.dlink. mydlinkunified	Android	1.0.3	✓		✓
Logitech Logi Circle	com.logitech .circle	Android	2.3.2220	✓		
Canary	is.yranac.canary	Android	2.14.0	—	—	—
Piper NV	com.blacksumac .piper	Android	1.4.0	—	—	—
Withings Home	com.withings .home	Android	1.5.3	—	—	—
MiCasaVerde VeraLite	com.vera .android	Android	7.25.47	✓		
August Doorbell Cam	com.august .luna	Android	6.1.4	✓	✓	
Logitech Harmony	com.logitech .harmonyhub	Android	5.1.1	✓		
Caseta Wireless	com.lutron .mmw	Android	5.1.0	✓		
Bose SoundTouch 10	com.bose .soundtouch	Android	17.170.82	✓	✓	✓
Harmon Kardon Invoke	com.microsoft .cortana	Android	2.10.2.2135		✓	
Roomba	com.irobot .home	Android	2.3.1	✓	✓	✓
Samsung SmartTV	com.samsung .smartviewad	Android	2.1.0.100			✓
Koogeek Lightbulb	com.tomtop .home	Android	1.2.2	✓	✓	✓
nVidia Shield	—	—	—	—	—	—
Chinese Webcam	—	—	—	—	—	—

TABLE III: An overview of the devices used in the evaluation.

Device	Category	Hub	Cloud Endpoints	Mobile Application		Communication	
				iOS	Android	IP	Low-Energy
Belkin WeMo Crockpot	Appliance		27	✓	✓	✓	
Roomba	Appliance		11	✓	✓	✓	
Belkin Netcam	Camera		79	✓	✓	✓	
Canary	Camera		22	✓	✓	✓	✓
Chinese Webcam	Camera		1	—	—	✓	
D-Link DCS5009L	Camera		4	✓	✓	✓	
Logi Circle	Camera		341	✓	✓	✓	✓
Nest Cam IQ	Camera		9	✓	✓	✓	✓
Nest Camera	Camera		7	✓	✓	✓	✓
Netgear Arlo	Camera		59	✓	✓	✓	
Piper NV	Camera		42	✓	✓	✓	✓
Withings Home	Camera		20	✓	✓	✓	✓
Amazon Echo	Home Assistant		221	✓	✓	✓	
Apple HomePod	Home Assistant		221	—	—	✓	✓
Google Home	Home Assistant		42	✓	✓	✓	
Google Home Mini	Home Assistant		221	✓	✓	✓	
Harmon Kardon Invoke	Home Assistant		128	✓	✓	✓	✓
August Doorbell	Home Automation		221	✓	✓	✓	✓
Belkin WeMo Link	Home Automation	✓	14	✓	✓	✓	✓
Belkin WeMo Motion	Home Automation		221	✓	✓	✓	
Belkin WeMo Switch	Home Automation		29	✓	✓	✓	
Caseta Hub	Home Automation	✓	221	✓	✓	✓	✓
Chamberlain myQ Garage Opener	Home Automation	✓	1	✓	✓	✓	✓
Insteon Hub	Home Automation	✓	20	✓	✓	✓	✓
Koogeek Lightbulb	Home Automation		1	✓	✓	✓	
LIFX Virtual Bulb	Home Automation		3	✓	✓	✓	
MiCasaVerde VeraLite	Home Automation	✓	74	✓	✓	✓	
Nest Guard	Home Automation	✓	14	✓	✓	✓	✓
Philips HUE	Home Automation	✓	27	✓	✓	✓	✓
Ring Doorbell	Home Automation		9	✓	✓	✓	
Samsung SmartThings	Home Automation	✓	10	✓	✓	✓	✓
TP-Link Wifi Bulb	Home Automation		11	✓	✓	✓	
TP-Link Wifi Plug	Home Automation		11	✓	✓	✓	
Wink 2	Home Automation	✓	12	✓	✓	✓	✓
Amazon Fire TV	Media		174	✓	✓	✓	
Apple TV (4th Gen)	Media		439	✓		✓	
Bose SoundTouch 10	Media		26	✓	✓	✓	✓
Logitech Harmony	Media		17	✓	✓	✓	✓
nVidia Shield	Media		261	—	—	✓	
Roku 4	Media		231	✓	✓	✓	
Roku TV	Media		226	✓	✓	✓	
Samsung SmartTV	Media		182	✓	✓	✓	
Sonos	Media		65	✓	✓	✓	✓
Google OnHub	Network		24	✓	✓	✓	
Securifi	Network	✓	938	✓	✓	✓	✓

TABLE V: Cloud Endpoint Evaluation.

Device	Domains						SSL			Services			
	Total	1st Party	3rd Party	Hybrid	Unknown	Host	Self-Signed	Domain Mismatch	Vuln SSL	Outdated OS	Information Discolsure	Cleartext Auth	Exploitable Service
Amazon Echo	221	15	191	3	12	17	✓		✓	—	—	—	—
Amazon Fire TV	174	100	17	14	43	99	—	—	—				✓
Apple HomePod	182	80	6	76	20	113	✓	✓	✓	—	—	—	—
Apple TV (4th Gen)	439	170	14	188	67	38	✓		✓	—	—	—	—
August Doorbell	55	7	12	34	2	32	✓		✓			✓	
Belkin Netcam	79	13	63	1	2	12			✓		✓	✓	✓
Belkin WeMo Crockpot	27	7	15	5	0	11			✓	✓	✓		✓
Belkin WeMo Link	14	4	6	4	0	11	—	—	—	✓			✓
Belkin WeMo Motion	24	7	12	5	0	9	—	—	—	—	—	—	—
Belkin WeMo Switch	29	5	19	5	0	10			✓	✓			✓
Bose SoundTouch10	26	10	10	6	0	11			✓		✓	✓	
Canary	22	19	3	0	0	9	✓			—	—	—	—
Caseta Wireless	22	2	11	5	4	6	—	—	—	—	—	—	—
Chamberlain myQ Garage Opener	1	1	0	0	0	1	✓			—	—	—	—
Chinese Webcam	1	1	0	0	0	1	—	—	—			✓	
D-Link DCS5009L	4	4	0	0	0	3			✓	—	—	—	—
Google Home	42	29	3	0	10	14	—	—	—	—	—	—	—
Google Home Mini	40	27	3	0	10	17	—	—	—	—	—	—	—
Google OnHub	24	24	0	0	0	15	—	—	—	—	—	—	—
Harmon Kardon Invoke	128	0	108	5	15	9	✓		✓		✓		
Insteon Hub	20	2	12	5	1	5	✓				✓		
Koogeek Lightbulb	1	0	1	0	0	0	—	—	—	—	—	—	—
LIFX Virtual Bulb	3	2	1	0	0	1	✓		✓	—	—	—	—
Logitech Harmony	17	6	5	6	0	8	—	—	—	—	—	—	—
Logitech Logi Circle	341	158	5	178	0	20	✓						✓
MiCasaVerde VeraLite	74	1	30	43	0	40	✓		✓	✓	✓	✓	✓
Nest Cam IQ	9	4	5	0	0	4	✓			—	—	—	—
Nest Camera	7	6	1	0	0	5	✓		✓	—	—	—	—
Nest Guard	14	6	6	2	0	4	✓				✓		
Netgear Arlo	59	23	2	7	27	18	—	—	—				✓
nVidia Shield	261	23	177	3	58	24	—	—	—	—	—	—	—
Philips HUE	27	14	8	0	5	11	—	—	—	—	—	—	—
Piper NV	42	24	16	2	0	16	✓		✓		✓		
Ring Doorbell	9	5	3	1	0	6	—	—	—	—	—	—	—
Roku 4	231	37	177	4	13	28	✓		✓		✓		
Roku TV	226	36	144	6	40	28	✓		✓		✓	✓	
Roomba	11	2	5	4	0	5			✓	—	—	—	—
Samsung SmartThings	10	6	1	3	0	4	✓		✓	—	—	—	—
Samsung SmartTV	182	27	138	2	15	20			✓	—	—	—	—
Securifi Almond	938	9	0	0	929	6			✓	—	—	—	—
Sonos	65	13	34	7	11	1	—	—	—	—	—	—	—
TP-Link WiFi Bulb	11	3	7	1	0	4	—	—	—	—	—	—	—
TP-Link WiFi Plug	11	3	7	1	0	4	—	—	—	—	—	—	—
Wink 2	12	3	7	2	0	4	—	—	—	—	—	—	—
Withings Home	20	12	2	2	4	9	—	—	—			✓	

Device	System Services			System Setup		
	Detected OS	Running Services	Issues Found	Pairing	Config.	Upgrade
Insteon Hub	Linux 2.6	4	6	Wired+Pin	F	C
MiCasaVerde VeraLite		4	6	Cloud+Pin	D	M
Wink 2	Linux 2.6	4	4	Wired	D	M
Sonos	Linux	3	3	Wired	D	C
nVidia Shield	Linux 2.6	2	3	Wired	D	M
Google Home	Linux 3.3	5	2	Wifi	F	A
Google Home Mini	Linux 3.3	5	2	Wifi	F	A
D-Link DCS5009L		3	2	Wired	D	M
Harmon Kardon Invoke	Linux 3.3	5	1	LE	F	A
Bose SoundTouch 10	Linux 2.6	4	1	LE	F	C
Chinese Webcam	Linux 2.6	4	1	Wired+HTTP	D	N/A
Samsung SmartTV	Linux 4.8	4	1	On-Screen	D	M
Logitech Harmony		2	1	LE	F	M
Securifi Almond	Linux 2.6	2	1	Wired	D	M
Belkin Netcam	Linux 2.6	1	1	Wifi+Pin	F	C
Belkin WeMo Link		1	1	Wifi+Pin	F	C
Belkin WeMo Motion		1	1	Wifi+Pin	F	C
Belkin WeMo Switch		1	1	Wifi+Pin	F	C
Samsung SmartThings	Linux 2.6	1	1	Wired	F	C
Apple HomePod	FreeBSD 6	4	0	LE	F	C
Apple TV (4th Gen)	tvOS	3	0	Wired	F	C
Piper NV		3	0	Wifi	F	A
Caseta Wireless	Linux 2.6	2	0	Wired	F	M
Koogeek Lightbulb		2	0	LE+Pin	D	C
Philips Hue	Linux 2.6	2	0	Wired+Button	F	C
Roku 4	Linux 3.3	2	0	Wired	D	M
Roku TV		2	0	Wired	D	M
Amazon Echo	Linux	1	0	Wifi	F	A
Amazon Fire TV	Linux 2.6	1	0	Wired	D	M
August Doorbell	Linux 2.6	1	0	Wifi	F	M
Chamberlain myQ Garage Opener		1	0	Wifi	F	M
Google OnHub	Linux 4.8	1	0	Wired	F	A
Roomba		1	0	Wifi	F	M
TP-Link Wifi Bulb		1	0	Wifi	D	M
Withings Home		1	0	LE	F	C
Canary		0	0	Wifi	F	C
LIFX Bulb		0	0	Wifi	D	M
Logi Circle		0	0	LE	F	A
Nest Cam IQ		0	0	Wired	F	A
Nest Camera		0	0	LE+Pin	F	A
Nest Guard		0	0	Wired	F	A
Netgear Arlo		0	0	Wired	F	M
Ring Doorbell		0	0	Wifi	F	M
TP-Link Wifi Plug		0	0	Wifi	F	M
Belkin WeMo Crockpot		0	0	Wifi+Pin	D	C

(**F**)orced configuration change when device is setup; (**D**)efault device configuration is acceptable and allows device to operate. (**C**)onsent by the user is required for the device to upgrade; (**A**)utomatic updates are applied without user intervention; (**M**)anual device update via user request. N/A means the category is not applicable.

TABLE VI: Device Evaluation.

Device	Observed IP Communication					MITM			Encryption		
	DNS	HTTP	UPnP	NTP	Custom	D-C	A-C	A-D	D-C	A-C	A-D
Google OnHub	✓-	✓+			✓	✗	✗	—	◐	●	—
Samsung SmartThings	✓	✓+	✓			✗	✗	✗	●	●	—
Philips HUE	✓	✓+	✓	✓		✗	✗	✓	●	●	c
Insteon Hub	✓	✓		✓		✓	—	—	○	—	—
Sonos	✓	✓+	✓		✓	✗	✓	✓	◐	○	○
Securifi Almond	✓			✓	✓	✗	✗	—	◐	●	—
Wink 2 Hub	✓	✓+	✓	✓		✓	✗	✓	●	◐	○
Belkin WeMo Motion Belkin WeMo Switch Belkin WeMo Link Belkin WeMo Crockpot	✓	✓+	✓	✓	✓	✗	✗	✓	◐	◐	○
LIFX Bulb	✓			✓	✓	✗	✗	✓	●	◐	○
Amazon Echo	✓	✓	✓	✓	✓	✗	✗	—	●	●	—
Belkin Netcam	✓	✓+	✓		✓	✗	✗	✓		◐	—
Ring Doorbell	✓				✓	✗	✗	—	●	●	—
Roku TV Roku 4	✓	✓+	✓		✓	✗	—	✓	●	—	○
Amazon Fire TV	✓	✓+	✓			✗	—	✗	●	—	◐
nVidia Shield	✓	✓+			✓	✗	—	—	◐	—	—
Apple TV (4th Gen)	✓	✓+		✓	✓	✗	—	✗	●	—	●
Netgear Arlo	✓	✓+		✓		✗	✗	—	●	●	—
D-Link DCS-5009L			✓			—	—	✓	—	—	○
Logi Circle	✓	✓+		✓		✗	✗	—	●	●	—
Canary	✓	✓+				✗	✗	—	●	●	—
Piper NV	✓-	✓+		✓	✓+	✗	✗	—	●	●	—
Withings Home	✓	✓+			✓	✗	✗	✗	●	●	●
MiCasaVerde VeraLite	✓	✓+	✓	✓	✓	✗	✓	✓	◐	●	○
Chinese Webcam		✓	✓		✓	✓	—	✓	○	—	—
August Doorbell	✓	✓+				✓	✗	✓	◐	◐	○
TP-Link WiFi Plug TP-Link WiFi Bulb	✓	✓+		✓		✗	✗	✗	●	●	●
Chamberlain myQ Garage Opener	✓				✓	✗	✗	—	●	●	—
Logitech Harmony	✓	✓+	✓			✗	✗	—	◐	◐	—
Caseta Wireless	✓	✓		✓	✓	✗	✗	✓	◐	●	○
Google Home Mini Google Home	✓-	✓+	✓	✓	✓	✗	✗	✓	◐	●	○
Bose SoundTouch 10	✓	✓+	✓		✓	✗	✗	✓	●	◐	○
Harmon Kardon Invoke	✓-	✓+		✓		✗	✗	—	●	●	—
Apple HomePod	✓	✓+		✓	✓	✗	—	—	●	—	—
Roomba	✓	✓+		✓	✓	✗	✗	✗	●	●	○
Samsung SmartTV	✓	✓+	✓			✗	—	✓	◐	—	◐
Koogeek Lightbulb	✓			✓	✓	—	✗	✗	—	●	●
Nest Camera		✓+				✗	✗	—	●	●	—
Nest Cam IQ	✓-	✓+				✗	✗	—	●	●	—
Nest Guard				✓	✓	✗	✗	—	●	●	—

TABLE VII: Communication Evaluation.
✓+ (TLS/SSL) — ✓- (3rd-party recursive DNS)

Device	System Services			System Setup		
	Detected OS	Running Services	Issues Found	Pairing	Config.	Upgrade
Insteon Hub	Linux 2.6	4	6	Wired+Pin	F	C
MiCasaVerde VeraLite		4	6	Cloud+Pin	D	M
Wink 2	Linux 2.6	4	4	Wired	D	M
Sonos	Linux	3	3	Wired	D	C
nVidia Shield	Linux 2.6	2	3	Wired	D	M
Google Home	Linux 3.3	5	2	Wifi	F	A
Google Home Mini	Linux 3.3	5	2	Wifi	F	A
D-Link DCS5009L		3	2	Wired	D	M
Harmon Kardon Invoke	Linux 3.3	5	1	LE	F	A
Bose SoundTouch 10	Linux 2.6	4	1	LE	F	C
Chinese Webcam	Linux 2.6	4	1	Wired+HTTP	D	N/A
Samsung SmartTV	Linux 4.8	4	1	On-Screen	D	M
Logitech Harmony		2	1	LE	F	M
Securifi Almond	Linux 2.6	2	1	Wired	D	M
Belkin Netcam	Linux 2.6	1	1	Wifi+Pin	F	C
Belkin WeMo Link		1	1	Wifi+Pin	F	C
Belkin WeMo Motion		1	1	Wifi+Pin	F	C
Belkin WeMo Switch		1	1	Wifi+Pin	F	C
Samsung SmartThings	Linux 2.6	1	1	Wired	F	C
Apple HomePod	FreeBSD 6	4	0	LE	F	C
Apple TV (4th Gen)	tvOS	3	0	Wired	F	C
Piper NV		3	0	Wifi	F	A
Caseta Wireless	Linux 2.6	2	0	Wired	F	M
Koogeek Lightbulb		2	0	LE+Pin	D	C
Philips Hue	Linux 2.6	2	0	Wired+Button	F	C
Roku 4	Linux 3.3	2	0	Wired	D	M
Roku TV		2	0	Wired	D	M
Amazon Echo	Linux	1	0	Wifi	F	A
Amazon Fire TV	Linux 2.6	1	0	Wired	D	M
August Doorbell	Linux 2.6	1	0	Wifi	F	M
Chamberlain myQ Garage Opener		1	0	Wifi	F	M
Google OnHub	Linux 4.8	1	0	Wired	F	A
Roomba		1	0	Wifi	F	M
TP-Link Wifi Bulb		1	0	Wifi	D	M
Withings Home		1	0	LE	F	C
Canary		0	0	Wifi	F	C
LIFX Bulb		0	0	Wifi	D	M
Logi Circle		0	0	LE	F	A
Nest Cam IQ		0	0	Wired	F	A
Nest Camera		0	0	LE+Pin	F	A
Nest Guard		0	0	Wired	F	A
Netgear Arlo		0	0	Wired	F	M
Ring Doorbell		0	0	Wifi	F	M
TP-Link Wifi Plug		0	0	Wifi	F	M
Belkin WeMo Crockpot		0	0	Wifi+Pin	D	C

(**F**)orced configuration change when device is setup; (**D**)efault device configuration is acceptable and allows device to operate. (**C**)onsent by the user is required for the device to upgrade; (**A**)utomatic updates are applied without user intervention; (**M**)anual device update via user request. N/A means the category is not applicable.

TABLE VI: Device Evaluation.

Device	Observed IP Communication					MITM			Encryption		
	DNS	HTTP	UPnP	NTP	Custom	D-C	A-C	A-D	D-C	A-C	A-D
Google OnHub	✓-	✓+			✓	✗	✗	—	◐	●	—
Samsung SmartThings	✓	✓+	✓			✗	✗	✗	●	●	—
Philips HUE	✓	✓+	✓	✓		✗	✗	✓	●	●	c
Insteon Hub	✓	✓		✓		✓	—	—	○	—	—
Sonos	✓	✓+	✓		✓	✗	✓	✓	◐	○	○
Securifi Almond	✓			✓	✓	✗	✗	—	◐	●	—
Wink 2 Hub	✓	✓+	✓	✓		✓	✗	✓	●	◐	○
Belkin WeMo Motion Belkin WeMo Switch Belkin WeMo Link Belkin WeMo Crockpot	✓	✓+	✓	✓	✓	✗	✗	✓	◐	◐	○
LIFX Bulb	✓			✓	✓	✗	✗	✓	●	◐	○
Amazon Echo	✓	✓	✓	✓	✓	✗	✗	—	●	●	—
Belkin Netcam	✓	✓+	✓		✓	✗	✗	✓		◐	—
Ring Doorbell	✓				✓	✗	✗	—	●	●	—
Roku TV Roku 4	✓	✓+	✓		✓	✗	—	✓	●	—	○
Amazon Fire TV	✓	✓+	✓			✗	—	✗	●	—	◐
nVidia Shield	✓	✓+			✓	✗	—	—	◐	—	—
Apple TV (4th Gen)	✓	✓+		✓	✓	✗	—	✗	●	—	●
Netgear Arlo	✓	✓+		✓		✗	✗	—	●	●	—
D-Link DCS-5009L			✓			—	—	✓	—	—	○
Logi Circle	✓	✓+		✓		✗	✗	—	●	●	—
Canary	✓	✓+				✗	✗	—	●	●	—
Piper NV	✓-	✓+		✓	✓+	✗	✗	—	●	●	—
Withings Home	✓	✓+			✓	✗	✗	✗	●	●	●
MiCasaVerde VeraLite	✓	✓+	✓	✓	✓	✗	✓	✓	◐	●	○
Chinese Webcam		✓	✓		✓	✓	—	✓	○	—	—
August Doorbell	✓	✓+				✓	✗	✓	◐	◐	○
TP-Link WiFi Plug TP-Link WiFi Bulb	✓	✓+		✓		✗	✗	✗	●	●	●
Chamberlain myQ Garage Opener	✓				✓	✗	✗	—	●	●	—
Logitech Harmony	✓	✓+	✓			✗	✗	—	◐	◐	—
Caseta Wireless	✓	✓		✓	✓	✗	✗	✓	◐	●	○
Google Home Mini Google Home	✓-	✓+	✓	✓	✓	✗	✗	✓	◐	●	○
Bose SoundTouch 10	✓	✓+	✓		✓	✗	✗	✓	●	◐	○
Harmon Kardon Invoke	✓-	✓+		✓		✗	✗	—	●	●	—
Apple HomePod	✓	✓+		✓	✓	✗	—	—	●	—	—
Roomba	✓	✓+		✓	✓	✗	✗	✗	●	●	○
Samsung SmartTV	✓	✓+	✓			✗	—	✓	◐	—	◐
Koogeek Lightbulb	✓			✓	✓	—	✗	✗	—	●	●
Nest Camera		✓+				✗	✗	—	●	●	—
Nest Cam IQ	✓-	✓+				✗	✗	—	●	●	—
Nest Guard				✓	✓	✗	✗	—	●	●	—

TABLE VII: Communication Evaluation.
✓+ (TLS/SSL) — ✓- (3rd-party recursive DNS)

附录 B 评估案例

我们的评估表明，某些设备比其他设备具有更好的安全状态。在本节中，我们将研究根据其总体安全评估进行分类的三种设备。我们提出了三类：良好，令人满意和需要改进，它们突出了良好的安全实践和缺点。

A.良好：Withings 主页

功能特点。 Withings Home 设备是与空气质量传感器配对的摄像机。该设备具有移动配套应用程序，与云端点集成，并通过 Internet 和本地网络进行通信。该设备公开了 mDNS 服务，该服务允许零配置协议找到并配置该设备（例如 Apple 的 Bonjour）。该设备最初使用低能耗协议蓝牙来配置设备，然后切换到 IP 通信。设备更新不会自动应用，但需要用户同意。

评定。我们发现设备上运行的 mDNS 服务没有问题。配套的移动应用程序正确使用安全存储设施来存储敏感数据，正确使用加密协议，并具有适当的权限设置。大部分云基础架构由诺基亚自行托管，并运行服务以支持用户通知和控制。设备到云，应用程序到云和应用程序到设备之间的网络通信使用完全加密，并且不受 MITM 攻击。该设备确实通过 Internet 进行了明文身份验证（一种不安全的做法），以将设备与运行 XMPP 服务器 4 的云管理接口相关联。

B. 满意：Nest Cam

功能特点。 Nest Cam 是一种室内摄像机，可感应运动，记录视频并通知用户活动。该设备使用强制配置，这意味着用户必须对其设备进行配置和设置，然后才能进行操作。相机使用蓝牙协议通过移动应用程序配置设备，该应用程序使用位于相机背面的密码/条形码进行配对。摄像机不使用局域网来控制设备，所有活动和控件都通过云端点进行操作。最后，未经用户同意，将自动应用设备更新，以确保设备始终具有最新的运行固件。

评定。 Nest Cam 不公开任何服务，而是使用客户端模型，在该模型中，设备充当直接与云端点通信的客户端。Nest Cam 缺少运行的公开服务，这大大缩小了攻击向量，并限制了基于 IP 的攻击者。Nest Cam 使用设备上的证书固定，以验证和验证设备与云的通信是否安全。设备设置和配置需要移动应用程序

Device	CVE	CVSS
MiCasa Verda VeraLite	CVE-2012-5958, CVE-2012-5959, CVE-2012-5960, CVE-2012-5961, CVE-2012-5962, CVE-2012-5963, CVE-2012-5964, CVE-2012-5965, CVE-2013-4863	Critical
	CVE-2012-0920	High
Wink 2	CVE-2016-7406, CVE-2016-7407	Critical
	CVE-2016-7408	High

表 VIII：CVSS 评分为 Critical 和 High 的设备及其 CVE 列表。

通过蓝牙进行配对，这既可以确保最终用户的距离，又可以限制远程攻击媒介。该移动应用程序管理所有 Nest 产品，包括 Nest Cam，该产品请求访问麦克风，相机/照片，地理位置和其他敏感服务。云端点完全管理 Nest Cam，这意味着如果无法访问 Internet，则无法访问该设备。通常，Nest 产品会强制使用 Google DNS 递归，而忽略本地网络上的 DHCP 配置。精明的用户可以在其网关上配置静态路由，以将 DNS 流量重定向到所需的解析器。

C.需要改进：MiCasa Verde VeraLite

功能特点。 VeraLite 是启用 Z-Wave 的智能家居控制器，可以监视和控制家居中的低能耗传感器和其他设备。设备使用设备背面的预打印图钉通过云门户进行配对。VeraLite 需要手动更新，但是该设备会通知用户新更新的可用性。该设备公开了四种服务，包括 Web，DNS，UPnP 和 SSH 服务器。移动设备请求过多的权限，例如呼叫，控制电话网络状态（开/关/飞行模式）以及访问相机。VeraLite 是已停产的产品，供应商不再提供。

评定。 VeraLite 设备提供了强化的设置，可禁用设备上许多正在运行的服务，但默认情况下它们处于启用状态。强化模式强制从云端点进行设备管理和监视。如表 VIII 所示，该设备具有多个可利用的漏洞。UPnP 服务使用易受攻击的版本 libupnp 库，而 SSH 服务使用易受攻击的 dropbear（2016.72）实现。

SSH 服务器的配置支持密码块链接（CBC）模式，特别是 3des-cbc，aes128-cbc 和 aes256-cbc 模式，攻击者可以利用该模式从密文中恢复明文。DNS 服务已配置为允许查询未设置递归位的第三方域。因此，允许攻击者窥探 DNS 缓存。该移动应用程序要求用户与 Vera 供应商建立帐户，从而允许最终用户管理其控制器。该设备不使用证书固定，这使部署容易受到 MITM 攻击。云端点使用明文身份验证，运行可利用的服务，公开敏感信息以及运行不受支持的操作系统。