1.SoK Security Evaluation of Home-Based IoT Deployments

基于家庭的物联网部署的SOK安全评估

目录

[摘要 2](#_Toc35955210)

[1.说明 2](#_Toc35955211)

[2.方法 4](#_Toc35955212)

[A.抽象模型概述 4](#_Toc35955213)

[B.安全属性 5](#_Toc35955214)

[C.系统化的方法 7](#_Toc35955215)

[D.评估范围和攻击模型 7](#_Toc35955216)

[3知识系统化 7](#_Toc35955217)

[A.设备 8](#_Toc35955218)

[B.移动应用 11](#_Toc35955219)

[C.云节点 13](#_Toc35955220)

[D.通信链路 16](#_Toc35955221)

[四．评价 20](#_Toc35955222)

[A.实验设置 20](#_Toc35955223)

[B.数据 21](#_Toc35955224)

[C.挑战 21](#_Toc35955225)

[D.设备 22](#_Toc35955226)

[E.移动应用 23](#_Toc35955227)

[F.云节点 23](#_Toc35955228)

[G.通信 24](#_Toc35955229)

[H.缓解措施 25](#_Toc35955230)

[五．建议 26](#_Toc35955231)

[六．结论 27](#_Toc35955232)

[七．致谢 28](#_Toc35955233)

# 摘要

基于家庭的物联网设备在安全性实践方面的声誉很差。从表面上看，物联网设备的不安全性似乎是由整体的问题引起的，可以通过简单的措施以解决这些问题，但是这项工作发现这是一个天真的假设。 事实是，物联网部署的核心是利用传统的计算系统，例如嵌入式设备，移动设备和网络。 这些组件有许多未被发掘的挑战，例如，越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论，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。我们使用这种方法对基于家庭的物联网的文献进行系统化，以了解攻击技术，缓解和利益相关者。此外，我们评估了45种设备以增强系统化的文献水平，以分辨被忽视的研究领域。 为了使该分析透明并易于被社区化的适应，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。**（提出了一种方法去帮助从业者对IOT设备环境进行安全评估，该方法以门户网站的形式公开）**

## 一.说明

涉及物联网(IoT)的安全问题继续造成严重的操作问题，高调攻击[1]，大规模开发设备[2]，以及引人注目的标题“外来”设备黑客[3]。对物联网设备的需求——尤其是在数十亿美元的房地产市场[4]——造就了一场现代版的淘金热。新公司和老牌公司都急于在物联网市场分一杯羹。随着上市时间和生产成本优先于谨慎的安全措施，物联网设备受损的熟悉景象正在变得稀松平常。为了解决物联网的不安全问题，研究人员和供应商正在奋起直追，但他们的努力大多是模糊和临时的。**（指出了面临的风险问题）**

一些工作组织或市场领导企业已经提出了对物联网设备的标准化[5]-[12], 但不幸的是，他们还没有就解决方案达成一致. 此外，基于家庭的物联网设备的异构性也加剧了这些不安全感，因为尽管核心功能相似，但基于设备类型的特定功能可能有很大的不同。例如，一个物联网吸尘器和一个家庭助理设备设备均使用嵌入的linux操作系统，但设备上运行的服务将是不同的。这些差异使得分析不同的基于家庭的物联网产品变得困难。**（指出了制定物联网设备标准化的困难性）**

国家支持的对手很清楚这些困境，他们利用这一点来运行复杂的网络操作[1]。**（指没有制定一个标准化为物联网设备）**更糟糕的是，一些供应商在他们的设备上留下服务后门，这些后门后来被僵尸网络[13]发现和利用。即使是不成熟的犯罪集团也在利用这种猖獗的不安全感来运行分布式拒绝服务(DDoS)攻击[2]。不幸的是，清理工作和漏洞补丁远非完美，随着更多的设备上线，针对它们的威胁变得多了起来，这使得它们能够进一步传播[14]。为了系统地解决这些安全问题，研究人员需要通过进行测量和深入研究来了解情况，从而对这些漏洞进行分类和处理。对于基于家庭的物联网安全，已经有了大量的研究工作，但这些研究还很分散。我们的社区需要对当前文献的理解，对见解的推导，以及对安全漏洞的识别。这些见解将使研究社区能够规范确定哪些不安全感会持续存在，建议的缓解措施是什么，以及利益相关者应承担哪些责任。此外，这些学院还研究了文献作品的分类，并向社会提供帮助，帮助他们分清工作的轻重缓急。**（我们做的工作对研究者有什么贡献）**

在这项工作中，我们提出了一种基于组件分析的基于家庭的物联网设备建模方法论，并评估其安全状态，即物联网设备、及其伴随的移动应用程序、云端节点和相关的通信通道。**（详细介绍工作内容，基于物联网安全的几个方面 设备 移动终端 云端 和通信链路）**利用我们的方法，我们系统化了基于家庭的物联网设备的研究文献，以理解攻击技术、提出的缓解措施和利益相关者的责任。我们利用这些知识来为我们的社区获取见解和研究机会。此外，我们评估了45种目前市场上可用的基于家庭的物联网设备，并概述了它们在物联网组件上的安全性。

在系统化和评价的基础上，我们比较了两种方法的异同。我们为每个组件提供一个缓解列表，并为不同的涉众提出解决发现的问题的策略。最重要的是，我们建立了一个门户（The evaluation portal is available online at: https://yourthings.info），在这里我们邀请我们的合作研究员、供应商和高级用户贡献新的设备评估，并使用发布的数据集和建议的方法来重现我们的结果。

## 二.方法

我们的工作的贡献是双重的，系统化的文献和评估的家庭物联网设备。这项工作依赖于一个将物联网部署划分为组件的抽象模型，我们将该模型统一应用于研究文献和设备的一致性评估。**（我们的工作有什么创新之处）**

### A.抽象模型概述

我们提出一个抽象模型来表示物联网部署及其拓扑。图1是一个多设备物联网家庭的例子。该方法涉及到将每个设备分割成各自的拓扑结构，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。总的来说，我们的抽象模型有四个主要组件:**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)。**

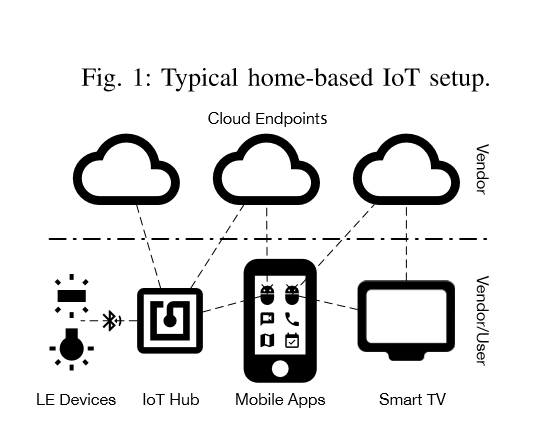


图1.典型的家用物联网设备安装

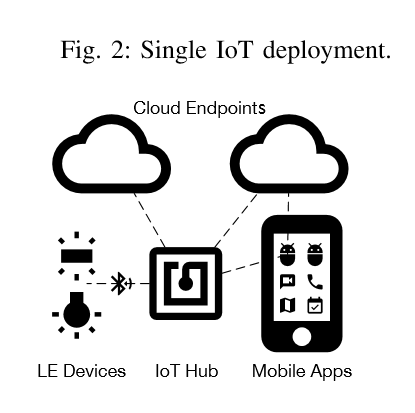


图2.独立物联网部署

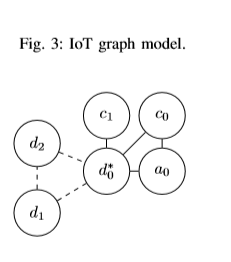


图3. IOT 图模型

对于每个设备部署，我们构造一个代表图并检查每个组件的安全属性.

### B.安全属性

安全属性有三类:**攻击载核、缓解措施和涉众**。攻击载体是用来规避物联网系统安全性策略的方法。缓和定义了应该采取哪些措施来处理攻击向量。最后，利益相关者代表了负责缓解的一方。

**攻击向量**.

设备有三种攻击类型:脆弱服务、弱认证和默认配置，定义如下:

* **脆弱性服务**：涉及到运行服务的脆弱性
* **弱认证**：指的是弱的或可猜测的凭证。
* **默认配置**：默认配置是指使用不安全工厂设置操作的设备。

移动应用程序有三个攻击类别:权限、编程和数据保护，定义如下:

* **权限**：是指移动应用程序被过度授权。
* **编程**：指的是包含易受攻击的实现的移动应用程序，包括不恰当地使用加密协议。
* **数据保护**：是指对敏感信息进行硬编码的移动应用程序。

组件的通信有两种攻击类型，加密和中间人(man-in-the-middle, MITM)，定义如下:

* **加密**：是指缺乏加密或支持弱加密协议。
* **MITM**：指的是对中间人攻击的易感性。

云端点与设备和通信边缘共享以下攻击类别:脆弱的服务、弱身份验证和加密(如上所述)。

**缓解。**缓解类别，补丁和框架，跨越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来修补组件，从而减少攻击向量。框架类别：减轻了需要新方法的基本问题。

**利益相关者**。涉众类别、供应商和最终用户跨越了所有四个组件。这些类别表明哪个利益相关者负责缓解攻击。如图1将物联网部署划分为供应商和用户控制的网络。云端点由供应商控制和缓解，而家庭网络中的组件可能会公开配置参数，以便用户可以禁用脆弱的特性。**（从涉及人上分类云节点有供应商负责控制，局域网由用户控制操作，包括组网等）**例如，如果设备有一个已知的默认密码，并且供应商允许用户更改默认密码，那么最终用户可以更改密码来保护设备。**（用户修改出厂设备的参数）**

### C.系统化的方法

系统化使用提出的抽象模型，该模型统一地呈现前面讨论的各个类别的文献，确定它们的**攻击技术、提出的缓解措施和涉众责任（上文提到的三个安全属性）**。每项工作都可以包含在一个或多个物联网组件中。系统化的文献选择基于以下标准：

* 优点:该作品是独一无二的，是第一批探索特定安全困境的作品之一。
* 范围:工作重点是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。
* 破坏:这项工作揭示了社区目前正在调查的一个新领域。

### 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来评估安全性能的家用物联网设备的评估。我们将我们的范围限制在基于家庭的物联网设备上，因为它们与系统化的工作相关，它们很容易获得，而且实验设置可以很容易地复制。

**攻击模型.** 为了进行评估，我们将攻击模型简化为一个互联网协议(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量(LE)的设备[15]，但它们需要专门资源在许多家庭网络中不可用的。我们认为集线器设备**(理解为网关等设备，网关在更高的层次上使用)**(低能量和IP之间的通信桥梁)的利用相当于利用所有连接的低能量设备，因为集线器和低能量设备之间存在一个信任会话。我们排除了对低能器件的直接评价，但考虑了对其集线器的评价。最后，我们认为家庭网络是一个不受信任的网络，我们不考虑移动应用程序、调制解调器/路由器或对家庭网络具有完全可见性的web浏览器([16])的安全状态。**（工作的第二个贡献）**

## 三、知识系统化

本节介绍了基于系统化抽象图模型的基于家庭的物联网研究(见图3)。表1概述了系统化工作及其相应的子节，我们在其中详细讨论了文献。组件分类强调了工作的重点，而**攻击载体、缓解和涉众**确定了方法。系统化突出代表工作;因此，它并没有提供所有相关工作的全面参考。

### 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的部署的基石。

#### 1)攻击向量:

若干工作([17]-[20])探讨物联网设备配置不安全感。Barnes [17]，建立在Clinton 等人的发现[18]，证明了如何暴露设备上的硬件针脚（hardware pins）允许他获得特权访问并监视最终用户。不安全的配置组合与弱或缺乏认证可能加剧Chapman [21] and Rodrigues [22].所示的问题。在运行服务时，弱认证或缺乏认证是关键促成了几个记录在案的攻击[23]-[26]。这些攻击表明，设备设置和配置是供应商必须考虑和评估的一个重要过程安全漏洞。供应商应该执行严格的身份验证策略，并让终端用户在允许设备操作之前对其进行配置。**(需要设备供应商考虑的问题身份认证问题和设备出厂设置问题)**

Max[23]评估了August智能锁的安全性，发现弱身份验证和不安全的默认配置破坏了锁的安全性。他发现了硬编码凭证**（****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**](https://baike.baidu.com/item/%E6%BA%90%E4%BB%A3%E7%A0%81/3587471)**中的软件开发实践，通常，各种应用程序都需要频繁访问数据库和其他应用程序，来查询与业务相关的信息。一般通过在配置文件和脚本中明文嵌入应用程序凭据（用户身份认证的口令），实现这种通信过程自动化。对于管理员而言，识别、更改和管理这些密码非常困难。因此，这些凭证一般都会长期保持不变，进而导致一些敏感系统受到未经授权的访问）**和允许修改和内省锁的配置错误。Obermaier[25]等人在基于云的相机上的工作发现，尽管该设备似乎有一个强密码(36个字母、数字和符号组成的字符)，但密码是反置的相机的MAC地址，编码为Base64**(厂商的默认设置)。**Kavalaris等人的[26]表明，Sonos设备在高端口上运行无文档记录和未经身份验证的服务，允许LAN客户端完全控制该设备。由于缺乏身份验证，Sonos设备容易受到未经授权的设备配对的影响。SmartAuth[24]发现，在物联网应用平台上，身份验证问题也通过越权的应用体现出来。设备配对在客户端和他们的设备之间建立一个受信任的通道。此外，IoT hub桥接了LE**（上文提及的低能耗设备）**设备到IP网络，它们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绕过设备或将其用作枢纽点。

物联网应用平台公开了一个基于许可的模型，允许第三方应用运行。Fernandes等人的[27]-[29]展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。在设备的平台中有许多子组件，这使得保护设备变得很困难。许多供应商都有良好的最佳实践来确保安全的身份验证和安全的默认配置(O 'Flynn[30]演示了这一点)，但是核心设备服务可能会受到侧信道信息泄漏的影响。Ronen等人的[15]表明，虽然飞利浦的Hue设备是相当安全的，但他们能够通过侧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结合起来，从而导致了一个蠕虫式的漏洞利用。

固件漏洞允许攻击者窃取WiFi证书[31]，将智能恒温器变成间谍设备[32]，勒索他们[33]，在智能电视[34]上运行任意命令，暗中控制家庭辅助设备[35]。Costin等人的[36]进行了大规模的固件分析研究，发现了一系列的缺陷。文献表明，设备安全需要防御方法来**保护侧信道、固件和硬件**。软件和硬件开发的工具链有一个定义良好的安全开发过程，供应商必须利用它。

#### 2)缓解（应对措施）:

为了解决易受**攻击的服务、配置错误和弱认证**，供应商通过设备更新进行修补，而物联网平台固有的设计缺陷则通过新框架得到缓解。Wang[37]等人提出了一个基于源(出处)的框架来聚合横跨一个部署的设备活动，从而可以检测错误和恶意活动。（理解为类似于入侵检测的框架）

SmartAuth[24]是一个识别运行在Smart Things and Apple Home等平台上的物联网应用所需权限的框架。FlowFence[28]是一个框架将应用程序代码分成敏感和非敏感模块，并通过不透明的处理程序编排执行。这种方法给开发人员带来了负担，因为他们必须注意什么代码操作敏感和非敏感数据。此外，研究人员在移动应用框架方面改善技术，以解决物联网平台的不安全问题。

#### 3) 涉众:

从表一可以看出，主要的涉众是供应商。供应商负责修补和更新易受攻击的设备，但可以通过配置将部分责任委派给用户。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，但是实现必须由供应商完成。用户可以选择授权给第三方应用程序的权限，从而获得控制权。Kavalaris等人的[26]演示了Sonos设备暴露的服务如何产生安全风险。用户可以通过网络细分来降低这种风险，但这需要一些技术专长。

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，除非他们有特权访问。根据所有提出的缓解措施，最终用户可以管理位于家庭界定端的配置或网络分段，如图1所示。终端用户没有太多的控制权，常常被给予一个最小化的界面，这限制了易受攻击服务的缓解性。另一方面，供应商有责任使设备保持最新。（以上关于安全责任问题的界定）

#### 4)措施（Take Away）:

这些文献论述了设备安全的一些方面。设备有相当多的组件综合于他们的整体安全，如**平台权限，未经认证的服务，不安全的配置，以及软件和硬件错误**。此外，当它们结合在一起时会被放大。设备的安全性不仅体现在软件上，还体现在硬件和旁路上。很多设备上都有嵌入式Linux，但是还没有安全的开放物联网平台，可以将新提出的框架[24]、[28]、[37]整合到社区中。

系统补丁解决了大部分漏洞。但修补过程不是完美的[32]，可以通过在其他计算领域实施的最佳实践来改进[67]。终端用户对设备的操作几乎没有控制或可见性。提供安全的健康测量和细粒度配置参数可以使用户减轻直接的风险。用户可以通过多种方式部署设备，这超出了供应商对于许可的最初假设，因此供应商在构建安全措施时应该假设设备是面向internet的。

通用计算系统也面临类似的问题，这些系统可以公开访问，并且运行脆弱的服务，或者使用弱身份验证(使用可猜测密码的SSH)。采用来自安全平台和操作系统的技术将改善许多IOT设备的安全状况。

设备:脆弱性在IOT系统表现在硬件、软件和侧通道上，当它们结合在一起时就会加剧安全威胁。物联网平台存在安全问题，但不同产品之间的常见漏洞需要系统分析。减轻漏洞严重依赖于供应商，但是供应商应该为用户提供一种方法来控制、检查和评估他们的设备。采用成熟的技术来管理物联网设备，可以显著提高物联网的安全性。

### B.移动应用

许多基于家庭的物联网设备都有一个配套的移动应用程序来控制、配置和连接设备。在我们的抽象模型中，我们将移动应用程序表示为一个顶点(参见图3)。

#### 1)攻击载荷

Acer[68]确定了Android移动应用程序问题的五个不同领域，即**权限演化、权限革命、网页化、编程导致的泄漏和软件的分发**。我们采用了Acar的方法，确定了影响物联网设备的三大类不安全因素:过度特权(权限[38]、[39])、编程错误(编程[40])和硬编码敏感信息(数据保护[41])。Max[23]展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、升级特权和规避August智能锁的安全性。除了Max的工作，没有利用移动应用绕过物联网设备的直接攻击。（主要的影响物联网设备的三大不安全因素越权，程序错误，硬编码信息敏感）

Chen等人提出了IoT Fuzzer，在物联网部署中利用移动应用程序查找物联网设备上的bug。Chen的方法是独特的，并且利用了供应商程序到应用程序中的语义。虽然目前还没有关于这种技术在外使用的报告，但理论上攻击者可以使用相同的方法来升级物联网设备上的特权。Sivaraman等人的[16]演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庭设备的信息，然后重新配置路由器/调制解调器防火墙规则，使设备面向Internet。Hanguard[42]展示了供应商对局域网的宽松的安全假设是如何暴露物联网设备的。配套的移动应用程序是设备的入口点，供应商通常认为部署的网络是可信和安全的。这些假设可能对设备的安全性产生严重影响，特别是当设备依赖未经身份验证的服务或未加密的通信时。

#### 2）缓解措施

Hanguard[42]提出了一个用户空间的移动应用程序，它通过基于角色的访问控制(RBAC)与路由器接口来控制访问。Hanguard的方法将阻止Sivaraman等人所讨论的攻击，但无法阻止来自被破坏的配套应用程序的攻击。通过黏附(adhering)来保护移动应用程序，根据Pscout[39]中讨论的最佳实践，Barrera等人[38]、Egele等人[40]、Viennot等人[41]降低了攻击面。不幸的是，正如Viennot等人在[41]中指出的，谷歌Play Store中的大部分应用程序都包含与权限、编程错误和信息泄漏相关的问题。移动应用程序平台已经成熟，并且具有内置的安全设施来促进良好的实践。开发人员和供应商应该坚持最佳实践，并定期审计他们的移动应用程序。（通过基于角色的访问控制与路由器接口控制有效的抵御来自于在本地网络使用应用程序收集有关家庭设备的信息）

#### 3)利益相关者:

移动应用组件既依赖于用户，也依赖于供应商。这部分是由于大多数移动平台向终端用户提供的权限模型。Hanguard[42]为用户提供了一个系统，可以通过路由规则(用户划分图1)在本地网络中进行部署，这与供应商无关。Sivaraman等人的[16]建议用户在自己的网络上运行移动应用程序时应保持警惕，只使用授权商店(谷歌Play、Apple App Store等)。供应商必须通过更新解决编程错误并保护信息存储。供应商必须熟悉移动平台，以便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。（针对涉众所提出的建议）

#### 4)措施:

Acar等[68]的工作表明了移动应用安全领域的成熟。移动应用程序被赋予了固有的信任，在许多情况下，移动应用程序控制着物联网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物联网设备或云服务之间的隐含信任。物联网供应商和开发商应遵循平台开发指南，并利用安全特性来确保适当的部署。通过细粒度的控制来限制移动应用程序对设备的访问是一个有前途的方向，可以减少攻击的影响。最后，应该进一步研究Hanguard的[42]方法，为最终用户提供控制以减少风险。

移动应用:移动应用受到物联网设备的信任，攻击者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。移动应用程序仍然受到权限过度特权、编程错误和硬编码敏感数据的困扰。在移动平台上坚持既定的安全发展准则将提高物联网的安全性。

### C.云节点

云终端是物联网部署的互联网组件，在某种意义上，它们定义了什么是物联网。它们提供**远程管理、警报和数字内容**等核心服务。物联网设备及其移动应用程序信任这些云端点，这给了对手一个额外的攻击点。我们将云端点建模为抽象图模型中的顶点(参见图3)。

#### 1）攻击向量:

TheattackbyMax[23]是一个很好的例子，它涉及到物联网生态系统的所有组件。该攻击在云端点上发现了用于August智能锁的不安全应用程序接口(API)，该锁将客户帐户升级为管理员帐户。（越权暴露不安全的应用程序接口）Blaich[45]检查了Wifi Barbie doll的各种漏洞，发现云端点没有对固件下载进行身份验证，存在多个跨站点脚本漏洞，允许用户枚举，没有暴力限制，并且发出了永不过期的cookie。（传统的基于web的攻击在物联网的应用场景下依然存在）Obermaier[25]等人对监控摄像头的云端点进行了审计，发现攻击者可以插入视频片段，触发假警报，并对摄像头系统进行拒绝服务攻击。这些攻击可能是由于基础设施配置、脆弱服务和不安全的api中引入的漏洞造成的。(针对于云端节点的攻击仍面临传统互联网领域受到的安全威胁)Zuo等人[69]利用客户端到云的信任来实现AutoForge，它伪造来自移动应用程序到云端点的请求，从而实现密码破解、密码探测和安全访问令牌劫持。物联网组件之间的隐含信任是敏感的，供应商必须在允许它们自由访问之前验证端点。（伪造请求从而获取敏感信息，重放攻击）

物联网集成平台, 像IFTTT[70]（自动化定义联动规则的网站）,automate.io[71]和CloudWork[72]是第三方云端点。他们使用OAuth令牌连接多个物联网设备来执行用户编程任务。Surbatovich[47]等人研究了方法2对隐私和完整性的安全影响，发现有些方法2可以让攻击者分发恶意软件并进行拒绝服务攻击。Nandi[44]等人通过触发操作编程(trigger-action programming, TAP)报告了一种类似的用户诱导编程错误，该错误会导致不正确的事件触发或缺少事件触发。Fernandes等人[48]指出，云集成平台可能会被破坏，这可能会公开暴露用户的OAuth令牌(OAUTH协议为用户资源的授权提供了一个安全的、开放而又简易的标准。与以往的授权方式不同之处是OAUTH的授权不会使第三方触及到用户的帐号信息（如用户名与密码），即第三方无需使用用户的用户名与密码就可以申请获得该用户资源的授权，因此OAUTH是安全的)。这些情况很可能发生在最近的平台妥协的基础上，如Equifax[73]和Orbitz[74]。Wilson[46]等人的工作并没有确定物联网生态系统的攻击载体，但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控制，它们会泄漏可能导致入侵的私有和敏感信息。(对于云集成服务的攻击向量的说明)

#### 2）缓解:

为了缓解这些攻击，Max[23]、Obermaier等人[25]和Blaich[45]推荐了**正确的配置和安全的认证机制**。Surbatovich[47]等人提供了一个框架来分析云平台的方法2（recipes)，这促进了以后的工作。Nandi[44]提出了一个自动触发器生成系统，它可以分析用户定义的错误触发器，并通过重写触发器来纠正这些错误。Fernandes等人的[48]提出了一种用于触发动作**可编程平台的去中心化框架**，称为DTAP。DTAP平台是物联网云平台与用户本地网络之间的垫片，基于传输令牌代理对物联网设备的访问(XTokens)。缓解技术包括保护云端点，提供分析第三方集成服务的工具，帮助开发人员为他们的应用程序生成正确的触发器，以及提供对设备功能的受限访问的短期令牌。

与此相关的是，Wilson等人的[46]研究了如何让那些信任供应商的物联网用

Recipe2是高级可编程指令，用于根据事件的发生触发物联网设备动作。

户能够使用他们的私人数据。这种技术称为TLS- rotate和Release (TLS- rar)，它需要一个收集TLS包的审计实体来请求来自供应商的会话密钥来解密通信。然后，供应商旋转TLS会话密钥，并向审计人员公开先前的密钥来解密收集的TLS包。审计系统必须部署在终端用户界定端，并收集他们希望审计的设备的流量。

#### 3）利益相关者:

供应商控制云端点(见图1)，用户没有办法检查或控制他们的设备发送到云端点的内容[66]、[75]。此外，第三方云提供商为物联网部署提供基础设施即服务(IaaS)和平台即服务(PaaS)。许多物联网设备依赖基于云的基础设施来运行它们的服务。意外停机[76]、基础设施折衷[77]和故意攻击[78]会影响云端点的部署。当涉及到云基础设施配置和API实现([23]、[25]、[45])时，供应商负责减少漏洞。

较新的物联网设备正在利用托管物联网平台，这些平台将大部分安全责任转移给了公共云提供商。另一方面，大多数建议的框架([44]、[46]、[48])是以用户为中心的，以有限的方式为最终用户提供可见性和控制。Fernandes等人的[48]和Wilson等人的[46]的工作是一种混合方法，可以由供应商和用户联合部署，也可以由可信的第三方部署。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少他们的风险。

#### 4)措施:

物联网云终端通过配置和API实现不安全的云部署，但这些漏洞可以通过现成的云安全工具来解决。为了进一步了解云部署中这些错误配置的程度，需要进行额外的测量。Censys项目[79]是一个有价值的数据来源，可以让研究人员对物联网基础设施进行历史性的分析。此外，物联网云集成平台引入了模仿传统工作(如分散的信任管理)的新挑战[80]。集成云平台为用户提供了一种基于事件的多物联网设备执行任务的方式，而用户会受到过度特权配方和隐私影响的困扰，这在Surbatovic[47]等人的工作中得到了证明。

Fernandes[48]等人通过将信任管理系统和令牌认证协议应用于物联网云平台，利用了之前的物联网云平台技术。供应商正在调整受管理的物联网云平台，将安全责任转移给亚马逊物联网等云提供商

Core[81]、Azure IoT Hub[82]、谷歌Cloud IoT[83]。物联网云终端更多地依赖于第三方基础设施来部署和运行它们的服务，这意味着供应商应该考虑针对意外停机和基础设施妥协的应急计划。需要进行更多的研究来了解托管物联网云平台以及可能存在的弱点。(供应商针对于云平台安全性提出的解决方案将云平台安全性委托给其他的云平台提供商)

### D.通信链路

云端点:云端点存在配置错误和易受攻击的服务，可以使用行业标准对这些服务进行适当的保护。第三方云提供商通过提供安全管理的物联网平台发挥了重要作用，供应商正在适应这些平台。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更多的关注。

物联网部署中的通信边界(见图3)分为两类协议:**互联网协议(IP)和低能量协议(LE)**。这两种通信都可以存在于网络的用户范围内(参见图1)，但是只有IP通信可以通过Internet进行。由于网络通信在其他领域的适用性，工业界和学术界的研究人员都在网络通信的安全性方面投入了大量的资金。大多数基于家庭的物联网系统实现四种类型的通信协议**:IP、Zigbee、Z-Wave和蓝牙(BLE)**。物联网设备选择使用IP套件进行通信，因为它的可靠性和已证明的能力，可以传输难以置信的全球网络流量。IP协议是无状态的，不提供安全性，但是可以通过使用TCP和TLS/SSL协议来补充，以提供所需的安全性特性。在文献的基础上，我们确定了基于家庭的物联网设备使用的五种流行的应用层协议，即:**DNS、HTTP、UPnP**（**通用即插即用**（英语：Universal Plug and Play，简称**UPnP**）是由“通用即插即用论坛”（UPnP™ Forum）推广的一套[网络协议](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E5%8D%8F%E8%AE%AE/328636" \t "_blank)。该协议的目标是使家庭网络（数据共享、通信和娱乐）和公司网络中的各种设备能够相互无缝连接，并简化相关网络的实现）**、NTP**（网络时间协议，英文名称：Network Time Protocol（NTP）是用来使计算机[时间同步](https://baike.baidu.com/item/%E6%97%B6%E9%97%B4%E5%90%8C%E6%AD%A5" \t "_blank)化的一种协议，它可以使[计算机](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA/140338)对其[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8/100571)或[时钟源](https://baike.baidu.com/item/%E6%97%B6%E9%92%9F%E6%BA%90/3219811)（如石英钟，GPS等等)做同步化，它可以提供高精准度的时间校正（LAN上与标准间差小于1毫秒，WAN上几十毫秒），且可介由加密确认的方式来防止恶毒的[协议](https://baike.baidu.com/item/%E5%8D%8F%E8%AE%AE/670528)攻击。NTP的目的是在无序的Internet环境中提供精确和健壮的时间服务。）**和自定义实现**。

1. 攻击向量:

DNS协议是互联网服务依赖的轻量级协议，但在递归和客户端配置的基础上，不经意间泄露了隐私信息。Kintis等人[64]发现，启用EDNS客户端子网功能(ECS)的开放递归DNS(嵌入客户端截短的部分IP地址)具有隐私含义。Selvi[55]演示了如何使用对NTP的MITM攻击来绕过HTTP严格传输安全(HSTS)。HTTP协议提供了更可靠的传输模式，但与DNS和NTP一样，它不提供任何机密性或完整性。Bellissimo等人[85]和Samuel等人[67]演示了HTTP等不安全协议如何允许攻击者MITM和后门系统软件更新过程。

物联网设备广泛依赖于通用即插即用协议（UPnP），以提供简单的配置和控制。通用即接（UPnP）程序使用HTTP协议，因此继承了同样的缺陷[86]。Garcia[50]展示了攻击者如何滥用UPnP，因为它缺乏身份验证、验证和日志记录。GNUcitizen[87]演示了启用UPnP了的设备容易受到跨站脚本攻击(cross-site scripting, XSS)（XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是JavaScript，攻击者可以使用户在浏览器中执行其预定义的恶意脚本，其导致的危害可想而知，如劫持用户会话，插入恶意内容、重定向用户、使用恶意软件劫持用户浏览器、繁殖[XSS蠕虫](https://baike.baidu.com/item/XSS%E8%A0%95%E8%99%AB/22777013)，甚至破坏网站、修改路由器配置信息等）的攻击，而HD Moore[88]在互联网上对启用UPnP的设备进行了统计和测量。他们的工作表明，未经身份验证和未加密的应用层协议的使用使攻击者能够大规模利用设备，从而导致额外的攻击。TLS/SSL会话提供机密性和完整性，这有助于解决这些通信协议中的固有缺陷。（协议本身的缺陷问题可以由相关安全协议弥补其安全缺失）

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]在TLS 1.0中暴露了初始化向量(IV)的缺陷，该缺陷允许攻击者预测消息流中下一条消息的IV。2012年，CRIME[58]展示了允许压缩的TLS会话(如谷歌的SPDY协议)如何容易受到会话劫持。2013年，AlFardan等人的[51]在MAC验证中使用变形包推断时间延迟(旁路攻击)，从密文中统计推断明文。AlFardan等人的[54]也展示了RC4流密码如何削弱TLS会话的安全性。POODLE[56]暴露了SSL 3.0中的一个降级缺陷，该缺陷允许双方进行不安全的通信。Beurdouche[59]等人发现，TLS/SSL库的几个客户端和服务器实现中存在允许MITM攻击的缺陷，包括异常的[57]漏洞。(TLS/SSL是具有缺陷的，其提供的安全服务存在问题)

Adrian等人披露的其他攻击[62]显示了实现安全通信协议的难度。许多物联网通信容易受到MITM攻击，因为它们支持较老版本的TLS/SSL协议。TLS/SSL也广泛用于受管物联网平台，以保护通信通道。新兴的物联网管理平台，如AWS物联网核心[81]、Azure物联网中心[82]和谷歌云物联网[83]，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，但是依赖经过时间检验的技术来实现安全的端到端通信。（中间人攻击 会话劫持 DNS欺骗）

BLE[89]、Zigbee[90]和Z-Wave[91]协议存在很多安全问题。Ryan[52]展示了蓝牙密钥交换协议，它允许攻击者被动地恢复会话密钥。Jasek[63]演示了攻击者如何被动和主动地滥用蓝牙网络栈中GATT层的通用属性配置文件。Zillner等人[61]研究了Zigbee联盟定义的默认信任中心链接键是如何在所有设备上相同的。[53]展示了Z-Wave固件中硬编码的常量是如何被用来派生会话密钥的，而这些密钥最终是众所周知的。**LE协议的旧版本存在严重的安全缺陷**，许多基于家庭的物联网设备都在硬件上实现了这些缺陷;因此限制了它们的抵御方法选择。（低功耗设备所使用的通信协议自身存在漏洞问题）

除了固有的缺陷之外，LE协议还提供了一种邻近特性，身份验证系统可以依赖这种特性来识别地理位置表示。Ho[92] 演示了如何通过串行化LE数据包并在IP上中继来攻击LE协议。研究人员已经证明，针对LE协议的MITM中继攻击是可行的并打破身份验证系统所依赖的地理邻近性。这些通信渠道可能存在隐私问题，Apthorpe等[65]和Wood等[66]已经证明了这一点。

1. 缓解:

对于HTTP、UPnP、DNS和NTP协议，建议的缓解方法包括禁用DNS中的ECS功能，使用NTP协议的更新版本(NTPv4)，以及使用TLS/SSL和安全协议(HTTPS)。对于TLS/SSL实现缺陷，将服务器端和客户端库升级到最新版本应该可以解决这些缺陷。此外，禁用弱的或脆弱的TLS/SSL版本会减少暴露，但会失去向后兼容性。对于基于LE的通信，第一代Zigbee和Z-Wave协议有严重的缺陷和有限的缓解选项。供应商可以以牺牲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在Apthorpe等人[65]和Wood等人[66]中发现的工作。Wood等人[66]提出了一种监测家庭网络并将物联网设备发送的敏感数据告知用户的系统。Apthorpe等人[65]演示了如何在家庭网络上进行流量整形以防止测信道分析。这一研究方向需要更多的关注，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，它提高了安全性[94]和无线(OTA)更新能力。此外，Zigbee还增加了一种新的安全模型，允许安全密钥分发，称为信任中心(Trust Center, TC)[95]。TC是Zigbee网络中受信任的实体，被授权向Zigbee客户端设备分发密钥。TC为每个Zigbee连接的设备提供一个惟一的加密密钥，这与传统的密钥分发模式不同。为了减少LE协议中的中继攻击，Ho等人[92]引入了一种使用身体区域网络(BAN)进行信号传播的基于触摸的意图通信方法。（针对于低功耗设备使用的网络协议存在的漏洞提出的改进措施）

1. 利益相关者:

终端用户无法解决通信缺陷，因为实现是在设备、云端点或移动应用程序上。此外，供应商在解决通信漏洞方面的选择有限，因为一些漏洞需要硬件升级，但在某些情况下，他们可以禁用这些漏洞[93]。供应商可以在设备、移动应用程序和云端点上修补脆弱的库。

互联网服务提供商(isp)可以看到基于IP的协议的使用情况，但他们不直接负责任何缓解措施。要让isp参与进来，它们必须提供定义其角色的网络和法律政策。至于LE协议，供应商可以通过禁用脆弱的配对来减少遗留设备。用户可以使用替代方法将LE设备和云节点配对，如果这种选项存在的话。用户可以购买提供下一代安全LE协议的新设备，比如Z-Wave Plus和Zigbee。

4）方法:

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，但它们受到遗留库的影响，在某些情况下无法修复。供应商负责解决通信通道中的漏洞。此外，云端点和移动应用程序可以由供应商直接更新，但供应商必须主动了解影响其软件的漏洞。物联网设备继续依赖于不安全的协议，如通用即插即用(UPnP)，我们接下来将展示，它们在局域网LAN中的通信很少加密。终端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。知情的高级用户可以将他们的本地网络划分为可信和不可信区域，以限制暴露。（在局域网中未使用加密传输导致信息容易被截获从而进一步发生中间人攻击）

TLS/SSL解决了易受MITM攻击的不安全协议，但它们也在实现和部署中显示出缺陷。Clark等人[96]的工作提供了关于SSL和HTTPS的额外分析。isp可以提供报告，概述关于设备和协议利用率的最佳网络实践和统计数据。受管理的云物联网平台使用自定义通信协议，这些协议依赖于公钥基础设施(PKI)和TLS/SSL协议。需要进一步的研究来调查托管云物联网平台使用的协议。这些新平台没有得到很好的研究，并应当予以警告要进行进一步的调查以确定任何弱点。

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，但通过使用TLS/SSL协议缓解了这些问题。许多设备在局域网中缺乏加密，这使它们容易受到MITM攻击。TLS/SSL协议在实现和部署方面存在缺陷，要求供应商保持警惕。受管理的云物联网平台使用定制协议，需要进一步审计。isp拥有丰富的信息，可以指导供应商进行安全部署。

（至此设备，移动应用平台，云节点，通信方面的问题全部阐述）

## 四．评价

我们评估了45种设备，包括家用电器、照相机、家庭助手、家庭自动化、媒体和网络设备。设备的完整概述见附录A表三。我们使用商业和开源工具进行评估;所有的商业工具都有相应的开源工具。我们的方法和评估需要最低限度的技术专长来复制，并有意设计来吸引广泛的技术受众，使他们能够为这项工作作出贡献。我们的评估结果汇总在表二，附加的评估细节见附录A表四。具体的设备评估案例见附录B。

### A.实验设置

我们的网络设置有三个主要组件:物联网子网、自定义Linux网关和一台评估机。评估机运行我们所有的评估工具，并与物联网设备位于同一子网上。我们的网关是一个Debian Jessie Linux（发行版）机器，管理网络服务(DHCP、DNS等)，并将物联网子网连接到互联网。此外，我们的网关捕获全包所有来自物联网子网的IP流量。我们使用一个24口交换机通过以太网连接有线物联网设备，并为需要802.11 WLAN的设备提供一个无线接入点。所有的物联网设备都根据它们的MAC地址分配一个静态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网络流量(通过边的节点交互，参见II-A节)，我们捕获、提取并将其分类到应用层协议中，以构建附录A表VII中的评估表。我们生成扫描数据基于安全审计工具,评估设备和云上运行服务端点,然后我们提供评估报告的附录表V和VI。我们使用移动应用程序审计工具来找到相关问题早在II-B节中定义的安全属性。审计报告提供了特权过度的应用程序、嵌入的敏感数据（硬编码）和编程错误的摘要。我们使用此数据摘要生成附录A表IV中的每个移动应用程序的评估报告。

### C.挑战

在评估物联网部署时，我们面临几项挑战，包括但不限于自动设备更新、云端点分类、无线网络分析和IOS应用程序的解密。自动更新会影响我们的设备评估，因为在应用更新时，设备状态会发生变化，而我们必须在可配置设备上禁用更新。由于增加了内容分发网络(CDN)的利用率，因此涉及到云端点分类，并且需要人工分析以确保较高的准确性。无线接入点使用WPA2配置，这限制了我们从物联网环境出口(网关)点收集的数据进行无线到无线设备通信的可见性。我们运行了两个不同的接入点，迫使流量通过网关，这样我们才能获得可见性。苹果的iOS应用程序在应用商店中被加密，需要越狱的iOS设备在本地下载、解密和复制iOS应用程序。一旦我们有了iOS应用程序的副本，我们就会使用各种开源和商业工具来审计它们。

### D.设备

我们使用Nessus扫描仪[97]来扫描设备，以进行服务发现、服务分析和漏洞评估。Nessus扫描器使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扫描器使用CVSS[99]评分系统对发现的漏洞的严重程度进行分级(从1到10)，并将它们分为低、中、高和临界。

我们认为任何分类的类别高或关键的CVSS评分系统是有问题的，并标注于记录于表二。

我们评估了45台设备，发现了84个正在运行的服务和39个与这些正在运行的服务相关的问题。我们找到了运行SSH、UPnP、HTTP web服务器、DNS、Telnet、RTSP和定制服务等服务的设备。许多设备为它们的服务配置了TLS/SSL，但是它们的配置有几个问题。例如，证书是自签名的，它们支持弱到中等的密码，它们使用短的TLS/SSL密钥，它们允许使用脆弱的SSL版本(v2、v3和CBC模式)，并且有过期的证书。此外，一些设备运行过时和脆弱的服务，这些服务允许远程代码执行、泄露敏感信息和运行未经身份验证的服务。

例如，*Insteon hub*在端口443上运行带有TLS的web服务器，并在端口22上监听SSH连接。用于TLS连接的证书已过期并进行了自签名，而TLS服务允许RC4这样的弱密码和SSLv3这样的不安全协议。同样，*Wink 2*、*Sonos音箱*、*nVidia Shield*、*Google Home*、*三星SmartTV*和*三星SmartThings*的证书或TLS/SSL配置都存在问题。*Wink 2和Sonos*都使用了1024位的短SSL密钥。其他设备，如*D-Link DCS5009L, Bose SoundTouch 10, Chinese webcam，*和*Securifi Almond*，都缺乏服务认证的加密功能，这使得局域网中的任何设备都可以窥探。

运行“通用即插即用”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、三星SmartTV*、*罗技和谐(Logitech Harmony)*和*Roku*等设备都运行“通用即插即用”服务，允许局域网中的任何人控制设备。具体来说，*MiCasaVerda VeraLite*使用具有公共漏洞的通用即插即用服务库的脆弱版本，如*libupnp* 1.6.18 (CVE-2012-5965)、*dropbear 2016.72 (CVE-2012-0920)*和*UPnP RunLua (CVE-2013-4863)*。一个完整的cve列表与CVSS得分高和关键是在附录B表八。

我们发现有16个运行服务的设备没有问题，还有10个设备没有公开运行服务。例如，Nest摄像机使用push/pull客户端方法，这限制了正在运行的服务的暴露。

**发现.**设备评估发现了与设备安装、软件更新和服务配置相关的问题。每个装置的附加评价结果见附录A表六。

### E.移动应用

我们使用MobSF[100]、Qark[101]和Kryptowire[102]的服务对物联网设备的每个移动应用程序进行静态和动态评估。我们查看了Android和iOS应用程序，并在表II中展示了这两种应用程序的弱点。有42台设备有配套的移动应用程序。我们一共分析了83个移动应用41个Android, 42个iOS。我们发现，39台设备存在一个或多个与权限、敏感数据或不正确使用密码有关的问题。我们观察了24个被过度授权的移动应用程序，它们请求对移动设备的权限，而应用程序代码并没有使用这些权限。

对于敏感数据，我们发现15个移动应用程序有硬编码的敏感数据，如用于谷歌地理编码的API Keys、谷歌地图、fabric.io, HockyApp, Localytics，微软虚拟地球，Umeng，以及其他云服务和设备服务。我们发现有17个移动应用程序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(IVs)。加密实现分别依赖于旧的或坏的算法，如AES-128和MD5散列函数。其他应用程序不强制使用SSL，允许通过未经验证的连接进行通信。

**发现.**评估确定了移动应用程序和设备之间固有的信任问题，系统化的工作忽略了这些问题。我们的移动应用评估摘要见表二，更多细节见附录A表四。

### F.云节点

我们使用Nessus扫描器来发现、分析和评估云端点上正在运行的服务。在物联网网络上，我们观察了45台设备上的4000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**。第一方是指基于云的服务,在供应商的基础设施上运行,第三方是指订阅等服务内容分发网络(CDN),混合是指基于云计算的基础设施(IaaS),如Amazon AWS或微软Azure,未知主机物联网云服务,是指由于歧义非机密的基础设施。我们将950个域名划分为第一方，1287个域名划分为第三方，630个域名划分为混合域名，1288个域名划分为未知域名。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应用程序使用的是AWS CloudFront域，它不会告诉我们该域属于Hulu还是智能电视。

对于每个云端点，我们评估了正在运行的服务和TLS/SSL配置(如果适用的话)。我们发现有18台设备使用了过时的服务，泄露了敏感信息，没有加密进行身份验证，或者运行了脆弱的服务。我们发现有8台使用云终端的设备容易受到攻击，存在公共漏洞。另外，7台设备以明文方式通过云端点身份验证。我们发现26个使用云端点的设备存在TLS/SSL配置问题，比如自签名证书、域名不匹配以及对脆弱的TLS/SSL协议版本的支持。

我们发现有10台设备使用了配置错误的云端点，这些端点允许文件路径和服务器上运行的进程等敏感信息公开。我们看到有4台设备使用了运行过时操作系统(Ubuntu 10和Ubuntu 12)的云端点供应商支持

**发现.**评估发现了部署不受支持的遗留操作系统和敏感信息公开方面的问题。我们在表二中总结了我们的发现，并在附录A表五中提供了更多的细节。

### G.通信

我们使用Nessus网络监视器[97]、ntop-ng[103]、Wireshark[104]和sslsplit[105]来分析每个设备的通信边缘。我们手动检查流量，并使用sslsplit测试它们的MITM攻击。物联网设备使用基于IP的通道与其组件进行连接，在模型图中以边表示(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个设备连接到云端点(D-C)， 35个移动应用程序连接到云端点(A-C)， 27个移动应用程序通过局域网(LAN)连接到设备(A-D)。

我们将这些连接分为五种应用协议，即DNS、HTTP、UPnP、NTP和定制协议。自定义协议类别是指特定于设备的应用层协议。智能设备使用许多协议，但在我们的实验室中，我们只观察上面列出的五种协议。我们发现有41台设备使用了DNS协议，其中6台设备没有使用网络配置的DNS递归服务器，而是使用了谷歌或OpenDNS的服务器。我们发现有38台设备使用HTTP协议，其中34台使用TLS/SSL会话(HTTPS)。我们发现了21个使用通用即插即用协议的设备，它们要么发送一个多播SSDP请求，要么响应一个SSDP请求。此外，我们还看到了25个使用NTP协议进行时间同步的设备。我们观察了28个使用特定于设备的自定义协议的设备。例如，谷歌产品(*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谷歌的服务器。

大多数设备使用互联网加密(D-C)。我们发现有25台设备加密了它们所有的通信，15台设备部分加密了它们的通信，还有2台设备没有加密它们与云端点的通信。对于移动应用程序(A-C)， 24个应用程序加密了它们所有的通信，10个应用程序部分加密了它们的通信，1个应用程序没有加密它到云端点的通信。在LAN (A-D)上，我们观察到5个设备对它们的通信进行了加密，2个设备对它们的通信进行了部分加密，还有20个设备没有对它们的通信进行加密。很少有设备，比如中国的网络摄像头，没有配套的移动应用程序，但提供了一个HTTP接口，允许局域网中的任何设备进行身份验证和交互。

除了进行通信分析外，我们还积极地对每一个通信边缘进行MITM攻击，以测试它们的易感性。我们发现，在总共20个设备中，有一个或多个易于受到MITM攻击的通信边缘。我们发现了四种设备到云(D-C)通信易受影响，两个移动应用到云(A-C)通信易受影响，和20个应用到设备(A-D)通信易受影响。

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

### H.缓解措施

**设备.**受影响的设备应通过安全通道进行修补，以确保更新的完整性。供应商可以限制在物联网设备上运行的服务，并采用客户端方法，通过使用push/pull请求的云端点管理设备。设备配置可以使用一种可操作之前配置的方法进行补救，在这种方法中，如果没有正确的配置和设置，设备将无法激活。许多设备遵循先配置后操作的方法，并且应该由行业标准强制执行。最后，端点(云或移动)验证确保只有经过身份验证的方可以与设备交互。供应商可以将交互限制在沙箱环境中，并为所需资源分配临时细粒度访问控制。受信任的端点不应该以不受约束的访问进行操作，设备应该强制所有各方的身份验证超时。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])来应用许多建议的缓解措施，这与人们普遍认为它们是动力不足和能源受限的设备的看法相反。

**移动.**特权过大的应用程序可能会涉及用户活动的隐私问题。移动平台应该实现一个基于应用程序功能分析的权限派生系统，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库中时，应该派生敏感信息，如API key。加密协议很难正确实现，因此开发人员应该依赖具有正确实现的成熟库。最后，开发人员应该遵循这些库附带的推荐准则.

**云.**托管平台和配置管理工具可以缓解云端点上的脆弱服务。供应商应该利用由经验丰富的专业人员管理的商业平台。类似地，通过API集成自动化云端点配置可以减少错误配置的机会。例如，Let 's Encrypt[108]可以自动更新服务器的证书。云终端不应该支持不安全的协议，相反，它们应该同时验证终端设备和移动应用程序。

**通信.**所有物联网组件之间的网络通信应遵循相同的安全标准(局域网或互联网)。供应商必须使用最新的安全协议，提供有限的向后兼容功能，执行协议升级需求，并验证端点。端点验证将确保MITM攻击不成功，并保护通信的完整性。如果端点无法验证，供应商应该默认为故障状态。此外，供应商可以提供在物联网部署中安装定制证书的选项，以提高透明度。

## 五．建议

A.涉众

**供应商.**供应商必须在每个层次上为每个组件获得正确的安全需求，包括物联网系统的设计、实现和部署。我们的评估显示，许多供应商努力争取设备安全，但往往失败的尽职调查。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。缺乏特定领域专业知识的供应商可以外包给专门的第三方来开发他们的产品。

**终端用户.**基于家庭的物联网部署将简单的家庭网络转变为复杂的企业网络。终端用户可以遵循良好的安全实践，将设备配置为使用加密、禁用远程管理功能并对其网络进行分段。最重要的是，消费者可以通过购买隐私感知和安全的设备来影响供应商。我们的门户旨在对物联网设备进行客观的安全评估，并让消费者做出明智的决定。

**其他部分。**互联网服务提供商(isp)不是直接的利益相关者，但无处不在的基于家庭的物联网设备影响着他们的网络运行。isp看到的大部分流量将被加密，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可能会采取技术补救措施来封锁某些端口，但需要法律政策来干预。由于物联网的全球性质和国际判例[4]，这些决定可能引发政策和合规争议。互联网服务提供商可以提供他们在运行和运营家庭互联网网络方面的专业知识，帮助识别基于家庭的物联网部署的影响。

云提供商为许多物联网供应商提供基础设施即服务，在开发、运行和保护云基础设施和平台方面有多年的经验。他们的产品对供应商来说是经济和实用的，但是他们偶尔也会遭遇中断[76]。云提供商在保障物联网部署方面发挥着重要作用，应该继续提供定制的云服务，减轻供应商的安全责任。

B．推荐

**措施.**我们建议对设备间通信、移动应用到设备间交互以及物联网组件之间的信任关系进行额外测量。设备间通信(设备到设备和移动应用程序到设备)在局域网内没有得到很好的研究。许多物联网系统，如家庭辅助设备，在未经用户同意的情况下，自动发现并与局域网中的其他设备进行交互，这需要进一步的调查，以了解这些通信对安全和隐私的影响。此外，进行纵向研究可以发现潜在的缺陷，如果没有时间分析，这些缺陷很难观察到。

**最佳实践.**物联网组件的最佳实践和指南很容易获得，但它们的利用率很低。一些被评估的设备具有非常好的实践，其他供应商可以从中受益，包括移动应用程序实现、云服务配置、设备供应以及组件的安全部署和交互。应该深入评估这些设计和实现模式，以了解它们对供应商的成本/收益。政府立法可以鼓励以经济或政策为基础的激励措施来影响供应商采用最佳实践。

## 六．结论

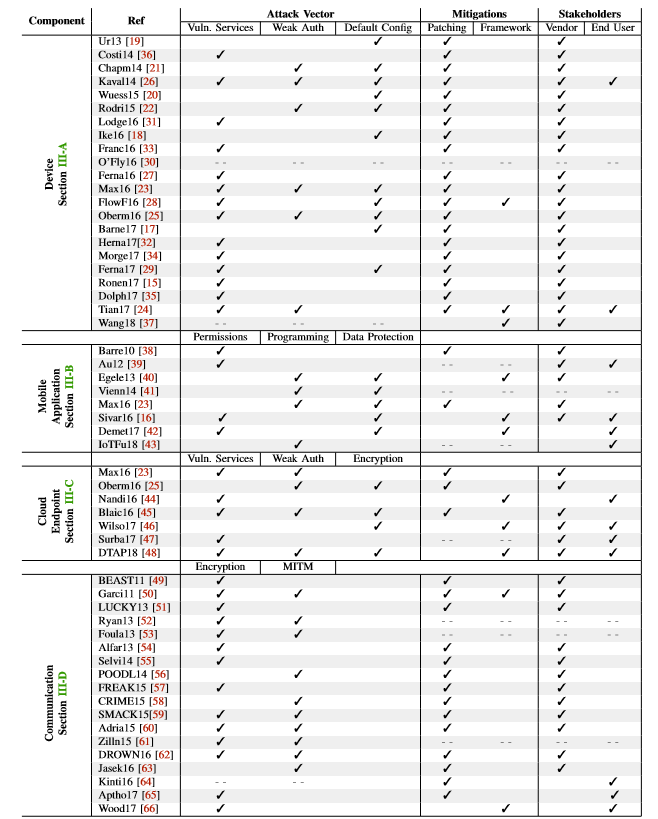
这项工作通过一个抽象的模型使现有的基于家庭的物联网设备的系统文献化，使我们能够从中获得见解。我们使用相同的方法来评估45种物联网设备，发现许多文献中讨论的问题如今也存在于物联网系统中。我们在门户网站上提供我们的结果和评估数据集，并邀请研究人员贡献和复制我们的工作。我们设想这项工作将成为评估基于家庭的物联网设备、为研究人员提供数据以及与供应商合作的中心支柱。

## 七．致谢

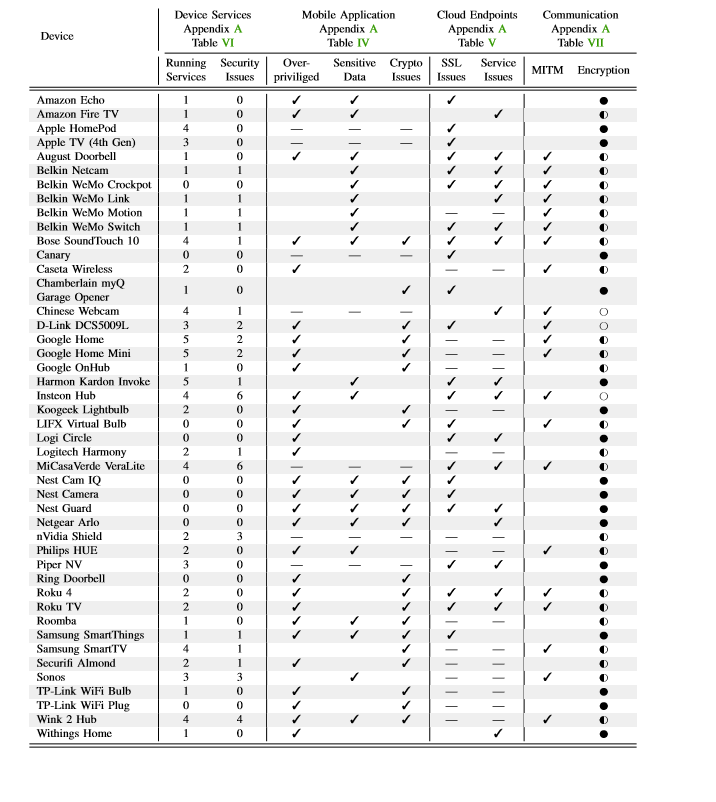
我们感谢匿名评论者和Jan Werner提出的深刻的评论和建议。我们感谢Kryptowire团队提供的自动化移动应用程序安全分析平台。本材料部分基于美国商务部批准的2106DEK和2106DZD，国家科学基金会(NSF)资助号美国空军研究实验室/国防高级研究计划局2106年dtx和2106有效马力。本材料中表达的任何观点、发现、结论或建议均为作者的观点，并不一定反映美国商务部、国家科学基金会、空军研究实验室或美国国防部高级研究计划局的观点。

参考文献

**表1**使用基于组件的分析使当前的文献系统化。每个部分都对应于方法中讨论的一个图组件，该方法涵盖了攻击向量、缓解和涉众。√意味着攻击、缓解或涉众的类别适用于讨论的文献。

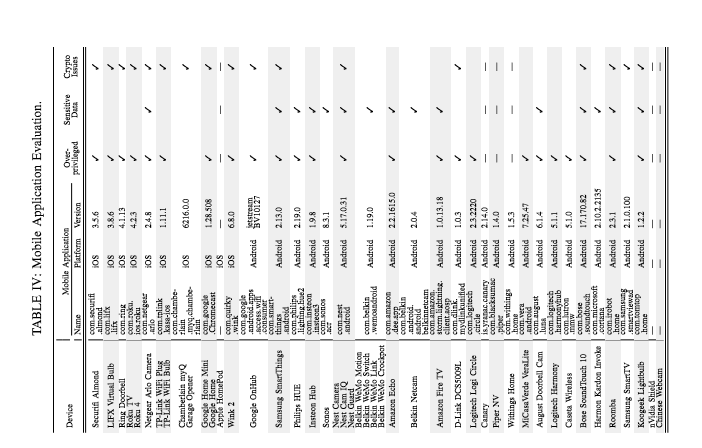


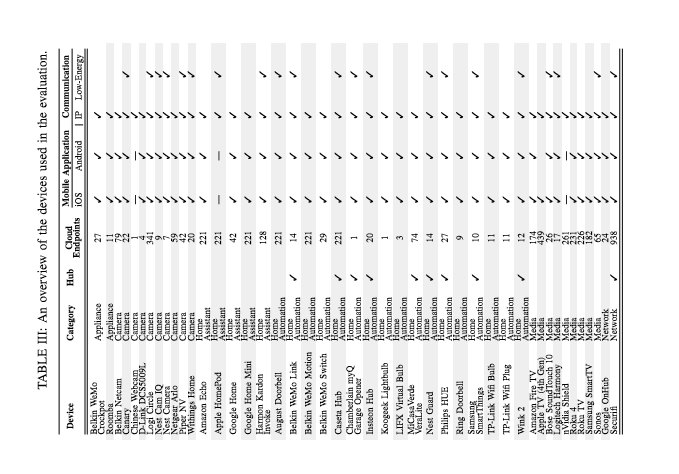
**表II:**该表是图3中每个图组件的每个评估设备的摘要。设备(D)、移动应用(A)、云端点(C)、通信通道(E)四个组件，评估使用Nessus扫描器对设备和云端点进行评估;Kryptowire、MobSF和Qark评估移动应用程序;Nessus Monitor、ntopng、sslsplit和Wireshark来评估通信协议。设备部分总结了运行服务的数量和发现的问题。移动应用程序总结了过多的权限、敏感数据或不正确地使用加密协议。通信类别将MITM攻击的易感性和通信通道状态总结为完全加密()、部分加密(#G)或未加密(#)。更多细节见附录A

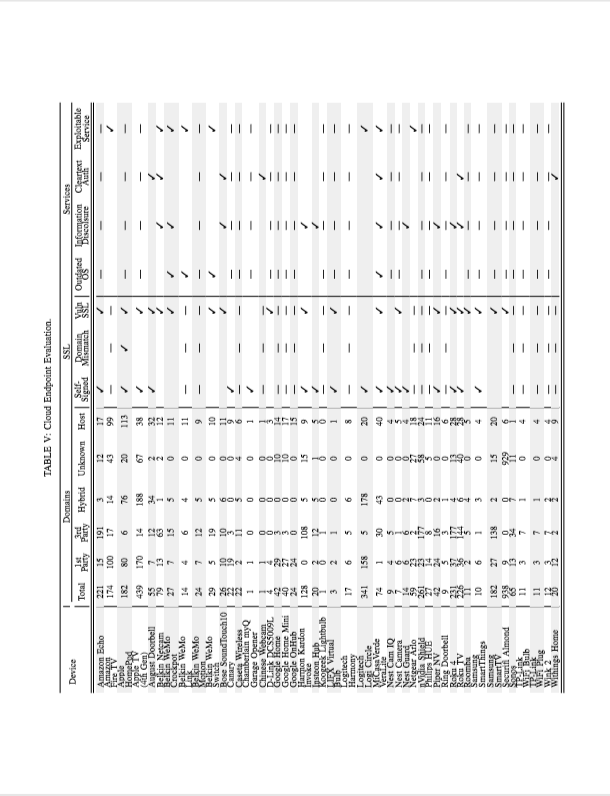
****

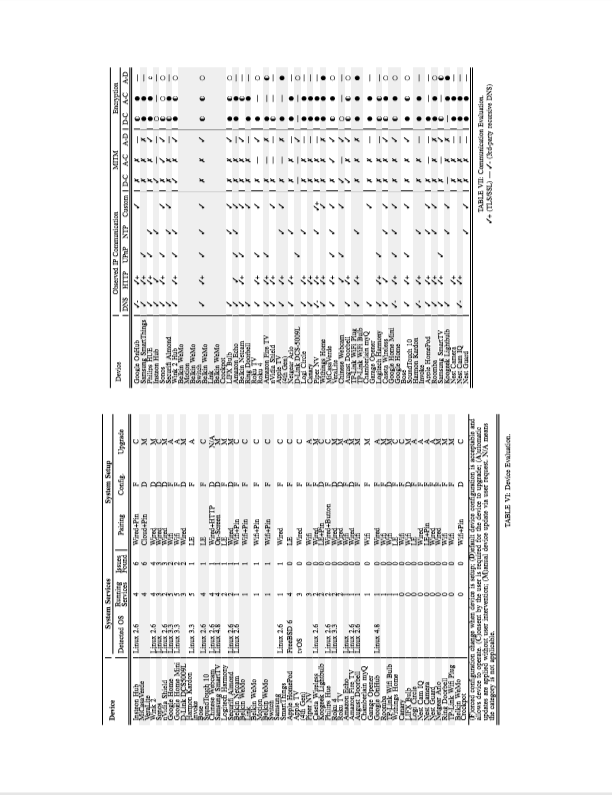
## 附录A

**评估表格**

****

****

****

****

## 附录B

**评估案例**

我们的评估表明，一些设备具有比其他设备更好的安全状态。在本节中，我们将根据总体安全性评估对三种设备进行分类。我们提出了三类:良好的、令人满意的和需要改进的，它们强调了良好的安全实践和缺陷。

1. 良好的 Withings Home

**功能特性.**Withings的家用设备是一个配有空气质量传感器的摄像头。该设备有一个移动伴侣应用程序，与云端点集成，并通过Internet和本地网络进行通信。设备公开mDNS服务，允许零配置协议查找和配置设备(即Apple s Bonjour)。该设备最初使用低能耗协议蓝牙对设备进行配置，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。

评估.我们发现设备上运行的mDNS服务没有问题。相应的移动应用程序正确地利用安全存储设施来存储敏感数据，正确地使用加密协议，并具有适当的权限配置。大多数云基础设施是由Nokia自托管的，并运行服务来支持用户通知和控制。设备到云、应用到云和应用到设备之间的网络通信使用完全加密，不容易受到MITM攻击。该设备确实在Internet上以明文(一种不安全的做法)进行了身份验证，以便将该设备与运行XMPP服务器4的云管理接口相关联。

1. 令人满意的：Nest Cam

**功能特性.**Nest Cam是一款室内摄像机，它可以感知运动、记录视频并向用户发出活动通知。该设备使用强制配置，这意味着用户必须配置和设置他们的设备才能进行操作。摄像头使用蓝牙协议，通过移动应用程序配置设备，移动应用程序位于摄像头背面。摄像机没有利用本地网络来控制设备，所有的活动和控制都是通过云端点进行的。最后，在没有用户同意的情况下自动更新设备，确保设备始终运行最新固件。

**评估.**Nest Cam不公开任何服务，而是使用客户端模型，其中设备充当直接与云端点通信的客户端。在Nest Cam上运行的公开服务的缺乏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来验证设备与云通信的安全性。设备设置和配置需要移动应用程序通过蓝牙进行配对，既保证了终端用户的接近，又限制了远程攻击的传播。该移动应用程序管理所有Nest产品，包括Nest Cam，后者请求访问麦克风、相机/照片、地理定位和其他敏感服务。云终端完全管理Nest Cam，这意味着没有互联网接入设备是无法访问的。Nest产品通常强制使用谷歌DNS递归，而忽略本地网络上的DHCP配置。精明的用户可以在网关上配置静态路由，将DNS流量重定向到所需的解析器。

1. 需要改进:MiCasa Verde VeraLite

**功能特性.**VeraLite是一款智能家居Z-Wave控制器，可以监控家中的低能传感器和其他设备。设备通过云门户配对，在设备背面使用预先打印的pin。VeraLite需要手动更新，但设备会通知用户新更新的可用性。该设备公开了四个服务，包括web、DNS、UPnP和SSH服务器。移动设备请求过多的权限，如呼叫、控制电话网络状态(开/关/飞行模式)和访问相机。VeraLite是一个停产的产品，不再由供应商提供。

**评估.**VeraLite设备提供了一个硬设置，可以禁用设备上的许多正在运行的服务，但它们在默认情况下是打开的。强化模式迫使设备管理和监视来自云端点。该设备有几个可利用的漏洞，如表VIII所示。UPnP服务使用libupnp库的一个脆弱版本，而SSH服务使用一个脆弱的dropbear(2016.72)实现。

SSH服务器的配置支持加密块链(CBC)模式，特别是3des-cbc、aes128-cbc和aes256-cbc，攻击者可以利用它们从密文中恢复明文。DNS服务被配置为允许对没有设置递归位的第三方域进行查询;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供应商建立一个帐户，这允许终端用户管理他们的控制器。设备不使用证书固定，这使得部署容易受到MITM攻击。云端点使用明文身份验证、运行可利用的服务、公开敏感信息和运行不受支持的操作系统。