
# 物联网（IoT）安全和隐私建议宽带互联网技术咨询小组技术工作组报告

## 统一协议报告

**发出：**

2016年11月

## 版权/法律声明

## 关于BITAG

宽带互联网技术咨询小组（BITAG）是一个非营利，多利益相关方组织，致力于将技术工作小组（TWG）中的工程师和技术人员召集在一起，就可能影响宽带网络管理实践和其他相关技术问题达成共识用户的互联网体验，包括使用互联网的应用程序，内容和设备产生的影响。

BITAG的任务包括：（a）就此类技术问题对政策制定者进行教育；（b）处理特定的技术问题，以尽量减少相关的政策纠纷；和(c) 充当新想法和网络管理实践的共鸣板。
TWG的具体职能还可能包括：（i）确定宽带提供商和其他实体的“最佳做法”；

（ii）解释和运用“安全港”做法；
（iii）否则向行业和公众提供技术指导；和/或（iv）就与TWG任务密切相关的技术问题发表咨询意见，这些技术问题可能是与宽带网络管理实践有关的争议。

BITAG技术工作组及其下属委员会通过共识流程做出决策，每份报告的封面都列出了相应级别的协议。每个TWG代表都致力于就各自组织支持的建议达成共识，尽管即使在最高级别的协议中，BITAG共识也不要求所有TWG成员组织都同意文件的每一句话。每个TWG委员会主席确定是否达成共识。如果委员会内部就是否达成共识存在分歧，则BITAG采用表决程序，可以更正式地达成和表明各种级别的协议。有关更多信息，请参见BITAG网站上的BITAG技术工作组手册。www.bitag.org. BITAG TWG报告主要侧重于技术问题，特别是那些可能被解释为反竞争，歧视或以其他非技术因素为动机的问题。尽管报告可能涉及与特定网络管理实践相关的广泛问题，但报告无意全面解决或分析该实践可能引发的经济，法律，法规或公共政策问题。 BITAG欢迎公众评论。请随时通过电子邮件发送书面评论。comments@bitag.org.

## 执行摘要

在过去几年中，许多连接到互联网的新设备不是个人计算机，而是嵌入了互联网连接和功能的各种设备。此类设备通常被称为物联网（IoT），并带来了新的安全和隐私风险。

术语“物联网”具有潜在的广泛范围。物联网可以指在家庭，企业，制造设施，运输行业和其他地方的部署。因此，物联网可以指的不仅仅是简单的面向消费者的设备。就本报告而言，尽管部分或全部建议可能更广泛地适用，但我们使用术语“物联网”仅指面向消费者的设备及其关联的本地和远程软件系统。此报告涉及消费者正在安装，配置和管理他们租赁或拥有的设备的场景。

消费物联网设备的数量和多样性正在迅速增长；这些设备为终端用户提供了许多新应用，将来可能还会提供更多新应用。许多物联网设备已经投入使用或正在为不久的将来开发部署，包括：

- 传感器更好地了解日常生活模式并监控健康
- 监控和控制家用功能，从锁到暖气和水系统
- 可以预期消费者需求并可以采取行动解决这些需求的设备和电器（例如，用于监控库存并自动为消费者重新订购产品的设备）

这些设备通常与网络上其他地方运行的软件进行交互，并且通常在不需要人工干预的情况下自主运行。此外，结合数据分析和机器学习，物联网设备可能能够采取更主动的行动，揭示有趣有用的数据模式，或向终端用户提出建议，改善他们的健康，环境，财务和其他方面。他们的生活。

尽管消费者会因使用任何互联网连接设备而面临一般安全和隐私威胁，但消费者物联网的性质却与众不同，因为它可能涉及非技术或不感兴趣的消费者，挑战设备发现和消费者家庭网络上的库存数量和数量。各种各样的设备激增，对消费者和运行在共享网络链路上的其他用户的互联网访问服务产生影响，以及对其他服务的影响，因为当物联网设备受到恶意软件入侵时，它们可能会成为有害数据流量的平台，例如垃圾邮件和拒绝服务攻击-可能干扰其他服务的提供。

最近的几份报告表明，某些设备不遵守基本的安全和隐私最佳实践。在某些情况下，设备会受到威胁，并允许未经授权的用户执行监视和监控，访问或控制，诱发设备或系统故障，并打扰或骚扰授权用户或设备所有者。

导致缺乏安全性和隐私最佳实践的潜在问题包括：缺乏物联网供应链的安全性和隐私经验，缺乏在首次出售后开发和部署更新的动机，安全的网络软件更新，设备困难硬件资源受限或受限（不包括某些基本或“常识”安全措施），用户界面受限或受限的设备（如果存在，可能仅具有最低功能），以及在制造过程中插入恶意软件的设备。

物联网的出现为从智能家居到智能城市的重大创新提供了机遇。在许多情况下，对设备开发，分配和维护流程进行直接更改，可以防止遭受重大安全和隐私问题的物联网设备分配。 BITAG相信，遵循本报告中概述的指导方针，可以极大地改善物联网设备的安全性和隐私性，并最大限度地减少与附带损害相关的成本，否则可能会影响最终用户和互联网服务提供商。此外，除非物联网设备部门（制造和分销这些设备的行业部门）提高了设备安全性

和隐私性，否则消费者的强烈反对可能会阻碍物联网市场的增长，并最终限制物联网拥有的承诺。

**观察。** **根据本报告的分析以及其成员在物联网设备方面的综合经验，BITAG技术工作组得出以下结论：**

- **安全漏洞：某些物联网设备“出厂时”配备的软件已过时或过时。其他物联网设备可能随附更多最新软件，但将来可能会发现漏洞。除非设备具有随后更新其软件的机制，否则在设备使用寿命内发现的漏洞可能会使设备的安全性降低。**

- **不安全通信：为更通用的计算设备设计的许多安全功能很难在IoT设备上实现，并且在现场已发现许多安全漏洞，包括未加密通信和来自IoT设备的数据泄漏。**
    - **未经身份验证的通信：某些物联网设备提供自动软件更新。但是，如果没有身份验证和加密，这种方法是不够的，因为可能会损害或禁用更新机制。此外，许多物联网设备在通信过程中不使用身份验证。**
    - **未加密通信：许多物联网设备以明文形式而非加密形式发送部分或全部数据。其他设备或攻击者可以观察到纯文本通信。**

- 缺乏相互认证和授权：允许未知或未经授权的当事方更改其代码或配置或访问其数据的设备是一种威胁。该设备可以揭示其所有者存在或不存在，促进恶意软件的安装或操作，或从根本上破坏其核心物联网功能。
- 缺乏网络隔离：这些设备还会带来新的风险，容易受到家庭内部攻击。由于默认情况下许多家庭网络不会将网络的不同部分相互隔离，因此网络连接的设备可能能够观察或交换同一家庭网络上的其他设备的流量，从而使一台设备可以观察或影响不相关设备的行为。

- 数据泄漏：物联网设备可能会从云（存储数据）和物联网设备自身之间泄漏私人用户数据。
  - 云泄漏：由于外部攻击或内部威胁，云服务可能会遇到数据泄漏。此外，如果用户对这些云托管服务依赖弱认证或加密方法，则用户数据也可能会受到威胁。
  - 设备之间以及设备之间的泄漏：在某些情况下，同一网络或相邻网络上的设备可能能够观察来自其他设备的数据，如房屋名称，房屋的精确地理位置，甚至是产品消费者购买的商品。

- 恶意软件感染和其他滥用行为的敏感性：恶意软件和其他形式的滥用行为可能会破坏物联网设备的运行，获得未经授权的访问或发起攻击。

- 服务中断的潜在可能性：可用性或连接能力的潜在丧失，不仅会降低物联网设备的功能，而且在某些情况下可能会降低设备的安全性，例如，如果没有此类连接，物联网设备无法正常运行（例如，如果失去连接，则关闭家庭报警系统）。

- 设备安全和隐私问题可能持续存在：由于制造商（或物联网供应链中的另一方，或物联网服务提供商）可能不提供软件更新，许多设备可能从未收到过软件更新，因此，物联网设备安全问题可能会持续存在更新或消费者可能无法应用已经可用的更新。
  - 许多物联网设备将永远无法修复：通常很难部署修补关键安全漏洞的软件更新。许多设备供应商和制造商没有将软件更新部署到数千个设备以及通过网络部署的系统或流程。

对在家用住宅中运行的设备进行更新非常困难，因为更新不当可能会中断服务，有时还可能“分解”设备。此外，某些设备甚至可能无法进行软件更新。

- 软件更新解决的不仅仅是错误：软件更新不仅仅是为了修复安全或隐私错误。它们也可能旨在引入主要的新功能或提高性能和安全性。
- 消费者不太可能更新IoT设备软件：很少有最终用户持续一致地自行更新设备软件；最好假设大多数最终用户永远不会独自采取行动更新软件。

- 设备更换可能替代软件更新–
  对于廉价或“一次性”设备：在某些情况下，完全更换设备可能替代软件更新。某些物联网设备可能是如此廉价，以至于更新软件可能不切实际或不具有成本效益。

建议。 BITAG技术工作组还负责以下工作：

*建议：*

- 物联网设备应使用最佳最新软件实践：
  - 物联网设备应配备合理的最新软件：BITAG建议，物联网设备应使用不包含严重已知漏洞的合理最新软件交付客户或零售商店。
  - 物联网设备应具有自动安全进行软件更新的机制：应将软件错误减至最少，但不可避免。因此，对于物联网设备而言，拥有一种自动安全软件更新机制至关重要。
    BITAG建议，因此，物联网设备制造商或物联网服务提供商应基于会随着时间发现新漏洞和漏洞的设计其设备和系统。他们应设计系统和流程以确保自动更新物联网设备软件，而不需要或期望任何类型的用户操作甚至用户选择加入。
  - 物联网设备默认应使用强身份验证：BITAG建议物联网设备默认为安全保护（例如，密码保护），且不使用常见或容易猜到的用户名和密码（例如“admin”，“password”）。
  - 应对物联网设备配置进行测试和强化：某些物联网设备允许用户自定义设备的行为。BITAG建议制造商使用一系列可能的配置（而非简单的默认配置）测试每台设备的安全性。

- 物联网设备应遵循安全和密码学最佳实践：BITAG建议物联网设备制造商使用传输层安全（TLS）或轻量级密码术（LWC）保护通信安全。如果设备依靠公钥基础设施（PKI），则授权实体必须能够在证书遭到泄露时吊销证书，制造商应注意避免使用已知弱点的加密方法，协议和密钥大小。其他加密最佳实践包括：
    - 默认情况下加密配置（命令和控制）通信
    - 与物联网控制器之间的安全通信
    - 加密敏感数据的本地存储
    - 验证通信，软件更改和数据请求的身份
    - 对每个设备使用唯一凭证
    - 使用可以更新的凭证
    - 关闭不必要的端口并禁用不必要的服务
    - 使用积极维护和支持的库

- 物联网设备进行通信时应具有限制性而不是允许性：在可能的情况下，默认情况下不应通过入站连接访问设备。物联网设备不应仅依靠网络防火墙来限制通信，因为家庭内部设备之间的某些通信可能无法穿越防火墙。

- 如果互联网连接中断，则物联网设备应继续运行：BITAG建议，即使是未连接到互联网，因为从意外错误配置到故意攻击等原因，互联网连接可能会中断。对用户安全有影响的物联网设备应在断开连接操作下继续运行，以保护消费者安全。

- 如果云后端发生故障，则物联网设备应继续运行：当与云后端的连接处于连接状态时，许多依赖或使用云后端的服务可以继续运行，即使处于降级或部分运行状态。中断或服务本身失败。

- 物联网设备应支持寻址和命名最佳实践：许多物联网设备在安装后可能仍会部署数年。支持用于寻址和命名的最新协议将确保这些设备在未来几年内保持正常运行。
    - IPv6：BITAG建议物联网设备支持最新版本的互联网协议IPv6。

- 域名系统（SECSEC）：BITAG建议当使用域名时，IoT设备支持域名系统安全扩展（DNSSEC）的使用或验证。

- 物联网设备应附带易于查找和理解的隐私政策：BITAG建议物联网设备随附有隐私政策，但对于典型用户而言，该政策必须易于理解和理解。

- 披露远程降低物联网设备功能的权利：BITAG建议，如果第三方（如制造商或物联网服务提供商）可以远程降低物联网设备的功能，则应在用户当时明确这种可能性购买。

- 物联网设备行业应考虑行业网络安全计划：BITAG建议物联网设备行业或相关消费电子集团考虑创建行业支持计划，在该计划下可以贴上某种"安全物联网设备"徽标或标记。物联网零售包装。一组行业支持的最佳实践似乎是平衡物联网创新与与网络安全的流动性相关的安全挑战，并避免认证流程可能出现的"清单心态"的最实用方法。

- 物联网供应链应在解决物联网安全和隐私问题中发挥作用：物联网设备的最终用户依靠物联网供应链（从制造商到零售商）保护其安全和隐私，以及物联网供应链的某些或全部部分在产品的整个生命周期中发挥关键作用。除了本节中的其他建议外，BITAG还建议物联网供应链采取以下步骤：

    - 隐私权政策：设备应具有清晰易懂的隐私权政策，尤其是在与持续服务一起出售设备的情况下。

    - 重置机制：设备应具有针对物联网设备的重置机制，当用户退回或转售设备时，清除所有配置以供使用。设备制造商还应提供一种删除或重置各自设备存储在云中的数据的机制。

    - 错误报告系统：制造商应提供一个错误报告系统，具有定义明确的错误提交机制和文档化的响应策略。

    - 安全软件供应链：制造商应保护安全软件供应链，以防止在制造过程中引入恶意软件；供应商和制造商应采取适当措施保护其软件供应链。

- 在整个生命周期内支持物联网设备：制造商应在整个生命周期内为物联网设备提供支持，从设计到设备退役，包括透明地计划为设备提供持续支持的时间，以及消费者应在设备使用寿命到期时从设备功能中获得期望。
- 明确的联系方式：制造商应为消费者提供明确的方法，以确定可以联系谁获得支持，以及联系消费者的方法，传播有关软件漏洞或其他问题的信息。
- 报告漏洞的发现和补救：制造商应报告对消费者构成安全或隐私威胁的软件漏洞的发现和补救。
- 清晰的漏洞报告流程：制造商应提供漏洞报告流程，包括定义明确，易于查找且安全的漏洞报告表格以及成文的响应策略。

# 目录

# 1 引言

在过去几年中，许多连接到互联网的新设备不是个人计算机，而是嵌入了互联网连接和功能的各种设备。此类设备的示例包括恒温器，智能插头和网络摄像机。此类设备通常被称为物联网（IoT），很显然，未来几年，这类新设备将实现强劲增长，不同来源的估算数据也不同，但都预测有数十亿此类设备。到2020年，智能手机设备数量[1]。

物联网设备的数量和多样性正在迅速增长；这些设备为终端用户提供了许多新应用，将来还会提供更多应用。许多物联网解决方案已经提供或正在为不久的将来开发而部署，包括：

- 传感器更好地了解日常生活模式并监控健康
- 监控和控制家用功能，从锁到暖气和水系统
- 可以预期消费者需求并可以采取行动解决这些需求的设备和电器（例如，用于监控库存并自动为消费者重新订购产品的设备）

此外，结合数据分析和机器学习，物联网设备可以采取更主动的行动，展示有趣的数据模式，或向终端用户提出建议，改善他们的健康，环境，财务和生活的其他方面。

物联网的出现为从智能家居到智能城市的重大创新提供了机遇。不幸的是，许多物联网设备出厂时都存在严重的安全和隐私漏洞[2]；第3节详细讨论了许多最新示例。这些缺陷使最终购买设备的终端用户以多种方式面临风险，并可能影响设备用户和流量通过相同共享互联网链接运行的其他用户的互联网访问服务。这些缺陷还会为攻击目标，互联网服务提供商（ISP）以及其他服务提供商（例如搜索引擎服务，基于网络的电子邮件和游戏网站）带来更广泛的安全和缓解问题，并且重要地引入了新的支持和缓解成本（通常会传递给最终用户）[3]。设备制造商本身也可能需要承担额外费用，可能需要采取措施缓解这些问题。

在许多情况下，对设备开发，分配和维护流程进行直接更改，可以防止遭受重大安全和隐私问题的物联网设备分配。 BITAG相信，遵循本报告中概述的指导方针，可以极大地改善物联网设备的安全性和隐私性，并最大限度地减少与附带损害相关的成本，否则可能会影响最终用户和互联网服务提供商。此外，除非物联网设备部门（制造和分销这些设备的行业部门）提高了设备安全性和隐私性，否则消费者的强烈反对可能会阻碍物联网市场的增长，并最终限制物联网对最终用户的承诺。

# 2 什么是物联网？

物联网（IoT）由充当传感器，执行器，控制器和活动记录器的设备组成。这些设备通常会与网络其他地方运行的软件（如移动电话，通用计算设备（如笔记本电脑），公共互联网上的机器（如“云”中）或其组合）交互。其中。 物联网设备通常无需用户干预即可自主运行。 术语“物联网”具有潜在的广泛范围。物联网可以指在家庭，企业，制造设施，运输行业和其他地方的部署。因此，物联网可以指的不仅仅是简单的面向消费者的设
备。

在本报告中，术语“ 物联网”仅指面向消费者的设备及其关联的本地和远程软件系统1，尽管我们建议的部
分或全部建议可能更广泛地适用。此报告涉及消费者正在安装，配置和管理他们租赁或拥有的设备的场景。

## 2.1 范围限制

该报告未直接考虑用于工业或企业对企业设置的设备，如酒店或机场网络中的传感器，智能城市，工业自动化，商业建筑控制或制造库存控制。在这种情况下，客户通常会拥有资源和激励措施来指定和管理所购买产品的安全和隐私功能。此外，许多此类设备使用的商业无线连接不提供对互联网的完全访问权限。话虽这么说，在这些环境中也可能存在本报告中涉及的一些相同问题。

本报告的范围也仅限于发起或终止数据流的物联网设备。更具体地说，该报告没有重点关注通过流量的设备，这些流量可能包含去往或来自物联网设备的数据，以及其他流量，如家庭网关，无线接入点或路由器。

此外，该报告仅侧重于使用互联网协议（IP）的设备和系统，无论是IPv4还是IPv6或两者兼而有之。各种各样的物联网设备使用其他传输机制，例如Zigbee 1.0 [4]，X10 [5]等。这些设备只能通过执行协议转换的设备连接到互联网。它们在隔离的网络上运行。但是，此处的建议仍适用于执行协议转换的设备（例如，家庭自动化集线器或网关）。

本报告重点关注本地IP网络上可以通过Internet通信的设备特有的问题。孤立出现的隐私和安全问题

1当BITAG使用术语“软件”时，旨在包括设备固件（所有形式的软件）和所有其他类型的软件。

无法连接到公共互联网的网络不在本报告范围之内。

### 2.2 用户已修改的物联网设备

某些设备可以从制造商的角度更新软件或用制造商未指定的软件替换，从很多方面来说，它们都可以创造新产品。例如，用户可以在设备上安装开源软件，而不使用供应商提供的软件。最终产品可能会受到本报告的考虑和建议，但在这种情况下，应将设备视为用户负责的不同产品。

## 3 为什么特别关注物联网安全和隐私

物联网设备面临着许多传统最终用户设备面临的相同类型的安全和隐私挑战。另一方面，物联网设备通常既不提供清晰的控件也不提供文档，以通知用户部署这些设备时可能带来
的风险。此外，研究表明，依靠终端用户做出安全和隐私决策很容易失败[6,7,8]。

### 3.1 非技术或无兴趣的消费者。

最终用户不具备评估任何特定物联网设备的隐私和安全隐患的技术专长，或者可能对此缺乏兴趣[9]。此外，通常情况下，部署的设备缺乏执行安全更新或实施安全策略
的自动化机制[9,10]。

### 3.2 挑战性的设备发现和清单。

消费者已经难以识别和故障排除当前连接到家庭网络的设备[11]。随着消费者将越来越多的设备连接到家庭网络，物联网设备将加剧这种情况。 随着时间的推移，用户可能会失去对哪些设备连接到互联网的跟踪，这将使保护设备更具挑战性。此外，互联网服务提供商（ISP）将难以帮助消费者识别安全问题的根源。尽管互联网服务提供商（ISP）可以确定客户家庭网络上的某些设备受到威胁，但由于网络地址转换（NAT）等技术可能掩盖个人身份，因此他们可能无法识别特定的受感染设备 。设备。

### 3.3 对互联网访问服务的影响。

恶意软件入侵的物联网设备（请参阅第4.5和5.3节）可能会影响此类物联网设备用户和流量通过相同共享互联网链接运行的其他用户的互联网访问服务。这些设备也可能对用户和恶意软件的其他目标构成威胁[12]。这种恶意软件可用于发起分布式拒绝服务攻击[13],

发送垃圾邮件，攻击用户网络上的其他设备，或者恶意干扰用户的互联网访问服务。

这些问题增加了互联网服务提供商（ISP）的成本，互联网服务提供商（ISP）必须花大力气缓解这些攻击，为无法确定其互联网访问服务行为不良或异常的用户提供帮助台支持，甚至禁用其互联网访问服务的用户设备正在执行恶意网络活动。这些问题还会通过降低性能和增加证书丢失的可能性而增加消费者的成本。最后，它们针对任何此类攻击和物联网设备制造商本身（或物联网供应链的其他部分），向目标施加成本，可能需要采取措施缓解这些问题。

### 3.4 对其他服务的影响。

被恶意软件入侵的物联网设备可能成为垃圾邮件和拒绝服务攻击（包括反射和放大攻击）等有害流量的平台，攻击者借此以受害者源地址欺骗的形式向设备发送流量，从而导致设备向受害者发送大量流量）[14] –可能会干扰服务提供商交付服务的能力[15]。遭到破坏的设备还可以用于窃听本地网络流量，或充当“垫脚石”，攻击客户本地网络上的其他设备和服务，造成数据泄漏的可能性 。提供搜索引擎，基于网络的电子邮件和游戏网站等服务的提供商必须投入资源以缓解这些攻击。这些攻击的受害者还将承担财务和隐私费用。受损的物联网设备有时还会影响服务提供商的业务模型。一个例子就是域名系统域名更改器（DNSChanger）恶意软件，攻击者可以利用它在受害者的网页中插入自己的广告[16]。

## 4 许多设备不遵循安全和隐私最佳实践

物联网设备已经成为滥用和攻击平台。许多技术人员发现了与现在可用的物联网设备相关的各种安全和隐私风险[17,18,19,20,21,22,23,24]。在未来几年内，可能会再部署数以千万计的物联网设备，从而有可能成为发动攻击的大型平台（既攻击用户家里的其他设备，也广泛传播整个互联网），并秘密收集有关特定的最终用户或用户组。 除了消费者可能遭受的损失外，互联网服务提供商可能会继续增加技术支持电话和攻击事件，从而增加传递给消费者的运营成本。

最近的几份报告研究了物联网设备的安全和隐私特征，发现一些设备不遵守基本的隐私和安全最佳实践[25,26,27,28,29,30,31]。在某些情况下，设备会受到威胁[32]。

导致缺乏隐私和安全最佳实践的潜在问题包括：

### 4.1 首次销售后缺乏开发和部署更新的动机

对于通过零售渠道出售的消费者物联网设备，设备供应商可能没有动力在首次销售后交付软件更新。如果设备的收入仅来自首次销售，那么设备的任何维护都会侵蚀该初始收入，从而降低利润。这种结构可以鼓励有计划的淘汰，供应商将新设备的销售优先于支持现有设备的设备。

### 4.2 安全的网络软件更新困难

物联网设备可能未设计和配置为通过网络接收安全软件更新，导致繁琐的更新过程。

### 4.3 设备资源受限

在利润率较低的消费环境下出售的物联网设备可能设计有限的硬件资源。结果，某些基本安全措施（如加密，软件签名验证和安全访问控制）不可行。因此，限制设备处理和存储能力的设计可能会阻止运行基于主机的安全软件或阻止对其进行安全升级。第5.1节更详细地讨论了这个问题。

### 4.4 接口受限的设备

许多类型的物联网设备具有有限或不存在的用户界面。即使设备通过辅助设备（例如，智能手机应用程序）公开用户界面，其功能也可能很小。因此，可能无法完成配置本地防火墙或禁用远程服务之类的任务。设备还可能无法显示有意义的错误状况，并向可能使用错误信息更好地保护设备的用户发出警报。

### 4.5 在制造过程中插入了恶意软件的设备。

制造商或其他有权进入制造或包装环境的员工可以在制造或包装时将恶意软件插入设备。受到感染的设备通常看起来似乎在正常运行，在这种情况下，安全或隐私违规行为可能会一直持续到检测到入侵为止。防火墙和网络隔离无法防御此类受损设备对隔离网络内部其他设备发起的攻击。有关此类受损设备的已知示例以及对恶意软件影响的更多讨论，请参见第5.3节。

### 4.6 缺乏制造商在安全性和隐私方面的经验

许多物联网设备制造商（以及物联网供应链的其他部分）没有设计，开发或维护互联网连接设备的经验，或者

处理消费者数据。这些制造商通常缺乏安全开发生命周期，事件响应团队以及隐私和安全工程经验。

### 4.7 易受攻击的设备引起的风险

以下示例说明了当物联网设备变得容易受到安全和隐私攻击时可能出现的问题的范围和程度。未经授权的用户可能能够：

- **执行未经授权的监视和监控。**
  - 知道一个特定的人是否在家，他们住什么房间，什么时候进入家
  - 了解其他哪些设备连接到家庭网络，以及用户如何与之交互
  - 远程激活设备上的麦克风或相机以窃听或监视某人[33]
  - 发现最近是否已打开和关闭门或车库，以确定是否有人在家中，以帮助进行物理入侵
  - 在物联网摄像头上安装恶意软件以访问摄像头的视频供稿[34]
- **获得未经授权的访问或控制。**
  - 在冬季，关闭恒温器，导致水管爆裂，对房屋造成伤害
  - 打开或关闭灯光，例如关闭外围照明设备以协助物理侵入
  - 解锁门以帮助物理入侵
  - 抑制门或窗户传感器发出的警报
  - 改变用于非法使用的设备的用途（例如，作为比特币矿工[35]）
- **导致设备或系统故障。**
  - 激活住宅空调系统，在电网上产生意想不到的电涌，试图创建节电或停电条件
  - 颠覆健康数据收集传感器，修改可能传输到健康监测服务或医疗设备（如胰岛素泵）的健康数据，如血压，血糖或体重信息

- 模拟设备的管理软件，使其看起来正常运行，但禁用重要功能或进行其他操作更改，导致设备或硬件系统以重要方式失效[36]
- 防止温度调节器控制建筑物的采暖或制冷，从而导致过热或过冷

- **干扰或骚扰用户。**
  - 远程激活扬声器并进行口头威胁或骚扰
  - 激活烟雾或其他安全警报

所有这些情况都会给最终用户和整个互联网造成严重的隐私和安全风险。某些最终用户安全和隐私风险也可能启用一种新形式的数字骚扰。在极端情况下，颠覆健康数据收集可能导致受伤或死亡。对于广泛部署的设备，成百上千的设备可能面临安全隐患，对关键基础设施造成分布式攻击。

物联网设备的安全和隐私问题最终可能会限制物联网行业的未来增长。少数引人注目的事件可能会降低对物联网设备的需求，或以其他方式限制物联网的增长和潜力。因此，解决这些问题对于支持物联网市场的长期健康，活力和增长至关重要。

## 5 关于物联网安全和隐私问题的意见

期望制造商创建无错误的软件产品是不现实的。所有软件均存在错误，而生产没有此类缺陷的软件仍未解决。结果，一些物联网设备“出厂”时软件已过时或过时。这与运送越野车软件无关，可以避免。相反，令人担忧的是，制造商可能会在运输设备时使用过时的软件，其中包含许多已记录的重要安全漏洞，其中一些可能会在设备首次连接到互联网后立即被利用[37]。

其他物联网设备可能随附了更新的软件，在发行时不包含主要的已知安全漏洞。即使在这些情况下，将来也可能会发现漏洞，除非设备具有随后更新其软件的机制，否则可能会逐渐降低设备的安全性。不幸的是，许多物联网设备缺乏安全的自动化软件更新机制，一旦设备就可以修补漏洞

2如果不广泛采用安全，自动化的软件更新方法，则在未来几年中，不安全和受到攻击的物联网设备数量可能会急剧增加。

带有安全和隐私问题或随着时间的推移而发展的物联网设备可以创建一批新的设备，供恶意黑客使用，例如进行反射和放大攻击[41]。这些设备不仅会对设备所有者本身构成风险，还可以被利用来滥用其他各方。因此，不仅物联网设备的制造商（以及物联网供应链的其他部分）和客户都对物联网设备的安全感兴趣，而且整个互联网也都对此感兴趣。

最后，尽管本报告提供了很多物联网应用设备曾经或曾经存在安全或隐私问题的例子，但在很多情况下，相关各方在本报告发布之前已经解决了此处强调的例子。

### 5.1 不安全的网络通信

物联网设备总体上可能会受到资源限制，缺乏第4节中讨论的移动电话，笔记本电脑和台式计算机等更传统的计算设备的计算能力和带宽。因此，许多安全功能是为更多的通用计算设备更难以在物联网设备上实现。例如，基于某些传输受限的物联网设备，基于传输层安全（TLS）[42]和数据报传输层安全（DTLS）[43]的现代安全通信基础上的公钥加密可能很难实现。例如，Arduino和Raspberry Pi设备可能需要数秒钟才能执行不对称加密或解密操作[44,45]。

除了物联网设备及其运行的物联网平台固有的局限性之外，现场还发现了许多安全漏洞，包括未加密通信，物联网设备数据泄漏以及对连接物联网设备的网络的负面影响[25,26,27,46,47]。

例如，某些TLS服务器实施很容易受到所谓的“降级”攻击，攻击者可以迫使服务器使用旧版本的TLS协议，TLS协议可能存在已知的安全问题，例如人身安全漏洞。中间攻击。在这些情况下，可能会损害物联网设备与支持该设备的云托管服务之间的通信。

- **未认证通信**

一些物联网设备提供自动软件更新。但是，如果没有身份验证和加密，这种方法是不够的，因为可能会损害或禁用更新机制[48]。更新机制本身和任何关联的命令

2在最近的大规模分布式拒绝服务针对krebsonsecurity.com网站引用的IoT摄像头是大华安全生产的。该公司发布了一份建议书[38]，建议设备所有者下载并更新固件[39]，并采取其他措施保护设备（大华安全默认不完成）[40]。

3不幸的是，许多物联网设备在通信过程中并未使用身份验证。例如，Lightwave RF Smart集线器每次重启时向网络上的远程服务器发送流量，随后每十五分钟检查一次软件更新[29]。如果连接不安全，具有网络访问权限的攻击者就可以发起中间人攻击。

- 未加密通信

许多物联网设备以明文形式而非加密形式发送部分或全部数据。这意味着数据可能“泄漏”并被其他设备或攻击者观察。

结果，一些物联网设备泄漏用户信息（例如，泄漏给网络流量观察者），这可以识别正在使用的物联网设备，并揭示当前用户活动和行为[17]。 4例如：

- 数码相框在同步照片时会以明文形式承载用户的电子邮件地址，当前用户活动也会以明文形式显示[10]。
- 网络摄像头以明文形式发送视频文件[29]。
- 音频个人助理以明文形式承载用户音频命令，传感器读数和用户电子邮件地址[29]。
- 温控器以明文形式保存本地天气数据和准确的用户位置信息，并根据使用的端口明确标识为特定品牌的温控器。5
- 物联网设备集线器具有明文流量配置文件，其规则性和特异性如此之高，仅通过对明文流量模式进行指纹识别即可识别设备集线器[29]。
- 一些支持物联网的起搏器使用未加密的通信通道[52]。

不建议在新部署中使用明文发送流量，否则会造成本地或互联网上的个人信息或其他信息泄漏的问题。例如，在这个问题上，互联网体系结构委员会（IAB）表示：“IAB敦促协议设计人员默认为机密操作进行设计……强烈鼓励开发人员在实现中纳入加密措施，并使其实现默认情况下加密。” [53]

3消息完整性：接收消息的端点可以验证消息在发送方和接收方之间的传输过程中没有被修改。
4可以识别设备或识别用户活动和正常行为不一定负面。为此可能存在合法的安全原因，可以为最终用户带来好处并总体上提高安全性和隐私性。
5在最近的一次涉及Nest恒温器的案例中，研究人员向Nest报告了此错误后，此错误已修复。
Nest恒温器可以执行自动软件更新[49,50]。不幸的是，自动更新本身引入了一系列不同的问题[51]。

- **缺乏相互认证和授权**

许多攻击源自家庭或其他地方网络边界的防火墙后面。因此，防火墙后的通信不一定被认为是可信赖的。因此，无论设备是在局域网还是在互联网上，设备都需要在设备之间建立信任。应假定默认情况下其他设备不受信任，并且应进行显式验证和授权。如果设备允许未知或未经授权的方更改其代码或配置或访问其数据，则是一种威胁；设备可以显示所有者存在或不在场，促进恶意软件的安装或运行，或从根本上破坏核心物联网功能。

幸运的是，与可能与许多互联网目的地通信的笔记本电脑等通用计算设备相比，物联网设备通常与少量定义明确的目的地通信。例如，设备只能与具有众所周知的域名系统（DNS）名称或IP地址的控制或更新服务器进行定期通信；可能会引起关注与其他目的地的大量通信。

- **缺乏网络隔离**

除了物联网设备在安装了物联网设备本身的家庭网络之外引入的安全和隐私风险（请参阅第4节）之外，这些设备还带来新的风险，并容易受到家庭内部攻击。由于默认情况下许多家庭网络不会将网络的不同部分相互隔离，因此网络连接的设备可能能够观察或交换同一家庭网络上的其他设备的流量，从而使一台设备可以观察或影响不相关设备的行为。

尽管通常使用防火墙将网络上的设备相互隔离，但仅靠防火墙无法始终抵御设备入侵或数据泄漏，也无法抵御家庭网络内部设备上的恶意软件。当今，典型的家庭网络几乎无法提供设备之间的隔离。第6节更详细地讨论了防火墙和其他网络隔离机制。

由于制造商的特定行动（或物联网供应链中其他各方的行动），以及设备遭到破坏，这种缺乏隔离性会对网络上所有设备的安全和隐私构成威胁[27,54,
55]。具体而言，攻击者可能能够从同一网络上的其他设备收集情报或个人信息。通常，家庭网络中的每台设备都可以看到来自同一网络上其他设备的流量。如果设备以明文传输流量，则一台设备可能能够发现另一台设备的活动的详细信息。最近的工作表明，即使能够观察更多“粗略”细节（如域名系统（DNS）查找和流量变化），也可能会泄露有关设备活动和用户行为的信息[56]。因此，攻击到一台设备的攻击者可能能够推断出有关终端用户的重要信息，例如，通过受损的门传感器或物联网设备中嵌入的麦克风和摄像机的音频和视频记录，进入和离开家庭的时间。许多家庭无线网络的安全设计能够实现“垫脚石”攻击[57]，攻击者可能会攻击一个易受攻击的物联网设备，并使用该设备

妥协是一种从网络内部访问其他连接设备的机制。示例包括：

- 智能手表产品包括一个正常运行的域名系统（DNS）服务器，外部攻击者可以使用该服务器攻击智能手表所连接的网络上的其他设备。同一产品存在一个漏洞，允许外部网络攻击者查看本地网络流量[27]。
- 可以诱骗智能灯泡发送无线网络凭证，然后外部攻击者可以使用这些凭证控制灯并查看本地网络流量[54]。
- 一些设备制造商和互联网服务提供商（ISP）公开了数百万个共享同一已知私钥的设备和客户端设备（如调制解调器，家用路由器）的不安全远程管理接口，使这些设备暴露于被动和主动人工干预中间攻击[55]。
- 某些型号的VoIP电话漏洞会使本地网络攻击者向电话提供恶意固件升级[58]。
- 一家Wi-Fi安全摄像头制造商使用对等网络软件设计产品，这种软件会“打通”本地网络防火墙中的多个漏洞，而且不容易停用。该软件使攻击者不仅可以从各种各样的端点攻击摄像机本身，还可以对本地网络上的其他设备发起攻击[31]。

## 5.2 数据泄漏

在家中安装物联网设备可能会导致这些设备从云（存储数据）和物联网设备自身之间泄漏私人用户数据。

### ▪ 云泄漏

物联网设备收集的大部分数据当前存储在家庭外部的云服务中；这些云服务可能会由于外部攻击或内部威胁而遭受数据泄露。

此外，如果用户对这些云托管服务依赖弱认证或加密方法，用户数据也可能会受到威胁。

一些示例包括：

- 与泰迪熊（鼻子上装有小型摄像头）相关的网络应用程序包含一个安全漏洞，使儿童的身份暴露无遗[59]。
- 玩偶使用的TLS版本很容易受到降级攻击，因此在玩偶和云托管服务器之间发送了加密聊天记录，有可能窃听儿童的录音[60]。

- 儿童玩具制造商的数据泄露事件暴露了超过六百万名儿童的个人数据[61]。
- 机动车辆Wi-Fi接入点配置不足，导致在收集Wi-Fi接入点名称及其位置的网站上跟踪了许多车辆位置[62]。
- 汽车制造商的系统以明文形式向中央服务器发送了燃油经济性统计信息，精确的地理坐标，速度，方向和目的地[63]。

这些设备存在许多其他数据泄露示例[25,28,30,32,64,65,66,67]。来自云计算的数据泄漏并不是新出现的，还是不是特定于物联网设备的，但对于托管和消费个人物联网设备而言，云托管服务中数据泄漏漏洞的普遍存在尤其成问题。

- **设备之间的泄漏**

运行许多不同软件应用程序的来自不同制造商的物联网设备可能都驻留在同一局域网中。尽管标准的Wi-Fi加密技术可以保护局域网上数据传输的机密性，但仅加密并不能确保用户隐私。

在某些情况下，同一网络或相邻网络上的设备可能能够观察来自其他设备的数据。例如，设备可能会将数据“泄漏”给附近的设备或用户（在同一局域网，Wi-Fi网络上，或就在附近）。即使使用Wi-Fi加密，一台设备仍然可以观察到同一局域网中其他设备的存在，而另一台设备的硬件地址（通常可以揭示设备的类型）通常也以明文显示。这种可见程度，例如，可以使数码相框上的软件监视用户与同一网络上其他设备的交互。

从一台设备泄漏到另一台设备的数据可能包括诸如房屋名称，房屋的精确地理位置甚至消费者购买的产品之类的信息。例如，最近的一项研究发现，恒温器正在从家里泄漏精确的地理信息[17]。在另一项最新研究中，研究人员能够根据从健身追踪设备通过蓝牙泄漏的加速度计数据确定用户的ATM PIN [68]。

### 5.3 恶意软件感染和其他滥用行为的易感性

恶意软件是一种安装在用户设备上的恶意软件，通常会破坏操作，获得未经授权的访问或发起攻击，可通过多种机制感染物联网设备。同样，还可能发生其他形式的滥用。一些示例包括：

- 制造商可能无法充分保护软件供应链[69]，从而无法将恶意软件放置在物联网设备[34]初始发货软件上，如第4.5节所述。

- 设备可能随附包含已知漏洞的过时软件。当用户将设备连接到网络时，设备立即成为攻击者的目标。过去的研究表明，在某些情况下，“生存时间”（即设备感染网络之前连接到网络的时间）可能少于十分钟[70]。6如果设备出厂时日期软件，并且不会立即检查软件更新，否则有被立即感染的风险。
- 软件更新机制可能不包括软件负载验证，以确保软件来自受信任来源。通过社会工程，可以影响或诱使用户将受感染的软件加载到物联网设备上。
- 该软件可能包括命令行功能或应用程序编程接口（API），可以利用这些功能（有或没有用户参与）将恶意软件加载到物联网设备上。
- 设备的不必要端口处于打开状态和不安全状态，例如远程登录。这些不必要的端口已被用于危及设备，例如，指示设备访问目的地以下载恶意软件[71,72,73]。不必要的端口也可以用于放大攻击。
- 设备使用弱默认身份验证，例如常见或容易猜到的用户名和密码（例如“admin”，“password”）[74]。此外，可能无法确保远程访问身份验证的安全性，从而使不在屋子里的其他人登录设备并在设备上安装恶意软件[13,75,76,77,78]。

### 5.4 潜在的服务中断

物联网设备安全性的重要方面是面对设备故障和攻击时的服务可用性。潜在的可用性或连通性丧失，不仅会降低物联网设备的功能，而且在某些情况下（例如，如果物联网设备如果没有此类连接就无法运行）可能会降低设备的安全性。丢失）。物联网设备可以通过几种方式遇到服务中断。

- **云托管应用程序失去支持。如果设备依赖与云服务的通信，则当设备与云服务失去连接时，可能无法正常运行。出现这种断开连接的原因可能多种多样，包括互联网连接中断，云软件服务中的错误，供应商或制造商倒闭或消费者决定中止服务订阅。**

6防火墙的存在并不一定能防御这种危害。第6节更详细地讨论了防火墙和其他网络隔离机制。

- 失去网络连接。例如，可能是由于拔下电源线，对Wi-Fi的无线电干扰或防火墙决定限制访问，家庭网络内的连接可能会中断。
- 损坏设备。设备可能会受到物理损坏，或者其软件可能会损坏或以其他方式无法运行（有时称为“桥接”设备）。

“实体”或“逻辑”损坏的“实体”设备可能无法恢复，而与云托管服务通信的设备可能会在恢复通信后恢复运行。

某些服务中断可能会损坏财产，并使用户面临危险。例如，物联网恒温器的软件错误导致家庭供暖系统无法运行，并因此导致房屋管道冻结[51]。加热和冷却系统故障可能导致死亡。当物联网设备负责从个人健康到家庭安全的所有事务时，用户安全的风险就很高。

### 5.5 设备安全和隐私问题将持续存在的可能性

本节简要讨论了上一节概述的安全问题为何可能持续存在。可以预期，由于制造商（或物联网供应链的另一方，或物联网服务提供商）可能不提供更新，或消费者可能不应用已经可用的更新，因此许多此类物联网设备可能永远不会收到软件更新。
。类似类型的设备有很多例子[79,80,81,82]。

- 许多物联网设备将永远无法修复

通常，部署修补关键安全漏洞的软件更新很困难，但物联网设备面临着独特的挑战。首先，许多设备供应商和制造商没有将软件更新部署到数千个设备（或更多设备）的系统或流程。其次，很难为在家用住宅中运行的设备部署网络更新，因为更新有时会中断服务，并且如果配置不当，可能会“砖化”设备。此外，某些设备甚至可能无法进行软件更新[83]。

消费电子行业出现了三种软件更新方法，其中两种依靠用户采取措施（一个基本缺陷），而第三种则是自动进行的，无需用户采取任何措施。在实践中，每种方法的有效性各不相同。这些方法如下：

- 用户启动的软件更新。这种方法要求设备的本地管理员手动启动对设备的任何软件更新的检查和安装。这种模式的一个例子是在典型的零售家庭网关或路由器设备市场。其中一些设备要求用户从制造商的网站下载新的软件映像，然后访问本地设备管理网页，找到软件升级界面并上传

文件。此过程不仅耗时，而且对于设备仍可能“足够好”运行的非技术或临时用户而言，可能会令人生畏。

- **在用户批准下，自动进行软件更新检查。这些设备会定期检查新软件更新。当有可用更新时，设备会向用户显示提示，询问是否允许继续进行更新。智能电视和控制台游戏设备通常使用这种方法。在这些情况下，应用任何特定的软件更新可能需要几分钟甚至更长的时间，这就是为什么向用户提供推迟安装选项的原因。**

- **全自动软件更新。某些设备会定期检查是否有新软件。如果是这样，他们将下载软件并进行安装，而无需用户干预[84,85]。在某些情况下，设备可以在一天的特定时间（例如深夜）或在一段时间内没有任何与设备有关的活动应用更新，以最大程度地减少用户干扰。不幸的是，对于一些拥有数据上限的用户（如适用），以及当更新本身引入新的错误时，自动化软件更新也可能会带来挑战[51]。**

常见的软件更新方法是用户发起或用户批准的，这两种方法都会导致相对较低的更新率[86]。因此，数百万客户拥有和维护的（COAM）家庭网关可能永远不会收到软件更新。例如，某些型号的NetGear家庭网关附带软件错误，导致这些设备每秒以数千个域名系统请求（每天多达数百万个）随机泛洪ISP DNS服务器，或向NTP服务器泛洪NTP查询[87,88,89,90]。尽管已经报告了这种特定的软件错误很多年，但网络运营商仍然可以观察到这些设备运行较旧的软件并且在网络上行为异常，由于软件错误无意中执行了分布式拒绝服务攻击。

- **软件更新解决的不仅仅是错误**

还需要记住的是，软件更新不仅仅是为了修复安全或隐私错误。它们也可能旨在引入主要的新功能。另外，它们可能更一般地与性能和安全性相关，例如与IPv6寻址，域名系统安全扩展（DNSSEC）验证和TCP缓冲区控制（例如“缓冲区膨胀”）或活动队列管理（AQM）。

- **消费者不太可能更新IoT设备软件**

很少有最终用户持续不断地自行更新设备软件，除非设备的图形用户界面（GUI）不断提醒用户这样做（即，PC上的常规弹出窗口，移动应用商店中的计数器），弹跳应用程序图标等），在人机交互学科中很好地理解这一课[86]。最近的其他工作表明，用户出于各种原因放弃在固定和移动设备上应用软件更新，包括工作周期中断到与软件更新相关的数据成本[86]。

尽管尚未针对物联网设备对用户软件更新行为进行深入研究，但其状况可能比传统或非物联网设备差。加上用户在软件更新方面本该具有风险的行为，许多物联网设备缺少GUI或其他指示器，表明新软件可用或必要。此外，设备数量（种类繁多）的激增，对于典型的互联网用户而言，更新跟踪软件成为一项艰巨的任务。

因此，对于物联网设备，最好假设大多数终端用户永远不会独自采取行动更新设备上的软件。

### 5.6 设备更换可能替代软件更新

在某些情况下，完全替换设备可能是软件更新的替代选择。某些物联网设备可能是如此廉价，以至于更新软件可能不切实际或不具有成本效益。例如，也许价格为0.99美元的充电适配器具有有限的物联网功能。以该单位成本计算，更新设备可能并不经济。相反，回收设备并购买替换产品可能更有意义。但是，这种方法需要以下要素才能提供安全的软件更新替代方案：

- 一种识别设备中一个或多个累积漏洞何时已经危及到应更换设备的方式。
- 一旦确定存在漏洞，一种禁用与设备通信的方法。潜在方法的示例包括从网络远程禁用设备，或阻止从家庭网关访问设备。
- 通知用户已禁用与设备通信的一种方法。

当然，即使在这些情况下，只要设备部分运行，用户可能仍然不愿意停止使用设备。但是，只要设备的通信能力被禁用，继续使用就不会构成安全漏洞。

## 6 家用网络技术的可能角色

默认情况下，设备制造商保护设备安全是改善IoT安全和隐私的重要一步，但这还远远不够。即使未感染恶意软件的物联网设备也可能会窃听其他家庭网络流量（例如，通过制造商安装的或第三方软件），从而危及用户隐私。家庭通常被认为是防火墙或隔离环境，并且多个不相关的物联网设备通常在该防火墙后面具有不受限制的访问。此外，如第3.4节和第5.1节所述，家庭网络中单个不安全或受损的设备可能会导致踏脚石攻击，因此“纵深防御”[91]至关重要。

最近的研究和报告表明，未来，家用网络设备可能会控制和管理物联网设备相互之间以及与其余互联网交换的流量[92]。这种网络设备可能的功能包括：

- 自动发现和清点室内互联网连接设备[93]。
- 向用户呈现清晰信息的机制，包括：（1）设备向互联网其余部分发送哪些数据；（2）该设备与之交谈的家庭其他设备（如过去针对智能手机和浏览器[94,95]。
- 一种机制，为用户提供简单的方法，以防止或禁用单个设备与家庭网络上的其他IoT设备通信或与云中的存储服务器通信，而不会损害设备的主要功能。最近的一项研究使用两个示例物联网设备，飞利浦色相灯泡和Nest恒温器实现了这一目标[92]。

改善安全性和隐私性的网络技术最终可能采用以下几种形式之一。单独的（例如，物联网中心或单独的家用路由器）或与ISP提供的设备集成的家庭网络网关可以在网络内执行测量，帮助用户了解家庭内物联网设备之间以及这些设备之间的复杂数据流设备以及家庭外第三方站点和服务。从这个意义上讲，监控设备流量的家庭网络技术最终可以帮助提高这些Io T设备行为的透明度。

在由集线器监控和管理物联网流量与流量本身的端到端安全性之间存在一些冲突。值得注意的是，即使这些设备之间的网络流量是端到端加密的，某些特征（例如其他设备和与任何特定设备通信的位置）仍然可以从该流量中明显看出。标准化后，通过此类物联网中心进行协作流量分类和保护，可以使设备成为生态系统中公认的身份验证部分，并为管理人员提供基于选择加入的细粒度控制。

除了简单地帮助可视化这些流量，此类网关还可以强制实施合理的默认设置，以提高连接的物联网设备的安全性和隐私性。例如，最近的研究表明，家庭网络防火墙可以防止某些设备向第三方云提供商泄露日志和其他信息，而不会削弱设备本身的功能[92]。一个悬而未决的问题涉及确定合理的默认防火墙设置，可以将其安装在此类网关上，以提高安全性和隐私性。鉴于这样的家庭网络防火墙可能会引发“隐私军备竞赛”（例如，可以想象设备制造商没有向阻止设备跟踪功能的用户提供安全更新），最终制造商和供应商的设备认证可能会在一方面包括确保消费者保留关于这些设备如何与第三方站点和服务通信的知情选择。

最后，物联网设备之间的交互可能需要更复杂的中介。例如，尽管用户通常可能不希望某些设备相互通信或交互，但可能会有特定的使用案例，允许特定任务的设备之间进行通信或交互。举一个可能的例子，考虑一种场景，用户可能希望在看电影时自动调暗灯光。

家。在这种情况下，应用程序可能会涉及流设备（例如Roku或Apple TV）和智能插头和交换机（例如Belkin WeMo交换机）之间的中介通信。另一方面，通常来说，用户可能不希望这些设备进行交互甚至观察对方的流量。因此，网络网关结合适当的用户界面，最终可以为此类复杂的中介互动提供更好的机会。

最近的报告表明，其中许多目标很可能实现。例如，研究人员使用家庭网络防火墙阻止Nest恒温器将状态日志发送到云，而不会损害设备本身[92]。但是，由于一般用户不太可能配置防火墙规则，因此在认为实用之前，此类防火墙功能必须更可用（如有可能，还应自动化）。

# 7 建议

报告的这一部分介绍了BITAG技术工作组（TWG）的建议。尽管本报告前面的部分讨论了长期，前瞻性解决方案的潜力（例如，家用网络技术在缓解设备不安全性方面的作用），但本节重点关注BITAG认为在短期内可行的建议使用现有技术。

## 7.1 物联网设备应使用最新的最佳软件实践

- **物联网设备应配备合理的最新软件**

  BITAG建议，物联网设备应使用不包含严重已知漏洞的合理最新软件运送到客户或零售商店。但是，软件错误在某种程度上是“生活中的事实”，在设备搁置后发现新漏洞的情况并不少见。因此，对于物联网设备而言，至关重要的是要有一种机制，使设备可以接收安全的自动软件更新（请参阅下一个项目符号）。

- **物联网设备应具有自动安全更新软件的机制**

  应尽量减少软件错误，但如上所述，它们是不可避免的。因此，如第5.5节所述，对于物联网设备而言，拥有一种用于自动安全进行软件更新的机制至关重要。

  BITAG建议，因此，物联网设备制造商或物联网服务提供商应基于会随着时间发现新漏洞和漏洞的设计其设备和系统。他们应设计系统和流程以确保自动更新物联网设备软件，而不需要或期望任何类型的用户操作甚至用户选择加入。

尽管对于终端用户而言，此类更新应该是自动的和强制性的，但如果出于某种原因，更新系统必须允许选择退出或选择加入，那么根据人机交互研究，任何此类系统均应选择-因此，默认情况下将自动进行更新，而无需用户干预，用户批准或其他最终用户操作。用户配置软件更新性质的能力对于某些最终用户而言可能至关重要，例如那些在资源受限设置下运行设备的用户（例如，卫星连接或其他数据成本较高的地方）。
在某些情况下，家庭内部网络设备可能会与消费者互动，发出定期警报，促进做出有意义的决策（例如，向用户询问他们可以理解的设备互动方式问题）。集成此类功能需要在设计时格外小心，以确保向用户发出的这些警报有意义，并且更新数量不占优势。可靠地实现此类功能可能会很复杂 。

- **物联网设备默认应使用强身份验证**

BITAG建议默认情况下保护物联网设备（例如，密码保护），并且不要使用常见或容易猜测的用户名和密码（例如“ admin”，“ password”）。最后，应该确保对远程访问的身份验证，因为它有可能允许不在屋子里的其他人监视和控制屋内的各个方面（例如，更改气候控制，监控用户活动）。 认证凭证对于每个设备应该是唯一的。

满足这些条件的可能的默认身份验证方法包括：

（1）为每台设备提供固定的默认密码，但要求用户在安装过程中（即在设备正常运行之前）进行更改；
（2）为每台设备运送每台设备唯一的密码，并将密码打印在设备的标签上。

- **物联网设备配置应进行测试和强化**

一些物联网设备允许用户自定义设备的行为。
BITAG建议制造商使用一系列可能的配置（而非简单的默认配置）测试每台设备的安全性。设备界面应防止（或至少积极劝阻）用户以降低安全性的方式配置设备。

## 7.2 物联网设备应遵循安全和密码学最佳实践

BITAG建议物联网设备制造商使用传输层安全（TLS）或轻量级密码术（LWC）保护通信安全[ 96,97,98]。有些设备可以近实时执行对称密钥加密。此外，轻量级密码技术（LWC）提供了其他选项，可确保往返资源-

受限设备。如果设备依靠公钥基础设施（PKI），则授权实体必须能够在证书被泄露时吊销证书，就像网络浏览器和PC操作系统一样[99,100,101,102,103,104,105]。云服务可以通过参与证书透明性来增强证书颁发机构颁发的证书的完整性[106]。最后，制造商应注意避免使用已知弱点的加密方法，协议和密钥大小。

依靠云托管的物联网设备支持的供应商应配置服务器以遵循最佳实践，例如将TLS实施配置为仅接受最新的TLS协议版本。

- **默认情况下加密配置（命令和控制）通信**

  如第5.1节所述，使用未经身份验证或明文通信管理设备会带来重大安全风险。 BITAG建议所有用于设备管理的通信均通过经过身份验证和安全的通道
  进行。

**与物联网控制器之间的安全通信**

- 如果物联网设备使用集中控制器促进与云服务的互联网通信，那么BITAG建议双向确保此通信通道安全。

**加密敏感数据的本地存储**

- BITAG建议将任何敏感或机密数据（例如，私钥，预共享密钥，用户或设施信息）驻留在加密存储中。

**验证通信，软件更改和数据请求的身份**

- BITAG建议物联网设备对与其通信的端点进行身份验证。对通信进行身份验证需要验证端点的身份，而这又需要验证端点使用的证书是由设备信任的证书颁发机构签署的，但尚未撤销。

**对每个设备使用唯一凭证**

- BITAG建议每台设备都有唯一的凭证。如果设备使用公钥加密技术（例如，签署消息，交换会话密钥或对自身进行身份验证），则每台设备应具有唯一的可验证证书。如果设备使用对称密钥加密，则端点对绝不能与其他方共享对称密钥。

**使用可以更新的凭证**

- BITAG建议设备制造商支持一种安全机制，可以更新设备使用的凭证。但是，

安全地实施此建议需要特别注意，因为错误的实施本身可能会引入新的攻击媒介。

- **关闭不必要的端口并禁用不必要的服务**

  BITAG建议设备制造商关闭不必要的端口，如远程登录，因为不必要的端口可能不安全或可能受到威胁[107]。设备应关闭或禁用未使用的管理接口和功能。设备也不应附带未使用的驱动程序。

- **使用积极维护和支持的库**

  本报告中的许多建议都要求实施安全通信渠道。然而，本地实施的加密协议和安全通信通道本身可能会引入漏洞。
  BITAG建议，在实施本报告中的建议时，设备制造商应尽可能使用积极支持和维护的库和框架。

### 7.3 物联网设备进行通信时应限制而不是允许

BITAG建议物联网设备仅与可信端点通信。如果可能，默认情况下不应通过入站连接访问设备 。物联网设备不应仅依靠网络防火墙来限制通信，因为家庭内部设备之间的某些通信不一定会穿越防火墙。

请注意，BITAG建议限制物联网设备通信的配置不应以开放生态系统为代价。用户应能够配置任意物联网设备之间的通信，并且应允许彼此信任的设备进行通信。安全通信可以引导受限的信任列表，这些信任列表反映任何给定设备期望与之通信的设备集。这些设备间通信仅应通过可信机制和安全通信通道允许。

### 7.4 如果互联网连接中断，物联网设备应继续运行

BITAG建议，即使未连接互联网，物联网设备也应能够执行其一项或多项主要功能（例如，电灯开关或恒温器应继续使用手动控制功能）。这是因为互联网连接可能会由于意外配置错误或故意攻击（例如，拒绝服务攻击）等原因而中断；面对这些类型的连接中断，设备功能应强大。

对用户安全有影响的物联网设备应在断开连接操作下继续运行，以保护消费者安全。在这种情况下，设备或后端系统应将故障通知用户。

在可能的情况下，设备制造商应让用户轻松禁用或阻止（例如，使用防火墙）各种网络流量，而不会影响设备的主要功能。

### 7.5 如果云后端出现故障，IoT设备应继续运行

当与云后端的连接中断或服务本身发生故障时，即使处于降级或部分运行状态，许多依赖或使用云后端的服务也可以继续运行。例如，可以通过云服务更改设置的恒温器在最坏的情况下应使用最新已知或默认设置继续运行。即使互联网连接失败，也应该可以从家庭内部访问云托管的家庭安全摄像机。

### 7.6 物联网设备应支持寻址和命名最佳实践

许多物联网设备安装后可能会保持部署多年。因此，物联网设备应支持相对较新（尽管当前）的最佳实践，即IP寻址和域名系统（Doman Name System，域名系统）的使用。支持最新的寻址和命名协议，将确保这些设备在未来几年内保持正常运行，性能良好以及可以支持重要的基于域名系统的安全功能。

- **IPv6**

  BITAG建议物联网设备支持最新版本的互联网协议IPv6。

- **域名系统**

  BITAG建议当使用域名时，物联网设备支持使用或验证域名系统安全扩展（DNSSEC）。例如，如果某物联网设备使用example.com域与云服务通信，则云提供商应能够对该域进行签名，而物联网设备应能够验证该签名（或确保其上游域名系统解析器）已经这样做，并在域名系统响应中指出了这一点）。

### 7.7 物联网设备应随附易于查找和理解的隐私政策

BITAG建议物联网设备随附隐私政策，但对于典型用户而言，该政策必须易于理解和理解。

### 7.8 披露远程降低物联网设备功能的权利

BITAG建议，如果第三方可以远程降低物联网设备的功能，例如制造商或物联网服务提供商，则应在购买时告知用户这种可能性。

### 7.9 物联网设备行业应考虑制定行业网络安全计划

BITAG建议物联网设备行业或相关的消费电子集团考虑创建一项由行业支持的计划，在物联网零售包装上可以贴上某种“安全物联网设备”徽标或标记。这样的程序可以类似于Wi-Fi联盟或其他团体验证设备符合各种标准和/或最佳实践的方式。

一组业界支持的最佳实践似乎是平衡物联网创新与与网络安全的流动性相关的安全挑战并避免认证流程可能出现的清单心态的最实用方法。

### 7.10 物联网供应链应在解决物联网安全和隐私问题中发挥作用

在如今的工厂到零售供应链中，通常很难定义各方在一段时间内扮演的角色。因此，这里仅将它们定义为“ 物联网供应链”。 物联网设备及其他设备的最终用户依靠物联网供应链保护其安全和隐私，并且物联网供应链的某些或所有部分在产品的整个生命周期中都扮演着至关重要的角色。除了本节中的其他建议外
，BITAG还建议物联网供应链采取以下步骤：

- 设备应具有清晰易懂的隐私政策，尤其是在与持续服务一起出售设备的情况下。
- 设备应具有针对物联网设备的重置机制，当用户退回或转售设备时，清除所有配置以供使用。设备制造商还应提供一种删除或重置各自设备存储在云中的数据的机制 。
- 制造商应提供一个具有明确定义的错误提交机制和书面响应策略的错误报告系统。
- 制造商应保护安全软件供应链，防止在制造过程中引入恶意软件；供应商和制造商应采取适当措施保护其软件供应链。
- 从设计到设备退役，制造商应在其整个生命周期内为物联网设备提供支持，包括对计划为设备提供持续支持的时间保持透明，以及消费者对物联网设备的期望设备使用寿命结束时设备的功能。
- 制造商应为消费者提供明确的方法，确定可以与谁联系以获得支持，并提供联系消费者的方法来传播有关软件漏洞或其他问题的信息。

- 制造商应报告发现和补救对消费者构成安全或隐私威胁的软件漏洞。
- 制造商应为漏洞报告流程提供定义明确，易于查找且安全的漏洞报告表格，以及书面记录的响应策略。制造商应考虑遵守漏洞报告处理标准ISO 30111 [108]。

## 8 其他关注此问题的团体

尽管BITAG在这个问题上有独特的见解，但值得注意的是，其他几个小组也专注于此方面。这些组包括：

- 智能对象联盟互联网协议（IPSO）[109]
- 电气电子工程师学会（IEEE）[110]
- 美国国家标准技术研究院（NIST）[111]
- 互联网工程任务组[112]
    - LWIG（轻量级实施指南）[113]
    - 6Lo（资源受限节点网络上的IPv6）[114]
    - 6TiSCH（IEEE 802.15.4e的TSCH模式下的IPv6）[115]
    - ROLL（低功耗有损网络路由）[116]
    - CoRE（受约束的RESTful环境）[117]
    - DICE（约束环境中的DTLS）[118]
    - ACE（受限环境的身份验证和授权）[119]
    - COSE（CBOR对象签名和加密）[120]
    - 6低功耗WPAN上的低端IPv6（已关闭）[121]
- GSMA：互联生活[122]
- IRTF：互联网研究任务组[123]
    - T2TRG：物联网研究小组[124]
- W3C：全球网络联盟[125]
    - 主题：物联网兴趣小组[126]
- 美国联邦贸易委员会（FTC）[127,128,129]
- 美国商务部国家电信和信息管理局（NTIA）[130，131]
- 互联网治理论坛（IGF）[132]
- 在线信任联盟[133]
- 国际标准化组织联合技术委员会1（ISO / IEC JTC1）[134]：成立了两个管理和物联网特别工作组；一种是由ANSI管理。
    - 国际电工委员会[135]：尽管IEC不仅限于物联网设备（并且适用于所有电气/电子技术），但它已经完成了多份有关物联网的研究论文，其中可能包含标准。
- 国际信息技术标准委员会（INCITS）[136]：由ANSI认证，“作为全球努力的美国中央技术咨询小组。”

- TRUSTe多方利益相关者物联网隐私技术工作组[137]：旨在起草技术标准，帮助公司开发保护物联网中消费者隐私所需的解决方案。
- 电气和电子工程师学会（IEEE）P2413 [138]：一个有关物联网架构框架标准的IEEE项目。
- 无线物联网论坛[139]："不是标准组织，但旨在向缺乏标准的标准机构（如远程无线连接）交付要求，并在存在相互竞争的标准（如家庭设备发现）下达成共识）。"
    - 应用程序组：审查标准API的工作组
    - 连通性小组：评估无线电接入的工作小组。
    - 监管组：协调全球免许可证法规和许可频谱可用性的工作组。
- 开放连接基金会（以前称为开放互连联盟）[140]：由英特尔，思科和三星创建的组织，旨在为物联网创建开放式互操作规范。还收购了UPnP论坛。
- 对象管理小组（OMG）[141]：一个国际非营利技术标准联盟，在工业物联网领域开展主要工作。
    - 工业互联网联盟[142]："…是开放性成员，国际非营利联盟……为工业互联网设定架构和方向。"致力于加快采用专用于物联网市场的无线广域网技术。由CISCO创立，包括埃森哲，Arkessa，英国电信Telensa和WSN。
- oneM2M [143]：制定技术规范，满足对可嵌入各种硬件和软件中的通用M2M服务层的需求
- 国际自动化学会（ISA）[144]："非营利性专业协会，为那些应用工程和技术改善现代自动化和控制系统的管理，安全和网络安全的人们树立了标准。"尽管没有工作组迹象，但已经对物联网进行了一些研究。
- OASIS [145]："非营利性财团，为全球信息社会推动开放标准的开发，融合和采用。"
    - OASIS高级消息队列协议（AMQP）技术委员会：定义一个无处不在，安全，可靠和开放的互联网协议来处理业务消息传递。
    - OASIS消息队列遥测传输（TC）技术合作中心：提供轻量级发布/订阅可靠消息传输协议，适用于需要少量代码占用和/或网络带宽极为宝贵的M2M /物联网环境中的通信。
    - OASIS开放式建筑物信息交换（TC TC）：使建筑物中的机电控制系统与企业应用程序通信。
- Hypercat [146]：为工业和城市提供安全和可互操作的物联网的联盟和标准驱动。
- AllSeen联盟[147]：创建了AllJoyn，这是一个"协作，开放的生态系统"。
- 线程组[148]：创建线程协议，该协议是物联网的免版税网络协议。提供产品认证。

# 9 参考文献


[1] James
Manika等人，《物联网：超越炒作绘制价值》，麦肯锡全球研究所，2015年6月，物理世界。http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-

2 [2] Brian Krebs，“物联网现实：智能设备，Dumb默认值”，Krebs安全性，博客，2016年2月8日，http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/.

[3] Kalev Leetaru，“物联网如何将客厅变成未来的网络战场”，2015年11月6日，福布斯（Forbes.com），future-cyber-battleground /（上次访问2016年11月18日）。http://www.forbes.com/sites/kalevleetaru/2015/11/06/how-the-internet-of-things-will-turn-your-living-room-into-the-

[4] IEEE标准协会，IEEE
802.15：无线个人局域网（PANs），https：//standards.ieee.org/about/get/802/802.15.
html（最新访问，2016年11月18日）。

[5] X10，https：ww（上次访问日期：2016年11月18日）。//w.x10.com/

*[6]* Hewlett Packard，《物联网研究研究：2015年报告》，惠普企业，2015年，请访问：
https：www//w.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

*[7]* 约翰·佩斯卡托尔（John Pescatore），“保护物联网安全调查”，无忧研究院分析师调查，2014年1月，网址：
https：www//w.sans.org/reading-room/whitepapers/analyst/securing-internet-things-survey-34785.

[8] 查理·奥斯本（Charlie
Osborne），“研究发现，物联网设备缺乏基本安全性”，ZDNet，2015年4月8日（最新访问，2016年11月18日）。http://www.zdnet.com/article/internet-of-things-devices-lack-fundamental-security-study-finds/

[9] Ye Ka-Ping Yee，“协调安全性和可用性”。IEEE安全和隐私2.5（2004）：48-55，见ieeesp2004.pdf。http://zesty.ca/pubs/yee-sid-

*[10]* Veracode，《物联网：安全研究》白皮书，2014年，请访问：
https：www//w.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf

*[11]* 丽贝卡·格林特（Rebecca E. Grinter）等人，“使家庭网络正常运行的工作”。ECSCW2005。施普林格荷兰，2005年，网址：
http://www.cc.gatech.edu/~beki/c27.pdf.

*[12]* Yin Min Pa Pa等。“IoTPOT：分析物联网威胁的增长。”（2015年），请访问：
https：www//w.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

*[13]* 赛门铁克，“物联网设备正越来越多地用于分布式拒绝服务攻击”，《赛门铁克安全响应》，2016年9月22日，网址：
http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks.

*[14]* 史蒂夫·罗杰森（Steve Rogerson），“将物联网归咎于拒绝服务攻击”，物联网MTM理事会，2015年4月29日，网址：
http://www.iotm2mcouncil.org/serviceattacks.

[15] Energin Janina，“分布式拒绝服务（DDoS）攻击使文件共享网站海盗湾（Pirate
Bay）脱机，”，2012年5月17日，ceoworld.biz，脱机。http://ceoworld.biz/ceo/2012/05/17/distributed-denial-of-service-ddos-attack-knocked-the-file-sharing-site-pirate-bay-

[16] Angela Moscaritolo，“联邦调查局逮捕了6次点击欺诈网络骗局，净赚1400万美元，”《SC
Magazine》，2011年11月9日，http://www.scmagazine.com/fbi-arrests-six-in-click-fraud-cyber-scam-that-netted-14m/article/216399/

[17] Sarthak Grover和Nick Feamster，未打补丁的物联网，PrivacyCon 2016，https：//
ww//w.ftc.gov/system/files/documents/public_comments/2015/10/00071-98118.pdf.

[18] 布鲁斯·施耐尔（Bruce
Schneier），“物联网极度不安全，而且往往不可修补”，《连线》，2014年1月6日，https：ww//w.schneier.com/essays/archives/2014/01/the_internet_of_thin.html.

[19] Bruce Schneier，“监控和物联网”，博客，2013年5月21日，https：//
ww//w.schneier.com/blog/archives/2013/05/the_eyes_and_ea.html.

[20] Matt
Loeb，“物联网安全问题需要对风险管理进行重新思考”，《华尔街日报》，2015年10月14日，http://blogs.wsj.com/cio/2015/10/14/internet-of-things-security-issues-require-a-rethink-on-risk-management/.

[21] Arik Hesseldahl，“物联网的黑客之眼”，Recode.net，2015年4月7日，黑客之物联网/。http://recode.net/2015/04/07/a-

[22] Arik
Hesseldahl，“物联网是黑客的新游乐场”，Recode.net，2014年7月29日，http://recode.net/2014/07/29/the-internet-of-things-is-the-hackers-new-playground/.

[23] 朱莉·努德森（Julie
Knudson），“物联网的安全挑战：物联网缺乏标准化协议和新的流量，使管理员的安全工作复杂化”，企业网络星球，2015年5月13日，http://www.enterprisenetworkingplanet.com/netsecur/security-challenges-of-the-internet-of-things.html.

[24] Reddit，“隐私讨论列表”，“我购买和退还了一套无线网络连接的家庭监控摄像头，忘记删除我的帐户，现在可以观看新主人”，https://www.reddit.com/r/privacy/comments/4ortwb/i_bought_and_returned_a_set_of_wifi_connected/ (last visited Nov. 18, 2016).

*[25]* 克里斯蒂娜·卡多萨（Christina Cardoza），“普林斯顿轮胎了解您的物联网设备是否安全”，《SD Times》，2016年1月22日，网址：http://sdtimes.com/princeton-tries-to-find-out-are-your-iot-devices-safe/.

[26] Christian Dancke
Tuen，“物联网系统安全”，硕士学位，挪威科学技术大学，远程信息处理部门，2015年6月，网址：https：//brage.bibsys.no/xmlui/bitstream/handle/11250/ 2352738 / 12892_FULLTEXT.pdf？sequence = 1＆isAllowed = y。

[27] Hewlett
Packard，《物联网安全研究：智能手表》，2014年IoT研究系列，http://go.saas.hpe.com/l/28912/2015-07-20/325lbm/28912/69038/IoT_Research_Series_Smartwatches.pdf.

[28] Kim
Zetter，“医院网络泄漏数据，使关键设备易受攻击”，2014年6月25日，https：ww//w.wired.com/2014/06/hospital-networks-leaking-data/.

[29] Mario Ballano Barcena和Candid Wueest，《物联网中的不安全性》，2015年3月12日，赛门铁克，https：//ww//w.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-things-ds.pdf.

[30] 凯蒂·纳托普洛斯（Katie
Natopoulos），“有人在看着：一个简单的攻击如何使陌生人利用私人安全摄像头”，2012年2月3日，The
Verge，http://www.theverge.com/2012/2/3/2767453/trendnet-ip-camera-exploit-4chan.

[31] 布莱恩·克雷布斯（Brian
Krebs），“这就是人们害怕物联网的原因”，2016年2月8日，克雷布斯网络安全，https：//krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet事物/

[32] Brady
Dale，“八种物联网安全失败：为善良设置路由器时更改路由器密码”，观察家，2015年7月16日，http://observer.com/2015/07/eight-internet-of-things-security-fails/.

[33] 迈克尔·温特（Michael
Winter），“加利福尼亚青年承认“美国青少年未成年小姐情节”，《今日美国》，2013年11月12日，http://www.usatoday.com/story/news/nation/2013/11/12/miss-teen-usa-sextortion-guilty-plea/3510461/.

[34] 凯文·汤森德，“亚马逊出售的物联网相机中发现恶意软件”，安全周刊，2016年4月11日，http://www.securityweek.com/malware-found-iot-cameras-sold-amazon.

[35] Johannes Ullrich，“硬币采矿DVR：从始至终的妥协”，SANS
ISC信息安全论坛互联网风暴中心，https：//isc.sans.edu/forums/diary/Coin+Mining+DVRs+A+comromise+from +开始+结束+18071 /。

[36] 金·泽特（Kim
Zetter），“全球首款数字武器STUXNET的前所未有的展示”，《连线》，2014年11月3日，https：//ww//w.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[37] Swati Khandelwal，“物联网僵尸网络-
25,000台CCTV摄像机被黑客发起了分布式拒绝服务攻击”，《黑客新闻》，2016年6月28日，http://thehackernews.com/2016/06/cctv-camera-hacking.html.

*[38]* 大华网络安全声明，新闻稿，2016年10月1日，网址：
http://www.dahuasecurity.com/en/us/single.php?nid=274.

[39] 大化，大化支持维基主页（最新访问，2016年11月18日）。http://www.dahuawiki.com/Main_Page

[40] 大华，如何创建更安全的安全系统，（最新访问，2016年11月18日）。http://www.dahuasecurity.com/en/us/best-practices.php

[41] 宽带互联网技术咨询小组（BITAG），SNMP反射放大分布式拒绝服务攻击缓解，2012年8月，http://bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf.

[42] T. Dierks＆E. Rescorla，“传输层安全（TLS）协议1.2”，RFC 5246，2008年8月，https：//tools.ietf.org/html/rfc5246。

[43] E. Rescorla＆N. Modadugu，“数据报传输层安全版本1.2”，RFC
6347，2012年1月，https：//tools.ietf.org/html/rfc6347。

[44] 亚伦·阿迪里（Aaron Ardiri），“是否有可能保护在物联网中使用的微控制器？”，EVO
Things，博客/教程，2014年8月27日，https：//evothings.com/is-it-possible-to-secure-micro- iot内使用的控制器/；

[45] Reinhard Seiler，博客，Raspberry Pi的Truecrypt基准测试，2012年7月20日，for-raspberry-pi.html。http://blog.rseiler.at/2012/07/truecrypt-benchmark-

[46] Darlene Storm，“ MEDJACK：黑客劫持医疗设备在医院网络中创建后门”，《计算机世界》，2015年6月8日，backdoors-in-hospital-networks.html。http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-

[47] Kim
Zetter，“小偷如何破解和禁用家庭报警系统”，《连线》，2014年7月23日，https：ww//w.wired.com/2014/07/hacking-home-alarms/.

[48] Marek
Majkowski，“说奶酪：来自物联网摄像头的大规模分布式拒绝服务攻击的快照”，2018年10月11日，Cloudflare博客，https：//blog.cloudflare.com/say-cheese-a-snapshot-of-the -mass-ddos-attacks-coming-from-iot-cameras /（最新访问，2016年11月18日）。

[49] Nest，“嵌套学习恒温器软件更新历史记录”，Nest支持，https：//nest.com/support/article/Nest-Learning-Thermostat-software-update-history（最新访问，2016年11月18日）。

[50] Nest，“如何更新Nest Learning Thermostat上的软件”，Nest支持，https：//nest.com/support/article/How-do-I-update-the-software-on-my-Nest-Learning -Thermostat（最后访问时间为2016年11月18日）。

[51] 尼克·比尔顿（Nick Bilton），“巢式恒温器让用户处于寒冷之中”，纽约时报，2016年1月13日，网址：http://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html.

[52] Catalin Cimpanu，“植入式起搏器的安全研究人员为IoT医疗设备敲响了警钟”，Softpedia，2016年1月5日，498448.shtml。http://news.softpedia.com/news/security-researcher-with-implanted-pacemaker-sounds-the-alarm-on-iot-medical-devices-

[53] Russ Housley，IAB主席的话：IAB关于互联网保密的声明，IETF期刊，2015年3月，https：//ww//w.internetsociety.org/publications/ietf-journal-march-2015/words-iab-chair-12.

[54] Jane Wakefield，“智能LED灯泡泄漏wi-fi密码”，BBC新闻，2014年7月8日，第28208905页。http://www.bbc.com/news/technology-

[55] SEC顾问，“密钥之家：行业范围内的HTTPS证书和SSH密钥重用危及全球数百万设备”，博客，2015年11月25日（最新访问，2016年11月18日）。http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html

[56] 埃里克·戴维斯（Erik C. Davis），“集群和离群点检测：智能家庭网络中的方法和应用”，本科论文，运筹学和金融工程。普林斯顿大学。 2016年6月。

[57] 张茵和韦恩·帕克森，“探测垫脚石”，USENIX安全研讨会，2000年8月，https：//ww//w.cs.utexas.edu/~yzhang/papers/stepping-sec00.pdf.

[58] 罗伯特·沃莫西（Robert Vamosi），“物联网琐碎的研究者的Covert黑客攻击”，摩卡纳，2014年2月28日，https：//ww//w.mocana.com/blog/2014/02/28/covert-hacking-iot-trivial-say-researchers.

[59] 洛伦佐·弗朗西斯·比奇埃莱（Lorenzo Franceschi-Bicchierai），“互联网连接的费舍尔价格泰迪熊离开孩子的身份暴露，”主板，2016年2月2日，http://motherboard.vice.com/read/internet-connected-fisher-price-teddy-bear-left-kids-identities-exposed.

[60] Lorenzo Franceschi-Bicchierai，“‘你好芭比”中的错误可能会让黑客监视儿童聊天，”主板，2015年12月4日，http://motherboard.vice.com/read/bugs-in-hello-barbie-could-have-let-hackers-spy-on-kids-chats.

[61] 洛伦佐·弗朗西斯·比奇埃拉伊（Lorenzo Franceschi-Bicchierai），“黑客玩具制造商伟易达公司承认实际上有630万儿童受到伤害”，主板，2015年12月1日，http://motherboard.vice.com/read/hacked-toymaker-vtech-admits-breach-actually-hit-63-million-children.

[62] 英国广播公司（BBC），“三菱欧蓝德混合动力汽车警报器'被黑客入侵'”，英国广播公司新闻：技术，2016年6月6日，http://www.bbc.com/news/technology-36444586.

[63] Darlene Storm，“日产聆风秘密泄露驾驶员的位置和网站速度”，《计算机世界》，2011年6月14日，网站.html。http://www.computerworld.com/article/2470123/endpoint-security/nissan-leaf-secretly-leaks-driver-location--speed-to-

[64] Leo Kelion，“日产聆风电动汽车漏洞披露”，BBC新闻：技术，2016年2月24日，http://www.bbc.com/news/technology-35642749.

[65] Colin Neagle，“智能冰箱黑客暴露凭证”，NetworkWorld，2015年8月26日，http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

[66] Newswise，“乔治亚理工大学在最新的“新兴网络威胁”报告中警告移动设备云数据存储的威胁”，新闻发布，2013年11月6日，最新网络威胁报告http://www.newswise.com/articles/georgia-tech-warns-of-threats-to-cloud-data-storage-mobile-devices-in-

[67] 佐治亚理工学院信息安全与隐私研究所，《2016年新兴网络威胁报告》，可查阅：http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf.

[68] Phys.Org，“您的智能手表正在赠送您的ATM PIN码”，2016年7月6日（最新访问时间：2016年10月7日）。http://phys.org/news/2016-07-smartwatch-atm-pin.html

[69] Robert J. Ellison等人，“评估和缓解软件供应链安全风险”，软件工程研究所，技术说明，2010年5月，网址：http://www.sei.cmu.edu/reports/10tn016.pdf.

[70] 互联网风暴中心，生存时间：摘要，https：//isc.sans.edu//survivaltime.html（最新访问时间：2016年11月18日）。

[71] 布莱恩·克雷布斯（Brian Krebs），“KrebsOnSecurity创下记录分布式拒绝服务命中率”，KrebsOnSecurity，2016年9月21日，https：//krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/（上次访问日期：2016年10月3日）。

[72] 闪点，“事物的攻击！”，博客文章，2016年9月17日，https：（最新访问时间：2016年11月18日）。//www.flashpoint-intel.com/attack-of-things/

[77] 德鲁·菲茨杰拉德（Drew Fitzgerald），“黑客感染相机，用于大规模互联网攻击的数字录像机”，《华尔街日报》，2016年9月30日（最新访问，2016年10
月3日）。http://www.wsj.com/articles/hackers-infect-army-of-cameras-dvrs-for-massive-internet-attacks-1475179428

[78] 联邦贸易委员会，“华硕解决不安全家用路由器和“云”服务给消费者隐私带来风险的FTC费用，”新闻稿，2016年2月23日，网址：https：// ww insecure-home-routers-cloud-services-放。//w.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-

[79] 网络世界，“ KrebsOnSecurity迁移到Project Shield以抵御分布式拒绝服务攻击审查”，史密斯女士女士，2016年9月25日，attack-censorship.html（2016年10月3日最后访问）。http://www.networkworld.com/article/3123806/security/krebsonsecurity-moves-to-project-shield-for-protection-against-ddos-

[80] 布莱恩·克雷布斯（Brian
Krebs），“审查制度民主化”，KrebsOnSecurity，2016年9月16日，https：//krebsonsecurity.com/2016/09/the-民主民主化审查制度/（最新访问，2016年10月3日）。

[81] 蒂姆·格林（Tim
Greene），“被劫持的物联网设备僵尸网络曾经进行的最大分布式拒绝服务攻击”，网络世界，2016年9月23日，（最后访问于2016年10月3日）。http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html

[82] 丹·古丁（Dan
Goodin），“据报道，超过14.5万台被黑客入侵的摄像头交付了打破记录的分布式拒绝服务”，ArsTechnica，2016年9月28日（最后访问于2016年10月3日）。 http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

[83] 大卫·庞卡（David Plonka）和伊丽莎·博斯基（Elisa Boschi），《不受管制的旧互联网》，2016年，网址：https://down.dsg.cs.tcd.ie/iotsu/subs/IoTSU_2016_paper_25.pdf。

[84] David Plonka，《物联网测量与分析》，2016年7月18日，网址：
https：www//w.ietf.org/proceedings/96/slides/slides-96-maprg-8.pdf.

[85] Lucian
Constantin，“攻击者劫持闭路电视摄像机发起分布式拒绝服务攻击，计算机世界”，2015年10月22日，http://www.computerworld.com/article/2996079/internet-of-things/attackers-hijack-cctv-cameras-to-launch-ddos-attacks.html.

[86] 克什米尔·希尔（Kashmir Hill），“这家伙的灯泡对他的整个智能住宅进行了拒绝服务攻击，”
Fusion.net，2015年3月3日，http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/.

[87] 汤姆·斯普林（Tom Spring），“不安全：查明问题”，ThreatPost，2016年7月21日，https：//threatpost.com/iot-insecurity-pinpointing-the-problems/119389/。

[88] DirectTV，用户指南：精灵和更早的高清DVR接收器，第16页。
107，http://www.directv.com/learn/pdf/System_Manuals/DIRECTV/DIRECTV_HDDVR_HR20-44.pdf.

[89] Roku，“如何在Roku播放器上更新软件？”，https：//support.roku.com/hc/en-us/articles/208755668-How-can-I-update-the-software-on- my-Roku-player-（上次访问日期：2016年11月18日）。

[90] Arunesh Mathur等。
“它们像僵尸一样不断回来：改善软件更新界面”，USENIX可用安全和隐私专题研讨会，2016年，网址：https：// ww mathur.pdf。//w.usenix.org/system/files/conference/soups2016/soups2016-paper-

[91] David Plonka，《有缺陷的路由器，威斯康辛大学互联网时间服务器》，2006年7月19日，http://pages.cs.wisc.edu/~plonka/netgear-sntp/.

[92]

[81] Comcast，“导致域名系统查询泛滥的某些NetGear路由器”，Comcast域名系统新闻，2013年5月20日，http://dns.xfinity.com/index.php/entry/some-netgear-routers-causing-flood-of-dns-queries.

[82] NetGear社区讨论列表，“每秒数千个域名系统请求！？”，2012年3月2日，https：//community.netgear.com/t5/General-WiFi-Routers/每秒数千个域名系统-请求/ td-p / 414710。

[83] BenoitPanizzon，Netgear产品的DDOS攻击是由CNAME而非A记录引起的？，[SWINOG]讨论列表，2013年6月27日，http://lists.swinog.ch/public /swinog/2013-June/005863.html.

[84] 国家安全局，《深度防御》，白皮书，2010年，网址：https：//citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf。

[85] Vijay Sivaraman等。“智能家居IoT设备的网络级安全和隐私控制”，IEEE无线和移动计算，网络和通信。2015年，https：//www.Level_Security_and_Privacy_Control_for_Smart-Home_IoT_Devices。//w.researchgate.net/publication/281275810_Network-

[86] Konstantinos Grivas和Stelios Zerefos，《增强型房屋清单》，欧洲环境智能会议，2015年。

[87] 威廉·恩克（William Enck）等。“TaintDroid：用于智能手机实时隐私监控的信息流跟踪系统”，Proc。于2010年10月在USENIX操作系统设计和实现专题讨论会（OSDI）上发布，网址为：http://appanalysis.org/tdroid10.pdf.

[88] 断开连接，断开隐私保护工具，https：//disconnect.me/（上次访问日期：2016年11月18日）。

[89] Masanobu Katagi和Shiho Moriai，《物联网的轻量级密码术》，2011年，https：// ww content / IAB-uploads / 2011/03 / Kaftan.pdf。//w.iab.org/wp-

[90] GitHub，“SSL和TLS部署最佳实践”，SSL Labs Wiki，https：//github.com/ssllabs/research/wiki/SSL-and-TLS- Deployment-Best-Practices（最新访问，2016年10月3日）。

[91] Mozilla，“安全/服务器端TLS”，Mozilla Wiki，https：//wiki.mozilla.org/Security/Server_Side_TLS（最新访问，2016年11月18日）。

[92] Dan Auerbach，“2011年回顾：证书颁发机构系统中的更清晰漏洞”，电子前沿基金会，2011年12月27日，https：//ww//w.eff.org/deeplinks/2011/12/2011-review-ever-clearer-vulnerabilities-certificate-authority-system.

[93] 维基百科，撤销列表，https：//en.wikipedia.org/wiki/Revocation_list（最新访问时间：2016年11月18日）。

[94] 丹尼斯·费舍尔（Dennis Fisher），“关于数字化黑客的最终报告显示出CA服务器的总体威胁”，ThreatPost，2012年10月31日，https：//threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers -103112 / 77170 /。

[95] 埃里克·米尔（Eric Mill），“证书颁发机构实际上是一个巨大的问题”，博客文章，2013年6月21日，https：//konklone.com/post/certificate-authorities-are-actually-a-tremendous-problem（上次访问11月18日），2016）。

[96] 切斯特·维斯涅夫斯基（Chester Wisniewski），“另一个证书颁发机构发布危险证书，裸体安全”，2011年11月3日，https：//nakedsecurity.sophos.com/2011/11/03/another-certificate-authority-issues-dangerous-certficates/（最后访问时间：2016年11月18日）。

[97] 格伦·弗莱什曼（Glenn Fleishman），“大多数人不知道的巨大网络安全漏洞及其修复方法，”《快速公司》（FastCompany），提供方式。http://www.fastcompany.com/3042030/tech-forecast/the-huge-web-security-loophole-that-most-people-dont-know-

[98] 史蒂夫·鲁萨（Steve Roosa），“证书颁发机构信任模型的有缺陷的法律体系结构”，向小叮当自由，2010年12月15日，https：//freedom-to-tinker.com/blog/sroosa/flawed-legal-architecture-certificate- Authority-trust-model /（最新访问时间：2016年11月18日）。

[99] Google，证书透明度项目，什么是证书透明度？，https：（最新访问，2016年11月18日）。//www.certificate-transparency.org/what-is-ct

[100]级别3威胁研究实验室，“攻击！”，级别3博客（最新访问，2016年11月18日）。http://blog.level3.com/security/attack-of-things/

[101]国际标准化组织，ISO / IEC 30111：2013：信息技术–安全技术–漏洞处理流程，2013，网址：http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231.

[102]IPSO联盟，（最后访问于2016年11月18日）。http://www.ipso-alliance.org

[103]电气与电子工程师学会（IEEE），https：（上次访问2016年11月18日）。//www.ieee.org

[104]美国商务部，国家标准技术研究院，（最后访问日期：2016年11月18日）。http://nist.gov

[112] 互联网工程任务组（IETF），（最后访问2016年11月18日）。http://www.ietf.org

[113] 互联网工程任务组（IETF），《轻量级实施指南》（lwig）https://datatracker.ietf.org/wg/lwig/（最新访问日期：2016年11月18日）。

[114] 互联网工程任务组（IETF），资源受限节点网络上的IPv6（6lo），https：//datatracker.ietf.org/wg/6lo/（最新访问，2016年11月18日）。

[115] 互联网工程任务组（IETF），IEEE 802.15.4e的TSCH模式下的IPv6（6tisch），https：//datatracker.ietf.org/wg/6tisch/（最新访问，2016年11月18日）。

[116] 互联网工程任务组（IETF），低功耗有损网络路由（滚动），https：//datatracker.ietf.org/wg/roll/（最新访问，2016年11月18日）。

[117] 互联网工程任务组（IETF），约束RESTful环境（核心），https：//datatracker.ietf.org/wg/core/（上次访问日期：2016年11月18日）。

[118] 互联网工程任务组（IETF），约束环境中的DTLS（骰子），https：//datatracker.ietf.org/wg/dice（最新访问时间：2016年11月18日）。

[119] 互联网工程任务组（IETF），约束环境的身份验证和授权（ace），https：//datatracker.ietf.org/wg/ace/（最新访问日期：2016年11月18日）。

[120] 互联网工程任务组（IETF），CBOR对象签名和加密（示例）https://datatracker.ietf.org/wg/cose/（最新访问日期：2016年11月18日）。

[121] 互联网工程任务组（IETF），低功耗WPAN上的IPv6（6lowpan），https：//datatracker.ietf.org/wg/6lowpan（最新访问时间：2016年11月18日）。

[122] 特殊移动用户协会（GSMA），GSMA IoT安全指南，（最新访问，2016年11月18日）。http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/

[123] 互联网研究任务组，（最后访问2016年11月18日）。http://irtf.org

[124] 互联网研究课题组互联网研究任务组，https：//irtf.org/t2trg（最新访问时间：2016年11月18日）。

[125] 万维网联盟（W3C），（上次访问2016年11月18日）。http://www.w3c.org

[126] 物联网利益集团万维网联盟（W3C），https：ww（最后访问日期：2016年11月18日）。//w.w3.org/WoT/IG/

[127] 联邦贸易委员会，消费者保护局和政策规划办公室，在《政府在培育物联网先进网络方面的利益，挑战和潜在作用问题》，案卷号160331306-6306-01，员工，https：// ww office-policy-planning-national-telecommunications / 160603ntiacomment.pdf。//w.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-

[128] 联邦贸易委员会，物联网：互联世界中的隐私与安全，员工报告，2015年1月，https：// ww internet-things-privacy / 150127iotrpt.pdf。//w.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-

[129] 丹尼斯·费舍尔（Dennis Fisher），FTC警告IoT设备中的安全和隐私风险，2016年6月3日，https：//www.iot-devices/。//w.onthewire.io/ftc-warns-of-

[130] 国家电信和信息管理局，物联网，https：ww Things（最新访问，2016年11月18日）。//w.ntia.doc.gov/category/internet-

[131] 美国商务部国家电信和信息管理局正在寻求对与物联网相关的潜在政策问题的评论，新闻发布，2016年4月5日，https：// ww release / 2016 / us-department-commerce-seeks-comment-potential-policy-issues-related-internet-thi//w.ntia.doc.gov/press-

[132] 互联网治理论坛，物联网动态联盟，https：ww 1 /文件。//w.intgovforum.org/cms/documents/igf-meeting/igf-2016/827-dciot-2015-output-document-

[133] 在线信任联盟，物联网，2016年9月19日，https：//otalliance.org/initiatives/internet-things（最新访问，2016年11月18日）。

[134] 国际标准化组织（ISO），ISO / IEC信息技术联合技术委员会，ommid = 45020（最新访问日期：2016年11月18日）。http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?c

[135] 国际电工技术委员会（IEC），（最后访问日期：2016年11月18日）。http://www.iec.ch/

[136] 国际信息技术标准委员会（最新访问，2016年11月18日）。http://www.incits.org/

[137] TRUSTe，2016年隐私风险峰会，2016年6月8日，http://www.truste.com/events/privacy-risk/

[138] 电子电气工程师协会（IEEE），P2413 – 物联网（IoT）架构框架标准，https：//standards.ieee.org/develop/project/2413.html（最新访问时间为11月18日， 2016）。

[139] 无线物联网论坛（最近一次访问是2016年11月18日）。http://www.wireless-iot.org/

[140] 开放连接基金会，https：//openconnectivity.org/（最新访问，2016年11月18日）。

[141] 对象管理小组（上次访问是2016年11月18日）。http://www.omg.org/

[142] 工业互联网联盟（上次访问2016年11月18日）。http://www.iiconsortium.org/

[143] oneM2M（最新访问时间为2016年11月18日）。http://www.onem2m.org/

[144] Bill
Lydon，“物联网：工业自动化行业探索和实施物联网”，InTech杂志，2014年4月4日，网址：https：ww//w.isa.org/standards-and-publications/isa-
出版物/ intech-magazine / 2014 / mar-apr / cover-story-internet-of-things /。

[145] OASIS，OASIS委员会类别：IoT / M2M，https：//www.oasis-open.org/committees/tc_cat.php?cat=iot（最新访问，2016年11月18日）
。

[146] HYPERCAT，（最后访问于2016年11月18日）。http://www.hypercat.io/

[147] AllSeen联盟，https：//allseenalliance.org/（最新访问于2016年11月18日）。

[148] Thread，（最后访问日期：2016年11月18日）。http://threadgroup.org/

## 10 文档贡献者和审稿人

- Fred Baker, *CISCO*
- Steven Bauer, *MIT*
- Richard Bennett
- Don Bowman, *Sandvine*
- William Check, *NCTA*
- kc claffy, *UCSD/CAIDA*
- David Clark, *MIT*
- Shaun Cooley, *CISCO*
- Amogh Dhamdhere, *UCSD/CAIDA*
- Nick Feamster, *Princeton University*
- Francis Ferguson, *Level 3*
- Joseph Lorenzo Hall, *Center for Democracy & Technology*
- Ken Ko, *ADTRAN*
- Jason Livingood, *Comcast*
- Patrick McManus, *Mozilla*
- Chris Morrow, *Google*
- Donald Smith, *CenturyLink*
- Barbara Stark, *AT&T*
- Darshak Thakore, *CableLabs*
- Matthew Tooley, *NCTA*
- Jason Weil, *Charter Communications*
- Greg White, *CableLabs*
- Todd Whitenack, *Cellcom*
- David Winner, *Charter Communications*