2017 年 6 月 6 日（星期二）

易受攻击的设备组成的物联网

引言

随着技术的发展，计算系统的体积不断缩小，价格不断下降，功耗也不断降低。这些微型计算系统能够集成到日常物品中；这些设备与无处不在的无线连接相结合，共同构成“物联网”。物联网可能会改善我们的生活，但是，只有我们妥善管理这些设备固有的安全风险，可能性才会成为现实。

Gartner 的研究表明，2016 年全球有 64 亿台设备连接互联网，该数字到 2020 年将达到 208 亿台。这相当于未来 4 年每天都有将近 1 千万的新设备连接入网，导致不安全设备的潜在受攻击面大幅扩大。由于企业部署这些系统的目的在于做出运营改善相关决策，或围绕物联网制定其业务策略，因此我们必须考虑设备的漏洞和所生成数据的真实性。

思科和 Talos 都非常关注物联网的安全性。我们的目标之一是迫使网络犯罪分子改河易道。因此，我们会寻找供应商并与之合作，在漏洞遭到滥用之前将其修复。例如，我们在特灵温控器内发现了硬编码凭证。如果威胁攻击者发现这一情况，他们本可以远程登录到温控器，并获得对设备的完全控制权。此时，他们将能够对本地网络进行侦察以发动攻击。我们为客户开发了防护措施，并推迟披露漏洞，直到供应商发布了用于解决该问题的补丁。

连接到企业网络的不安全物联网设备无异于又一台可能为攻击者提供进入点的计算机。一旦遭到入侵，攻击者可以使用物联网设备从网络中收集信息，或对其他系统发起攻击。但是，不同于大多数联网计算机，物联网设备不太可能装有防病毒软件或安全软件。这意味着攻击者可以长时间潜伏其中，被发现的风险微乎其微。

犯罪分子觉察到物联网带来的机会。他们“圈定”了许多安全防护水平低下的物联网设备，构成 Mirai 僵尸网络。该僵尸网络发起了历史上最大规模的拒绝服务 (DoS) 攻击，利用窃取的计算能力和不安全设备的互联网连接来扰乱 Twitter、Paypal、Spotify 及其他网站提供的服务，使这些服务整天断断续续。犯罪分子还会入侵闭路电视 (CCTV) 系统中使用的易受攻击的数字视频录像机。目的不是清除可定罪的视频监控镜头，而是安装恶意软件以窃取处理能力，并将其用于比特币挖矿，从中获利。

不仅设备本身可能易受攻击，而且犯罪分子可能利用从物联网设备中收集数据的系统，进行一些令人关注的攻击。例如，以色列研究团队发现，他们可能诱使流量信息系统相信存在伪造的流量堵塞，方法是通过伪造的物联网设备发出假冒的流量数据。

与外界交互的不安全互联网设备可能被入侵，导致功能改变。例如，电子酒店锁让访客可以使用门卡进入房间。但是，这些设备上的通信端口可能遭到黑客攻击，他们利用锁上的安全功能不足，使任何具有必要知识的人无需门卡即可开门。

甚至不太可能的物品（如玩具和家居用品）也可以被视为物联网设备，并且被发现包含网络漏洞。黑客可能入侵已联网的芭比娃娃对您进行窥探，并破坏婴儿监视器，监控您和您的孩子。甚至可以通过您的智能电视来“监视”您。

压力导致物联网安全问题

随着全球构建基础设施并部署组成物联网的设备，我们整个社会有机会运用在互联网发展过程中学习到的数十年良好实践，其中包括关于安全重要性的惨痛教训。

物联网发展的前提基于这一理念：在许多地方部署许多便宜、连接互联网的设备。随着市场发展，制造商加快将设备以可能的最低价格推向市场，并且很少买家会坚持认为安全要求应作为其采购流程的一部分。这种情况导致市场上出售的许多物联网产品包含已知的漏洞，并且没有或很少考虑如何能将更新应用于设备，以便修复安全问题。

如果在设计阶段早期考虑安全问题，就可以在系统内构建防护措施。物联网系统的各项功能（从设备本身到无线通信、用户界面、管理界面）均与众所周知且有特征的薄弱环节相关。同样，对于这些类型的薄弱环节所做的防御也是众所周知的。如果规定系统安全性是系统的一项要求，并指出需要的防护类型，则将有助于系统更具恢复能力、不太可能被入侵、在发生入侵时不太可能遭受重大损失，并且更易于更新以便在发现问题时修复问题。

如果不解决安全问题，可能会付出沉重的代价。安装不安全的电子锁意味着有锁可能还不如没有锁。这些锁可能被入侵，变成任何人均可打开。部署连接至企业网络的不安全设备就像使办公室大门一整晚未上锁一样，任何人都可以悄悄潜入，带走他们想要的东西。易受攻击的物联网产品可能被完全禁止，例如德国的一款连接互联网的玩具 Cayla。

安全问题以多种形式存在。解决任何单个问题首先需要意识到问题、了解问题如何产生，以及如何修复或缓解问题。只有到那时，我们才能制定适当的安全策略。

软件漏洞是影响物联网的此类安全问题之一。Talos 有专门的团队负责寻找物联网和其他系统中的软件漏洞。当我们发现新漏洞时，我们会遵循已发布的负责任披露政策，确保我们的客户受到保护，并且问题得到修复。通过共享这些发现，我们可以通知并保护整个用户社区，并为关于保护物联网的讨论做出贡献。

“欺骗”物联网

任何参与编写代码或确保 IT 项目按时间和预算要求完成的人员都会同意这一点：编写软件一项艰难的工作。创建符合要求、基于软件的系统则难上加难。为确保安全，系统不仅必须按预期运行，而且不能做其他任何事情。

漏洞是系统中的薄弱环节，可用于“欺骗”系统执行其不应该执行的任务。漏洞通常处于潜伏状态，未被发现，因为我们需要一组特定的情况才可发现他们，也就是说，除非我们专门探测这些漏洞，否则我们不会发现它们。一旦攻击者发现漏洞，就会获得访问资源和数据的权限，甚至能够以系统设计人员从未想象或希望的方式运行代码。

任何包含软件的系统几乎肯定都包含漏洞。从这个意义上讲，物联网与任何其他计算机设备没有区别。如果持续将安全性视为要求、系统设计和开发的一部分，会有助于在早期发现潜在错误，以便纠正错误。在开发流程的越晚阶段发现安全问题，修复的成本就越高昂。

虽然尽了最大努力，但是几乎可以肯定的是，最终的系统将包含漏洞。应鼓励将负责任地披露漏洞与快速“修复”流程相结合，这样做有助于最大限度降低风险和减少损害。这也意味着软件工程社区可以从其他人的错误中吸取教训，不重复犯同样的错误。

现实生活中的物联网风险

Talos 经常看到的关键问题之一是系统内的硬编码用户名和密码。在发现这种情况后，攻击者可以利用这些信息获得全球各地共用这些默认凭证的所有设备的访问权限。就在去年，我们在特灵温控器内发现了这一问题。我们与 Trane 合作以确保问题得到修复。

物联网系统均要求通过管理界面来控制设备的运行，并处理收集到的数据。此外，我们最近发现了攻击者可用于控制 LabVIEW 所控制的物联网设备的一种方式，此外还发现了攻击者可以如何攻击 Aerospike 数据库以控制该平台。

需要做出哪些改变

除非人们意识到问题，否则不会发生任何改变。在遇到漏洞时对漏洞持开放态度，将有助于用户考虑自身的安全要求，并评估他们可能需要部署的其他安全功能。它帮助用户区分修补方案的优先次序，甚至更好的是，只是告知他们为何已应用自动系统更新。除了那些想要利用漏洞攻击系统的黑客以外，对安全问题保持沉默对任何人都没有好处。

供应商必须确保他们开发的软件在设计、开发和测试方面尽可能地安全。虽然供应商尽了最大努力，但是黑客仍会发现漏洞，因此系统需要修补。应使修补流程尽可能地轻松快捷（最好自动进行），这有助于分发具有新特性和功能的安全更新。要使企业和消费者真正采用便利而强大的物联网，他们必须充分信任我们在构建物联网时将安全摆在首位。

保护您的系统

要点：使安全成为购买流程的一部分。询问供应商如何发现并解决漏洞。如果他们的回答不符合您的期望，不要进行购买。

对包含物联网设备的网络进行分段。无需使可能易受攻击的联网温控器与您的客户数据库在同一个网络上。将网络隔开，这样即使某台设备遭到入侵，破坏潜力也有限。

采用适当的网络安全措施来保护物联网设备。物联网设备是计算机，需要采用与任何其他联网设备相同的安全措施。使用防火墙保护它们以阻止未允许的网络连接，并使用 IDS/IPS 系统针对未经授权的网络流量进行阻止和发出警报。

计划您将如何使系统保持已完全修补状态、如何了解所需的补丁，以及在供应商不愿意或无法发布补丁时您将做什么。

不要忽略管理系统。数据库和控制面板与许多安全风险相关，尤其是对用户进行身份验证和确保数据收集完整性方面的安全风险。验证单台遭到入侵的设备不会导致整个数据库遭到泄露或删除。同样，请确保图形前端不易遭受跨站脚本 (XSS) 攻击。这种攻击可能导致攻击者获得访问敏感系统的权限。

总结

物联网系统能够对我们的职业和个人生活做出巨大改变。物联网能够减少浪费、提高效率，并通过新的机遇和新收集的数据创造新的市场。

换句话说，物联网将使我们的社会能够发展、进步和改善。但是，我们必须对这些设备的安全性充满信心，才能充分实现其优势。我们知道物联网系统可能如何被攻击和破坏。我们知道这些攻击的后果，并且知道如何防御和缓解这些攻击。

社会可以保护物联网系统免遭破坏，但前提是部署、购买和交付系统的人员坚持采用适当的防护措施。买家必须要求提供更好的安全性，制造商必须了解形势的严重性。制造商不能再只是追求率先将产品推向市场，还必须追求将最安全的产品推向市场。如果我们都开始要求提供更好的安全性，制造商会优先考虑安全性。

发布者：MARTIN LEE 发布时间：13:00
标签：物联网、IOT、漏洞、漏洞