如何保证安全的物联网设计？

现如今智能的连接设备已经广泛布局在我们的家中或者我们的工作环境中，这些设备很棒，但它们也会暴露出许多新的攻击面，“设计安全”框架可以提供最佳的保护方案。该框架是硬件和软件开发中的一系列原则，侧重于将安全性作为设计和开发过程中的核心问题。

我们越来越多地用旧式计算机之外的“智能”／连接设备填充家庭，从恒温器到安全系统甚至到厨房用具。企业在线提供一系列流程，对象和空间，以扩大智能服务的潜力。物联网（IoT）具有巨大的潜力，但连接一切都有副作用：那就是增加漏洞。

我们必须考虑物联网网络安全的基本原则，以保护自己的个人隐私甚至企业安全。其中最受关注的是“设计安全”概念和设备安全认证计划。

物联网设备安全101

保护物联网设备的关键步骤包括以下几种实践：

执行例行更新。制造商会不定期发布更新，可以通过软件改进产品的安全性。一旦产品掌握在您的手中，快速安装更新将有助于保护您免受最近发现的威胁。但请记住，不完美的更新可能会暴露新的安全漏洞。

控制访问。考虑是否需要连接到互联网才能使用该设备。如果您不需要连接，那么您只需授予对家庭网络的访问权限。

关闭通用即插即用功能。UPnP是路由器，相机，打印机和其他设备的弱点。同时，安全的互操作性是物联网的必要条件。

改善密码。密码必须要足够长，并且最好是字母数字的，以及避免重复，尤其不要使用字典单词和个人相关名称。许多设备目前都附带了令人难以置信的可怕密码，如“admin”和“password”，因此请及时与您的硬件供应商联系，确保您的物联网端点安全。

保护您的连接。使用专用网络将设备连接到Internet时，如果要提高稳定性，请确保您使用适合设备类型。

设计安全与设计隐私

除了了解设备可以采取的几个步骤之外，选择一个遵循设计安全性的制造商是有帮助的。设计安全性是硬件和软件开发中的一系列原则，侧重于保护系统并降低潜在风险。遵循这些原则允许制造商知道他们正在保护用户并遵守欧盟的通用数据保护法规（GDPR），使用此方法构建的系统包含诸如遵守编码最佳实践，实施身份验证保护和部署连续测试等元素。

设计安全如此重要的关键原因是软件通常首先考虑其功能，安全性成为次要问题，开发人员必须将安全漏洞作为持续关注而不是通过优化安全性来构建它。通过设计安全，您可以确定制造商正在有效且快速地修复安全问题。

设计安全性包含以下原则：

安全默认值。以标准方式创建安全体验。如果需要，允许用户删除保护。

正确修复安全问题。请注意设计模式，这可能会在您尝试修复代码时引入回归，需要测试所有相关应用程序。

保持安全简单。代码尽可能简单，这也更容易减少攻击面积。

深度防御原则。虽然只有一个控件可能是合理的，但添加更多控件可以使您的防御更深。

最小特权原则。应为帐户提供最低可能的权限级别，以完成其业务功能。

不要相信服务。您可以利用外部提供商进行处理，但请记住，默认情况下，服务不应该受信任。

通过隐藏避免安全。您不应仅仅通过隐藏关键细节来尝试保护关键数据，但这是一个不充分的安全控制。

职责分离。通常，管理员不应该是应用程序的用户。

验证失败。验证您的代码永远不会以默认情况下使用户成为管理员。

尽量减少攻击面积。应尽可能限制攻击面积，所有功能都会增加风险。

设计隐私是GDPR中的一个概念，类似于设计的安全性。设计隐私的两个核心要素是：

默认情况下保护数据。数据控制器应该只在必要时存储数据，应该只在必要的范围内处理数据，并且只应处理必要的特定数据；

设计数据保护。数据控制器应通过实施假名和其他保护措施，尽可能限制个人数据的处理。

寻找认证

虽然设计安全的原则有助于理解设备制造商的期望，但当您只需寻找遵循这些原则的认证时，一切都变得更加简单。ThingsCon和Mozilla提出了可信技术标志，专注于安全和隐私。ThingsCon的分析师使用五个主要标准来衡量产品：

开放性。是否生成或使用了开放数据？制造商和设备的流程是否开放？

稳定性。可以期待什么样的生命周期？设备有多稳定？

透明度。数据的使用方式和设备与消费者的沟通方式是什么？

隐私。用户权利是否受到尊重？数据实践是否具有领先优势？

安全。安全实践和保护是否反映了当前的环境？

另一个认证项目是网络安全认证计划，来自爱立信和AT&T。该系统收集有关物联网威胁的信息并将其发送给设备制造商，允许这些公司及其开发人员快速发现和修复任何漏洞。

保护物联网

到2025年，根据麦肯锡，物联网每年将产生3．9万亿美元到11．1万亿美元的经济影响。然而，这种巨大的回报也带来了巨大的风险。通过考虑上述最佳实践，并通过设计和认证计划了解安全性，您可以更好地了解如何安全地推进物联网项目或购买设备。

原文地址：http://www.china-nengyuan.com/tech/136314.html