信息安全前沿课堂讨论

陆皓喆 2211044 网络空间安全学院

2023 年 12 月 19 日

5 目前智能家居存在的各种安全隐私问题，并简介对应的解决方案。

智能家居技术的快速发展带来了许多便利，但也引发了一些安全和隐私方面的关切。

关于这个问题需要从智能家居目前面临的安全威胁谈起。我们可以将智能家居的安全威胁大致分为四大类:

（一）设备的假身份

大多数智能家居设备都拥有某种形式的设备标识符，作为唯一的 ID 或证书。但是，一旦攻击者了解其生成过程，就能够克隆没有密码保护的惟一标识符。一旦可以在未经授权的情况下克隆惟一标识符，攻击者就可以通过克隆的设备立即访问网络，然后从那里部署后续攻击。例如，关键信息可能被窃取，网络带宽可能被滥用，恶意软件和病毒可能被注入。另一方面，验证服务器标识也同样重要。如果家庭设备连接到恶意服务器，关键用户数据可能被窃取，更糟糕的是，整个家庭网络都可能受到攻击。

（二）数据窃听

智能家居环境中使用的通信接口大多基于无线技术，如蓝牙、ZigBee、Wi-Fi 等。虽然大多数无线技术都有某种形式的安全保护机制，但是由于用例的限制，它们不够稳定。例如，蓝牙通常依赖于简单的密码进行配对，这增加了通过通信接口窃听用户关键和敏感数据的风险。使用加密密钥对通信数据进行加密，以保护通信数据的机密性和完整性，这也是很常见的，因此，保护加密密钥不被窃取和提取就显得尤为重要。例如，三年前，Context Security 公司展示的某些智能灯泡的安全弱点。这些 LED 灯泡连接到一个启用 WI-FI33 的电路板，专家发现，当灯泡通过网状网络 (6LoWPAN 供电) “交谈” 时，信息中包含用户名和密码。由于底层的预共享密钥从未更改，白帽黑客可以设置一个类似的电路板，模拟其中一个智能灯泡并请求加入网络。这使得他们能够窃取证书，并最终获得对网络上所有灯光的控制。报告说明，潜在的攻击者如果能接近灯泡 30 米，就能轻易进入私人住宅或企业。更糟糕的是，他们还指出，这样的攻击可能不会被网络所有者发现。

（三）数据操作

除了窃听的风险，关键数据也有可能被恶意攻击操纵/更改，因此数据完整性保护是智能家居环境安全的另一个重要方面。计费信息、敏感配置数据或资源使用等关键信息不能作为操作值进行通信和存储。

（四）恶意软件感染

进入网络后，一个典型的攻击是安装恶意软件，使受影响的设备成为下一级攻击的来源。最近在一些主要电信网络中发生的事件就是这种攻击的典型例子。一旦连接的家庭设备被安装恶意软件攻破，这些设备就可能被添加到僵尸网络，并开始发出 DDoS 攻击。因此，许多智能家居设备——不仅仅是

电脑——成为 DDoS 攻击的潜在来源。这类智能家居设备 (例如智能摄像头、家庭路由器等) 的数量远远超过连接到网络的计算机数量，因此僵尸网络 DDoS 攻击造成的破坏规模和速度也可以显著得多。

上述智能家居环境中的安全威胁可以从三个基本的安全理念来解决:

(一) **"保密性"**：对敏感数据进行加密；

(二) **"完整性"**：利用密码信息认证码功能或数字签名保护数据；

(三) **"真实性"**：使用强度高的密码认证方案。这三个安全基石的核心是加密密钥，用于加密/解密、计算 CMACs 和支持强大的加密身份验证方案，因此，使用防篡改的硬件信任锚来保护这些密钥是至关重要的。目前，纯软件解决方案通常都有共同的弱点，如软件 bug 或恶意软件攻击。而且，读取和覆盖软件也相对简单，这意味着攻击者也更容易提取密钥。而基于硬件的安全解决方案提供了更高的安全级别，可用于存储访问数据和密钥，其存储安全级别与用于存储机密文档的保险箱相同。

以下是智能家居存在的一些安全隐私问题以及对应的解决方案。

1. 数据隐私和安全漏洞：

问题：智能家居设备收集大量个人数据，可能存在数据泄露或未经授权的访问。

解决方案：加强数据加密技术、双重身份验证和权限管理，确保数据传输和存储的安全。定期更新设备固件和软件以修复已知漏洞也是关键。

2. 远程访问漏洞：

问题：智能家居设备通常通过互联网远程访问，可能成为黑客攻击的目标。

解决方案：使用强密码和安全网络，启用防火墙和网络安全软件来防范未经授权的访问。此外，定期更新设备以修复安全漏洞，限制远程访问权限也是重要的措施。

3. 隐私侵犯：

问题：某些智能家居设备可能在未经用户允许的情况下收集个人信息或录制音频/视频。

解决方案：严格审查隐私政策，选择可信赖的制造商，并了解设备收集和使用个人数据的方式。对设备进行定期审查以确保其行为符合用户期望。

4. 供应链攻击：

问题：制造商或供应商网络受到攻击可能会导致恶意软件或后门注入到智能家居设备中。

解决方案：选择信誉良好的品牌和供应商，了解其安全措施，遵循最佳实践，如定期更新固件、使用安全的网络和设备管理。

5. 缺乏标准化安全措施：

问题：智能家居行业缺乏统一的安全标准，导致设备安全性各异。

解决方案：支持和倡导行业标准化，制定统一的安全标准和认证体系，以确保智能家居设备的基本安全性。

6. 物联网攻击面：

问题：连接的设备增加了物联网的攻击面，使家庭网络更容易受到攻击。

解决方案：使用独立的网络用于智能家居设备，对设备进行隔离，确保安全性，同时定期监控和更新网络安全设置。

在选择和使用智能家居设备时，用户应该审查隐私政策，了解设备如何收集和处理数据，同时遵循最佳的网络安全实践。同时，制造商和行业也应该合作制定更严格的安全标准，以保护用户数据和隐私。