物联网环境下的安全漏洞及跨系统攻击防范策略

黄可欣
国网广安供电公司

摘　要：本研究对物联网环境下的安全漏洞及跨系统攻击防范策略进行了深入探讨。首先，分析了物联网系统面临的安全威胁。其次，针对这些威胁，提出了一系列有效的防范措施，包括加强用户认证、建立安全防护机制、提升用户的信息素养等。这些措施的有效实施能够互联网技术的发展提供保障，并且营造一个健康安全的物联网环境。这一研究为保障物联网系统的安全性和稳定性提供了重要的理论支持和实践指导。

关键词：物联网环境；安全漏洞；跨系统攻击；防范策略
【DOI】10.12252/j.issn.2096-6288.2023.12.083

引言

随着物联网技术的快速发展，物联网系统已经广泛应用于各个领域，成为推动经济发展和社会进步的重要力量。然而，随着物联网系统的普及，安全问题也日益突出。由于物联网系统具有高度互联性和复杂性，因此容易遭受各种攻击和威胁。因此，需要研究有效的防范策略，以保障物联网系统的安全性和稳定性。

一、物联网环境下安全问题的重要性

物联网作为当今科技领域的重要发展方向，已经深入到我们生活的各个方面。然而随着物联网设备的普及和应用的广泛，其安全问题也愈发凸显出来，成了不容忽视的挑战。

首先，物联网环境中包含了大量的设备，这些设备之间互相连接、互相通信，形成了一个庞大的网络。这就意味着，一旦其中任何一个设备出现安全漏洞，就可能会对整个网络造成威胁。攻击者可以利用这些漏洞，入侵网络，窃取数据，甚至控制设备，给我们带来巨大的损失。其次，物联网环境中处理的数据往往具有高度的敏感性和价值性。例如，在智能家居中，我们的私人信息、生活习惯等都可能被收集并处理；在工业控制中，物联网设备控制着生产线的运行，一旦遭受攻击，可能导致生产中断或设备损坏。再者，物联网的发展也推动了其与各个行业的深度融合，这意味着物联网的安全问题不仅关乎到个人权益，更可能影响到国家安全、社会稳定和公共利益。

因此，物联网环境中的安全问题至关重要。只有确保物联网的安全性和可靠性，才能充分利用其带来的便利和效益，推动社会的科技进步。为此需要不断加强物联网安全技术的研究和创新，建立完善的安全标准和规范，提高用户的安全意识和操作技能，共同维护物联网的安全稳定。

二、物联网环境下的安全漏洞分析

（一）感知层安全漏洞

在物联网环境中，感知层作为信息收集和传输的起点，其安全性对整个系统的安全至关重要，然而，目前感知层存在多重不同的漏洞。首先是设备认证漏洞，这一漏洞使得大量物联网设备在出厂时就存在安全隐患。这些设备往往预设了过于简单的固定密码或者直接无需任何认证，这意味着攻击者可以轻易接入这些设备，进而对其进行控制或窃取存储的敏感数据。其次，由于感知层设备如传感器、RFID等通常部署在公共场所或者无人值守的区域，这使得它们很容易成为物理攻击的目标。恶意行为者可能会对这些设备进行破坏、篡改或者替换，从而导致数据的不准确、系统的瘫痪甚至更为严重的后果。[1]最后，在很多物联网应用中，为了降低成本或者简化设计，设备之间的通信并没有采用加密技术，这意味着攻击者可以轻易地截获这些传输的数据，并进行解析和利用。这不仅可能导致用户的隐私泄漏，还可能使攻击者进一步渗透到整个网络中，造成更大的破坏。

（二）网络层安全漏洞

物联网的网络层作为数据传输和交换的关键环节，也存在着诸多安全漏洞。其中，拒绝服务攻击是常见的威胁，由于物联网设备资源有限，常常成为攻击的目标，导致服务不可用。此外，中间人攻击更是让设备间的通信变得不再安全，攻击者可轻松窃取或篡改数据，而设备用户却浑然不觉。更为严重的是，路由和网关设备的问题也为攻击者敞开了大门。很多时候，这些设备的配置并不严谨，或者未能及时更新固件，都为潜在的安全隐患埋下了伏笔。因此，对于物联网的网络层安全，我们必须予以高度重视，不仅要加强设备的安全防护，更需要定期检查和更新系统，确保网络的安全稳

定。

（三）应用层安全漏洞

在物联网的应用层，安全漏洞同样不容忽视。例如，常见的注入攻击，如SQL注入和跨站脚本，能让攻击者趁机执行恶意代码、窃取数据或控制设备，给系统带来严重威胁。同时，应用层中常存在的弱密码、密码重置漏洞和权限管理不当等问题，也为攻击者提供了可乘之机，使其轻易获得访问权限。[2]此外，数据的存储和访问在应用层中往往缺乏严格的安全控制，这增加了数据泄漏或被篡改的风险。因此，对于物联网应用层的安全漏洞必须保持警惕，采取有效的安全措施来防范这些潜在威胁，确保系统的安全稳定运行。

三、跨系统攻击对物联网环境的影响

跨系统攻击是一种复杂的网络攻击方式，可以穿透不同系统之间的界限，从而对物联网环境造成严重影响。这种攻击方式的主要影响体现在数据泄漏、设备瘫痪和恶意传播等方面。

（一）数据泄漏

物联网设备通常连接在一起，并存储大量的敏感数据，包括个人隐私和商业机密等。如果攻击者成功地实施跨系统攻击，他们可能会获得访问这些数据的权限，并将其泄漏给不法分子。这些数据可能会被用于各种恶意目的，如进行诈骗、窃取财产或进行其他非法活动。这种数据泄漏不仅对个人隐私构成威胁，也可能对企业的声誉和财务状况产生重大影响。

（二）设备瘫痪

攻击者可以通过控制物联网设备或破坏其正常功能，使设备无法正常工作。这可能导致各种服务中断和生产停滞等问题，从而对个人和企业造成巨大的经济损失。例如，如果物联网设备用于关键基础设施的监控和控制，如电力网、交通系统或工业生产线，设备瘫痪可能会对公共安全和社会运转产生严重影响。[3]

（三）恶意传播

跨系统攻击还具有恶意传播的特点，一旦攻击者成功地渗透到一个物联网系统中，他们可能会将恶意软件或病毒传播到其他设备或系统中。这种传播可以通过各种途径实现，如网络连接、移动存储介质或供应链攻击等。恶意软件的传播不仅会导致更多的设备受到攻击和感染，还可能对整个网络造成严重的破坏，甚至扩散到其他与之连接的系统和网络中。这种传播范围广泛的攻击可以迅速蔓延并造成大规模的破坏，对物联网环境的稳定性和可靠性构成严重威胁。

四、物联网环境下的安全漏洞及跨系统攻击防范策略

（一）加强设备安全性与认证机制

在物联网环境中，设备的安全性和认证机制至关重要。为了确保设备的安全性，我们必须从源头做起，选择经过验证的、可靠的硬件供应商。这不仅可以降低设备本身存在的安全风险，还可以减少潜在的安全隐患。加密技术是保护设备通信和数据传输的有效手段。通过对数据进行加密，即使攻击者截获了传输中的信息，也无法读取其内容。这种技术为物联网设备提供了一层额外的安全保障，确保其通信的机密性和完整性。此外，实施严格的设备认证机制也是防范策略中的关键一环。[4]我们可以利用设备指纹、数字证书等技术，确保只有经过授权的设备才能接入物联网系统。这种认证机制可以有效地防止恶意设备或未经授权的设备进入系统，从而大大降低系统遭受攻击的风险。与此同时，定期为设备更新安全固件也是非常重要的。随着新的安全漏洞不断被发现，只有及时为设备打上“补丁”，才能确保其不受这些已知漏洞的影响。综上所述，加强物联网设备的安全性和认证机制是确保整个系统安全稳定运行的基石，通过提高物联网系统的安全防护能力，可以哟西奥减少潜在的安全风险。

（二）建立完善的网络安全防护体系

物联网的普及使得网络安全问题日益凸显，建立完善的网络安全防护体系成为当务之急。为了有效应对各类网络攻击，首要任务是部署高效的安全设备，如防火墙和入侵检测系统。这些设备能够实时监控网络流量，迅速识别异常行为，阻挡外部威胁，为网络构建起第一道坚固的防线。但在物联网时代，远程访问成为常态，如何保障其安全性成为一个挑战。此时，虚拟专用网络（VPN）技术发挥了巨大作用。通过加密通道，VPN确保了远程访问的数据传输的安全性和私密性，使得地理位置不再成为安全的制约因素。当然，单纯依赖外部防御是不够的，我们还需要在网络内部实施隔离和分段策略。[5]这种策略的核心思想是将网络划分为若干个子网，每个子网之间相互独立，即使某个子网遭受攻击，攻击者也难以在其他子网中自由移动，从而降低了整体网络的风险。最后，定期的安全审计和风险评估也是防护体系中不可或缺的部分。通过对网络进行全面的检查和评估，我们可以及时发现潜在的安全隐患和管理上的不足，然后采取针对性的措施进行修复和改进。

（三）强化应用层安全防护措施

在物联网环境中，应用层的安全防护同样重要。为了有效应对潜在的安全威胁，强化应用层的安全防护措施势在必行。首先，应用程序的安全开发是基础。开发人员必须遵循严格的最佳实践，如实施输入验证、参数化查询等技术，以确保应用程序不受SQL注入、跨站脚本等常见攻击的影响。同时，选择安全的通信协议也是关键。HTTPS等协议通过加密技术，确保了数据传输和访问的安全性，有效防止了数据在传输过程中被截获或篡改的风险。对于敏感数据，加密存储和传输是保障其机密性的重要手段。只有经过授权的用户才能解密和访问这些数据，大大降低了数据泄漏的风险。此外，实施严格的访问控制和权限管理也是确保应用层安全的有效方法。通过对用户和角色进行细分，我们可以确保只有具备相应权限的用户才能访问和执行特定的操作，从而避免了未经授权的访问和操作所带来的潜在危害。综上所述，通过安全开发、使用安全的通信协议、加密敏感数据以及实施访问控制和权限管理，我们可以大大提高系统的安全防护能力，降低潜在的安全风险。[6]

（四）提升用户安全意识与操作技能

物联网安全不仅仅是技术问题，用户的安全意识和操作技能同样关键。为了确保系统的安全稳定，我们必须重视并提升用户的安全意识和操作技能。定期开展安全培训活动是提高用户安全意识的有效途径。通过这些培训，我们可以让用户更加深入地了解物联网安全的重要性，学习如何识别和应对潜在的安全威胁。同时，为用户提供简洁明了的安全指南和操作手册也很有必要。这些资料可以帮助用户快速掌握基本的安全操作技能，如如何设置复杂密码、如何识别和避免网络钓鱼等。鼓励用户使用强密码和多因素身份验证方法也是增强账户安全性的重要手段。通过这种方式，即使密码被泄漏，攻击者也难以轻易登录用户的账户。当然，当用户遇到安全事件时，有一个快速响应的机制也非常重要。建立安全事件报告和响应机制，可以让用户及时上报和处理安全事件，防止损失扩大。总之，提升用户的安全意识和操作技能是物联网安全防护中的重要环节，通过培训、提供资料、鼓励使用强密码和建立响应机制，可以让用户成为系统安全的有力守护者，大大降低由于人为因素导致的安全风险。

（五）实施定期的安全评估与漏洞修复

物联网系统面临着日益复杂的安全挑战，其中，定期的安全评估和漏洞修复是防范策略的核心环节。为确保系统的稳健，我们必须时刻保持警惕，定期审视系统的安全状况。通过对物联网系统进行全面的安全评估和漏洞扫描，我们可以深入了解系统的安全状况，及时发现潜在的安全风险。这种评估就像一个体检，帮助我们识别哪些部分需要加固，哪些漏洞需要紧急处理。当发现安全漏洞时，及时修复显得尤为重要。延迟修复可能意味着给攻击者留下了可乘之机。[7]因此，一个高效的安全团队和快速的响应机制是必不可少的。为了确保漏洞能够得到统一、标准化的处理，建立明确的安全漏洞管理和修复流程至关重要。这不仅可以提高修复效率，还可以确保每次修复都是经过严格测试的，从而避免引入新的问题。当然，物联网的安全不仅仅是企业自己的事情。与相关的安全研究机构和社区保持紧密的合作，可以让我们获取到最新的安全信息和漏洞情报，提前做好准备，防患于未然。

结语

物联网环境下，安全漏洞与跨系统攻击是我们必须面对的现实问题。只有通过不懈的努力，加强研究，提高防范意识，才能确保物联网的稳健发展，发挥其最大潜力。防范策略不仅是技术层面的任务，更需要全社会的共同参与。让我们携手努力，保护物联网的安全，共创智能、安全的未来。

参考文献

[1]邵林；牛伟纳；张小松.物联网应用场景下自助终端网络安全威胁评估与应对[J].四川大学学报（自然科学版），2023（01）：103-113.

[2]张婧.物联网信息安全与隐私保护研究[J].软件，2022，43（10）：135-137.

[3]赵阳.物联网智能终端安全对国家安全威胁影响及对策[J].中国经贸导刊（中），2021，（11）：10-13.

[4]杨毅宇；周威；赵尚儒；刘聪；张宇辉；王鹤；王文杰；张玉清.物联网安全研究综述：威胁、检测与防御[J].通信学报，2021，42（08）：188-205.

[5]苏盛；汪干；刘亮；陈清清；王坤.电力物联网终端安全防护研究综述[J].高电压技术，2022，48（02）：513-525.

[6]曹蓉蓉；韩全惜.物联网安全威胁及关键技术研究[J].网络空间安全，2020，11（11）：70-75.

[7]彭安妮；周威；贾岩；张玉清.物联网操作系统安全研究综述[J].通信学报，2018，39（03）：22-34.