基于嵌入式开发技术的计算机网络安全防护模式

张颖忠
杭州云寰科技有限公司　浙江杭州　310000

摘　要：本文剖析嵌入式系统面临的恶意软件攻击、数据泄露等网络安全威胁，阐述基于嵌入式开发技术构建的网络安全防护模式，通过综合运用密钥管理、访问控制与身份验证、防火墙技术、漏洞扫描与修复等核心策略能够有效抵御各类网络攻击，保障嵌入式系统网络的安全性与稳定性。

关键词：嵌入式系统；计算机网络安全；防护

随着计算机网络的迅速发展，其所面临的安全风险也越来越大，传统的保护方法已经不能满足不断变化的攻击手段。由于其灵活高效和可定制等优点，使得其在网络安全方面具有很大的应用前景。

一、嵌入式系统面临的安全威胁

（一）资源有限性导致的安全挑战

从RAM和ROM容量小方面来看，其产生安全问题的原因主要有两方面，一方面有限的内存空间限制了安全软件的部署，完整且功能强大的安全防护软件通常需要较大的内存来存储代码和数据，而嵌入式系统的小容量RAM和ROM无法满足这些软件的运行需求，一些先进的加密算法和入侵检测程序，由于代码量较大难以完整地加载到嵌入式系统中运行，使得系统无法得到全面的安全防护。另一方面内存不足也会影响系统的正常运行和数据处理，在嵌入式系统中当运行多个任务时有限的内存会导致数据频繁地在内存和外部存储之间交换，不仅降低了系统的运行效率，还增加了数据在传输过程中被窃取或篡改的风险。

（二）部署环境多样化带来的风险

在工业生产环境里，嵌入式系统通常用于控制生产流程、监测设备状态，工业生产现场往往存在大量复杂的电气设备和机械设备，电磁干扰较为严重，这些干扰会影响嵌入式系统的正常通信和数据传输导致数据丢失或错误，使得系统发出错误指令，影响生产安全和产品质量。工业生产环境中的网络环境复杂，存在多个不同协议的网络相互连接，安全防护措施参差不齐，为攻击者提供了可乘之机，他们可以通过网络漏洞入侵嵌入式系统，篡改生产数据、破坏生产流程，造成严重的经济损失甚至人员伤亡。

（三）物理访问风险

从部署在公共或半公共环境来看，嵌入式系统面临着极大的物理访问风险，在公共交通站点、商场、酒店大堂等公共环境中嵌入式设备往往暴露在大量人员的视野范围内，任何人都有机会接近这些设备。一方面，普通公众可能因好奇或无意识的行为对设备进行操作，例如随意触摸、插拔设备的接口等导致设备的物理损坏或系统故障，影响设备的正常运行[1]。另一方面，心怀不轨的人可能会利用这个机会对设备进行恶意攻击，他们可以通过物理手段打开设备外壳获取内部存储的数据或者篡改设备的硬件电路和固件，实现对设备的控制或破坏，在半公共环境如企业办公区域，虽然有一定的人员限制，但也难以完全杜绝外部人员进入，外来访客可能会趁机对嵌入式系统进行物理接触，实施盗窃或破坏行为。许多嵌入式系统在设计和部署时没有充分考虑物理安全防护，一些设备没有安装坚固的外壳或防护装置容易被拆卸和破坏，部分设备没有设置有效的访问控制机制使得任何人都可以轻易地打开设备进行操作，在设备的安装位置上没有选择安全隐蔽的地方，而是随意放置在容易被触及的地方。

（四）通信安全威胁

如今，嵌入式系统广泛应用于智能家居、工业自动化、智能交通等众多领域，大量设备相互连接形成庞大的网络，在这个网络中设备之间需要实时、高效地交换数据以实现各种功能，例如智能家居系统中传感器会不断收集环境数据并传输给中央控制器，控制器再根据这些数据控制家电设备的运行，这种高频次的数据交换使得通信链路时刻处于繁忙状态，增加了数据暴露的机会[2]。

表1　网络安全威胁类型表

威胁类型	具体表现	影响范围
恶意软件攻击	病毒、蠕虫、木马等恶意程序感染嵌入式系统	系统功能异常、数据损坏
数据泄露	敏感数据被非法获取和传输	用户隐私泄露、商业机密丢失
拒绝服务攻击（DoS）	通过大量请求使系统资源耗尽，无法正常响应服务	系统瘫痪、业务中断
中间人攻击	攻击者拦截并篡改通信数据	数据完整性破坏、信息泄露

通信被窃听、篡改的风险增加也有其多方面原因，一方面无线通信技术在物联网中得到广泛应用，无线信号在空间中传播容易被不法分子利用专业设备进行截获和监听，攻击者可以在信号覆盖范围内设置监听装置获取通信数据，进而分析其中的敏感信息，另一方面通信协议本身可能存在安全漏洞，一些早期的通信协议在设计时没有充分考虑安全性容易被攻击者利用进行中间人攻击，攻击者可以在数据传输过程中插入虚假数据或篡改原有数据，导致系统接收到错误的信息，做出错误的决策引发严重的安全事故[3]。

二、基于嵌入式开发技术的网络安全防护策略

（一）密钥管理

对称加密与非对称加密在嵌入式系统中各有优势且应用广泛，对称加密算法因其加密和解密使用相同密钥，具有较高的加密效率，在资源受限的嵌入式设备中AES可以以较快的速度对大量数据进行加密，其加密速度能达到每秒数兆甚至数十兆字节，满足实时性要求较高的应用场景。而非对称加密使用公钥加密、私钥解密，提供了更高的安全性和身份验证功能，虽然RSA的加密速度相对较慢，通常每秒只能处理几百字节到数KB的数据，但在安全要求极高的场景如数字签名和密钥交换中不可或缺。在安全存储方面，嵌入式设备可以采用硬件安全模块（HSM）来存储密钥，HSM提供了物理级别的安全防护，能够有效防止密钥被非法读取和篡改，使用加密技术对密钥进行二次加密存储，例如使用Triple-DES算法对密钥进行加密进一步增强密钥的安全性。在密钥分发环节可采用Diffie-Hellman密钥交换算法，该算法允许通信双方在不安全的信道上安全地交换密钥，通过数学运算双方可以在不直接传输密钥的情况下生成相同的会话密钥，降低密钥在传输过程中被窃取的风险[4]。

（二）访问控制与身份验证

常见的身份验证方式有基于密码、令牌和生物特征识别等，基于密码的验证是最传统的方式，通过用户输入预设的密码与系统存储的密码进行比对来确认身份。为提高安全性要求密码具有一定的复杂度，通常密码由字母、数字和特殊字符组成且长度不少于8位，复杂密码能使暴力破解的时间从数秒延长至数年，令牌验证则利用硬件令牌或软件令牌生成动态密码增强身份验证的安全性，一些金融机构使用的USB令牌，每秒能生成不同的一次性密码，大大降低密码被盗用的风险[5]。权限管理策略是对已通过身份验证的用户进行细粒度的访问控制，可以采用基于角色的访问控制（RBAC）模型，根据用户的工作职责和业务需求分配不同的角色，每个角色对应特定的权限集合，如在一个工业嵌入式系统中普通操作员角色可能只有查看设备状态和执行基本操作的权限，而管理员角色则拥有系统配置、用户管理等高级权限，通过这种方式可以严格限制用户对系统资源的访问，防止越权操作[6]。

（三）防火墙技术

软件防火墙通常部署在嵌入式系统的操作系统中，成本较低且易于部署和配置，以常见的Linux系统中的iptables为例，它作为一款优秀的软件防火墙能灵活地对网络数据包进行过滤和转发，但软件防火墙依赖于系统资源，当嵌入式设备资源有限时会影响系统性能，在资源紧张的设备上运行软件防火墙可能会使系统CPU使用率提高10%-20%。防火墙规则的设置与优化是确保防火墙有效工作的核心，合理的规则能精确地控制网络流量，阻止非法访问，在设置规则时需遵循“最小权限”原则，只开放必要的端口和服务，对于一个只提供Web服务的嵌入式系统仅开放80或443端口，同时要根据实际业务需求和安全威胁动态调整规则，优化防火墙规则时可采用规则排序和规则合并的方法，将常用的规则放在前面能减少匹配时间，合并相似规则可降低规则数量提高防火墙的处理效率。

（四）漏洞扫描与修复

由于嵌入式系统运行环境复杂且面临着不断变化的网络攻击威胁，定期扫描能够及时发现系统中存在的安全漏洞，对于安全性要求较高的嵌入式系统建议每周进行一次全面的漏洞扫描，而对于一般应用场景的系统至少每月进行一次扫描。漏洞扫描工具可以检测缓冲区溢出、SQL注入等多种类型的漏洞，以Nessus为例，其作

为一款知名的漏洞扫描工具能够检测出超过45000种不同的安全漏洞，通过定期扫描可以构建系统安全状况的动态画像，及时发现新出现的漏洞为后续的修复工作提供依据[7]。

漏洞的及时修复与补丁管理可以消除安全隐患，一旦发现漏洞应立即评估其风险等级并根据等级制定相应的修复计划，对于高危漏洞必须在24小时内完成修复、中危漏洞可在一周内修复、低危漏洞则可以在一个月内安排处理。补丁管理是确保漏洞修复的有效方式，要建立完善的补丁管理流程，在部署补丁前需要在测试环境中进行充分测试确保补丁不会对系统的正常运行产生负面影响。

表2　不同防护策略对比表

防护策略	实现方式	优点	缺点
密钥管理	对称加密、非对称加密等	安全性高，可有效保护数据隐私	计算复杂度高，密钥管理难度大
访问控制与身份验证	密码验证、令牌验证、生物特征识别等	精确控制用户访问权限，防止非法登录	部分验证方式成本较高，如生物特征识别设备
防火墙技术	软件防火墙、硬件防火墙	阻止非法网络访问，过滤恶意流量	可能影响网络性能，规则配置复杂
漏洞扫描与修复	自动化漏洞扫描工具、定期手动检查	及时发现并修复系统漏洞，降低安全风险	扫描结果可能存在误报，修复过程可能影响系统正常运行

结论

网络安全是一个动态的、不断发展的领域，随着嵌入式技术的不断演进和网络攻击手段的日益复杂，需要持续关注和研究新的安全问题，不断优化和完善现有的防护模式。未来的研究可以进一步探索人工智能、区块链等新兴技术在嵌入式网络安全防护中的应用以应对更加严峻的网络安全挑战，为计算机网络的安全稳定运行提供更加坚实的保障。

参考文献

[1]赵鹏翔，马智超，刘菲，等.基于嵌入式开发技术的计算机网络安全防护模式研究[J].网络安全和信息化，2024，(12)：134-136.

[2]张玥.嵌入式系统中PLC模块的网络安全应对策略[J].网络安全和信息化，2024，(08)：147-149.

[3]周建华，李丰，湛蓝蓝，等.一种基于无害处理识别的嵌入式设备漏洞检测方法[J].信息安全研究，2023，9(10)：954-960.

[4]胡军.面向嵌入式操作系统的安全通信技术研究与实现[J].长江信息通信，2023，36(09)：156-158.

[5]张锋，孙慧洋，朱振荣.融合MAC-Lite私有协议的国产化嵌入式高速网络安全加密子系统研究[J].警察技术，2023，(04)：55-58.

[6]张慧.嵌入式治理：网络安全防御体系的制度嵌入原理[J].华侨大学学报(哲学社会科学版)，2023，(02)：103-116+129.

[7]陈为桢，面向物理隔绝网络的嵌入式处理器安全扫描技术.四川省，四川高速通科技有限公司，2023-03-01.