互联网智能终端安全防护技术研究

吕晓霖　王雪梅
国网天水供电公司　甘肃天水　741000

摘　要：互联网智能终端安全问题是不可回避的安全问题，对这一安全问题的妥善解决和加强维护，关系到国家网络安全建设的重要工作。因此，本文首先对互联网智能终端安全的诸多方面进行阐述，包括智能终端物理安全、智能终端软硬件安全、智能终端运行安全、智能终端数据安全以及智能终端数据安全五个方面。此外，为了解决这五个方面的安全问题，通过安全选型、启动安全、数据安全以及安全传输四个方面进行论述，提出，要在安全选型方面，选用具有可信平台模块或安全功能的硬件；要在启动安全方面，利用安全驱动保证系统安全；要在数据安全方面，采取轻量级密码算法加密数据；要在安全传输方面，践行TLS/SSL协议加密传输。

关键词：智能终端；安全防护；互联网技术

一、互联网智能终端安全概述

互联网的快速发展使得智能终端成为生产生活中不可或缺的一部分。然而，随之而来的是，人们对互联网智能终端安全的关注。本文将从多个角度探讨互联网智能终端的安全问题，主要包括智能终端物理安全、智能终端软硬件安全、智能终端通信安全、智能终端运行安全、智能终端运行安全、智能终端数据安全。如下图1所示。

1.智能终端物理安全

首先从智能终端的物理安全方面展开讨论，互联网智能终端的物理安全是指保护智能终端设备免受物理损害和未经授权的访问。以下是几个需要考虑的物理安全问题。

其一，内部人员管理。互联网智能终端一般位于智能工厂内部，接触终端的人员主要是内部人员。为了确保终端的物理安全，应加强内部人员管理，建立严格的设备管理制度。只有经过授权的人员才能接触终端设备，这样可以减少未经授权的访问和潜在的安全风险。

其二，设备状态监控。为了及时发现异常情况，可以对智能终端设备进行设备状态监控。通过监控设备的上下线情况，可以及时发现异常上下线情况，并进行报警和拒绝非授权接入。这样可以有效防止未经授权的人员对终端设备进行访问，保护设备的物理安全[1]。

2.智能终端软硬件安全

随着互联网的快速发展，智能终端安全问题的日益突出。下面将从智能终端软硬件安全的角度出发，探讨智能终端安全的重要性以及存在的问题，并提出相应的解决方案。

其一，智能终端硬件安全。智能终端的硬件安全是保障整个系统安全的基础。然而，智能终端的芯片可能存在致命的安全后门或漏洞，这些安全隐患可能被黑客利用，导致用户的个人信息泄露、设备被远程控制等问题。因此，智能终端制造商应加强对硬件的安全性检测和控制，确保芯片的安全性。

其二，智能终端软件安全。智能终端的软件安全同

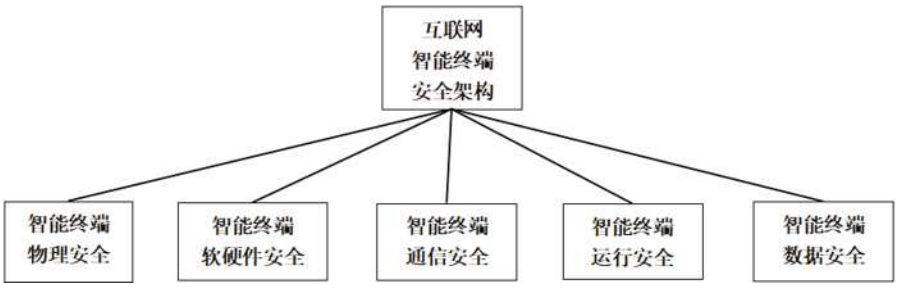

图1　互联网智能终端安全架构示意图

作者简介：
吕晓霖（1977.08）男，汉，籍贯：山东省莱州市，职称：副高，学历：本科，研究方向：信息网络。
王雪梅（1992.01）女，汉，籍贯：甘肃省兰州市，职称：中级，学历：硕士，研究方向：信息安全。

ISSN: 2661-3719(Print); 2661-3727(Online)

样重要。在出厂前，智能终端可能预装了操作系统和一些应用软件，然而，这些软件可能存在各种漏洞，如代码缺陷、权限不当等。黑客可以通过利用这些漏洞来入侵用户的设备，获取用户的敏感信息。因此，智能终端制造商应加强对软件的安全性测试和更新，及时修复漏洞，确保用户的数据安全[2]。

3.智能终端通信安全

在互联网的蓬勃发展的新时代，智能终端通信安全的问题已经不容忽视。下面将从智能终端通信安全的角度出发，探讨如何保障智能终端的通信安全，以防止窃听、篡改和破坏等安全威胁。

其一，加密传输。智能终端应该具备加密传输的能力，将重要数据进行加密后再进行传输。这样即使被窃听，攻击者也无法获取有用的信息。常见的加密算法有AES、RSA等，可以根据具体情况选择合适的加密算法。

其二，身份鉴别和认证。智能终端在进行通信时，应该对设备进行身份鉴别和认证。这可以通过使用数字证书、密钥交换协议等方式实现。只有通过身份验证的设备才能进行通信，从而防止欺骗攻击[3]。

4.智能终端运行安全

在互联网中，各种智能终端设备对实时性和可用性的要求较高。因此，为了防止智能终端因电力、网络、软件等故障而导致互联网系统停摆，我们需要采取一系列措施来保障智能终端的运行安全。

其一，备用电源和不间断电源（UPS）等设施能够有效地自动切换，以确保在电力故障时智能终端能够继续正常运行。备用电源可以是电池、发电机等，能够提供持续的电力供应，保证智能终端的稳定运行。

其二。通过采用Supreme-Ring等协议来保障网络冗余。网络冗余是指在网络中设置多条冗余路径，当某一路径发生故障时，可以自动切换到其他可用路径，确保数据的传输不受影响。这样一来，即使某个网络节点出现故障，智能终端仍然能够与其他节点进行通信，保证互联网系统的连续性。

其三，严格进行软件安全测试也是保障智能终端运行安全的重要措施。在开发和部署智能终端软件时，应进行全面的安全测试，确保软件与终端的兼容性和稳定性。同时，及时修复软件中的漏洞和安全隐患，以防止黑客利用这些漏洞进行攻击。

5.智能终端数据安全

智能终端上的数据安全是指在数据的收集、存储、处理、传输、备份和删除等环节中保护数据的安全性。在智能互联网中，智能终端上的数据种类繁多，有着不同的安全要求，有些需要实时性和高可靠性，有些需要高保密性，还有些需要保护隐私。

其一，根据数据的重要性和敏感性，将数据分为不同的等级，并采取相应的安全措施。比如，对于高保密性的数据，可以采用加密技术进行保护，确保只有授权人员能够访问和使用这些数据。对于实时性要求高的数据，可以采取实时备份和冗余存储的方式，以防止数据丢失或损坏。

其二，数据的传输过程也需要注意安全性。在数据传输过程中，可能会面临窃听、篡改和伪造等风险。因此，应该采用安全的传输协议和加密技术，确保数据在传输过程中的机密性和完整性。同时，还可以使用数字签名等技术来验证数据的真实性和可信度。

其三，智能终端上的数据还需要进行安全备份和删除。安全备份可以保证数据在意外情况下的恢复能力，而安全删除可以确保数据在不再需要时被彻底清除，避免被恶意利用。

二、互联网智能终端安全防护

互联网的飞速发展，使得互联网智能终端安全的问题逐渐棘手。故而，为了妥善处理上述各项安全隐患，需要针对安全选型、启动安全、数据安全、安全传输等各个环节提出措施，以加强对互联网智能终端安全防护。下面是互联网智能终端安全防护架构图。

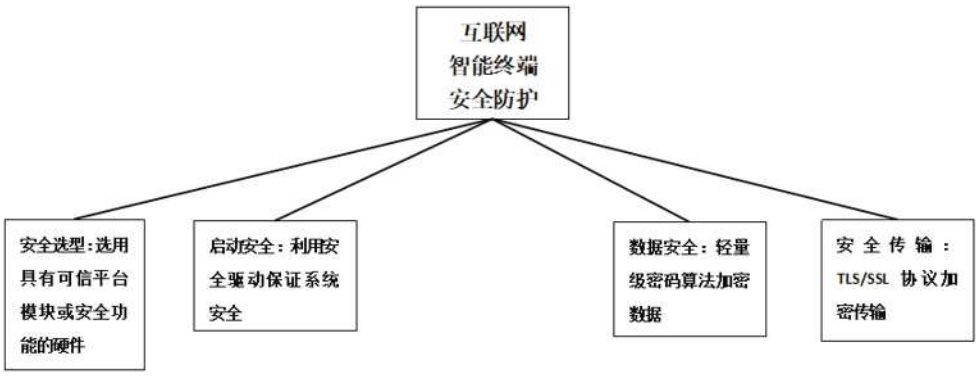

图2　互联网智能终端安全防护架构图

1.安全选型：选用具有可信平台模块或安全功能的硬件

在选择互联网智能终端时，应优先选择具有可信平台模块（TPM）或其他安全功能的硬件。可信平台模块是一种硬件安全芯片，可以提供安全存储、加密计算和身份验证等功能。通过使用可信平台模块，可以保护终端设备的安全性，防止恶意软件的攻击和数据的泄露。此外，还可以选择具有硬件加密引擎、安全启动功能和安全存储功能等的硬件，以提高终端设备的安全性。

2.启动安全：利用安全驱动保证系统安全

启动安全是保证互联网智能终端系统安全的重要环节。在启动过程中，如果系统被恶意软件篡改或感染，将会导致严重的安全问题。为了保证启动安全，可以利用安全驱动来验证系统的完整性和真实性。安全驱动可以对系统进行数字签名验证，确保系统没有被篡改或感染。此外，还可以使用启动密码或生物识别技术来加强系统的身份验证，防止未经授权的访问。

3.数据安全：轻量级密码算法加密数据

面将从数据安全的角度，介绍互联网智能终端的安全防护措施，包括轻量级密码算法、自主商用密码体系和互联网数据分类分级安全。

其一，国外轻量级密码。数据安全是互联网智能终端安全的重要组成部分。为了保护数据的机密性和完整性，可以采用轻量级密码算法来加密数据。轻量级密码算法是一种针对资源受限设备设计的密码算法，具有较低的计算和存储开销，适合在互联网智能终端上使用。国外已经有一些成熟的轻量级密码算法，如PRESENT、SIMON和SPONGENT等。这些算法可以有效地保护数据的安全性，防止数据被未经授权的访问和篡改。

其二，自主商用密码体系。除了使用国外的轻量级密码算法，还可以推动自主商用密码体系的发展。自主商用密码体系是指由国内自主研发的密码算法和密码技术。通过自主商用密码体系，可以减少对国外密码算法的依赖，提高数据安全的可控性。目前，国内已经有一些自主商用密码算法，如SM系列算法和国密算法等。这些算法在保护数据安全方面具有重要的意义，可以在互联网智能终端上得到广泛应用。

其三，互联网数据分类分级安全。此外，互联网中的数据种类繁多，有些数据具有较高的保密性要求，有些数据需要实时性和高可靠性，因此需要对数据进行分类分级处理。通过对数据进行分类分级，可以采取不同的安全措施来保护数据的安全性。比如，对于高保密性的数据，可以采用加密技术进行保护；对于实时性要求高的数据，可以采取实时备份和冗余存储的方式；对于一般性的数据，可以采取常规的安全措施来保护[4]。

4.安全传输：TLS/SSL协议加密传输

随着互联网智能终端的广泛应用，安全传输成为了保护用户隐私和数据安全的重要环节。下面将从安全传输的角度，介绍互联网智能终端的安全防护措施，包括HTTPS和TLS/SSL协议以及基于零信任架构的安全传输体系。

其一，HTTPS和TLS/SSL协议。安全传输是保证互联网智能终端数据安全的重要手段。为了防止数据在传输过程中被窃听或篡改，可以采用TLS/SSL协议进行加密传输。TLS（Transport Layer Security）和SSL（Secure Sockets Layer）是一种加密协议，可以在通信双方之间建立安全的通信通道，保护数据的机密性和完整性。通过使用TLS/SSL协议，可以有效防止中间人攻击和数据篡改，确保数据在传输过程中的安全性。另外，为了进一步提高安全传输的可靠性，可以采用HTTPS和TLS/SSL协议来保护数据的传输。

其二，基于零信任架构的安全传输体系。基于零信任架构的安全传输体系也是一种重要的安全防护措施。零信任架构是一种安全理念，认为在互联网环境中，任何设备和用户都不可信，需要对其进行严格的身份验证和访问控制。

三、结语

为了实现互联网技术稳步发展，加快互联网基础建设持续推进，必须切实做好互联网智能终端安全基础建设的技术支撑工作和相关安全指标体系的建设工作。面对互联网基础设施安全防护工作，必须深挖各种技术安全防护办法，切实提升互联网运行质量和网络安全。

参考文献：

[1]彭光彬.工业互联网智能终端安全防护技术研究[J].工业信息安全，2022（09）：20-26.

[2]喻俊浔，沈宏杰.能源互联网信息安全威胁防护架构研究[J].科技广场，2017（07）：99-102.

[3]智能终端将成为网络安全防护的重点目标[J].计算机安全，2012（07）：95.

[4]单寅.移动互联网安全备受关注　加大立法和监管势在必行[J].世界电信，2012，25（04）：65-69.