# LTE Standard

# 安全防护设计

**LTE Standard 模块系列**

版本：LTE_Standard_安全防护设计_V1.0

日期：2019-10-24

状态：受控文件

上海移远通信技术股份有限公司始终以为客户提供最及时、最全面的服务为宗旨。如需任何帮助，请随时联系我司上海总部，联系方式如下：

上海移远通信技术股份有限公司
上海市闵行区田林路 1016 号科技绿洲 3 期（B 区）5 号楼　　邮编：200233
电话：+86 21 51086236　　邮箱：info@quectel.com

或联系我司当地办事处，详情请登录：
http://www.quectel.com/cn/support/sales.htm

如需技术支持或反馈我司技术文档中的问题，可随时登陆如下网址：
http://www.quectel.com/cn/support/technical.htm
或发送邮件至：support@quectel.com

**前言**

上海移远通信技术股份有限公司提供该文档内容用以支持其客户的产品设计。客户须按照文档中提供的规范、参数来设计其产品。由于客户操作不当而造成的人身伤害或财产损失，本公司不承担任何责任。在未声明前，上海移远通信技术股份有限公司有权对该文档进行更新。

**版权申明**

# 文档历史

## 修订记录

| 版本 | 日期 | 作者 | 变更表述 |
| --- | --- | --- | --- |
| 1.0 | 2019-10-24 | 李循威 | 初始版本 |

# 目录

# 1 引言

## 1.1. 简介

LTE Standard 模块默认 Linux 系统不接入网络，因此攻击者无法远程登录或控制模块操作系统。

如果需要使用 ECM、RNDIS、SGMII 和 Wi-Fi 等功能，则应该通过模块 AP 侧 Linux 系统的 TCP/IP 协议栈接入 Internet 网络。Linux 系统接入网络时，需要在客户设备与通信模块两部分都进行网络安全防护。网络安全框架如下图所示。

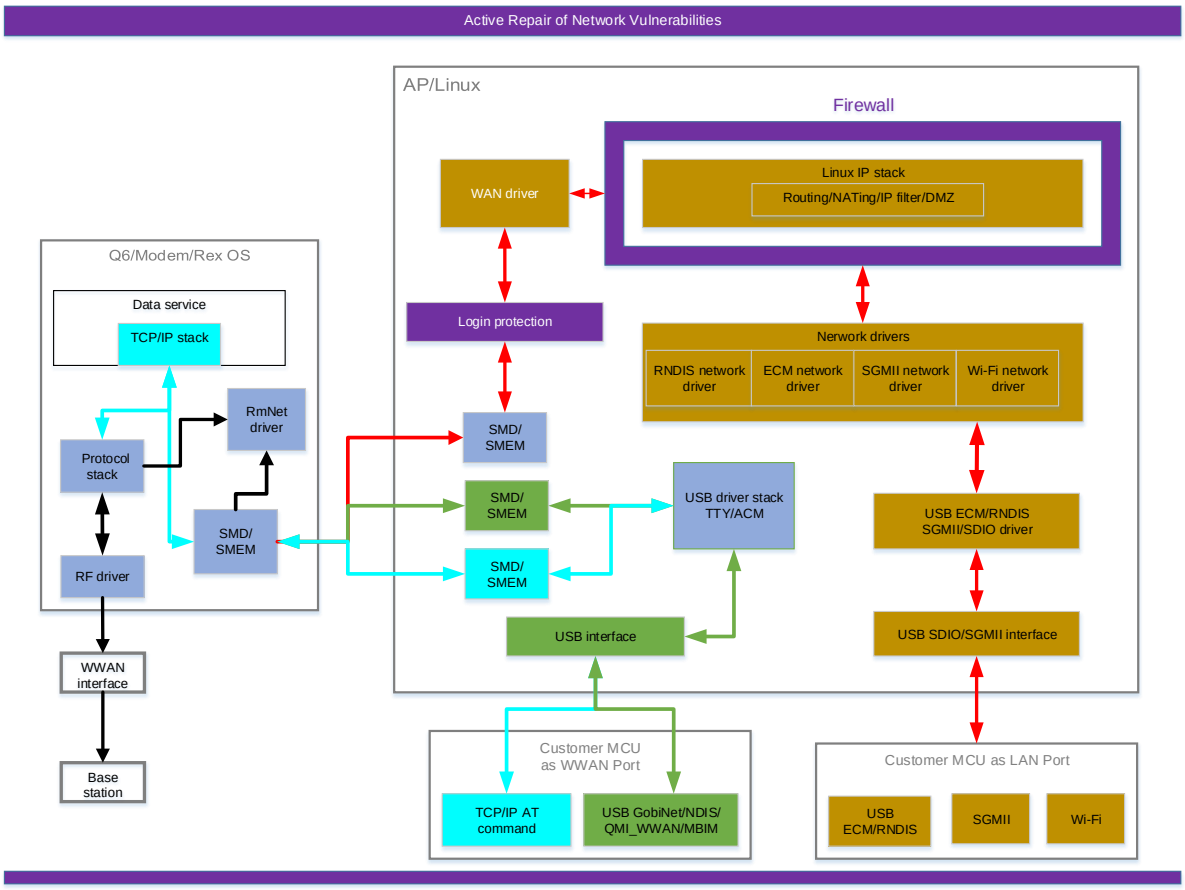


图 1：网络安全框架

## 1.2. 适用模块

本文档适用于以下 LTE Standard 模块：

- EC2x：EC25、EC21、EC20 R2.0、EC20 R2.1
- EG2x-G: EG25-G、EG21-G
- EG9x：EG91、EG95
- EM05
- EP200F

# 2 安全防护措施

移远通信将持续在模块固件中合入 patch 以修复各类公开的软件漏洞，以及启用防火墙机制，关闭所有不必要的远程监听端口、远程登录服务和网络端口（如 ADB 远程调试端口），从而避免模块被远程破解和控制。

同时，移远通信将启用 Linux 控制台的登录防护，以避免恶意登录和调试。如果需要使用 Linux 控制台进行必要的调试，需采用 RSA 非对称加密算法或采用硬件 ID 绑定的方式，且仅在通过由移远通信内部服务器密码认证后方可开启相关服务。

## 2.1. 网络安全防护

网络安全防护支持基于 Netfilter 的防火墙功能并定期修复公开的网络程序漏洞，主要防护措施如下。

1. 过滤传入/传出数据包，以防御 SYN Flood、ping Flood、UDP Flood、Fragmentation bomb、ICMP routing redirect bomb 等攻击；
2. 端口保护，即禁用不使用的端口，以及关闭端口扫描应答；
3. 若使用内置协议栈 SSL，移远通信后续将提供安全存储方案，用于储存客户的通信证书，避免客户密钥证书被窃取。

## 2.2. Linux 登录防护

Linux 控制台的登录防护是安全防护的核心内容，主要防护措施如下。

1. 默认禁止远程登录端口和远程登录服务。如需开启 Linux 控制台，使用 RSA 非对称校验算法并通过移远通信内部服务器密码认证后方可开启相关服务；
2. 禁止未授权用户登录（未授权用户无法获取模块登录信息）；
3. 绑定初始密码和硬件 ID，并采用强密码技术，避免一个模块密码被破解导致所有模块都被破解。

# 3 常见攻击方式及防御手段

## 3.1. GSM 伪基站攻击

**攻击方式：**

攻击者利用模块接入的 GSM 网络将模块接入伪基站中，通过伪基站对模块进行网络攻击。

**防御手段：**

当客户程序与客户服务器进行端到端通信时，使用双向认证机制；在双向认证机制下，即便模块接入伪基站后也不会将伪基站当成服务器。

## 3.2. 私有 APN 攻击

**攻击方式：**

攻击者接入模块所属的私有 APN 网络并进行扫描，寻找可以攻击的模块。

**防御手段：**

建议客户与运营商沟通，将私钥 APN 网络进行网络隔离，保证模块通信端口不会暴露在 APN 网络中。

## 3.3. 模块 AT 命令漏洞攻击

**攻击方式：**

攻击者通过 **AT+QLINUXCMD** 及功能上与其类似的 AT 命令对模块实施 linux 命令注入攻击。

**防御手段：**

模块已经不支持 **AT+QLINUXCMD** 及功能上与其类似的 AT 命令，不预留命令相关调试后门。

## 3.4. SSL KEY 泄漏攻击

**攻击方式：**

攻击者通过模块 SSL KEY 明文保存获取 KEY，从而伪装成服务器与模块进行通信并控制模块。

**防御手段：**

若使用移远通信内置协议栈，模块支持安全存储功，移远通信可将 SSL KEY、证书、模块硬件 ID 进行加密绑定，并写入特殊文件系统，建议客户在生产的过程中将 SSL KEY 及证书植入到模块中。

若使用外置协议栈，客户端需确保 SSL KEY 和证书的安全存储。

## 3.5. OTA 攻击

**攻击方式：**

攻击者劫持 OTA 服务器，获取升级包，从而实施攻击。

**防御手段：**

建议客户采用安全机制以保护 OTA 服务器，避免被攻击者劫持。模块端的升级程序将会对升级包进行合法性验证。

## 3.6. TSP 攻击

**攻击方式：**

攻击者利用单向认证机制，伪装成 TSP，从而实施攻击。

**防御手段：**

建议客户应用程序与 TSP 服务器通信采用双向认证机制，防止中间人进行攻击。

# 4 安全防护建议

在使用模块时，建议客户采取如下安全防护措施：

1. 与运营商沟通，将私有 APN 网络进行网络隔离，避免攻击者通过客户的私有 APN 网络对同一 APN 网络下的其他的设备发起攻击。
2. 当客户应用程序与客户服务器通信时，采用双向认证机制，避免中间人攻击，移远通信将提供该机制所需的组件。
3. 对于客户设备远程控制接口，比如远程短信 AT 命令接口，需要采取双向鉴权或者启用白名单机制，避免设备被非授权设备恶意控制。
4. 客户 OTA 服务器采用 OTA 安全机制，避免 OTA 服务器被攻击者劫持后下发错误的升级包导致模块工作异常。

# 5 附录 A 术语缩写

表 1：术语缩写

| 缩写 | 英文全称 | 中文全称 |
|---|---|---|
| ACM | Abstract Control Model | 抽象控制模型 |
| AP | Application Processor | 应用程序处理器 |
| APN | Access Point Name | 接入点 |
| DMZ | Demilitarized Zone | 隔离区 |
| ECM | Ethernet Networking Control Model | 以太网网络控制模型 |
| GSM | Global System for Mobile Communications | 全球移动通信系统 |
| ICMP | Internet Control Message Protocol | 互联网控制报文协议 |
| MCU | Micro Control Unit | 微控制单元 |
| OTA | Over-The-Air | 空中下载 |
| RNDIS | Remote Network Driver Interface Specification | 远程网络驱动接口规范 |
| SDIO | Secure Digital Input and Output Card | 安全数字输入输出卡 |
| SGMII | Serial Gigabit Media Independent Interface | 串行千兆媒体独立接口 |
| SMD | Shared Memory Driver | 共享内存驱动 |
| SMEM | Shared Memory | 共享内存 |
| SSL | Secure Sockets Layer | 安全套接层 |
| TCP/IP | Transmission Control Protocol/Internet Protocol | 传输控制协议/网际协议 |
| TSP | Telematics Service Provider | 远程通信服务提供商 |
| USB | Universal Serial Bus | 通用串行总线 |
| WWAN | Wireless Wide Area Network | 无线广域网 |