LTE Standard
Security Protection Design

LTE Standard Module Series

Rev. LTE_Standard_Security_Protection_Design_V1.0

Date: 2019-10-24

Status: Released

Our aim is to provide customers with timely and comprehensive service. For any assistance, please contact our company headquarters:

Quectel Wireless Solutions Co., Ltd.
Building 5, Shanghai Business Park Phase III (Area B), No.1016 Tianlin Road, Minhang District, Shanghai, China 200233
Tel: +86 21 5108 6236
Email: info@quectel.com

Or our local office. For more information, please visit:
http://www.quectel.com/support/sales.htm

For technical support, or to report documentation errors, please visit:
http://www.quectel.com/support/technical.htm
Or email to: support@quectel.com

GENERAL NOTES

COPYRIGHT

About the Document

History

Revision	Date	Author	Description
1.0	2019-10-24	Darren LI	Initial

Contents

1 Introduction

1.1. General Description

By default, the Linux OS of Quectel LTE standard modules will not access the network, and thus the attacker cannot remotely log in or control the operating system of the module.

If features of RNDIS, ECM, SGMII and Wi-Fi drivers are needed, the module will access the Internet through the TCP/IP protocol stack of Linux system on AP side. When Linux system accesses the Internet, the security protection must be performed both in customers' device and the module. The network security framework is shown as the following figure.

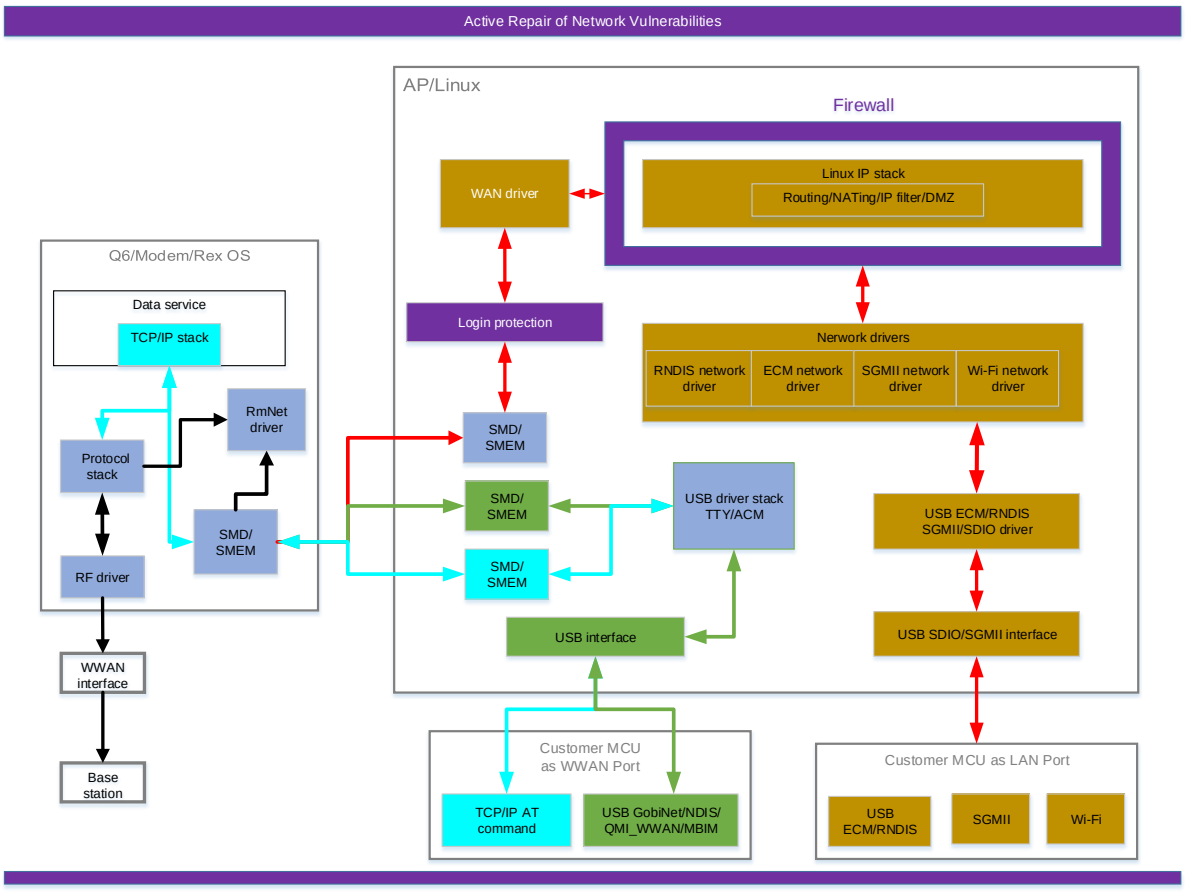

Figure 1: Network Security Framework

1.2. Applicable Modules

This document is applicable to the following Quectel LTE Standard modules.

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

2 Security Protection Measures

Quectel will continuously merge the patches into the module's firmware to fix various public software vulnerabilities, and enable the firewall to turn off all the unnecessary remote listening ports, remote login services and network ports (such as ADB remote debug ports) to prevent module being remotely cracked and controlled.

Meanwhile, Quectel will enable the login protection for Linux console to avoid malicious login and debugging. If the Linux console needs to be used for debugging, the RSA asymmetric encryption algorithm or the hardware ID binding will be used; and the Linux console can only be enabled after passing the password authentication of Quectel's internal server.

2.1. Network Security Protection

With the Netfilter-based firewall function supported and the public software vulnerabilities regularly fixed, the main network security protection measures are as follows.

1. Filter incoming/outgoing packets for protecting against attacks like SYN Flood, ping Flood, UDP Flood, Fragmentation bomb, ICMP routing redirect bomb, etc.
2. Protect the port, i.e. disable the unused ports and their scanning response function.
3. If the built-in protocol stack SSL is used, Quectel will provide a security storage solution for storing the customers' communication certificate to avoid their key certificate being filched in the future.

2.2. Linux Login Protection

The login protection for Linux console is the core of the security protection, and the main protection measures are as follows.

1. Disable the remote login port and service by default. If the Linux console needs to be enabled, the RSA asymmetric encryption algorithm should be used and the related services of the console can only be enabled after passing the password authentication of Quectel's internal server.
2. The unauthorized user login is prohibited (Unauthorized users cannot obtain the login information).
3. Bind the initial password to the hardware ID, and use the strong password technology to prevent the module's password from being cracked and causing all modules to be cracked.

3 Common Attacks and Defense Methods

3.1. GSM Pseudo Base Station Attack

Attack Method:
The attacker uses the GSM network accessed by the module to make the module access the pseudo base station and performs network attack through the pseudo base station.

Defense Method:
When the customers' application program performs end-to-end communication with their server, the two-way authentication mechanism will be used, in which the pseudo base station is not regarded as a server even after the module accesses the pseudo base station.

3.2. Private APN Attack

Attack Method:
The attacker accesses the private APN network which the module accesses and scans it to find the module that can be attacked.

Defense Method:
It is recommended that customers communicate with the operator to isolate the private key APN network and ensure that the module communication port is not exposed to the APN network.

3.3. Module AT command Vulnerability Attack

Attack Method:
The attacker performs a Linux command injection attack on the module through AT command like **AT+QLINUXCMD** and the commands with the similar functions to it.

Defense Method:
LTE Standard modules do not support AT commands like **AT+QLINUXCMD** and the commands with the similar functions to it anymore. Additionally, the related debugging backdoor will not be reserved.

3.4. SSL KEY Vulnerability Attack

Attack Method:
The attacker obtains the KEY through the SSL KEY plaintext store, thereby disguising as the server to communicate with the module and control it.

Defense Method:
If the Quectel's' built-in protocol stack is used, the module will support security storage feature and Quectel will encrypt and bind the SSL KEY, certificate, and hardware ID, and store them to the special file system. It is recommended that customers embed the SSL KEY and certificate into the module during the production process.

If an external protocol stack is used, the security storage of the SSL KEY and certificate need to be ensured on client side.

3.5. OTA Attack

Attack Method:
The attacker hijacks the OTA server and obtains the upgrade package to perform the attack.

Defense Method:
It is recommended that customers take security mechanisms to protect OTA servers from being hijacked by attackers. The upgrade program of the module will verify the validity of the upgrade package.

3.6. TSP Attack

Attack Method:
The attacker uses a one-way authentication mechanism to disguise as a TSP server to perform the attack.

Defense Method:
It is recommended to use the two-way authentication mechanism between the communication of customer application program and TSP server to prevent the attack by the man-in-the-middle.

4 Security Protection Recommendation

It is recommended for customers to take the following security protection measures when using modules.

1. Communicate with the operator to isolate the private key APN network to prevent the attacker attacking other devices over the same APN network through the customers' private APN network.
2. Take the two-way authentication mechanism for the communication between customer application program and customer server to avoid the attack from the man-in-the-middle, and Quectel will provide the necessary components for the mechanism.
3. For remote control interface of customers' device, such as for remote SMS AT command interface, two-way authentication or enabling the whitelist mechanism are required to prevent the device from being maliciously controlled by the unauthorized device.
4. Take the security mechanisms of OTA servers to prevent the OTA server being attacked and sending the wrong upgrade package to cause the module to work abnormally.

5 Appendix A Terms and Abbreviations

Table 1: Terms and Abbreviations

Abbreviation	Description
ACM	Abstract Control Model
AP	Application Processor
APN	Access Point Name
DMZ	Demilitarized Zone
ECM	Ethernet Networking Control Model
GSM	Global System for Mobile Communications
ICMP	Internet Control Message Protocol
MCU	Micro Control Unit
OTA	Over-The-Air
RNDIS	Remote Network Driver Interface Specification
SDIO	Secure Digital Input and Output Card
SGMII	Serial Gigabit Media Independent Interface
SMD	Shared Memory Driver
SMEM	Shared Memory
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TSP	Telematics Service Provider
USB	Universal Serial Bus
WWAN	Wireless Wide Area Network