QuecOpen

安全技术导读

LTE 系列

版本： QuecOpen_安全架构介绍_V0.1

日期：2018-07-30

状态：临时文件

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
上海市徐汇区虹梅路 1801 号宏业大厦 7 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://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://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	2018-07-30	钱润生	初始版本

目录

表格索引

未找到图形项目表。

图片索引

1 引言

1.1. 定义

保护的对象：

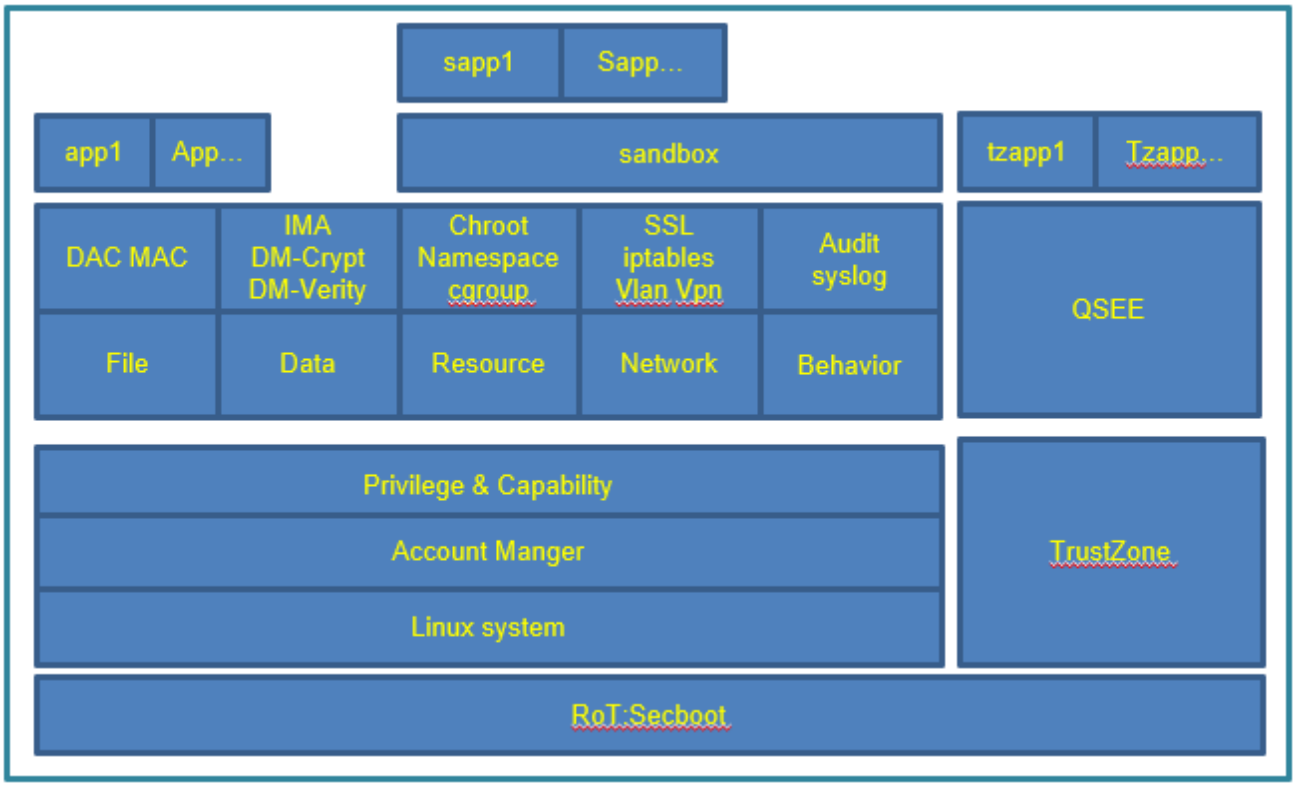
1）设备
2）信息
3）人

软硬件怎么保护？

1）安全启动: Root of Trust
1）平台安全：安全的起点，。
2）数据安全：机密性，完整性，合法性。
3）行为安全：访问控制与记录，限制隔离，通信保密。
4）？

硬件的安全除了保护设备和数据，还有人。本文尽量从软件的角度考虑，对于硬件安全不做过多展开讨论，只顺带提及一下。

1.2. QuecOpen 安全框架



1.3. QuecOpen 安全功能状态

功能	状态	下一步计划	备注
Secboot	开发完毕	完善 pki	
Dm-verity	开发完毕	完善 pki	仅限 AG35&AG36
Tz APP 环境开放	正在研究		仅限 AG35 le2.2 基线
TZ 安全存储	正在研究		仅限 AG35
TZ 加密服务	部分实现	完善加密服务	仅限 AG35
Selinux	开发完毕	内部培养接口人	仅限 AG35
AB 系统	开发完毕		仅限 AG35&AG36
Linux 系统安全	随系统自身特性而定		
Linux 网络安全	随系统自身特性而定		
CVE 漏洞检查			
Sandbox 系统	暂时未启动		

2 密码技术

机密性，完整性，认证（授权与鉴权），不可否认性。

2.1. 对称密码

介绍一下原理，模式

2.2. 公钥密码

介绍一下密钥构成

2.3. 单向散列

2.4. 消息认证

2.5. 数字签名

2.6. 随机数

2.7. 证书与 CA

证书格式标准规范由相关 PKI 组织制定，通常常用标准 X509、PKCS#7，PKCS#12

2.8. PKI

公钥基础设施（PKI）是为了能够有效地运用公钥而制定的一些列规范和规格的总称。PKI 提供的功能由包含上述说的秘密算法、证书、认证机构， 以及特定的业务应用。

（1）ITU 提出的 X509 规范。

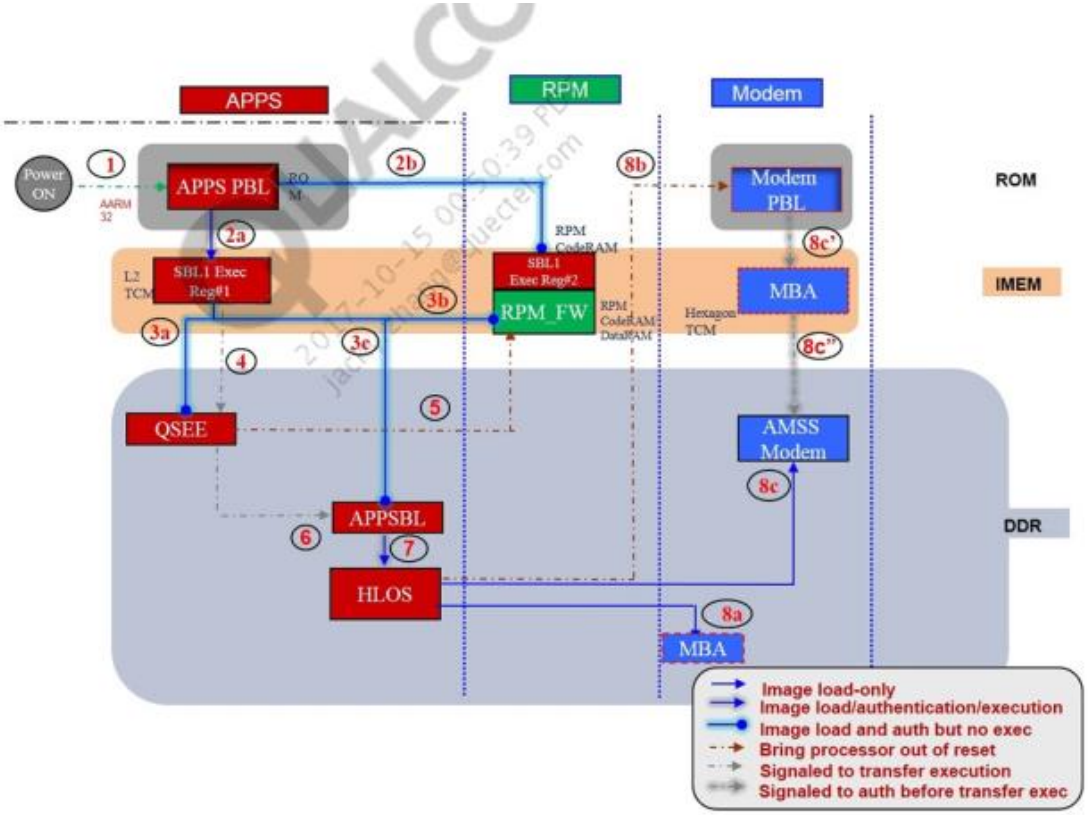
（2）RSA 公司提出的 PKCS 规范

（3）各个政府、企业也会提出。

3 平台安全

从物理 Rot 的建立、运行环境隔离、设备的稳定性三方面入手。

3.1. SECBOOT



MDM9628 secure boot flowchart

图 2 AG35 固件启动流程

3.2. 物理隔离

3.2.1. TrustZone

Quectel 提供 TrustZon 加解密功能：
对称加解密(AES)：生成秘钥、导入秘钥、加密、解密；
非对称加解密（RSA）：生成钥对、导入钥对、签名、校验、导出公钥。

3.2.2. 调试口保护

（1）硬件封装。
（2）软件关闭 JTAG、adb、fastboot, ssh。

3.3. 稳定性技术

这里从软件的角度考虑

3.3.1. 看门狗

3.3.2. EMC 保护

//不讨论

3.3.3. 高低温保护

低功耗技术，其他

3.3.4. 备份还原

AB 系统

4 Linux 系统安全

以下部分安全特性默认不开启，对于 open 客户需要自己去打开内核选项。

重点目标：用户、文件、CPU、MEM、FLASH、网络。

4.1. 账户管理

4.2. 文件访问控制

4.2.1. DAC

本模块默认支持的访问控制就是传统的 Linux 自主访问控制模式（DAC）

4.2.1.1. 标准模式

就是传统的根据文件的属主、组，允许位（rwx）以及进程的 uid 、euid 等管理进程的访问权限控制。另外，部分文件系统（ext 、ubifs 等）还支持隐藏属性模式控制文件权限，使用 lsattr chattr 查看和修改。

4.2.1.2. 扩展模式

文件的扩展属性，有一部分用于 DAC 模式，另一部分用于 MAC 模式。这里介绍 ACL：

ACL 参数是保存在文件系统里面。使用时不同文件系统（ext tmpfs 等）需要打开内核选项（注 UBIFS 文件系统不支持），同时还需要安装 attr 和 acl 软件工具包。

4.2.2. MAC

4.2.2.1. SELinux

Quectel 会提供该功能的开关功能，针对进程服务、文件的增加安全权限策略提供方案技术。SELinux 的工作过程如下图所示：

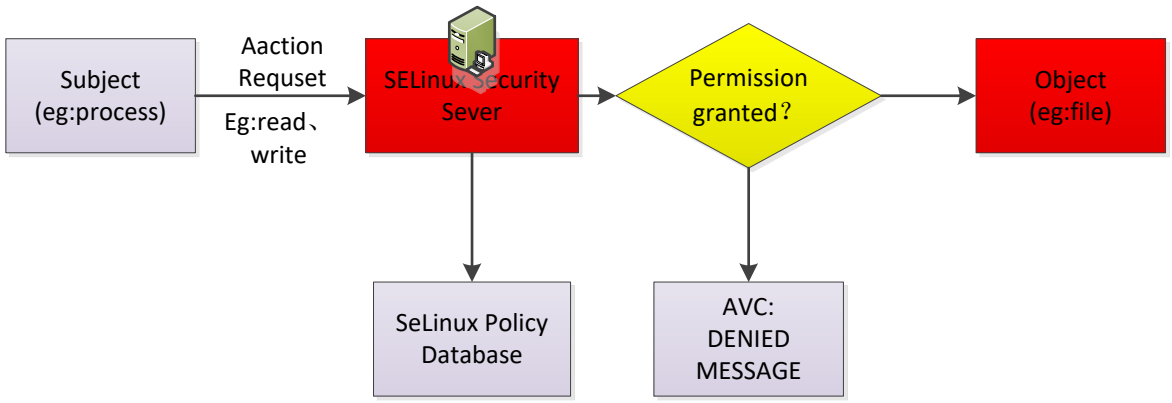


图 4 SELinux 工作过程

当一个主体 subject(如: 一个应用)试图访问一个客体 object(如：一个文件)，Kernel 中的策略执行服务器将检查 AVC (Access Vector Cache), 在 AVC 中，subject 和 object 的权限被缓存(cached)。如果基于 AVC 中的数据不能做出决定，则请求安全服务器，安全服务器在一个矩阵中查找“应用+文件”的安全环境。然后根据查询结果允许或拒绝访问，拒绝消息细节位于/var/log/messages 中。

使用步骤简要如下：

开启 SELinux 功能

为资源（文件）设定标签

针对特殊的 subject 和 object 建立 policy 并添加到 policy 数据库

策略文件可以单独存放于一个分区中，便于单独升级策略。

4.2.2.2. SMACK

与 SELinux 功能互斥，内核只能二选一，除了安装文件系统的扩展模式的工具，不需要安装别的额外工具。

Legato 默认使用 SMACK 此功能。

4.3. 数据安全保护

4.3.1. 密钥管理

Kernel key

4.3.2. 数据加密

针对文件---eCryptfs,针对分区----dm-crypt

4.3.3. 数据完整性

（1）Dm-verity 实现对整个只读分区文件系统保护（在 Linux 下其实就是 dev 下面一个设备）。

（2）IMA/EVM 实现对文件系统里面各个文件的保护，防止被离线修改。

4.3.3.1. DM-verity

QUCETL 实现基于 DM-Verity 机制实现对文件系统的安全检查，使用的基本步骤如下：

- 生成文件系统 image.
- 生成文件系统 image 的 hash 树.
- 构建 此 hash 树的 dm-verity 表.
- 对 dm-verity 表签名.
- 绑定 dm-verity 表和签名到元数据 metadata.
- 连接 image、verity metadata 和 hash 树.

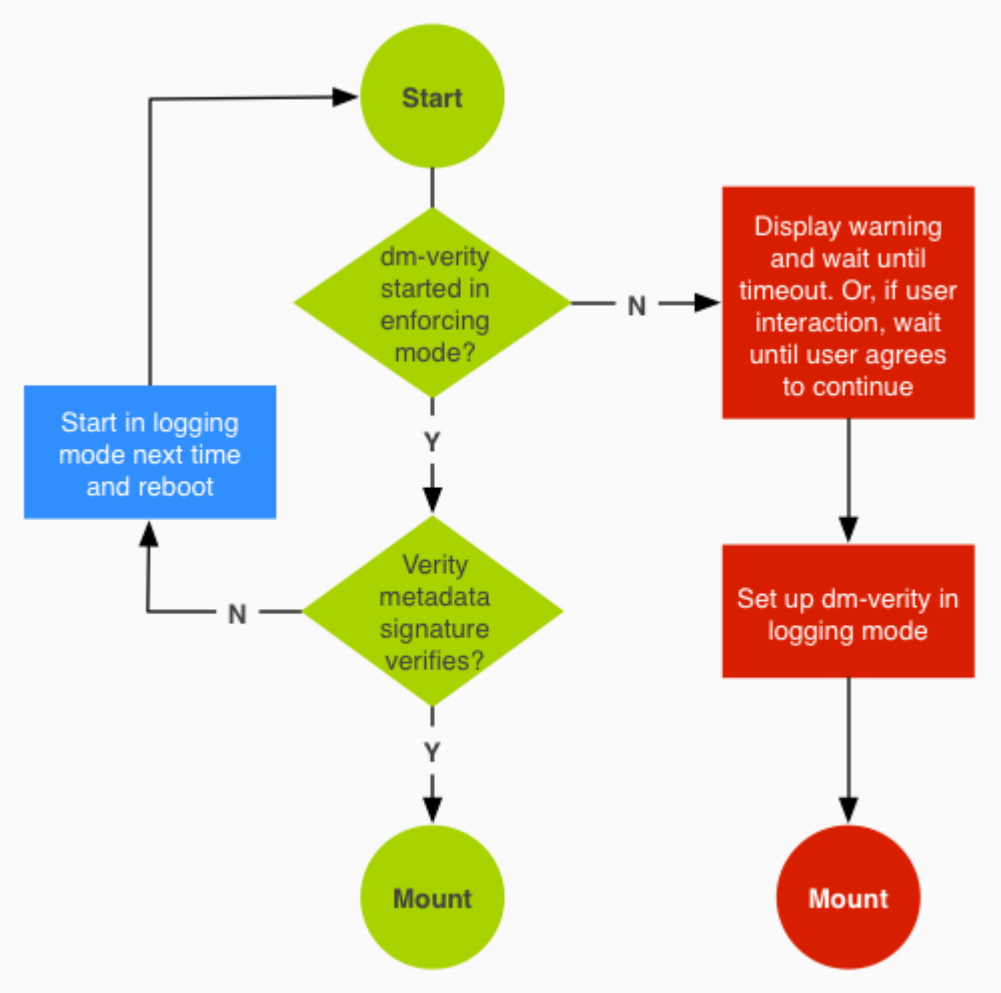


图 3 DM-Verity 工作机制

4.3.3.2. IMA/EVM

文件完整性保护技术，需要打开内核选项。

4.4. 资源限制与隔离

以进程为目标，实现对一组资源使用的限制隔离

4.4.1. 特权与能力

从 linux 内核 2.2 开始，Linux 把特权用户不同单元的权限分开，可以单独的开启和禁止，称为能力(capability)。可以将能力赋给普通的进程，使其可以做 root 用户可以做的事情。使用时需要安装一个 libcap 软件工具包。

4.4.1.1. 特权(privilege)

传统 UNIX 系统，只要进程的有效用户 id(euid)为 0，内核则认为该进程拥有全部特权。拥有特权的进程可以超越传统的 DAC 方式（允许位和属主）控制，甚至 MAC 策略控制。

4.4.1.2. 能力(capability)

能力是对特权的细分，是 root 用户(euid 为 0 的进程)向普通用户(euid 不等于 0)提供的访问控制机制。root 用户可以任意修改非 root 用户的能力。能力不针对具体文件，而是真的一组功能。

4.4.2. Chroot

早期的进程根文件系统隔离技术

4.4.3. Namespace

现代隔离技术，提供了 MOUNT、UTS、IPC、PID、NET 和 USER 命名空间。使用时内核选项（general 选项）需打开。

4.4.4. Cgroup

限制技术，主要限制 CPU 内存等资源控制，内核选项（general 选项）需打开

4.4.5. Seccomp

限制技术，主要限制进程系统调用，内核选项（general 选项）需要打开。

4.4.6. 其他技术

4.4.6.1. Quota

用户磁盘配额技术，内核选项需要打开(filesystems 里面)+quota 工具。仅支持 EXT,JFS,reiserfs 等块文件系统。UBIFS 不支持此特性。

4.4.6.2. OverlayFs

文件系统覆盖技术，可以解决只读目录下挂载可写目录。内核选项需要打开

4.4.6.3. 堆栈溢出保护

堆栈溢出保护和防止溢出攻击。内核选项需要打开，应用程序编译时 gcc 要带上-fstack-protector-all 和—noececstack

4.4.6.4. ASLR 技术

将进程的某些内存空间地址进行随机化来增大入侵者预测目的地址的难度。在使用 gcc 进行编译链接时添加 **-fpie -pie** ，程序运行前设置/proc/sys/kernel/randomize_va_space 为 1 或者为 2。

4.4.6.5. OOM-Kill

OOM(Out Of Memory)机制为 Linux 内核中一种自我保护机制，当系统分配不出内存时(触发条件)会触发这个机制，由系统在已有进程中挑选一个占用内存较多，回收内存收益最大的进程杀掉来释放内存。

4.5. 审计与日志

4.5.1. Audit

对用户的进程行为进行审查记录，产生审计消息

4.5.2. Syslog

用户进程主动行为，注意客户不要加一下敏感数据

5 Linux 网络安全

目标：文件，流量，隔离

抽时间培训一下以下网络知识。

5.1. Iproute2/net-tools

局域网内部，专网和公网分隔。

5.2. Iptable

Quectel 针对客户特定的应用场景实现各种复杂安全路由策略。
端口限制
流量和速度限制
某些服务控制

5.3. TLS/SSL

Quectel 提供标准的开源执行库和 API 接口头文件，定时完善安全漏洞，协助客户开发。

5.4. DNS

5.5. 网络隔离技术

5.5.1. Bridge

实现不同网口设备互访。

5.5.2. VLAN

是传统局域网内部的分割与隔离技术，对广播域进行二层分割。

5.5.3. VPN

实现局域网到局域网访问，需要 VPN 网关，建立在 IP 层之上，实现有 2 层（PPTP）和 3 层隧道协议(IPSEC).

PPTP

6 公共安全漏洞检查

6.1. CVE 漏洞合入

6.1.1. Kernel

6.1.2. Glibc

6.1.3. Openssl

6.2. 代码静态扫描

Coverity