LTE 接入过程中的安全机制

许杨春 （诺基亚西门子通信）

摘要：本文通过对一个接入实例分析了 LTE 安全机制的要点

关键词： LTE SAE（系统架构演进）EPS(演进分组系统) 安全

在 LTE 接入过程中，有多种安全机制用于保证用户数据和信令的安全，已经有很多文章就此做出探讨，但是各知识点阐述的比较孤立。本文以一个完整的流程为实例来说明相关要点。

一、 概述

LTE 的安全机制主要在 3GPP TS 33.401 “SAE: Security architecture” 为首的规范中加以规定。接入过程中涉及的有：终端和网络的双向认证，接入层的加密和完整性保护，非接入层(NAS) 的加密和完整性保护。

LTE使用的加密和完整性算法框架称之为MILENAGE，除了一系列算法外，还有以下参数：

- K每个用户独有的密钥，它是 ***f1***, ***f1****, ***f2***, ***f3***, ***f4***, ***f5*** 和***f5****算法的输入。
- OP，它是***f1***, ***f1****, ***f2***, ***f3***, ***f4***, ***f5*** 和***f5****算法的一部分，其值由运营商设置。为了防止OP泄露，可以用K对它加密得到每个用户唯一的OPc。

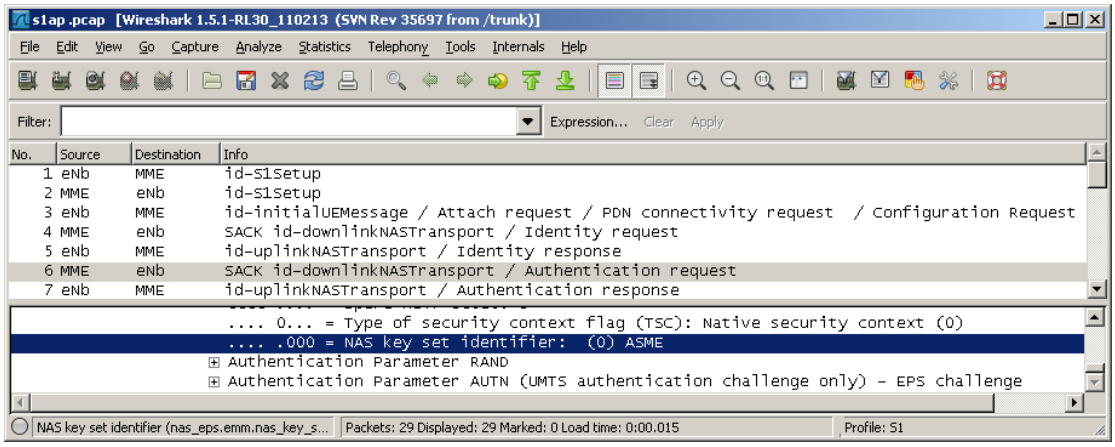
K，OP或OPc分别存在USIM和网络侧HSS。

LTE 的认证是UE 和MME双向认证，该过程称之 为EPS AKA（Authentication and Key Agreement），认证过程中明确了K_{ASME}值，该EPS安全上下文存续期间使用的所有的密钥都可以由它推导得到。一个EPS安全上下文包括接入层和非接入层两部分，它用eKSI值来标识，终端在Attach request，TAU等消息里可以附带eKSI来标识使用的安全上下文，如果没有有效的当前上下文的话就用"111"值来重新协商安全上下文。

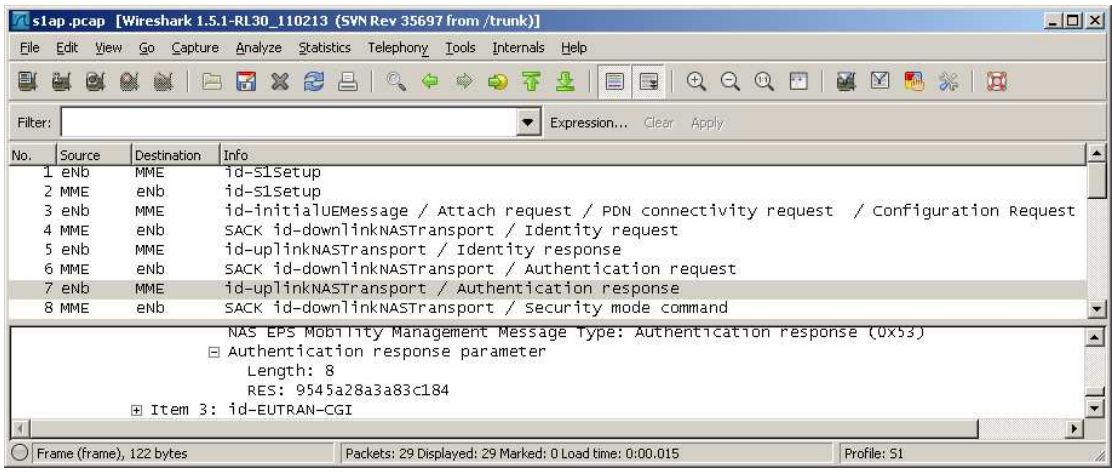
本文第二第三节描述的是接入过程中涉及的 S1AP 信令，包括了认证和 NAS 层的安全过程，它由 Wireshark 在 S1 接口抓获和解析。接入层的 RRC 信令在第四节描述。

二、 认证流程

下图消息 6 和 7 为一次成功的认证。认证需要的参数网络侧由 HSS 生成，MME 通过 IMSI（用户识别码）检索相关参数。



如果网络无法由Attach request（消息3）直接或间接得到获得终端的IMSI，MME会发起一个Identity Request（消息4）/Identity response（消息4）向终端查询。MME 获得IMSI后，向HSS检索与该终端对应的参数，其中随机数RAND，令牌AUTN会通过送Authentication Request（消息6）发给终端，XRES和K_{ASME}会保存备用。信令中的NAS key set identifier 即eKSI，如认证成功，终端和MME都使用其值来标识上下文。

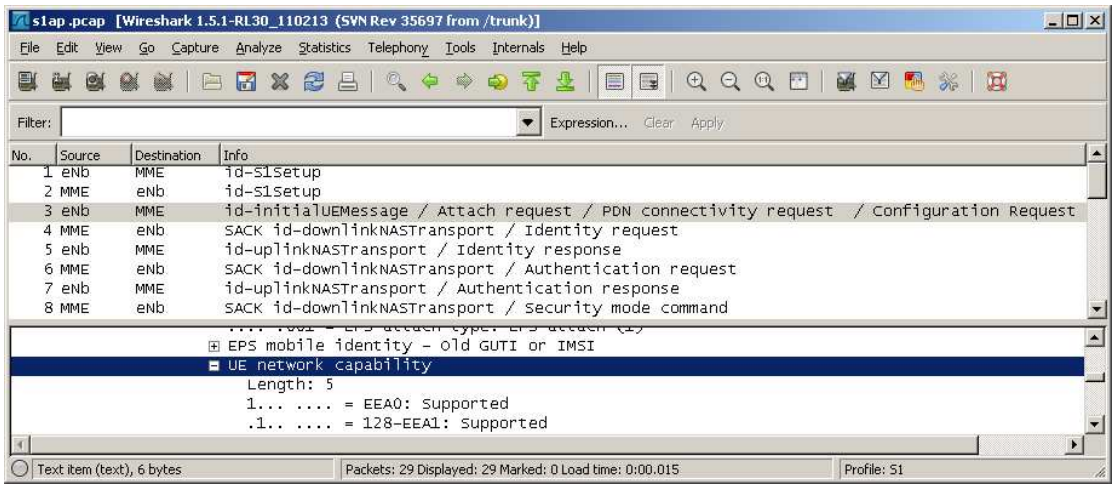


终端收到 Authentication Request 消息后，用 AUTN 对网络认证。如果成功，终端计算 RES 值，在 Authentication Response（消息 7 ）中返回，MME 收到 RES 后与存贮的 XRES 比较。认证成功后，终端和网络分别根据 K 值推出一对密钥 CK/IK（加密/完整性密钥）。这一对密钥再推出 K_{ASME} 值。K_{ASME} 值可以看作根密钥，其他密钥都由它导出，这一点在后面有例为证。

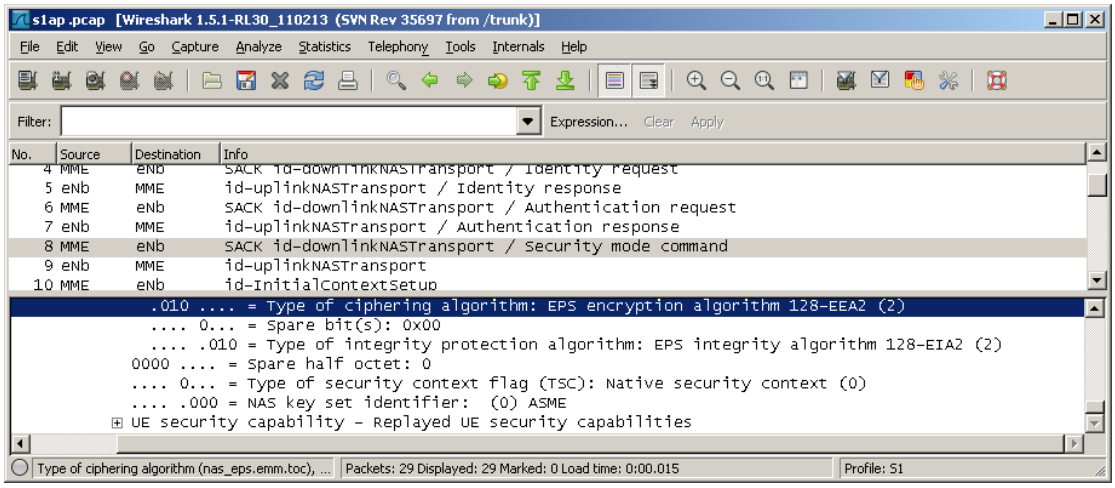
如果认证失败，终端返回 Authentication Reject。

三、 NAS 的加密和完整性保护流程

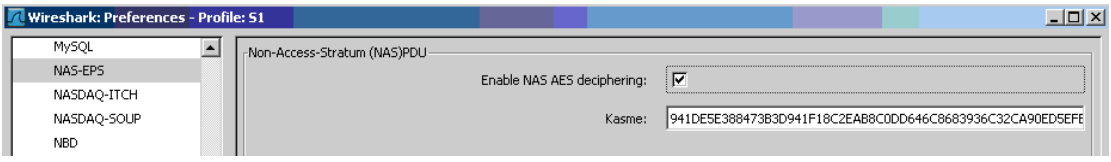
在 NAS 层，终端和 MME 协商使用一定的算法对信令加密和完整性保护，这是通过 Security mode command/Security mode complete NAS 信令实现的，这一过程对基站是透明的。规范 33.401 中定义了 EEA0/EEA1/ EEA2 三种加密算法，EIA0/EIA1/ EIA2 三种完整性算法，其中 EIA0 一般不使用。终端则通过 Attach Request（消息 3）中的 UE network capability 字段上报其支持算法，MME 负责从中选择。



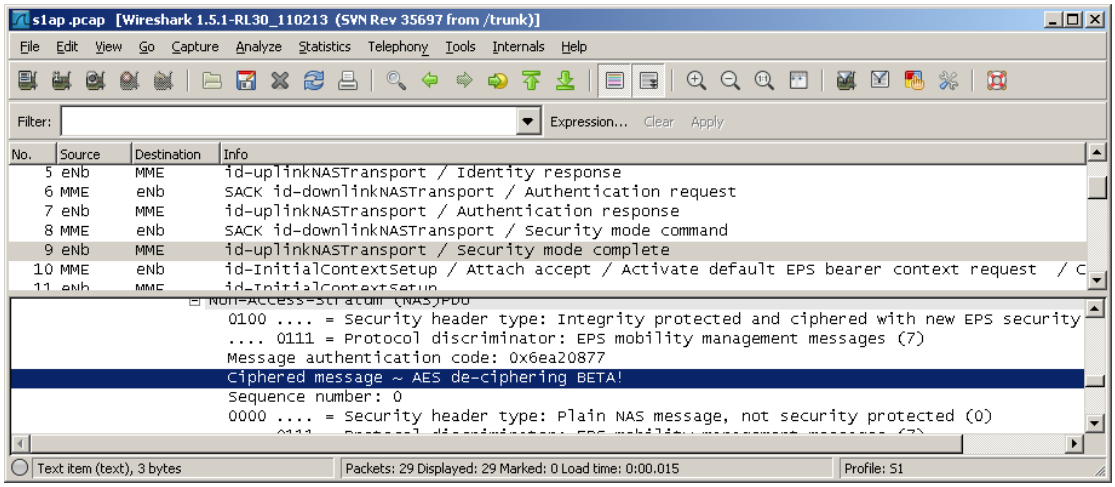
本例中终端支持除 EIA0 之外的所有算法。



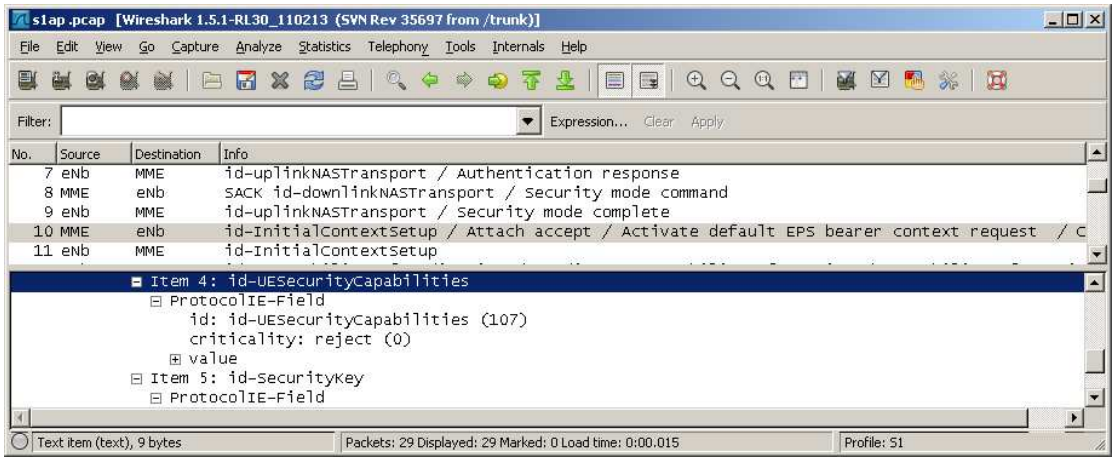
认证过程结束后，MME 选择一种终端与 MME 都支持的算法，通过 Security Mode Command（消息 8）告知终端，本例中 MME 选择了 EEA2/EIA2。终端收到该消息后，就开始上行数据的安全性保护，所以上图消息 9 信令部分已经加密，无法解得具体内容。如果在 Wireshark 中设置 NAS 数据解密用的 K_{ASME} 值。



NAS 信令就能被解析。在下图消息 9 NAS PDU 部分解析得到 Security mode complete 信令，Wireshark 标记 PDU 是用 AES ,也即是用 MME 选择的 EEA2 解密的。该解析实例，也证明了 K_{ASME} 是各个密钥之源。



MME 收到 Security mode complete 信令后，下行 NAS 信令例如消息 10 也开始加密。解密后的消息 10 显示：MME 通过 initial UE context setup request 这一 S1AP 消息告知基站终端的能力。不同与以往的一些消息，这些消息不是封装在透传的 NAS 信令中,所以基站可以得知这些消息。在该消息中，MME 还指定了接入层使用的密钥（SecurityKey），如果值为 0，并且 UE 也支持，完整性算法就使用 EIA0。



消息 10 后就开始接入层的加密和完整性保护过程。

四、 接入层的加密和完整性保护流程

接入层的终结于终端和基站，它们协商使用一定的算法对 RRC 信令和用户数据局加密；完整性保护仅用于 RRC 信令。接入层可选的算法同样来自终端则通过 Attach Request 的上报消息，但基站独立选择使用的算法，接入层使用的密钥不同于 NAS 层，但同样由 K_{ASME} 推导得到。

接入层的 RRC 信令可以在终端或基站获取。以下就以一基站的记录为例说明涉及的 RRC 信令，为了节省篇幅，无关部分已省略。

在上一节，NAS 层的安全流程结尾时，MME 通过 S1AP 消息 Initial Context Setup Request 通知基站可以开始接入层的安全流程，消息中有两个元素：UE Security Capabilities，Security Key，它们说明了终端支持的算法和密钥。基站在配置的时候对于支持的加密算法和完整性算法定义了优先级，收到该消息后，基站选择双方支持并且优先级最高的算法，然后通过

RRC 信令 SECURITY MODE COMMAND 通知终端。

```
DL-DCCH-Message : {
 message c1 : securityModeCommand : {
     rrc-TransactionIdentifier 2,
     criticalExtensions c1 : securityModeCommand-r8 : {
         securityConfigSMC {
          securityAlgorithmConfig {
           cipheringAlgorithm eea1,
           integrityProtAlgorithm eia2
     …..
}
```

本例中，由于基站选择的是 EEA1 加密算法和 EIA2 完整性算法，这说明加密算法和完整性算法的选择也是独立的。

当 UE 收到 SECURITY MODE COMPLETE 消息后，如果接受通过 RRC 信令 SECURITY MODE COMPLETE 答复。发送完该消息后，空口数据已加密。但在传送 NAS 信令和数据前 RRC 还需作以下工作：

在此之前，所有的 NAS 信令都和 RRC 消息混在一起通过 SRB（信令无线承载）1 上传输，还需要增加 SRB2 用于 NAS 信令传输（它还继续封装在 RRC 中透传），DRB（数据无线承载）用于用户面数据传输。这是通过以下消息实现的：

```
DL-DCCH-Message : {
 message c1 : rrcConnectionReconfiguration : {
          …..
           srb-ToAddModList {
           {
            srb-Identity 2,
            ……
          },
          drb-ToAddModList {
           {
            eps-BearerIdentity 5,
            drb-Identity 4,
          ….
          },
```

上一节消息 10 中出现的 NAS 信令：ATTACH ACCEPT 和 ACTIVATE DEF EPS BEARER CONTEXT REQ 也可以封装在这一 RRC 信令中递交给终端。收到 rrc Connection Reconfiguration 后，终端以 rrc Connection Reconfiguration Complete 答复。至此，在空口，接入层信令，非接入层信令和用户面数据实现了分离。

接入层的安全流程可概括为：MME 通过 Initial Context Setup Request 通知基站终端的安全能力。基站收到消息后，通过 RRC 信令 security Mode Command 告知终端接入层选择的算法，终端以 security Mode Complete 加以确认，然后激活无线数据承载。

五、 总结

通过多种安全机制的引入，LTE 中从终端到基站的空口数据得到加密和完整性算法的保护，可以防止被窃听和篡改。基站到核心网的信令也得到类似算法的保护，算法使用的密钥是在认证过程中确定的。

如果基站处于非安全区，它到核心网的数据通路也需要一定的机制加以保护，如 IPsec 等 VPN 技术，这些安全机制应该在基站开通时配置完成，

参考文献

1 3GPP TS 33.401 3GPP System Architecture Evolution (SAE):Security architecture

2 3GPP TS 35.206 Specification of the MILENAGE algorithm set