ICS 33.060.01
M 36

YD

中华人民共和国通信行业标准

YD/T 2036-2009

基于终端安全评估的移动网络接入安全技术要求

Terminal Security Evaluation Based Security Technology Requirement for Mobile Network Access

2009-12-11 发布　　2010-01-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言

本标准对应于ITU-T X.1125:《关联响应系统》，与ITU-T X.1125的一致性程度为非等效。与X.1125相比，本标准定义的系统架构与流程与X.1125基本等同，其差异在于：

— 文档结构有所不同；

— 本标准增加了第4章（安全威胁）；

— 本标准第8章（SCA和SCS之间的通信）对应ITU-T X.1125的第9章（Communication between SCA and SCS）在对SCA与SCS之间传输的消息定义上不等同；

— 与ITU-T X.1125不同，本标准未对CRS传输消息的XML schema和ASN.1格式进行定义；

— 本标准中的第12.1,12.2,12.3章分别与ITU-T X.1125的非规范性附录I.1,I.2,I.3对应；

— 本标准中未提供SCI Report和SCI Response的示例。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：华为技术有限公司、中国移动通信集团公司、工业和信息化部电信研究院、中兴通讯股份有限公司、国家计算机网络应急技术处理中心。

本标准主要起草人：位继伟、贾　科、刘淑玲、姬长锋、郑志彬、刘利军、落红卫、蒋　亮、舒　敏。

基于终端安全评估的移动网络接入安全技术要求

1 范围

本标准确立了在移动通信中用于应对来自不安全终端潜在安全威胁的关联反应系统（CRS）的开放式体系架构。并规定了关联反应系统的系统描述、策略及相关通信过程等内容。

本标准适用于移动通信网络中的终端及接入控制设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

ITU-T X.1121　移动端到端数据通信的安全技术框架（2004）

IETF RFC 2748　COPS协议

IETF RFC 3084　COPS协议用于策略提供

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

移动台　Mobile Station

一个实体，其具备无线网络访问功能和连接到网络和应用服务器或其他移动台进行数据通信的功能。在本推荐标准中，移动台包含从手机到接入无线网的笔记本等多种设备。

3.1.2

移动网络　Mobile Network

为移动台提供无线网络接入服务的网络。

3.1.3

移动用户　Mobile Subscriber

一个人，其使用和操作移动台从应用服务提供商处获取各种服务。

3.1.4

应用服务　Application Service

网络侧对用户提供的各种服务，比如移动银行、移动商务、在线视频、下载、网页浏览、收发邮件等等。

3.1.5

应用服务器　Application Server

一个实体，其连接到开放的网络环境，与移动台通信并为其提供应用服务。

3.1.6

应用服务提供商　ASP Application Service Provider

一个实体 （人或者组织），其通过应用服务器向移动用户提供应用服务。

3.1.7

移动安全网关 Mobile Security Gateway

一个实体，其中继移动台和应用服务器之间的数据通信，从移动网络到开放网络或者反向，更改安全参数或者通信协议，并且能执行移动端到端数据通信的安全策略管理功能。

3.1.8

关联反应系统 CRS，correlative reacting system

一种机制，其能使移动台和网络共同应对各种潜在的安全威胁，比如病毒、蠕虫、特洛伊木马、移动台的不当行为导致的网络攻击等。此外，当病毒或者蠕虫已经在网络中存在时，CRS能保证其传播速度可控限度内，从而提供足够的时间来进行网络和移动台的恢复，将可能的损失降低到最小。

3.1.9

网络访问控制器 NAC，network access controller

移动网络的网元，提供移动用户访问网络的控制功能，能根据网络访问控制策略对特定的不安全用户进行带宽限制。网络访问控制设备通常网关，比如，移动网络的SGSN或者宽带IP网络的宽带接入服务器。

3.1.10

应用服务控制器 ASC，application service controller

移动网络的网元，提供对移动用户应用服务访问的控制功能。通过和安全相关服务器（SCS）的关联反应，根据CRS中的应用服务控制策略对特定的不安全用户执行应用服务限制。

3.1.11

安全应用软件 SAS，security application software

为移动台系统提供特定类型安全功能的应用软件，比如，反病毒软件、防火墙软件等。

3.1.12

安全应用软件服务器 SAS-S，security application software server

位于网络侧的安全应用软件的服务器，其提供安全文件或者描述文件的更新，提供其他移动台安全应用软件的在线安全服务。

3.1.13

安全相关代理 SCA，security correlation agent

嵌入移动台的一个实体，其搜集移动台的安全相关信息，并和移动网络侧的SCS通信，为移动台的安全升级和SCS对移动台的安全情况评估提供实时信息。

3.1.14

安全相关服务器 SCS，security correlation server

移动网络侧和SCA通信的服务器，负责从SCA接收安全相关信息并评估移动台的安全状况，同时根据评估结果为NAC/ASC对移动台提供相应的控制信息；当SCS上被定义了或者输入新的策略时，SCS也可以主动向NAC/ASC发送对移动台提供相应的控制信息。

3.1.15

安全相关信息 SCI，security correlative information

和移动台安全环境相关的信息块，如移动台操作系统版本、反病毒软件版本、病毒扫描结果等。

3.1.16

移动台操作系统　MSOS，mobile station operating system

可按照SCA收到的SCS指示信息与MSOS-ES和SAS-S通信，进行自身的软件升级、安全漏洞补丁更新和TOS上第三方安全应用软件的更新，比如，反病毒、防火墙等软件的更新。

3.1.17

移动台操作系统更新服务器　MSOS-US，mobile station operating system updating server

为移动台操作系统提供补丁、软件更新、升级等服务的服务器。

3.1.18

关联反应系统应用协议　CRSAP，correlative reacting system application protocol

在安全代理SCA和安全服务器SCS之间封装、传输CRS消息的应用层协议。

3.1.19

专用安全设备　DSD，dedicated security device

防火墙、IDS、安全网关、安全管理服务器等为无线数据网络提供的特殊安全功能的安全设备。

3.1.20

受控对象　Controlled Object

CRS系统控制的移动台，即单个移动台或一组（多个）移动台。

3.1.21

策略　Policy

CRS系统用于执行对移动台相应控制的规则集合。

3.2　缩略语

下列缩略语适用于本标准。

3GPP	3rd Generation Partnerships Project	第三代合作伙伴项目
API	Application Programming Interface	应用编程接口
APN	Access Point Name	访问点名称
ASC	Application Service Controller	应用服务控制器
ASP	Application Service Provider	应用服务提供商
COPS	Common Open Policy Service	通用开放策略服务
CRS	Correlative Reacting System	关联反应系统
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DNS	Domain Name System	域名系统
DoS	Denial of Service	拒绝服务攻击
DDoS	Distributed Denial of Service	分布式拒绝服务攻击
GGSN	Gateway GPRS Support Node	网关 GPRS 节点
GMM/SM	GPRS Mobility Management and Session Management	GPRS 移动性管理和会话管理
GTP	GPRS Tunneling Protocol	GPRS 隧道协议
IDS	Intrusion Detection System	入侵检测系统

IETF	Internet Engineering Task Force	互联网工程任务组织
IMEI	International Mobile Equipment Identity	国际移动设备身份标识
IMSI	International Mobile Subscriber Identity	国际移动用户身份标识
IP	Internet Protocol	互联网协议
ISP	Internet Service Provider	互联网服务提供商
MBT	Message Block Transport	消息块传输
MMS	Multimedia Messaging Service	多媒体消息服务
MSOS-US	Mobile Station Operating System Updating Server	移动台操作系统更新服务器
NAC	Network Access Controller	网络接入控制器
NSAPI	Network layer Service Access Point Identifier	网络层服务访问点标识
OS	Operating System	操作系统
PDN	Packet Data Network	分组数据网络
PDP	Packet Data Protocol	分组数据协议
PDU	Protocol Data Unit	协议数据单元
PLMN	Public Lands Mobile Network	公用陆地移动网络
P-TMSI	Packet TMSI	分组临时移动用户识别码
QoS	Quality of Service	服务质量
RA	Routing Area	路由区
RAI	Routing Area Identity	路由区标识
SAS	Security Application Software	安全应用软件
SAS-S	Security Application Software Server	安全应用软件服务器
SCA	Security Correlation Agent	安全相关代理
SCI	Security Correlation Information	安全相关信息
SCS	Security Correlation Server	安全相关服务器
SGSN	Service GPRS Support Node	服务 GPRS 节点
SIM	Subscriber Identity Module	用户识别模块
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全
UDP	User Datagram Protocol	用户数据报协议
USIM	Universal SIM	通用用户识别模块
WLAN	Wireless Local Area Network	无线局域网
WiMAX	Worldwide Interoperability for Microwave Access	微波接入全球性互通
WTLS	Wireless Transport Layer Security	无线传输层安全
XML	eXtensible Markup Language	可扩展标记语言

4 安全威胁

4.1 概述

随着无线数据网络的普及，越来越多的人开始使用移动终端设备享受网络服务，分组数据业务逐渐

取代传统电路业务，移动运营商网络趋于IP化。传统标准3GPP、WLAN、WiMAX中的安全机制对用户接入认证、业务传输安全提供了保障，但由于应用服务提供者和IP网络本身的开放性和安全漏洞（以TCP/IP协议为基础的因特网体系中，每个网络节点、每台主机、每个用户是平等的，如一点被突破、全网都会面临安全威胁），导致来自应用层面的安全威胁（如病毒、蠕虫、黑客攻击、用户信息盗用等）层出不穷，传统标准中的安全机制对这些安全威胁无法应付。

来自运营商核心网内部的安全威胁容易得到有效管理，而对于从接入网接入核心网的移动台而言，其安全管理相对困难得多。小的移动台因为资源有限导致防护能力较低，其操作系统漏洞或安全应用未及时更新，很容易导致病毒入侵，而且移动台数量众多、分布范围广泛、移动性强，一旦其感染病毒并成为病毒传播的源头，运营商从网络侧很难在保证网络安全和为用户提供高品质服务之间做出合适的选择。

在传统的有线网络领域，TCG组织提出的基于Internet网络的可信网络互连架构TNC规范，提出了网络接入终端的完整性概念，只有通过网络侧验证，符合网络安全策略的终端才能接入网络；但TNC规范对于移动网络中终端的移动性、漫游、终端硬件能力、终端易丢失、无线空口连接不可靠等问题，其并没有针对性的考虑。参考ITU-T X.1121标准中移动数据服务端到端的安全特性，移动网络用户特有的服务特性也需要重新考虑，例如：移动台感染病毒、蠕虫后向数据网发送垃圾信息，发送探测和攻击报文等，往往造成运营商对移动用户的不合理收费等问题；另外，移动网络手机终端的机卡分离、独立的无线接入协议等问题，也都是待考虑的。

4.2 无线应用发展带来的安全威胁

由于无线应用业务发展迅速，第三方ASP逐渐增加，业务趋向增值服务和精细化经营，移动用户在享受更多样化的服务的同时，其自身和移动网络面临的安全风险也大大增加。例如：由于通过无线数据网接入企业内网的员工用户身份失窃，企业有可能使自己的内部资源暴露给非授权用户，应用系统可能被滥用或遭到攻击、破坏，导致应用服务质量下降甚至不可用。

病毒技术的迅速发展，使得当病毒大规模爆发时，网络中传输的大量数据流量是由病毒产生的垃圾数据和探测、攻击流量，造成移动网络拥塞，严重影响了运营商的网络效率和安全，也对用户的终端和业务产生不利的影响和安全威胁。

4.3 关联反应系统应对的安全威胁

关联反应系统（Correlative Reacting System）的目的，是保护移动网络应对来自不安全终端（即不符合移动网络指定的安全策略的终端，例如，有安全漏洞或感染病毒的终端）的安全威胁。

攻击分为两类：基于网络层的网络攻击和基于应用层的服务攻击，前者发生在无线网络连接建立阶段和应用服务之前，后者则发生在无线网络连接建立后，在提供应用服务的过程中。往往网络攻击以服务为载体，而攻击的目的是危害网络系统和服务系统。

为了从源头上对抗由不安全终端带来的网络安全威胁，关联反应系统提供从网络接入控制到应用服务控制的多层安全控制手段。应用服务控制可以与网络接入控制相互补充，同时弥补网络接入控制的局限性，有效控制网络蠕虫、黑客攻击等基于复杂机制的安全风险；另一方面，通过应用服务控制，可以从源头上阻止针对特定服务的攻击带来的网络流量冲击，有效阻止病毒在网络的传播。

关联反应系统（Correlative Reacting System）针对移动端到端应用数据业务，构建了解决如下安全威胁的基础：

- 移动用户：窃取移动用户私有信息；滥用移动用户有偿服务。
- 终端系统：系统被破坏，造成性能下降或系统不可用；成为DoS和DDoS攻击的执行者，例如，用户防范意识差、终端安全配置有限，都可能导致移动终端成为病毒攻击的跳板。
- 移动网络系统：病毒或蠕虫传播造成网络拥塞、资源浪费，病毒攻击特定的网元或传输体系，造成移动网络传输质量、可靠性和可用性下降。
- 应用服务系统：服务器被攻击、中毒、用户服务签约信息泄漏等应用服务的可用性和安全性问题。

关联反应系统的实质是通过移动台和网络侧的安全联动，对移动台的网络接入进行控制，对移动台的应用服务接入进行限制，从而为网络提供抵御病毒、网络攻击等安全威胁的能力。

5 关联反应系统描述

5.1 关联反应系统的前提

CRS服务的完成和性能基于CRS与如下一些CRS系统外部功能的联动：

- 网络侧基于网络层执行的网络访问控制；
- 网络侧基于应用层执行的应用服务访问控制；
- 移动台操作系统更新服务器和安全应用软件服务器为移动用户终端提供的自动、实时安全更新服务；

注：如无特别指明，本标准中的安全更新是指软件程序的更新和升级，包括程序更新、程序升级、补丁安装等等。

- 防火墙、安全网关、安全管理中心服务器等专用安全设备（DSD）为无线网络提供的特殊安全功能；
- 安全应用软件（SAS）为SCA提供终端的安全信息，并在CRS的指示下自动同安全应用软件服务器（SAS-S）通信并进行安全更新；
- 移动台操作系统（MSOS）为终端提供安全相关的系统配置信息，并在CRS的指示下自动同移动台操作系统服务器（MSOS-US）通信并进行安全更新。

能够实现上述外部功能的实体可以通过本文档定义的接口和CRS实体（比如SCA和SCS）通信，并能假设可通过这些接口和CRS联动，执行CRS安全策略。

CRS消息的传输，依赖于现有的低层传输协议，例如基于TCP、UDP等。CRS消息传输的安全性，依赖于现有的安全协议，例如基于TLS、AKA、IPsec、WTLS等。

5.2 对关联反应系统的需求

- CRS系统能够通过网络侧对终端侧安全情况的实时评估，并根据评估结果对移动台进行实时控制的方式防止如病毒、木马等网络威胁在无线数据网络的快速蔓延，控制对网络的恶意攻击，最终保证无线网络的安全。
- CRS系统能够实现网络侧辅助移动台进行安全相关的更新和升级。
- CRS系统能够解决移动台在部署了CRS系统的无线数据网和未部署CRS的无线数据网间漫游时，用户的无线数据业务和CRS消息传输都可以正常进行。
- CRS系统能够保证SCA的可用性。具体而言：在用户上线时，CRS系统应检测移动台SCA的配置，若移动台未安装SCA安装，则应该保证SCA的安装。对已经安装有SCA的用户则应该保持SCA的更新。
- 一个SCS服务器可控制一个或多个NAC/ASC,每一个NAC/ASC都有一个优先选择的SCS服务器，但NAC/ASC应同时与多个SCS服务器相连。这样当某一个SCS服务器出现问题的时候，NAC的安全策略

提供服务可实现不间断执行。

5.3 关联反应系统体系结构

关联反应系统（CRS）是一个应对不安全移动台对移动网络所造成的潜在安全威胁的联动系统，关联反应系统通过对移动台的安全状况进行评估，来指导网络侧网元设备对移动台实施动态的网络访问控制和应用服务限制，并根据安全状况评估结果辅助移动台及时进行自身安全相关的更新、升级，从而同时给移动网络和移动台都提供了增强安全的手段，并提供了一种防止病毒或者蠕虫在网络中快速蔓延的机制。

图1显示了关联反应系统的体系结构和环境。

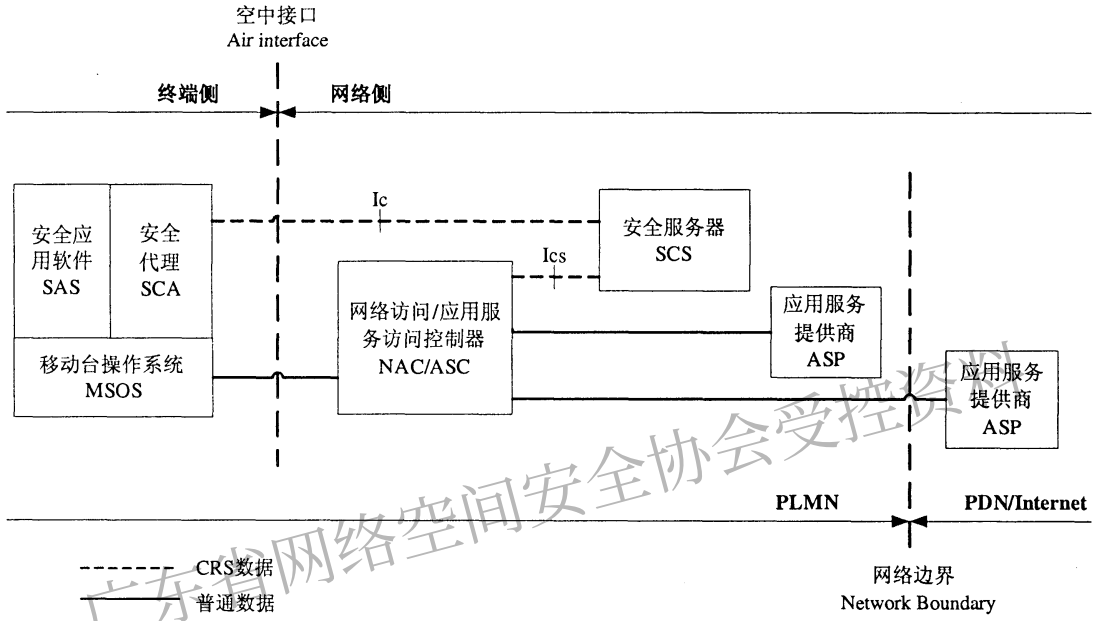


图1 关联反应系统（CRS）体系结构和环境

关联反应系统（CRS）主要的实体包括：

- 移动台侧的安全代理（SCA）；
- 网络侧的安全服务器（SCS）；
- 网络侧的网络接入控制器（NAC）。

安全代理和安全服务器通过Ic接口进行通信，同时，安全服务器通过Ics接口和PLMN中的其他网元通信，通过它们之间的通信和交互，关联反应系统提供对移动台的控制功能。

安全代理负责收集移动台的安全相关信息，对其进行处理并和安全服务器进行通信。安全服务器通过安全代理收集到的安全相关信息来评估和判断移动台的安全状况和安全等级，以及移动台的安全状况是否被允许访问网络和申请各种应用服务。

当安全服务器收到安全代理发来的安全相关报告（SCI报告）后，进行相关的评估，如果安全服务器根据分析认为移动台不够安全，安全服务器会指示NAC或ASC对移动台的网络访问和应用访问作适当的控制，安全服务器也会将对移动台的控制情况通知SCA。

如果有适合移动台进行自身操作系统升级的补丁、组件或者安全相关应用软件的更新时，安全服务器SCS会通知安全代理SCA协助移动台进行相应的升级或者更新，这些更新或者补丁、升级包都在SAS-S和MSOS-US服务器上，并由这些服务器提供升级、更新服务，这些服务器的拥有者一般是移动台操作系

统生产商和移动台安全应用软件生产商，它们也可以被看作是一种类型的ASP。

移动台的安全相关更新升级也包括安全代理SCA自身的更新和升级，当安全服务器SCS检测到安全代理SCA的版本低于目前的最新版本时，会立刻通知SCA相关信息，指示安全代理SCA进行自身的更新和升级。

如图1所示，一些ASP可以通过和PLMN的运营商签约建立合作关系，将自己的服务部署在PLMN之中，PLMN的运营商本身也可以是ASP，这些ASP的设备应该与SCS服务器之间实现Ics接口用于和SCS服务器进行通信，并从SCS服务器处获取不安全的移动台的列表等信息，从而可以在服务端对一些应用访问进行安全控制。

SCS服务器对于移动用户的网络访问控制和应用服务控制，是通过对用户所使用的移动台的控制来实现的，其基础信息来源是SCA向SCS服务器发送的SCI报告和移动用户在移动数据网络（下文中“数据网络”不特指时即为移动数据网络）中已经申请或定制的各种服务。对于已经安装SCA的移动台，当移动台连接到数据网络时，SCA的功能同时启动。

与关联反应系统共同工作的现有网络实体还包括但不限于以下专用安全设备（DSD）：

- 防火墙：为网络边界提供安全保护。
- 安全网关：对流量进行分析，并可以过滤其中的病毒流量、攻击流量。
- 安全管理服务器：为SCS服务器提供网络侧知识和策略支持。
- IDS：对网络入侵和攻击进行检测。

5.4 关联反应系统（CRS）的实体

5.4.1 安全代理（SCA）

5.4.1.1 安全代理（SCA）的功能结构

移动台侧安全代理的功能主要包括以下几个方面。

— 安全相关信息交换功能

收集来自移动台的安全相关信息，这里的安全相关信息包括：移动台安全事件、移动台操作系统版本和补丁信息、安全应用软件的版本/数据库日期、安全应用软件的日志信息、移动台用户ID、移动台ID、遗留在移动台中的网络病毒踪迹等。

将SCS服务器发来的安全相关更新信息和指令，通过SCA和移动台操作系统和安全应用软件之间的接口，提供给移动台操作系统和安全应用软件的补丁、升级信息，并辅助其进行更新、升级。

— 安全相关信息分析筛选功能

SCA按照本地或者SCS服务器发来的策略，处理和组织移动台安全相关信息，将筛选过滤后的信息上报给安全服务器。同时接收安全服务器的发来的安全更新命令和指示、移动台安全评估等级、移动台网络访问受限等信息，筛选后实时通知给移动台用户或者生成本地安全报告/日志供移动台用户主动查询。

— 安全通信功能

负责和SCS服务器之间进行互认证，协商、建立安全的CRS消息传输通道，保证与SCS服务器之间进行可靠的CRS消息传输。

— 用户界面

提供移动台用户和SCA之间进行信息交互的功能，为用户提供提示信息或者接受用户对SCA安全报告、网络侧对移动台的安全等级评估结果等安全相关信息的查询。

安全代理SCA应该可以根据其搜集到的移动台安全相关信息和SCS服务器反馈给SCA的移动台安全评估等级等信息，生成一份可供移动台用户查询的移动台安全状态报告。

通常情况下，提供给移动台用户的安全报告主要作为SCA的运行日志等方式来存储并等待用户主动查询。如果移动台被SCS服务器评估为安全性很低或者其上实时发生了严重的安全事件，SCA可选择主动给用户发送提示消息并建议用户阅读安全报告，以提示用户注意防范安全威胁。

－ 本地数据存储

用于存储SCA涉及的安全相关信息、日志和各种策略等。

移动台侧安全代理的功能结构如图2所示。

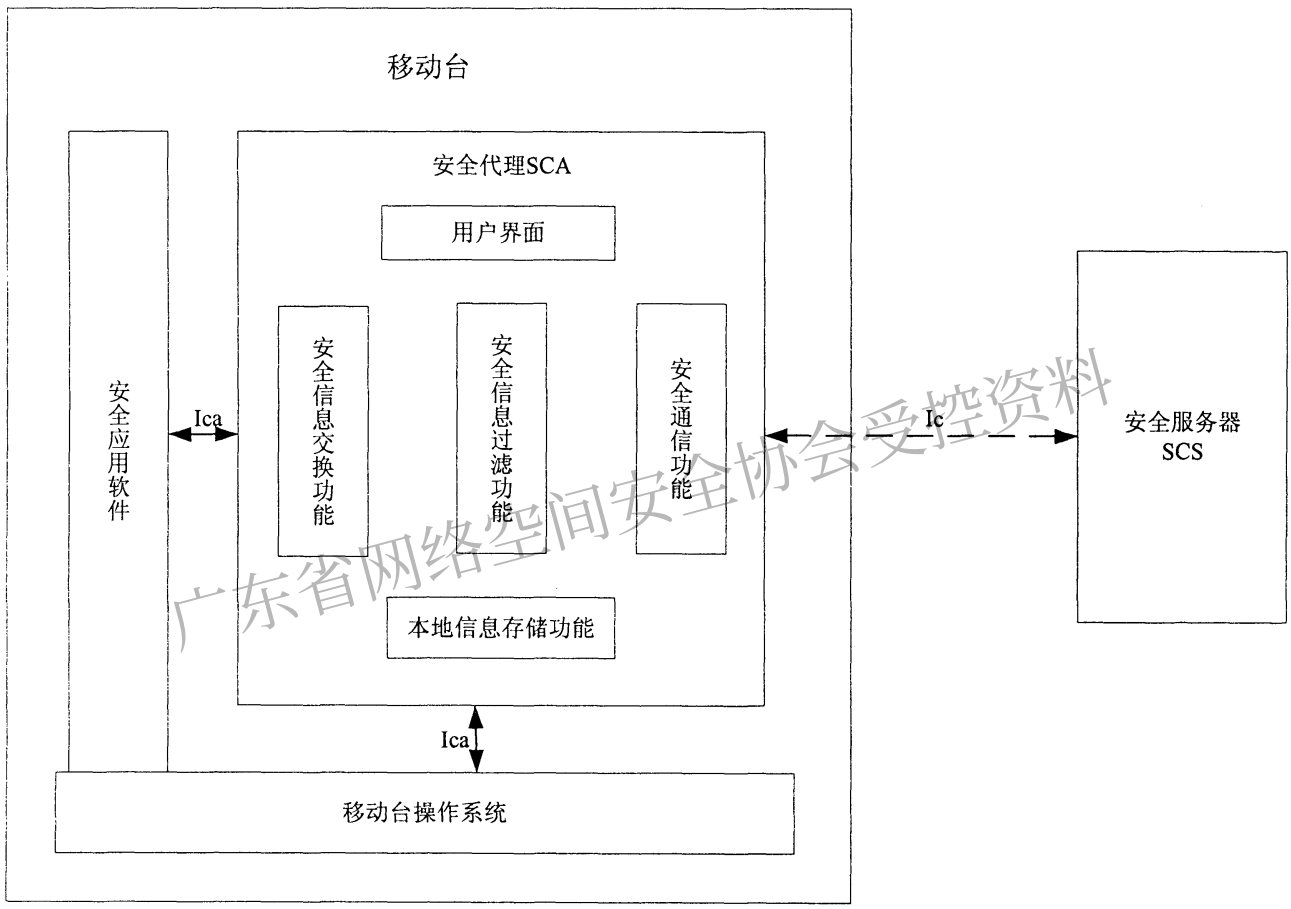


图2 安全相关代理（SCA）的模块结构

5.4.1.2 对安全代理（SCA）的要求

- SCA具备从移动台上收集安全相关信息的能力。
- SCA具备将移动台安全相关信息安全可靠地报告给SCS的能力。
- SCA具备自动发现网络SCS的能力。
- SCA具备即时响应SCS消息的能力。
- SCA具备在必要时将相关信息报告移动用户的能力。
- SCA具备协助终端操作系统、安全应用软件进行安全更新的能力。
- SCA具备能够保证来自Ica数据真实性的能力。
- SCA具备要保证其本地数据存储信息的安全的能力。
- SCA应禁止用户对SCA配置进行任何形式更改，SCA的配置参数只能由SCS根据移动台和网络的

安全状况，综合分析后动态地修改。

5.4.2 安全服务器（SCS）

5.4.2.1 安全服务器（SCS）的功能需求

安全服务器（SCS）是一个逻辑的概念，由以下几个功能模块组成，每个功能模块都可以是一个物理设备，安全服务器的结构如图3所示。

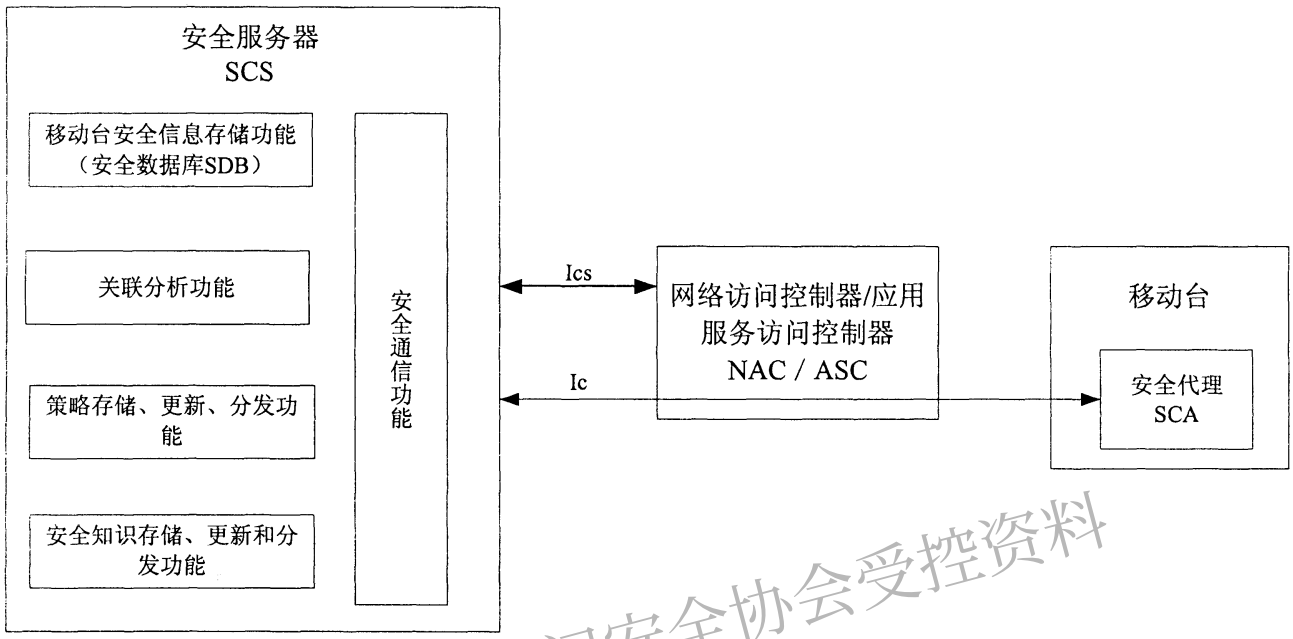


图3 安全服务器（SCS）结构

a）通信功能

通信功能负责在SCS服务器和SCA、NAC、ASC之间建立安全可靠的传输通道，保证CRS消息传输的一致性、完整性和机密性。通信功能还负责在SCS服务器的不同功能模块之间共享信息。

b）移动台安全信息存储功能

SCS服务器包含一个安全数据库（SDB），用于存储移动台SCA向SCS服务器上报的SCI报告信息和SCS服务器对移动台安全等级的评估结果以及目前正在执行的移动台控制策略。在SDB的数据结构中，可以用IMSI来唯一的标识一个移动用户，用IMEI来惟一的标示一个移动终端。可以有相关的数据库表来记录移动台IMEI、移动用户IMSI、SCA ID三者之间的当前和历史的联系。

c）关联分析功能

SCS服务器可以根据其上的安全策略和安全知识，利用移动台SCA上报的SCI报告来分析和评估单个移动台的安全等级，也可以对多个移动台上报的SCI报告和其单独的安全等级评估结果进行关联分析，得出连接到某个数据网络的所有移动台的总体安全情况，或者是某个路由区域内的所有移动台的总体安全情况。

d）策略存储、更新、分发功能

策略包括面向系统控制的策略和安全分析评估策略（见5.5节）等等，策略应该预先定义完善并存储在SCS服务器中，可以通过SCS服务器的通信功能将策略分发给SCA、NAC、ASC，以指导它们的行为。应该定义策略管理接口，以便管理员或其他外部策略管理单元手工或自动地对SCS服务器中的策略进行更新。

e）安全知识存储、更新和分发功能

安全知识包含所有网络侧提供的知识和信息。安全知识包括各种已知网络安全威胁及其应对方法，移动台补丁、升级包信息和资源地址，移动台安全应用软件更新升级信息和资源地址，SCA的各个版本信息和下载地址等等。对于CRS系统，保持安全知识的及时更新非常重要，它反映了CRS系统对于已知安全威胁的反应速度。大部分的安全知识应该由移动台操作系统生产商、移动台安全应用软件生产商和第三方安全研究机构提供。安全知识用于指导移动台进行安全相关的更新、升级，并作为参考信息用于SCS服务器的关联分析和策略管理单元对安全策略的制定。

安全知识存储、更新和分发功能应该包含SCS服务器和网络侧安全设备（如网络安全管理服务器、防火墙、IDS、防病毒网关、移动终端操作系统更新服务器、安全应用软件更新服务器）之间的接口，使得SCS服务器可以和网络侧安全设备之间进行交换信息、安全联动，此接口的定义不在本标准的范围内。

5.4.2.2 对安全服务器（SCS）的要求

- 能够获得移动台安全相关信息。
- 能够获得网络侧的安全策略和安全知识，并根据其对移动台安全报告内容进行分析和评估，决定移动台的安全等级。
- 能够在网络侧通过与NAC/ASC的通信，完成对移动台的安全控制。
- 能够对判定为不安全的移动台进行安全更新。
- 能够通过Ic接口控制SCA的行为，并能对其进行自动更新。
- 能够获得移动台的安全能力，并能与其协商建立安全通道。
- 能够与NAC/ASC协商建立安全通道。
- 能够对多个移动台的信息进行安全关联分析，得出连接到某个数据网络或某个区域内的移动台总体安全状况。

5.4.3 网络接入控制器（NAC）和应用服务控制器（ASC）

5.4.3.1 网络接入控制器（NAC）和应用服务控制器（ASC）在关联反应系统（CRS）中的功能

网络接入控制器和应用服务控制器是移动台访问无线数据网络的控制设备，比如，GPRS里的SGSN。网络接入控制器和应用服务控制器是逻辑上的概念，它们之间的区别在于对移动台访问数据网络控制的层次不同，网络接入控制器主要在移动台通过权鉴后连接到无线数据网络，控制其连接的建立、维护、断开等，应用服务控制器在移动台连接到无线数据网络后，控制移动台对特定应用服务的访问。

网络接入控制器和应用服务控制器通过Ics接口和安全服务器（SCS）通信，通信内容主要包括以下两类。

- 网络接入控制器和应用服务控制器向安全服务器发送移动台的相关信息

这里移动台的相关信息指网络侧的网络接入控制器和应用服务控制器可以获得，并且SCS服务器需要知道的移动台相关信息，例如，移动用户ID、移动台PDP上下文、移动台能力信息。

- 接受安全服务器发来的对移动台的控制决策并执行

网络接入控制器和应用服务控制器接受安全服务器发来的对移动台的控制决策并执行，然后反馈执行结果给安全服务器。

网络接入控制器和应用服务控制器作为网络侧的设备，在移动台进行无线数据网络附着时，会得到移动台的各种能力信息。移动台PDP上下文激活时，网络接入控制器和应用服务控制器应该立刻将移动台能力信息、移动台PDP上下文、移动用户ID发送给安全服务器（SCS），通知安全服务器移动用户开始使

用无线数据网络，关联反应系统开始对此移动台的网络访问和应用服务访问进行动态控制。

5.5 关联反应系统的接口

5.5.1 Ic 接口

Ic接口用于SCA与SCS之间的互通信。SCA向SCS发送SCI报告，SCS基于此返回回复信息。回复信息的内容包括SCA控制策略（见6.2.3节）以及安全更新信息。

在SCA和SCS服务器之间交换移动台安全相关信息之前，可以协商建立安全的通信通道，安全通道的建立可以采用WTLS、AKA协商、IPsec等安全机制。

5.5.2 Ics 接口

Ics接口用于NAC/ASC与SCS之间的与控制策略相关的信息交互。NAC/ASC向SCS请求下发针对受控对象（SCS控制的单个移动台或一个移动台组）的控制策略，SCS分析评估受控对象的安全等级后，返回相应的安全控制策略。

在Ics接口中，NAC/ASC与SCS之间的连接采用基于IP的TCP连接，以保证两者通信的可靠传输。NAC/ASC和SCS服务器之间的互相寻址是静态配置在两者的配置文件中的，当NAC获得SCS服务器的地址之后，就会和SCS服务器协商建立消息传输通道。这个通道采用的安全机制可以是IETF的TLS和IPsec。

6 关联反应系统的策略

6.1 移动台安全等级划分策略

6.1.1 概述

基本上，评估和确定移动终端的安全等级是CRS的核心。具体而言，SCS根据安全评估策略分析单个移动终端的安全状况（基于MS的SCI报告），进而确定移动终端的安全等级。针对每一个移动终端，基于其安全等级，CRS采用不同的安全控制策略。这种基于安全等级保护用户终端和网络的思想区分了应用于CRS中的策略，使其能更有针对性和适应性地适应移动台的各种不同状况。总之，等级化使得策略的执行更加合理。

安全等级划分的具体策略不在本文中定义，本节仅提供划分等级的基本原则。

6.1.2 等级评估参数

各种参数是CRS系统对移动台进行安全等级评估的依据，这些参数主要在终端内通过本地的Ica接口传输的安全信息获取。通常，为了进行综合分析，CRS至少需要获取两个终端的安全信息。

Ica接口实现了SCA与MSOS/SAS之间的信息交互。通过Ica接口，SCA能够从MSOS和SAS获取安全相关信息。另外，SCA也能够基于终端安全更新的目的传递相应的信息给MSOS/SAS。由于SCA是应用层上的功能实体，这个Ica接口可以基于MSOS提供的API设计实现。通过MSOS的API，SAS应用也能够通过Ica接口与SCA通信。SCA接收到的信息应保证可信和未篡改，并且这些信息不应暴露给其他软件。在传输的过程中，完整性保护也应提供。

安全信息包括安全配置信息和/或安全事件信息。安全配置信息包括系统安全配置信息、应用安全配置等信息。安全事件信息包括病毒事件信息、攻击事件信息和非法扫描等信息。根据安全信息和用户相关的信息，可以析出表1所示的几种参数。

表1 等级评估参数

用户信息	用户标识	用来关联安全等级评估、控制策略与用户的对应
	签约服务	用于评估移动台的安全问题对用户使用某项签约服务时是否会带来较大的风险，是影响CRS系统评估移动台安全等级的一个因素。这部分信息可从网络侧获得
	当前业务	用于评估移动台的安全问题为用户当前正在使用的业务是否会带来较大风险，是影响CRS系统评估移动台安全等级的一个重要因素。这部分信息可从网络侧获得
移动台操作系统信息	操作系统/平台类型	不同的操作系统/平台安全隐患不同，一般地，市场占有率越高，则受到的威胁越大
	版本	一般地，版本较旧的操作系统，隐患更多一些
	补丁安装情况	操作系统/平台补丁对于系统的安全非常重要，一些关键的补丁未安装可能直接导致系统受到热门病毒的攻击
	当前开放端口状况	一般地，为保证安全，OS应关闭不必要的通信端口。这是因为端口开放地越多，安全漏洞越多
安全软件信息	安全软件类型	移动台安装了何种安全软件，有何功能。一般地，安装的安全软件种类越多，功能越强大，则安全性越高，但也会耗费移动台的本地资源
	版本	一般地，版本较新的安全软件，其功能及保障安全的能力更强一些
	病毒、木马检测结果	这是一条重要的参数，对移动台安全等级评估有较大影响。一般地，若检测到破坏性或传播性较强的病毒、木马而无法查杀，则会把该移动台列为高级别的安全等级
	攻击检测结果	反映移动台遭受攻击的情况
	安全日志	移动台安全软件得出的安全状态分析结果，对安全等级评估有参考意义
	病毒库版本	病毒库应保持更新，版本越新，则安全性越好
移动终端信息		提供移动终端的产品类型、型号、版本。不同的移动终端安全性也不同，如利用笔记本接入移动网络，其威胁可能就要比手机接入大。或者当某一款终端产品发现漏洞时，这个参数将影响安全等级的评估

6.1.3 安全等级划分

评估结果分为两大类：移动台攻击性安全等级，分高、中、低三级；移动台脆弱性安全等级，分高、中、低三级。

攻击性安全等级表示该移动台对其他用户及网络的威胁程度，对于这类危险因素，主要采取限制其活动的方式来控制；脆弱性安全等级表示该移动台收到攻击的可能性，对于这类危险因素，主要采取安全更新的方式来控制。攻击性和脆弱性两者不是完全独立的。实际上，两者之间有一定联系，它们可以共存，有时会发生转换，如，当一个脆弱的移动台受到感染病毒后，很可能就会成为病毒的传播者，从而具有了攻击性。通常，为了全面的安全评估，一个移动台应同时具有两类安全级别。

高中低三个等级划分，应根据网络实际情况而定，下面给出一种一般情况下等级的参考划分方法。

- 高度攻击性：对其他用户和网络具有严重的、直接的威胁。该威胁具有很强的破坏性和传播性，攻击完全可以实施，如恶性病毒等。
- 中度攻击性：对其他用户和网络具有一定的威胁，该威胁具有较小的破坏性和传播性，攻击有一定的实施可能性。如基于移动台的Dos攻击等。
- 低度攻击性：对其他用户和网络具有潜在的威胁，攻击实施的可能性很小。如广告程序等。
- 高度脆弱性：随时都会受到攻击，且对用户影响比较严重，如操作系统的重大漏洞等。
- 中度脆弱性：有可能会受到攻击，对用户有一定影响，如操作系统开放端口过多等。

- 低度脆弱性：有潜在的受到攻击的可能性，对用户影响很小，如杀毒软件版本不是最新等。

6.1.4 等级化策略制定原则

根据安全等级制定相应策略时，应综合考虑核心网的安全与服务质量的保障这两个问题，尽量使得两者保持平衡。不同安全等级对两者有不同取舍，主要有以下两条基本原则：

- 优先权原则

即确定以保障服务质量为优先还是以保障网络的安全为优先。当两者冲突时，若以保障服务质量为优先，则适当延迟安全策略的执行；反之，则中断服务，执行安全策略。

- 可选/必选原则

即安全策略是否需要强制执行。对于可选的，由用户来决定；必选的，系统强制执行。

以下给出一种参考的不同等级的安全策略制定原则：

- 高度攻击性：安全优先，必选执行安全策略，若有必要可中断用户当前的上行连接或限制其服务。
- 中度攻击性：服务优先，必选执行安全策略，若有必要可限制用户服务。
- 低度攻击性：服务优先，可选执行安全策略，根据提示用户可以接收或拒绝执行安全策略，不对用户服务进行限制。
- 高度脆弱性：安全优先，必选执行安全策略，若有必要可中断用户当前的下行连接或限制其服务。
- 中度脆弱性：服务优先，必选执行安全策略，若有必要可限制用户服务。
- 低度脆弱性：服务优先，可选执行安全策略，根据提示用户可以接收或拒绝执行安全策略，不对用户服务进行限制。

6.2 安全控制策略

6.2.1 概述

安全控制策略是定义并存储在SCS的数据库里。这些控制策略与安全等级相对应，对应关系由SCS设置。从功能上来说，一般可分为用户控制策略和SCA控制策略。用户控制策略是指用于SCS指导网络接入设备（即NAC/ASC）对终端设备进行网络接入的控制和/或应用服务接入控制的策略。SCA控制策略是指控制SCA及时收集、报告移动台安全相关信息的策略。控制策略的具体形式由网络运营商自己定义，本节内容仅提供用于定义控制策略的参考基准。

6.2.2 用户控制策略

用户控制是指SCS通过与SCS和NAC/ASC的联动，利用限制访问、QoS重配置和重定向等技术手段，实现对用户接入网络的限制，以防止不安全终端对网络资源的不合理占用，阻止病毒在网络中传播。

限制访问策略可以宽泛地设置为无限制、全限制和部分限制。无限制意味着对终端不采取任何控制措施；全限制是指终端不可访问任何网络资源；部分限制是指仅允许或禁止终端访问某些特别地址。这里的特别地址可以被分为两类：信任地址和受限地址。前者是指那些足够安全的终端和应用服务提供商。通常MSOS-US和SAS-US属于此类地址。对应地，后者是指那些足够不安全的终端和ASPs。

重定向策略是指允许访问网络但是所有的报文被重定向至某些专用安全设备（DSD），如防病毒防火墙。DSD首先过滤这些报文，如果发现某些报文可能导致病毒的传播则丢弃这个报文，否则将此报文转发至目的地址。

运用QoS重配置策略，CRS系统可以依据移动台的安全状态动态地调整提供的服务质量。一般而言，提供给移动台的服务质量与移动台的安全状况成正比。

依据移动台的安全等级，网络接入控制策略在定义时应参考表2所示基准。

表2 用户控制策略

移动台安全等级	用户控制策略
高度攻击性	全接入限制或重定向策略
中度攻击性	重定向 或 QoS重配置（限制带宽）并且仅允许其访问信任地址
低度攻击性	对网络访问不作限制
高度脆弱性	仅允许其访问信任地址 限制移动台访问网络的带宽
中度脆弱性	禁止其访问受限地址
低度脆弱性	对网络访问不作限制

另外，当SCS服务器没有依照SCA控制策略的规定接收到SCA发送的SCI报告，SCS无法评估移动台的目前安全状况。此时，为了保证网络的安全，NAC执行默认的网络接入控制策略。默认的网络接入控制策略可以是禁止移动台访问移动数据网络或Internet的任何资源；默认策略也可以是NAC将移动台发出的所有报文重定向到专用的安全设备处理，比如，重定向到反病毒网关先进行过滤，然后再向报文的目的的转发。

6.2.3 SCA 控制策略

SCA控制策略包括SCI报告策略和SCI搜集策略。

a）安全信息报告策略

安全信息报告策略包括SCA向SCS报告移动台SCI时报告的内容、编码格式以及报告时机等参数的规定。其中的报告时机是指报告的发送周期设置以及对在何种安全事件（如当移动台感染了某种病毒、受到某种网络攻击、用户卸载了移动台上的某种安全软件等）发生的情况下即时发送SCI报告的规定。根据报告发送时机的不同，安全信息报告策略可有以下4类划分。

（1）初始SCI报告策略

当移动台连接到数据网络，SCA接收到来自SCS的SCA探测请求时，SCA必须向SCS服务器发送移动台初始的SCI报告。此报告向SCS提供最全面的安全相关信息以方便SCS对移动台的安全状况进行全面的评估并划分对应的安全等级。这个初始SCI报告应包括在6.1.1中提及的所有安全评估参数。

（2）周期SCI报告策略

移动台连接到数据网络后，SCA需要定期向SCS服务器发送安全信息报告，直到移动台断开到数据网络的连接。SCA发送安全报告的周期的初始设置为SCA默认的安全报告发送周期和报告内容；在移动台与网络连接的过程中，SCS可基于对网络和终端安全状况的综合考虑，即时更改SCA内安全报告发送周期的设置（见SCA控制策略）。例如：当移动台的安全等级降低后，SCS可以指示SCA缩短发送安全报告的时间间隔，以更密切地关注移动台的安全状况并在必要时采取相应的控制措施。反之，SCS则可以指示SCA以较长的时间间隔发送安全报告。

周期安全报告的基本内容需要包括一个报告周期内移动台安全状况的变化以及安全事件的统计信息。例如报告周期内受到某网络攻击的类型、攻击的次数和攻击来源等。在网络连接的过程中，SCS同样有权限依据基于安全等级的SCA控制策略（见SCA控制策略），更改周期报告的内容配置。

与移动台的安全等级对应，设计周期SCI报告策略的参考原则见表3。

表3 周期SCI报告策略

移动台安全等级	SCA控制策略
高度攻击性	● 频繁发送安全报告 ● 丰富的安全报告内容
中度攻击性	● 默认安全报告的周期 ● 默认安全报告的内容
低度攻击性	● 缩短安全报告的周期 ● 减少安全报告的内容
高度脆弱性	● 频繁发送安全报告 ● 丰富的安全报告内容
中度脆弱性	● 默认安全报告的周期 ● 默认安全报告的内容
低度脆弱性	● 缩短安全报告的周期 ● 减少安全报告的内容

（3）安全事件报告策略

移动台上发生的任何安全事件，都会触发SCA向SCS发送安全事件报告。特别地，不管安全事件是否造成了破坏移动台安全状况的后果，SCA都需要将此安全事件报告给SCS。例如，当移动台感染某种病毒，但病毒已被隔离或清除，移动台的安全性并未被破坏的情况下，SCA仍旧需要向SCS报告此事件。根据这些报告，SCS进行关联分析网络内发生的安全事件，预测安全威胁的趋势，做好积极防范的准备。

这个报告的内容包括:

- 安全事件类别。安全事件包括移动台感染病毒、受到网络攻击、安全应用软件被卸载/更改、某个端口和服务被开启等。
- 安全事件的名称。
- 发生的时间、安全事件的来源。
- 安全应用软件采取的针对性措施。
- 其他相关内容。

例如当报告病毒感染的安全事件时，需包括病毒名称、病毒类型、感染的时间、病毒来源、感染文件类型、防病毒软件采取了何种措施等。

（4）受邀SCI报告策略

当SCS临时需要SCA汇报移动台安全相关信息时，可以主动请求SCA发送SCI报告， SCA必须按照SCS的指示，在SCS规定的时间报告SCS感兴趣的移动台安全相关信息。

b）安全信息收集策略

安全信息的收集通过位于SCA端的Ica接口实现。收集信息的对象主要有以下几种：

（1）MSOS相关信息；

（2）安全应用程序相关信息；

（3）移动终端设备的信息。

这些信息由相关软件收集并通过Ica接口传递给SCA，收集信息的具体内容请参见章节6.6.1描述。SCA进行信息收集的时机依赖安全信息报告策略的规定，其具体的实现不在本标准研究范围之内。

6.3 群组属性管理

为了提高CRS系统对移动台的控制执行效率，减轻CRS系统的负担，CRS系统应提供对群组管理的支持。对于每一个在线的移动台，SCS都会基于此移动台的综合评估结果，动态地为其设置群组属性。群组属性的配置在SCS、NAC/ASC和SCA之间需保持一致。

在移动台上线后，SCS就可以依据SCA上报的SCI报告对移动台的相关状态信息进行分析评估，为移动台设置群组属性。一个移动台可以同时加入多个群组，具备多群组属性。基于不同的应用场景和实现目的，群组属性可以有多种多样的划分，如移动台类型群组、所处区域群组、安全等级群组和服务类型群组等。表4给出一个群组属性的应用示例。

表4　某移动台的群组属性

群组类型	群组标识	群组描述
移动台类型群组	Type-PDA	移动台为 PDA
平台类型群组	OS-Windows Mobile	操作平台是 Windows Mobile 的移动台
区域群组	LA-A	处于位置域 A 的移动台
安全等级群组	SecLevel-V3	由 SCS 评估为高脆弱性安全等级的移动台
服务类型群组	Service-VIP	安全服务等级为 VIP 的移动台

为方便CRS后续的群组管理，SCS应将群组属性告知NAC和SCA。SCS可以通过第一次向NAC下发的控制策略指令将移动台的群组属性告知NAC；同时SCS也可以通过向SCA发送的第一次SCI Response告知SCA移动台的群组属性。在移动台连接的过程中，SCS也可以分别通过后续的控制更新请求和SCI Response更改移动台的群组属性。

群组属性可以应用在CRS的各种流程，包括SCS更新NAC中一组移动台的用户控制策略，SCS向一组移动台发送更新提醒或请求SCI报告等等。10.2节是群组属性管理的一个具体应用。

7　SCA 和 SCS 之间的通信

7.1　消息承载协议

CRS应用协议用来实现安全代理SCA和安全服务器SCS之间的CRS消息传输。实体发现过程（见9.1节）的消息传输需要采用确认模式，即信息发送者需要接收者确认接收到发送的消息。然而，大多数用于传递安全相关数据信息的消息（如SCI报告），既可以使用确认模式，也可以使用无确认模式（详述见第9章）。

CRS应用协议位于TCP/UDP的传输层之上，CRS应用协议可以选择基于可靠的底层传输协议，如TCP，也可以基于不可靠传输协议，如UDP。选择的依据是消息类型和内容本身的安全性要求。

7.2　安全性

在安全代理SCA和安全服务器SCS之间传输的CRS消息为应用层消息，承载在安全协议和传输层协议之上。协商建立CRS消息的安全传输通道的协议可以为TLS、WTLS、IPsec等。CRS系统不严格限制采用哪种安全机制。另外除非特殊情况，如网络侧发起的移动台大规模安全更新，一般SCA和SCS之间的所有CRS消息都应该通过安全通道传输。

如果SCA和SCS的通信没有可用的安全通信通道，而CRS消息要求其传输必须基于安全通道同SCA进行通信，则SCA首先需要向SCS发送安全通道建立请求。

7.3　传输的消息

7.3.1　概述

CRS消息分为三个组成部分：消息头、消息主体和消息尾（可选）。CRSAP消息采用XML语言描述

如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
xmlns:CRS="http://www.huawei.com/crs/schema/crs-schema"
targetNamespace="http://www.huawei.com/crs/schema/crs-schema"
elementFormDefault="qulified" attributeFormDefault="unqualified"
  version="1.0" id="CRSAP-Message">
<xs:element name="CRSAP-Message">
  <xs:complexType>
    <xs:element name="Header-Unit" type="CRSAP:Header-Unit" minOccurs="1" maxOccurs="1"/>
    <xs:element name="Body-Unit" type="CRSAP:Body-Unit" minOccurs="1" maxOccurs="1"/>
    <xs:element name="Tail-Unit" type="CRSAP:IntegAuth-Unit" minOccurs="0" maxOccurs="1"/>
  </xs:complexType>
</xs:element>
```

消息头部分长度固定，消息体和消息完整性校验部分长度可变，消息完整性校验为可选内容，消息头中的相关标志位标识 CRS 消息中是否包含消息完整性校验部分。

7.3.1 消息头

CRS应用协议消息采用如下统一的消息头格式，CRSAP消息头采用XML语言描述如下：

```
<CRSAP:complexType name="Header-Unit">

  <xs:attribute name="Version" type="xs:string" use="required">
  </xs:attribute>

<xs:attribute name="Flag" type="CRSAP:Header-Flag" use="required">
  </xs:attribute>

<xs:attribute name="Type" type="CRSAP:Header-MsgType" use="required">
  </xs:attribute>

<xs:attribute name="Length" type="xs:nonNegativeInteger"use="required">
  </xs:attribute>

<xs:attribute name="SCS-ID" type="CRSAP:ID" use="required">
  </xs:attribute>

<xs:attribute name="SCA-ID" type="CRSAP:ID" use="required">
  </xs:attribute>
</CRSAP:complexType>

<CRSAP:simpleType name="Header-Flag">
  <xs:restriction base="xs:string">
  <xs:minLength value="1"/>
  <xs:maxLength value="1"/>
```

```
    </xs:restriction>
  </CRSAP:simpleType>

  <CRSAP:simpleType name="Header-MsgType">
    <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
    <xs:maxLength value="1"/>
    </xs:restriction>
  </CRSAP:simpleType>

  <CRSAP:simpleType name="ID">
    <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
    <xs:maxLength value="32"/>
    </xs:restriction>
  </CRSAP:simpleType>
```

（1）Version

表示CRSAP协议的版本号。

（2）Flag

多位标志位。此标志位至少应包含一个‘M’位和‘T’位。M位用于标识此消息是组播方式还是单播方式。‘T’位表示此消息是否包含消息尾。

（3）Precedence

用于消息接收者判断消息的处理优先级。

（4）Type

消息的类型，用于标识SCA和SCS服务器之间传递的消息类型。‘O’位用于指示消息的传输方向。代表不同消息类型的type值见表5（详述见第9章）。

表5　SCA-SCS通信消息类型

消息类型代码（十进制）		消息类型含义	是否需要可靠传输
O位	各方向具体消息类型		
0	1	SCI Report	可选
0	2	SCA Probe Response	
0	4	Ack	
0	5	Error Notification	
1	1	SCI Response	可选
1	2	SCA Probe Request	
1	3	SCI Report Request	必选
1	4	Acknoledgement	
1	5	Error Notification	

注：对于上述的数据元素，在用XML编码的情况下，需要转换为ASCII码。

（4）Length

消息长度。CRS消息长度是消息头、消息主体和消息完整性校验（如果存在的话）三部分长度的总和。

（5）SCS ID

安全服务器标识，全球唯一标识SCS。

（6）SCA ID

安全代理标识,SCA ID应该在一个安全服务器SCS服务器的管理范围内唯一，SCA ID可由网络侧分配。SCA ID也可能是一个用户组ID。

7.3.2 消息主体

CRS应用协议的消息主体长度是可变的。一个消息主体可以包含多个子类型的消息，消息主体格式的XML描述如下：

```
<CRSAP:complexType name="Body-Unit">
  <xs:sequence>
   <xs:element name="Sub-Msg1-Name" type="CRSAP:Sub-Msg1-Type" minOccurs="0" maxOccurs="1"/>
   <xs:element name="Sub-Msg2-Name" type="CRSAP:Sub-Msg2-Type" minOccurs="0" maxOccurs="1"/>
   ...
   <xs:element name="Sub-Msgn-Name" type="CRSAP:Sub-Msgn-Type" minOccurs="0" maxOccurs="1"/>
  </xs:sequence>
</CRSAP:complexType>
```

目前已定义的 CRSAP 消息类型和子消息类型见表 6。

表6 消息类型和子消息类型

消息类型	消息子类型
SCI Report	移动台用户标识
	移动台 ISDN
	移动终端设备标识
	移动台操作系统类型和版本
	移动台操作系统补丁信息
	移动台安全应用软件和版本、数据库信息
	移动台硬件信息
	上报目前的 SCI 报告策略给 SCS
	上次通信的 SCS 服务器域名、地址和端口、SCS ID 信息
SCI Response	安全等级评估结果
	下发新的 SCI 报告策略给 SCA
	用户网络访问、应用服务受限通知
	对 SCI Report 的确认
SCA Probe Request	安全服务器 SCS 的域名、地址和服务端口信息
SCA Probe Response	上次 CRS 通信的 SCS 服务器域名、地址和端口、SCS ID 信息
	上次 CRS 通信用的 SCA ID
SCI Report Request	要求 SCA 报告的 SCI Report 消息子类型列表
	本次报告的时机
Ack	被确认消息类型的代码

7.3.3 消息尾

消息尾为CRS应用协议消息中的可选项，用于接收端对收到的消息进行完整性检查以及源端认证。当承载CRS消息的安全协议已经对CRS消息实施了完整性保护时，CRSAP消息本身可不选择包含此消息尾。在其他情况下，CRS应用协议消息必须包含此消息尾。

CRSAP消息尾格式的XML描述如下：

```
<CRSAP:complexType name="Tail-Unit">
  <xs:sequence>
    <xs:element name="AlgorithmID" type="CRSAP:ID" minOccurs="1"
     maxOccurs="1"/>
    <xs:element name="MsgID" type=" CRSAP:ID" minOccurs="1"
     maxOccurs="1"/>
    <xs:element name="MsgDigest" type="CRSAP:MsgDigest" minOccurs="1" maxOccurs="1"/>
</xs:sequence>
</CRSAP:complexType>

<CRSAP:simpleType name="MsgDigest">
  <xs:restriction base="xs:string">
  <xs:minLength value="8"/>
  <xs:maxLength value="32"/>
  </xs:restriction>
</CRSAP:simpleType>
```


（1）AlgorithmID

算法标识，用于通信双方标识进行CRS消息完整性保护和源端验证时所用的算法。

（2）MsgID

消息序列号，用于SCS或者SCA来标识其互相间消息传输的先后顺序。在SCA和SCS服务器之间消息传输的两个方向上，应分别采用各自的MsgID和不同的MsgID初始值。

（3）MsgDigest

消息摘要可以是CRSAP消息头和消息主体的Hash值，为32bit的整数倍，用于存放加密后的消息完整性运算结果。

8 NAC/ASC 和 SCS 服务器之间的通信

8.1 概述

NAC/ASC与SCS之间的通信目的是用户控制策略的有效传达和执行，即基于策略的对移动台用户的有效控制。

本文档推荐采用IETF COPS协议承载在SCS和NAC/ASC之间传递的消息。NAC/ASC是策略执行点，SCS是策略决策点；NAC/ASC向SCS请求控制策略，SCS返回控制策略；如果SCS判定需要对移动台的用户控制策略进行更新，SCS会主动下发更新的策略信息。

注：有关COPS的详细信息见IETF RFC 2748和RFC 3084。

与COPS规定的消息相似，本章介绍在SCS和NAC/ASC之间传输的消息。

8.2 安全性

CRS消息的安全性由承载协议提供，但消息级的完整性保护必须保证。另外，传输层安全性必须由TLS或者IPsec提供。

8.3 传输的消息

8.3.1 控制策略请求

针对每一个受控对象，作为控制执行设备，NAC/ASC发送*Object Policy Request*消息，请求SCS下发针对此对象的控制策略。控制策略请求消息中，应包括的内容有：

— 控制策略请求编号：由 NAC/ASC 分配，用于唯一地标识针对一个控制对象的控制策略请求。一个受控对象只有一个控制策略请求编号。

— 策略请求类别：网络访问控制类或应用服务控制类。

— 受控对象类型：单个移动台/一个移动台组等。

— 受控对象标识：对于单个移动台可以用 IMSI+IMEI 识别；同安全等级移动台组的标识可以用安全等级编码来标识；对于同路由域移动台组标识则可以用 RAI（路由域标识）来标识。

— 控制对象相关信息：一些附加的与 CRS 控制相关的信息，如移动台寻址信息。例如，在 GPRS 网络中，对于单个移动台对象，此控制对象相关信息应包括移动台的 PDP 地址、RAI, 以及安全能力信息等。

控制策略请求消息发送的情况有以下两种：

— NAC/ASC 向 SCS 请求移动台初始控制策略

当移动台通过认证、成功连接到数据网络并获得 PDP 地址后。此时，NAC 应立刻将此移动台的地址、移动台用户 ID 等信息作为移动台连接报告发给 SCS 服务器，请求 SCS 提供针对此移动台的控制策略。SCS 服务器收到 NAC 发来的有效的移动台连接报告后，应向 NAC 返回执行默认控制策略（此初始控制策略应允许移动台访问 SCS）；然后立刻向移动台的 SCA 发送 SCA 探测请求消息，尝试与其进行通信，获取移动台的初次 SCI 报告。可选地，SCS 服务器也可利用移动台连接报告中的用户身份信息查询移动台用户的定制服务，并索引 SCS 服务器上已经存储的历史 SCI 报告。

— SCS 指示 NAC/ASC 向其请求新的策略

SCS 指示 NAC/ASC 可以向其请求提供针对相同安全等级或相同路由域的一组移动台的控制策略。此策略是基于移动台安全等级划分及移动台所处位置的统计信息制定。

8.3.2 控制策略交付

当SCS接收到*Object Policy Request*消息时，SCS确定何种用户控制策略适合受控对象，然后将此策略交付给NAC/ASC。NAC/ASC根据收到的策略执行对受控对象的控制。

在NAC/ASC向SCS发送了一个对象控制策略请求之后，如果SCS并不知道控制对象的目前安全状况，即SCS还未接收到移动台的SCI，SCS默认地发送如允许此对象访问SCS或将此移动台的网络访问重定向至某个专用安全网关之类的安全控制策略给NAC/ASC。

在之后的过程中，当SCS受到外部事件（如接收到来自移动台的SCI报告或网络管理员的直接策略配置操作）的触发，将发送后续的*Object Policy Decision*给NAC/ASC，用于更新NAC/ASC对移动台的控制策略，指明删除何种策略，安装何种策略。

特别地，当SCS在规定的时间范围内未收到来自SCA的SCI报告或主动请求SCI报告无响应时，SCS视此移动台安全状况不明朗，应将默认控制策略发送给NAC/ASC以保证网络的安全性，并启动SCA是否工

作正常的检测机制，可能触发SCA的自动安装过程。

另外，当SCS认为有必要下发针对新的策略控制对象的控制策略时（如基于对来自每个移动台的SCI报告的统计结果，SCS决定要对某移动台组下发统一的控制策略），也可以通过此消息通知NAC/ASC向SCS发送一个新的*Object Policy Request*来交付此策略。

不管何时NAC/ASC接收到来自SCS的*Object Policy Decision*，都必须回复SCS *Policy Decision Response*以通知SCS对其所发控制策略的执行结果。如果策略执行失败，NAC/ASC依旧按照上一个成功执行的控制策略执行，同时给SCS回复附带有何种策略不能被执行以及执行失败的原因等信息。

8.3.3 策略执行状态报告

NAC/ASC必须定期地向SCS报告目前对移动台控制策略的执行状况。这个报告的信息的内容包括目前执行策略的列表和针对每条策略执行的统计信息，便于SCS掌握控制策略的有效性。

8.3.4 控制策略同步

基于对接收到的NAC/ASC策略执行状态报告和来自SCA的SCI报告的分析，若SCS发现策略决策与NAC/ASC的执行策略之间存在不同步的情况，应请求NAC/ASC执行策略同步的过程，当NAC/ASC接受请求后，发送所有SCS针对受控对象的控制策略给NAC/ASC，后者接收到此消息后，返回策略同步完成信息。控制策略同步的过程如下所述：

（1）SCS指示NAC/ASC执行控制策略同步流程；

（2）在接收到此指令后，NAC/ASC为指定的控制对象反馈对象策略请求；

（3）SCS下发相应的完整策略决策；

（4）NAC/ASC接收到策略并告知SCS控制策略同步已完成。

8.3.5 控制策略终结

当NAC/ASC发现不再需要对某受控对象进行控制时（如用户离线或离开控制范围），应通知SCS终结控制策略提供的服务。

9 关联反应系统的一般过程

9.1 安全代理 SCA/安全服务器 SCS 发现过程

对于已经安装SCA的移动台，SCA需要得到SCS服务器的地址以便与其进行通信，这里SCS服务器的地址是指SCS服务器的PDN地址，比如IPv4地址或者IPv6地址。图4所示过程是CRS系统定位SCS服务器的方法之一。

（1）移动台经过正常的认证计费流程连接到无线数据网，PDP上下文激活、移动台获得IP地址以后，NAC立刻向SCS服务器发送移动台连接报告（MS Connect Report），报告SCS有新的移动台连接到了部署CRS的数据网络。移动台连接报告包含移动终端的PDP上下文、RAI、移动台用户ID、移动台ID、移动台能力信息等。

（2）SCS服务器向NAC确认收到有效的移动台连接报告。

（3）SCS服务器向SCA发送SCA探测请求（SCA probe request）用来检测移动台是否已经安装了SCA或者已经安装的SCA能否正常工作。SCA探测请求消息中包含SCS服务器的地址和服务端口等信息，这些信息方便SCA进行与SCS通信的必要初始化设置，这在移动台漫游到部署了CRS系统的新的数据网络时是必要的。如果在没有部署CRS系统的数据网络上，因为不存在SCS服务器，移动台SCA一直都不能收到SCS服务器发来的SCA探测请求消息，这样SCA就可以初步判断移动台连接的数据网络中没有部署CRS系统，

这种机制适用在当移动台漫游到没有部署CRS系统的数据网时。

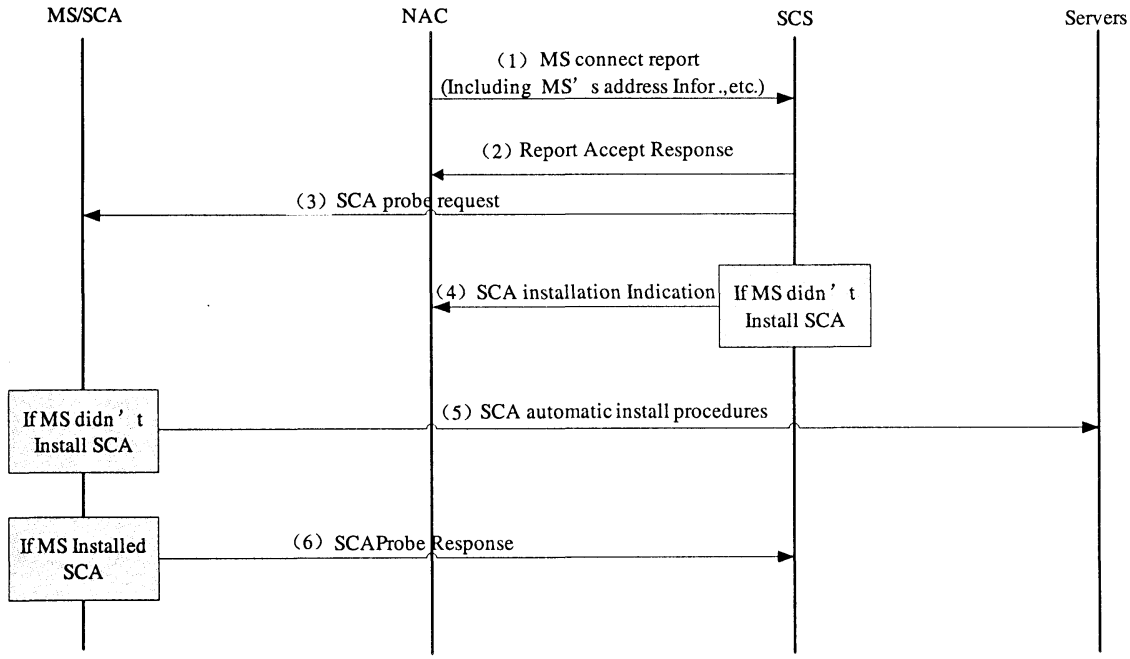


图4 CRS系统SCA/SCS服务器发现过程

（4）如果移动台在规定时间内，没有正确地回应SCS服务器发出的SCA探测请求消息，SCS服务器就认为移动台没有安装SCA或者其上安装的SCA不能正常工作，于是通知NAC，移动台需要安装SCA，进行步骤（5）。

（5）如果移动台没有安装SCA或者已经安装的SCA不能正常工作，则SCA自动安装过程开始，这部分在6.4中作为一个单独的过程来描述。

（6）如果移动台的SCA工作正常，其收到SCS服务器发来的SCA探测请求后会立即回应SCA探测应答报文给SCS服务器，SCS服务器收到此报文后，认为移动台的SCA工作正常，不需要进行SCA的安装。

9.2 SCI 报告和移动台控制过程

在CRS系统中，安全代理SCA发给安全服务器SCS的移动台安全状态报告称为安全相关信息报告（SCI报告），SCI报告主要用于SCA将收集到的移动台的安全现状通知给SCS服务器，以便SCS服务器评估移动台的安全等级，根据安全等级对移动台进行适当的控制，并帮助移动台进行相关的安全更新和升级，从网络侧实时控制和移动台侧安全增强两个方面来保证移动网络的安全。

SCI报告可以包含下述的一些内容。

a）报告序列号

报告序列号是一个渐增的正整数，用于标识移动台的一次数据网络连接会话过程中各个SCI报告的先后顺序。SCS可以利用报告序列号来识别SCI报告是否发生了重传、丢失、乱序。

b）SCA ID

SCA ID用来在移动台中唯一标识一个已安装的SCA。SCA ID用来标识SCS服务器的SCI响应消息应该发给哪个SCA，如果SCA从SCS服务器收到了一条消息，但其中的SCA ID和自己的不符，SCA就认为发生了错误，丢弃这个消息并向SCS服务器发送错误通知。SCA ID可以由访问网络的SCS服务器分配，当移动台漫游到其他的CRS域以后，也可以重新分配。在3G中，可以考虑将SCA ID映射为用户的P-TMSI + 移动台的IMEI。

c）移动终端ID

移动终端ID用来唯一的标识一个移动终端的硬件设备。对于各种手机来说，移动终端ID就是IMEI。

d）SCS ID

SCS ID用来唯一的标识一个SCS服务器，如果SCS服务器收到一个SCI报告，其中的SCS ID和自身的不符，则丢弃此报文。

e）移动台用户ID

移动台用户ID用来唯一的标识一个移动台用户，在3G中，移动台用户ID是用户的IMSI。SCS服务器通过移动台用户ID来识别用户并向其提供定制服务或其他的差异化服务器。

f）SCI报告主体

SCI报告主体包含SCA发送给SCS服务器的所有移动台安全相关信息，包括移动台操作系统类型、版本、补丁信息，移动台安全应用软件的类型、版本、数据库、日志信息等。

安全代理发送SCI报告和安全服务器对移动台的控制过程是CRS的各种过程中最基本的过程，此过程发生在移动台认证通过、连接到数据网络时。此时，安装在移动台中的SCA被激活、生成安全相关信息报告（SCI报告）、开始与SCS服务器通信并发送SCI报告给SCS。SCS服务器分析完SCI报告后，确定移动台的安全状态等级，并下发相应的控制信息给NAC/ASC，对这个特定移动台的网络访问/应用服务访问进行控制。SCS也可以预先下发一些控制策略给NAC/ASC作为其上的本地策略或者默认策略，这样NAC/ASC就可不必为每个事件都向SCS申请策略。

SCI报告和移动台控制过程如图5所示。

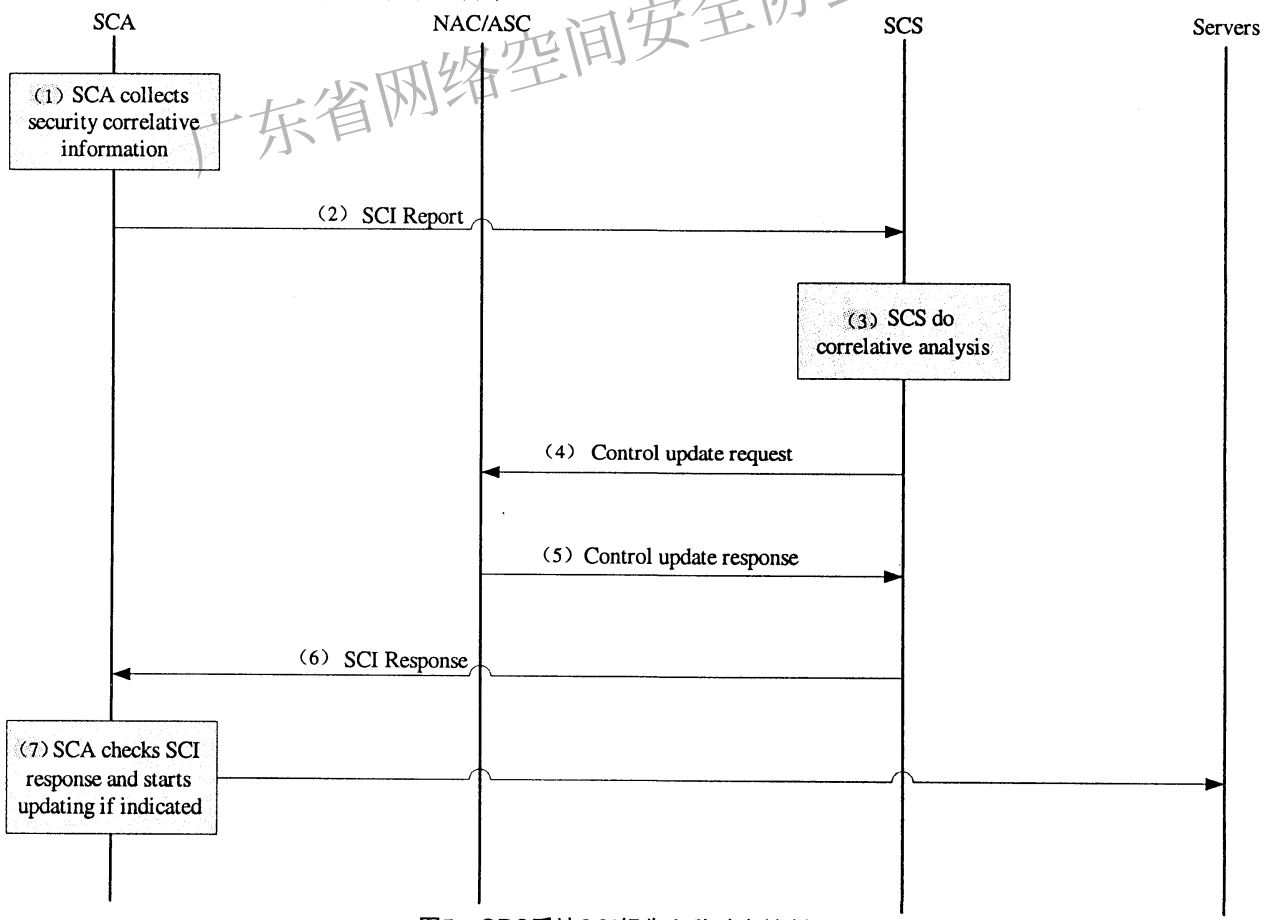


图5 CRS系统SCI报告和移动台控制过程

（1）SCA收集移动台安全相关信息。

（2）SCA基于步骤1的信息生成SCI报告，SCI报告生成过程中参考安全报告策略。SCA发送SCI报告给SCS服务器。

（3）SCS服务器受到SCA发来的SCI报告后首先检查其有效性，然后根据报告的内容和SCS上存储的安全分析策略进行关联分析，判断移动台上的安全状态等级。

（4）如果SCS服务器认为需要对移动台的网络访问控制/应用访问控制进行更新，则发送控制信息给NAC/ASC。

（5）如果步骤4发生，则NAC/ASC需要向SCS服务器反馈控制更新的执行结果。

（6）SCS服务器向SCA发送SCI响应，通知SCA移动台的安全等级评估结果。SCI响应中还可以包含SCA生成和发送SCI报告的策略、SCA收集整理移动台安全相关信息的策略等信息。如果SCS服务器认为移动台需要进行安全更新，SCI响应报文中还要携带安全更新的获取地址和移动台进行安全更新的策略。SCA收到SCI响应后进行有效性检查，然后分析报文内容，使用其中的信息更新SCA的本地信息和策略。

（7）如果SCI响应报文中指示移动台需要安全更新，则SCA按照报文中的信息和策略协助移动台进行安全更新。这里的安全更新也包括SCA自身的升级和更新。

上述过程中，（4）、（5）、（7）是可选步骤，不一定每次都会执行。

9.3 SCA 自动安装和更新过程

9.3.1 SCA 自动安装过程

在部署了CRS的移动网络中，移动台必须安装SCA才能进行正常的无线数据业务，如果移动台没有安装SCA或其上安装的SCA不能正常工作，除了控制Internet应用对移动网络提供的服务以外，移动网络还需帮助移动台自动安装SCA。移动网络中负责这项工作的网元是NAC，在2.5G GPRS网络中，SGSN实现NAC的功能。

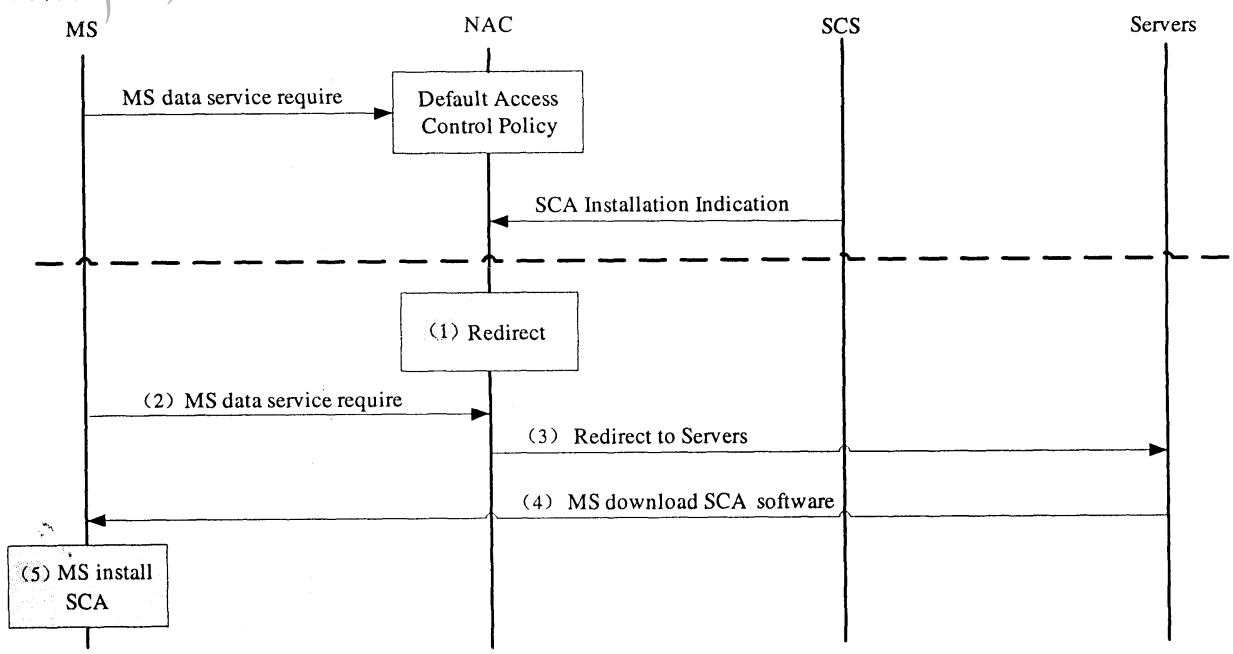


图6 CRS系统SCA自动安装过程

CRS系统SCA自动安装过程如图6所示，下述两个步骤分别代表在SCS做出移动台是否需要安装SCA的判断前移动台发送数据报文的行为和NAC对这部分报文的处理。

（1）移动台请求某种应用服务。

（2）此时SCS服务器还不能评估移动台的安全状况，NAC也不知道是移动台是否需要安装SCA，因而NAC按照默认策略处理步骤1的报文。

当NAC接收到SCS的SCA安全指令后，开始SCA的自动安装过程：

（1）NAC接到SCS的通知——移动台需要安装SCA，NAC开始针对移动台执行重定向措施；

（2）移动台继续发送数据报文或请求某种应用服务；

（3）NAC重定向移动台所有的服务请求至提供SCA安装服务的服务器；

（4）移动台和SCA安装服务器通信，下载合适的SCA安装程序；

（5）移动台安装SCA。安装完成后，立即进行SCA的初始化和SCI报告过程。

在上述过程中，在SCA安装、初始化和SCI报告过程完成之前，移动台可能会持续发送发起Internet服务请求的各种报文，这些报文都将通过移动台的IP网关（即NAC）转发。通过网络侧的配置，管理员可以通过对上述移动台发出报文的控制，进而对移动台的行为进行控制。由于此时SCS服务器还不能评估移动台的安全状况，移动台发送的这些报文可能对整个网络的安全产生潜在的威胁，NAC的配置应该考虑到这些因素，比如，默认策略不允许移动台访问数据网络；默认策略只允许移动台访问特定的服务；或者将用户发送的所有报文重定向到专用的安全设备，如反病毒网关、防火墙等。

当SCA开始工作后，在第一个SCI报告和移动台控制过程中，SCS服务器得到移动台本次连接到数据网络后的第一个SCI报告，在评估移动台安全状况后，SCS通知NAC调整对移动台的控制，此后，移动台就可以进行正常的网络访问，如果需要的话，还可进行安全相关的更新和升级。

9.3.2 SCA 自动更新过程

安全代理SCA的自动更新过程分为两种情况，一种是网络侧的安全服务器主动发起SCA自动更新过程，另一种情况是安全代理发送移动台安全报告触发SCA自动更新过程。安全服务器主动发起的SCA自动更新过程如图7所示。

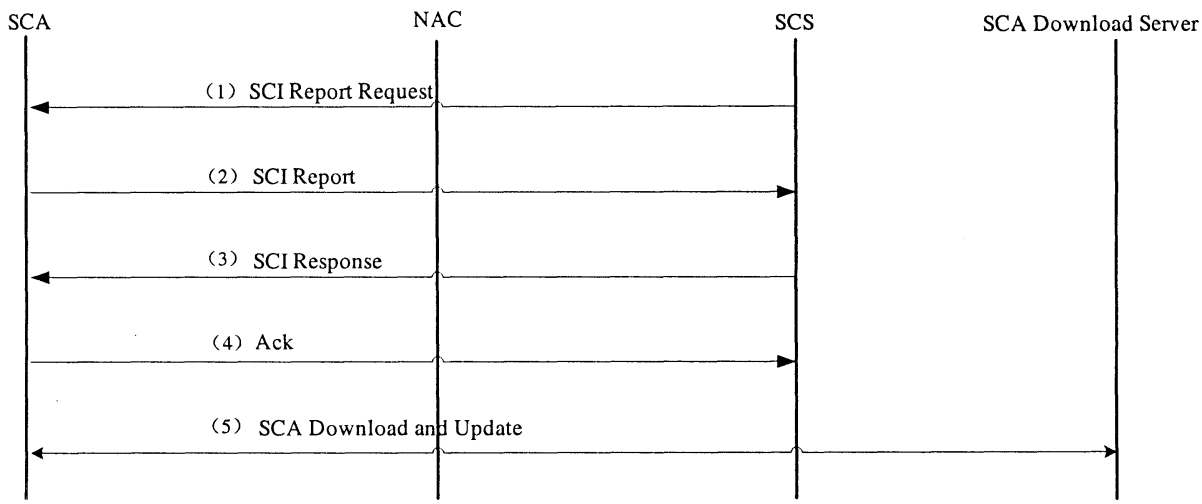


图7 安全服务器主动发起的SCA自动更新过程

（1）当网络侧SCS服务器获知有SCA的新版本发布时，安全服务器SCS向SCA发送安全报告请求（SCI Report Request），要求移动台安全代理SCA向网络侧发送移动台安全报告（SCI Report），报告移动台安全代理SCA的版本信息。

（2）移动台安全代理SCA向网络侧安全服务器SCS发送移动台安全报告（SCI Report），报告SCA的

版本信息。

（3）安全服务器SCS分析移动台安全报告（SCI Report）后，将SCA自身需要更新、升级的相关信息放入安全响应（SCI Response）中发给移动台安全代理SCA。

（4）移动台安全代理SCA对收到的安全响应（SCI Response）内容进行分析，获得更新信息后，SCA向SCS服务器反馈确认消息。

（5）安全代理SCA向网络侧的SCA更新服务器发起SCA自身的更新、升级过程，进行在线SCA自动下载更新。

在上述的安全代理SCA自动更新过程中，网络侧SCS服务器判定SCA需要更新，在步骤1网络侧的安全服务器SCS向移动台侧的安全代理SCA发送安全报告请求（SCI Report Request）之前，如果SCA首先发送了移动台安全报告（SCI Report）给安全服务器SCS，并且安全报告（SCI Report）中携带了安全代理SCA的版本信息，则步骤1可以省略。

这样，SCA自动更新过程就变为由安全代理SCA发送移动台安全报告（SCI Report）触发，其过程如图8所示。

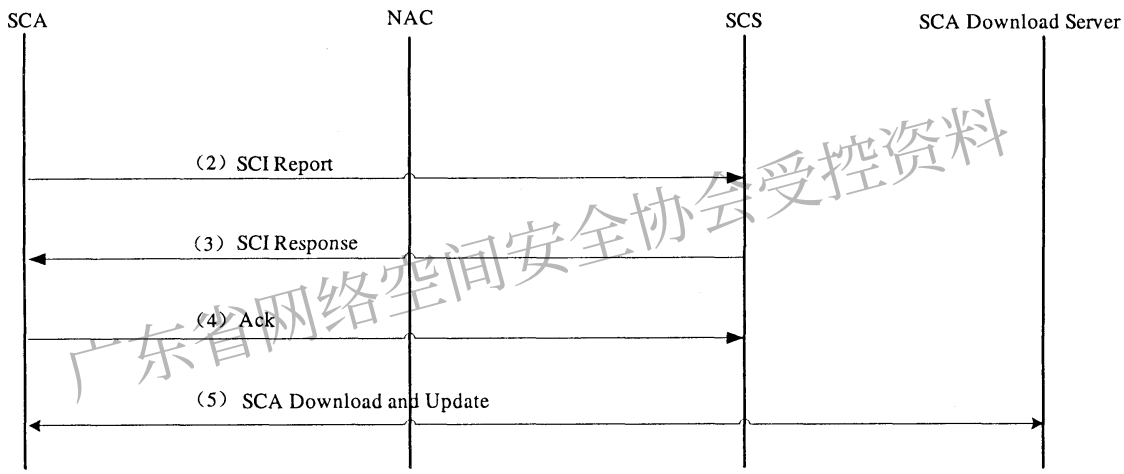


图8　安全代理发送移动台安全报告触发的安全代理自动更新过程

9.4　控制策略生成和下发过程

当安装了SCA移动台连接到网络，需按照SCI报告策略向SCS提供SCI报告，SCS依据此报告内容和SCS内存储的相关安全信息分析评估MS的安全等级，下发相应的安全控制策略，其具体流程如下。

（1）SCS接收到来自SCA的SCI报告。

（2）分析判断此SCI是否符合SCS规定的SCI报告策略。如果不符合，SCS则发送报告拒绝信息并附带新的SCI报告策略信息给安全代理。

（3）如果符合报告策略，SCS对SCI进行筛选，并存储相关的移动台安全信息。

（4）SCS基于安全数据库里存储的安全分析评估策略进行关联分析，评估移动台上的安全等级，并从选取对应的安全控制策略。如果新选择的策略与目前控制执行单元（即网络访问控制器、应用服务控制器和SCA）执行的控制策略存在不同，则发送新的安全控制策略更新消息至控制执行单元。同时，可选地，SCS服务器可以通过SCA将移动台安全等级评估结果及其采用的对应控制策略报告给移动台用户。

（5）SCS关联分析安全知识与SCI报告，如果需要则发送安全更新信息给SCA，指示SCA何种补丁/升级包需要在何处下载安装及更新。

9.5　移动台安全更新过程

移动台的安全更新过程分为两种情况，一种是网络侧的安全服务器主动发起移动台安全更新过程，

另一种情况是移动台安全更新过程由安全代理发送移动台安全报告触发。安全服务器主动发起的移动台安全更新过程如图9所示。

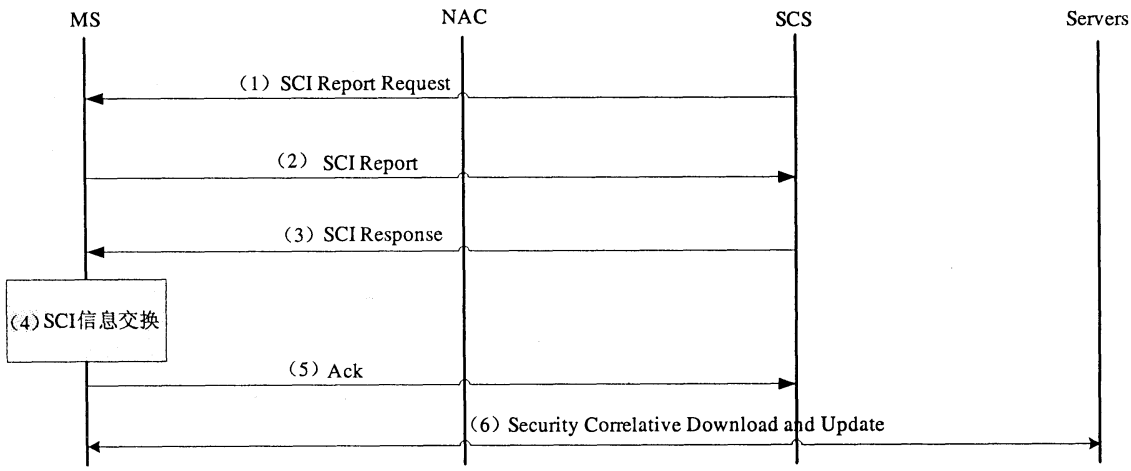


图9 安全服务器主动发起的移动台安全更新过程

（1）当网络侧有新的安全更新时（如移动台操作系统有了新的补丁和升级、移动台安全应用软件有了数据更新等），安全服务器SCS向移动台发送安全报告请求（SCI Report Request），要求移动台安全代理SCA向网络侧发送移动台安全报告（SCI Report），报告移动台操作系统和安全应用软件现有的版本、补丁、数据库日期等信息。

（2）移动台安全代理SCA通过Ica接口从移动台操作系统和安全应用软件搜集安全相关信息（移动台操作系统和安全应用软件到安全代理SCA的信息交换），整理、筛选后，向网络侧安全服务器SCS发送移动台安全报告（SCI Report），报告移动台操作系统和安全应用现有的版本、补丁、数据库日期等信息。

（3）安全服务器SCS分析移动台安全报告（SCI Report）后，将移动台需要更新、升级的相关信息放入安全响应（SCI Response）中发给移动台安全代理SCA。

（4）移动台安全代理SCA对收到的安全响应（SCI Response）内容进行分析，然后通过Ica接口将相关更新、升级信息和更新资源所在的URL地址发送给移动台操作系统/安全应用软件（SCI信息交换），操作成功SCA向SCS反馈确认消息。

（5）步骤（4）安全代理SCA到移动台操作系统和安全应用软件的信息交换成功完成后，移动台侧的安全代理SCA向网络侧的安全服务器SCS发送确认消息。

（6）移动台操作系统或安全应用软件向网络侧的更新、升级服务器发起更新、升级过程，进行在线的安全更新。

Servers包含移动台操作系统和安全应用软件的更新、升级服务器，移动台安全应用软件包含安装在移动台上的防火墙、反病毒软件等。

在上述的移动台安全更新过程中，网络侧SCS服务器判定移动台需要进行安全更新，在步骤1网络侧的安全服务器SCS向移动台侧的安全代理SCA发送安全报告请求（SCI Report Request）之前，如果移动台首先发送了移动台安全报告（SCI Report）给安全服务器SCS，并且安全报告（SCI Report）中携带了移动台操作系统版本/补丁信息、安全应用软件的版本/数据库日期等网络侧期望了解的信息，则上述步骤1——安全服务器SCS给安全代理SCA发送的移动台安全报告请求（SCI Report Request）可以省略。

这样，移动台的安全更新过程就变为由移动台侧的安全代理发送移动台安全报告（SCI Report）触发，过程各步骤如图10所示。

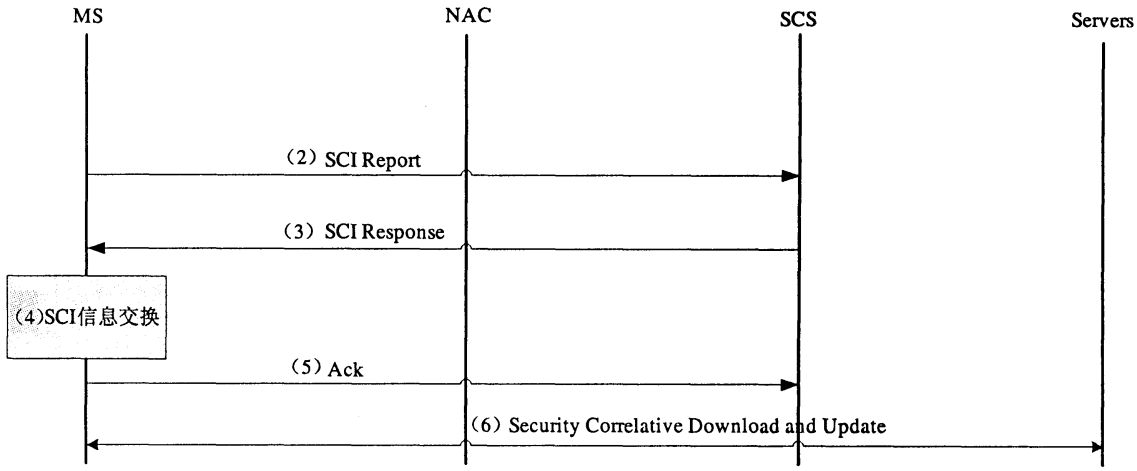


图10 安全代理发送移动台安全报告触发的移动台安全更新过程

9.6 移动台离开数据网络的下线过程

移动台离开数据网络的下线过程如图11所示。

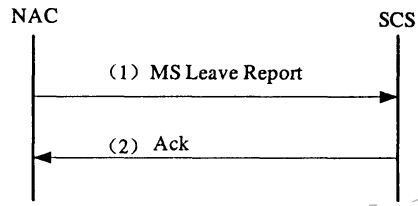


图11 移动台离开数据网络的下线过程

（1）当移动台或者网络侧发起PDP去激活过程，NAC在执行完移动台离开无线数据网的标准流程后（如3GPP的PDP上下文去激活过程），NAC向安全服务器SCS发送移动台下线报告（MS Leave Report）给安全服务器SCS，通知安全服务器移动台已经离开无线数据网。移动台下线报告中应该包含移动用户ID、SCA ID、移动终端ID、移动台PDP上下文等信息。

（2）安全服务器收到移动台下线报告后，将相关移动台标记为下线状态，在移动台下一次连接到数据网络之前，安全服务器SCS将不再主动向移动台安全代理SCA发送任何消息。对于收到的移动台下线报告，安全服务器需要向NAC发送确认信息。

如果移动台以异常方式离开数据网络，NAC的移动性管理功能（如GPRS网络中SGSN的移动性管理功能）负责移动台的通信以及移动台与移动数据网络连接状态的维持。在此情况下，移动性管理功能应首先探测到此事件并启动此移动台离线流程。

10 特殊处理流程

10.1 大范围安全更新

10.1.1 概述

当SCS发现某个安全更新的重要级别达到需要对受控移动台进行大范围的紧急安全更新时（即此更新所针对的安全漏洞对网络和终端的安全性具有严重的破坏作用时），CRS需启动大范围安全更新流程。为避免在大范围安全更新时由于数目过多的移动台同时访问安全更新服务器和SCS，导致此流程衍变成一种对CRS系统的DDOS攻击，破坏CRS系统的可用性，本节提出了一个基于群组管理的解决方案。整个方案分三个阶段执行：更新执行前，更新执行过程中及更新完成后。

10.1.2 更新执行前

在大范围更新执行前，CRS需要做的准备工作是为移动台设置更新服务群组属性配置并将此群组属性告知NAC和SCA.

（1）群组属性设置

如前文所述，当接收到移动台的初始SCI报告后，SCS会评估移动台的安全状态。在此期间中，SCS可以基于评估的结果将移动台加入的具有相应的执行优先级的更新服务群组。更新服务群组的划分需综合考虑的因素包括移动台的类型（如笔记本电脑，PDA，智能手机等等）、操作系统平台类型（如Symbian，Windows Mobile等），移动台的安全等级，更新对象的类型，用户定制的安全服务等。例如，基于WINDOWS MOBILE平台的高脆弱性PDA移动台设置为更新服务群组A，低脆弱性的则设置为更新服务群组B,在执行大范围安全更新时，群组A先于群组B执行。

另外，基于对网络流量/带宽、更新的估计执行时间和流量需求，以及SCS自身负载能力等因素的衡量，更新服务群组的成员数量应允以限制，避免更新的执行超出网络和安全更新服务器的负载能力。

（2）群组属性传达

在移动台上线后，SCS在第一次向NAC下发的控制策略指令时，就应将移动台的更新服务群组属性告知NAC；同时通过第一次SCI Response告知SCA移动台的群组属性。在移动台的连接的过程中，SCS可以基于接收到的SCI报告动态更改此群组属性，并分别通过后续的控制更新指令和SCI Response通知NAC和SCA此属性变化。

10.1.3 更新执行过程中

当SCS发现某个更新的重要级别达到需要对受控的移动台进行大范围的紧急安全更新时，SCS触发大范围更新流程。具体过程如图12所示。

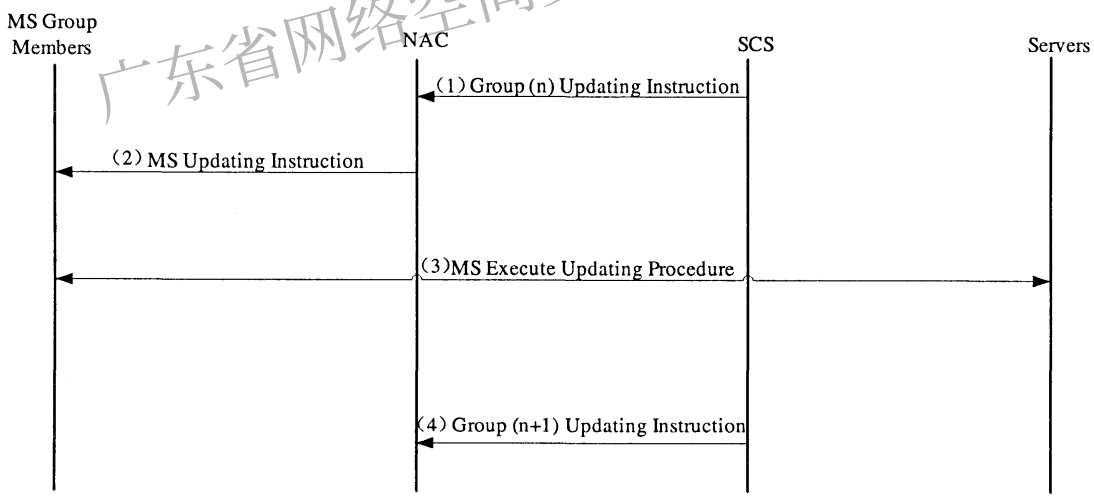


图12 执行群组更新

（1）SCS发送群组更新指令给NAC

SCS按照更新服务群组优先级顺序向NAC发送群组更新指令，这个指令需包括的信息见表7。

表7 群组更新指令

项 目	说 明
SCS ID	SCS 的标识
NAC ID	NAC 的标识
指令序列号	唯一标识一个指令
指令有效期	超出此有效期后，NAC 不应执行此指令
指令类别	大范围更新

表 7（续）

项　目	说　明
群组标识	标识启动更新流程的群组
更新资源地址	获取此次安全更新的更新资源地址
移动台更新指令	封装在此指令中，并通过 NAC 转发给所有群组成员的更新指令
SCS 数字签名	SCS 对整个群组更新指令的数字签名

（2）NAC向所有群组成员转发移动台更新指令

当NAC收到此指令后，首先检查收到的指令是否为重复/过期的指令，然后读取群组标识和更新资源地址并验证SCS的数字签名。接着，查找该群组所有成员的地址，将封装在群组更新指令中的移动台更新指令转发给所有群组成员。另外，作为一种紧急事件的处理方案，在执行大范围更新流程中，本文档建议NAC在执行第一个群组更新指令时更改用户策略为禁止除此群组成员以外的所有移动台访问指定的更新资源地址，直到收到SCS后续的控制更新指令。移动台更新指令中需包含信息项目信息见表8。

表8　移动台更新指令

项　目	说　明
SCS ID	SCS 的标识
指令序列号	唯一标识一个指令
指令有效期	超出此有效期后，SCA 不再控制移动台更新
指令类型	群组更新
群组标识	标识启动更新流程的群组
更新对象	指示需要更新的安全应用软件/操作平台/SCA
更新的类型	软件补丁、版本升级、数据库更新（如病毒定义）等
更新的名称/代码	用于唯一标识此更新
更新资源地址	获取此次安全更新的更新资源地址
SCS 数字签名	SCS 对此移动台更新指令的数字签名

（3）SCA控制移动台执行安全更新

当SCA接收到由NAC转发的移动台更新指令后，首先验证是否是重复/过期的指令，如果验证通过，则SCA解析更新项目信息并验证SCS的数字签名。如果数字签名验证通过，则开始执行此指令。SCA需首先检查此更新是否已在移动台上安装，如果更新已被安装，SCA应立刻向SCS发送SCI报告，告知SCS这一情况。如未安装，则SCA控制移动台立刻启动更新流程，访问更新资源地址，下载并安装指定的更新。安装完成后，移动台上的安全状态已发生变化，SCA应立即以安全事件报告的形式向SCS发送SCI报告，告知SCS这一情况。

（4）启动下一个群组的更新流程

基于收到的SCI报告，SCS可以监控群组成员完成该更新的情况。如果完成此次更新的在线移动台成员数目超过网络运营商预先设定的阀值时，SCS指示NAC执行下一个群组的群组更新，回到第一步。

需要说明的是,在执行大范围安全更新的过程中，如果有新的移动台上线，SCS服务器不应直接在SCI Response中将更新指令发给此移动台的SCA或者将此移动台加入正在执行更新服务的群组，而应依据此移动台的评估服务等级，顺延加入等待更新服务的群组中；另外，如果当最后一个群组的安全更新已执行但未结束时，如果有超过一定数量的移动台上线，则可以将这些新上线的移动台加入一个新增的群组，等待执行下一群组的更新流程。

这里需要说明的是，作为一种紧急事件处理方案，当更新服务群组的所有成员完成强制安全更新后,SCS需要向NAC发送控制策略更新指令，禁止该群组的所有成员继续访问安全更新服务器，以保障后续更新服务的可用性。

10.1.4 更新完成

当SCS基于接收到的SCI报告，获知更新服务群组的所有成员完成更新后，大范围安全更新流程结束。对于后续上线的移动台，其更新流程按9.5节所述流程处理。

11 漫游的处理

11.1 概述

CRS的漫游是指移动台离开对其执行控制的NAC的覆盖范围。

11.2 在部署了 CRS 的无线数据网内漫游

移动台在部署了CRS的无线数据网络中两个NAC/ASC间切换的流程主要为了SCS服务器能够适时地同负责对移动台进行控制的新的NAC/ASC——New-NAC/ASC进行通信，下发控制策略，并让SCS能够通知Old-NAC/ASC，释放对MS的控制策略和资源。

移动台在NAC/ASC（比如无线核心网的SGSN）之间切换时，要在MS、HLR、New-NAC/ASC、Old-NAC/ASC等设备之间进行GPRS路由域更新流程。移动台在部署了CRS的无线数据网络中两个NAC/ASC间切换时，涉及CRS的流程发生在GPRS路由域更新流程中New-NAC/ASC收到Update PDP Context Response消息以后，移动台在部署了CRS的无线数据网络中两个NAC/ASC间切换的流程如图12所示。

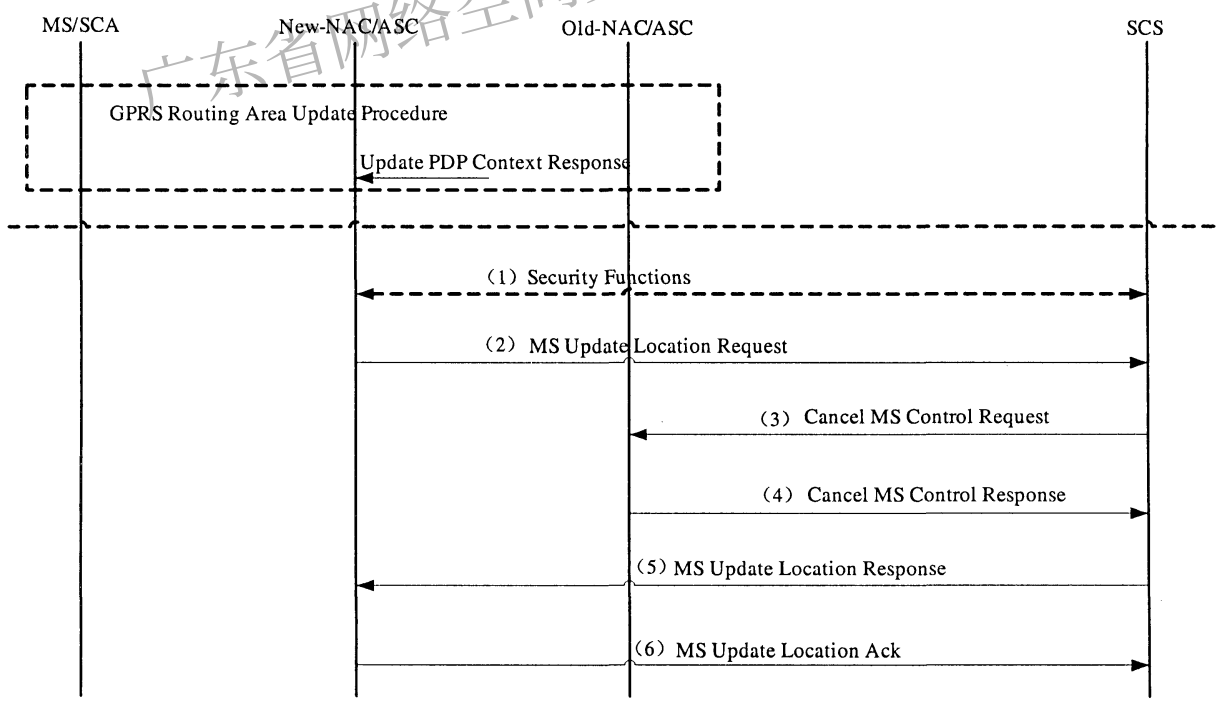


图13 移动台在部署了CRS的无线数据网络内漫游

（1）此步骤为可选，用于New-NAC/ASC与SCS服务器之间进行安全相关的交互，互认证、协商建立安全的消息传输通道。

（2）New-NAC/ASC向SCS服务器发送MS Update Location Request消息，向SCS服务器报告移动台新

的位置，并请求对移动台的控制策略，MS Update Location Request消息中包含移动用户身份标识（比如IMSI）、移动终端标识（比如IMEI）、移动台PDP上下文等信息。

（3）SCS服务器根据New-NAC/ASC发来的MS Update Location Request消息中的移动用户身份标识信息，可以获知移动台是从哪个NAC/ASC切换到目前的NAC/ASC来的，即SCS服务器可以获知移动台的Old-NAC/ASC。SCS服务器于是向Old-NAC/ASC发送Cancel MS Control Request消息，通知Old-NAC/ASC移动台已经切换到其他的NAC/ASC控制范围内，释放CRS系统在Old-NAC/ASC上申请的用于控制移动台的资源。Cancel MS Control Request消息中包含移动用户身份标识（比如IMSI）、移动终端设备标识（比如IMEI）、移动台PDP上下文等信息。

（4）Old-NAC/ASC收到SCS服务器发来的Cancel MS Control Request消息后，释放CRS系统为控制移动台而在Old-NAC/ASC上申请的资源，并向SCS服务器反馈Cancel MS Control Response消息，向SCS服务器确认处理完毕。

（5）SCS服务器向New-NAC/ASC发送MS Update Location Response消息，下发移动台的控制策略。

（6）New-NAC/ASC向SCS服务器反馈移动台控制策略的执行情况。

在上述过程中，安全代理SCA与安全服务器SCS之间的通信连接可以保持不变。

11.3 在两个部署了 CRS 的无线数据网间漫游

当移动台从部署了CRS的无线数据网漫游到一个新的数据网络，移动台安全代理SCA得到拜访网络SCS服务器地址并与之通信。拜访网络SCS服务器可以得到移动台用户信息和移动台SCI报告并评估其安全等级，但拜访网络SCS服务器没有移动台用户的控制策略和定制服务信息，这就要求拜访网络SCS服务器向移动台用户的归属网络SCS服务器请求相关的信息。

移动台在两个部署CRS的移动网络之间漫游时，要在MS、HLR、VLR、归属网络H-NAC/ASC、拜访网络V-NAC/ASC等设备之间进行GPRS路由域更新流程。移动台在部署了CRS的归属无线数据网络H-NAC/ASC和拜访无线数据网V-NAC/ASC之间切换时，涉及CRS的流程发生在GPRS路由域更新流程中V-NAC/ASC收到Update PDP Context Response消息以后，移动台在两个部署了CRS的无线数据网络之间漫游的流程如图14所示。

（1）此步骤为可选，用于V-NAC/ASC与V-SCS服务器之间进行安全相关的交互，互认证、协商建立安全的消息传输通道。

（2）V-NAC/ASC向V-SCS服务器发送MS Update Location Request消息，向V-SCS服务器报告移动台新的位置，并请求对移动台的控制策略，MS Update Location Request消息中包含移动用户身份标识（比如IMSI）、移动终端标识（比如IMEI）、移动台PDP上下文等信息。

（3）此步骤为可选，用于V-SCS与H-SCS服务器之间进行安全相关的交互，互认证、协商建立安全的消息传输通道。

（4）V-SCS向H-SCS发送Subscriber Data Request消息，向H-SCS请求移动用户的定制CRS服务情况、移动台近期的安全评估等级等信息，Subscriber Data Request消息中包含移动用户身份标识（比如IMSI）、移动终端设备标识（比如IMEI）等信息。

（5）H-SCS根据V-SCS发来的Subscriber Data Request消息中的移动用户身份标识信息，可以获知移动台是从哪个H-NAC/ASC切换到V-NAC/ASC的，即SCS服务器可以获知移动台的H-NAC/ASC。SCS服务器于是向H-NAC/ASC发送Cancel MS Control Request消息，通知H-NAC/ASC移动台已经切换到其他的

NAC/ASC控制范围内，释放CRS系统在H-NAC/ASC上申请的用于控制移动台的资源。Cancel MS Control Request消息中包含移动用户身份标识（比如IMSI）、移动终端标识（比如IMEI）、移动台PDP上下文等信息。

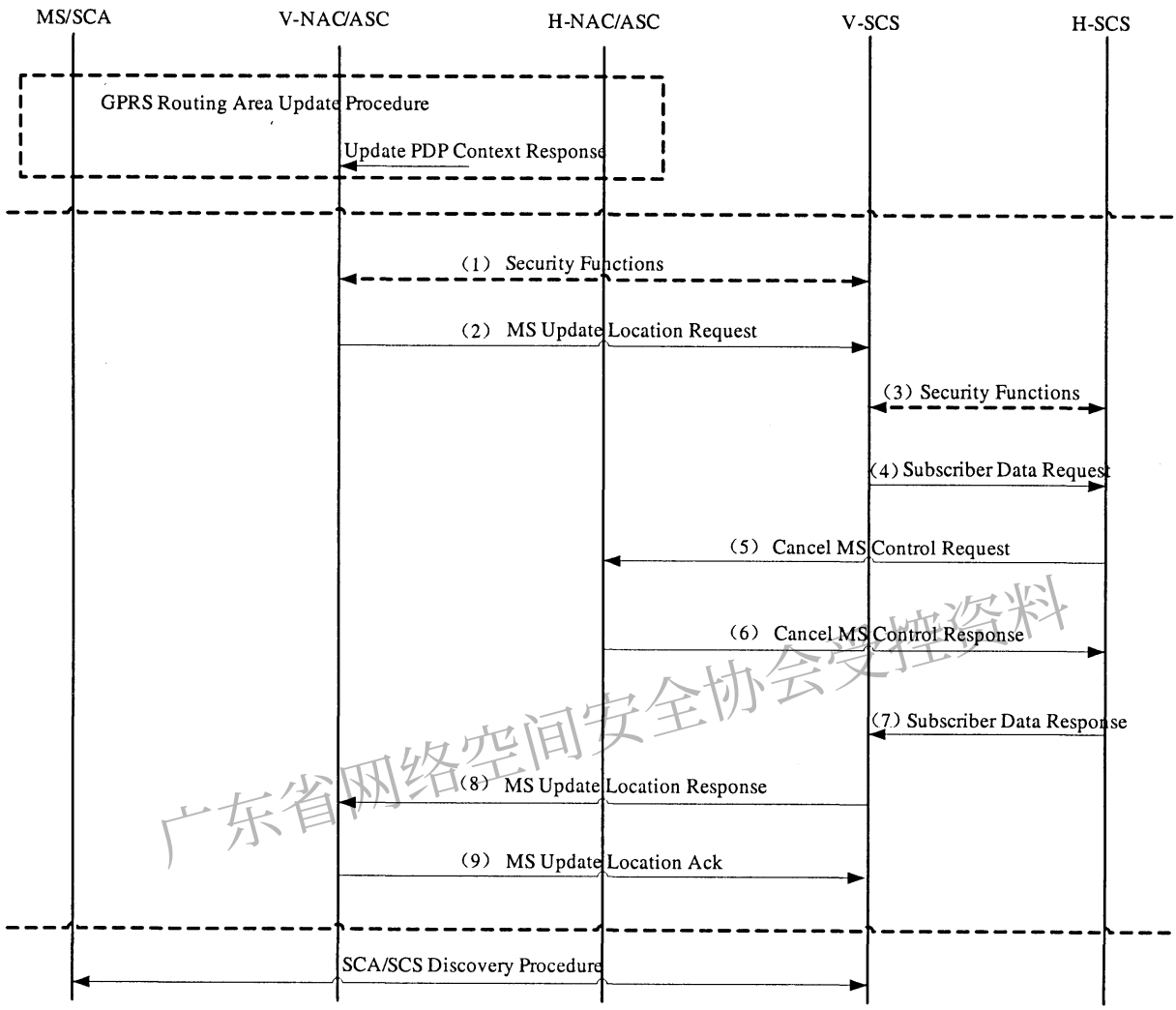


图14 移动台在部署了CRS的两个无线数据网络间漫游

（6）H-NAC/ASC收到H-SCS服务器发来的Cancel MS Control Request消息后，释放CRS系统为控制移动台而在H-NAC/ASC上申请的资源，并向H-SCS服务器反馈Cancel MS Control Response消息，向H-SCS服务器确认处理完毕。

（7）H-SCS向V-SCS发送Subscriber Data Response消息，向V-SCS反馈移动用户的定制CRS服务情况、移动台近期的安全评估等级等信息，Subscriber Data Response消息中包含移动用户身份标识（比如IMSI）、移动终端设备标识（比如IMEI）等信息。

（8）V-SCS服务器分析Subscriber Data Response消息消息的内容后，向V-NAC/ASC发送MS Update Location Response消息，下发移动台的控制策略。

（9）V-NAC/ASC向V-SCS服务器反馈移动台控制策略的执行情况。

在上述过程中，安全代理SCA切换到与拜访网络的安全服务器V-SCS进行通信。其后，安全代理SCA与拜访网络的安全服务器V-SCS之间就可以开始SCA/SCS的发现过程。

11.4 移动台在部署 CRS 和未部署 CRS 的无线数据网之间漫游

如果移动台的归属网络部署了CRS，而拜访网络没有部署CRS系统，当移动台从归属网络漫游到拜访网络时，移动台上的SCA有以下两种选择可以考虑。

（1）移动台的SCA和移动台用户归属网络SCS服务器通信，只向其归属网络SCS服务器请求移动台操作系统和安全相关应用的更新、升级服务。移动台在拜访网络的访问不受CRS系统的任何限制。

（2）由于拜访网络没有部署CRS系统，移动台的SCA进入休眠状态，等待激活事件。激活事件可以是移动台获得了一个SCS服务器的地址（通过DHCP协议或者在PDP上下文激活过程等方法获得）或者移动台SCA收到了某个SCS服务器发来的有效SCA探测请求报文等。

当移动台从一个没有部署CRS的无线数据网络，漫游到一个部署了CRS的无线数据网络时，部署了CRS的无线数据网络对移动台的控制方式可以是：

（1）如果移动台支持安装SCA，可以触发SCA自动安装流程，为移动台安装SCA，然后按照CRS的正常的流程处理移动台的SCI报告和无线数据访问。

（2）如果移动台不支持安装SCA，部署了CRS的无线数据网络按照运营商的策略管理移动台的无线数据访问，这些策略可以是：将移动台的数据流量重定向到专用安全设备进行过滤；限制移动台访问拜访网络提供的某些无线数据应用；禁止移动台访问无线数据网络等等。

12 对于实现的考虑

12.1 SCA 的部署

12.1.1 SCA 软件的安装和分发

大多数情况下，SCA的初次安装由SCA自动安装流程来完成，此外，还有其他的一些SCA安装方法。SCA的安装方法如下。

— SCA自动安装

移动台没有安装SCA，当MS访问部署了CRS的无线数据网时，SCA自动安装流程（参见9.3.1节）完成SCA的安装和初始化。

— SCA作为一个组件，嵌入到移动终端中

在移动终端出厂前，移动台或移动台操作系统生产商将最新版本的SCA嵌入到移动终端中，然后将移动台分发给最终的移动用户，即SCA是移动台的一个预装组件或SCA作为SAS的一个组件同SAS一起安装到移动台上。

— SCA作为一个组件，嵌入到用户的电信智能卡中

电信智能卡的生产商将最新版本的SCA嵌入到电信智能卡中分发给移动用户，即SCA是嵌入到用户的电信智能卡中的一个组件，SCA通过用户购买新卡或换卡的方式分发给移动用户。

12.1.2 SCA 软件的安装位置

SCA可以安装到以下几个位置。

— SCA安装到移动台存储介质中

SCA作为一个独立软件安装在移动台存储介质中。此种情况下，SCA安装程序应该限制SCA安装在移动台自身相对固定的存储介质中，不推荐安装到移动台外部存储介质、可拆卸存储介质上，以保证SCA的连续可靠工作，避免因为SCA程序所在存储介质的变化而导致SCA工作不正常，从而频繁触发SCA的自动安装过程。

— SCA嵌入到SAS中

SCA作为一个组件嵌入到SAS中。此种情况下，SCA与MSOS和其他SAS之间的通讯通过MSOS和SAS之间的应用程序接口实现，承载在应用程序接口之上的通讯内容符合Ica接口的要求。SCA和其所属的SAS之间的通讯属于软件内部信息交换。SCA嵌入到SAS中的情况如图15所示。

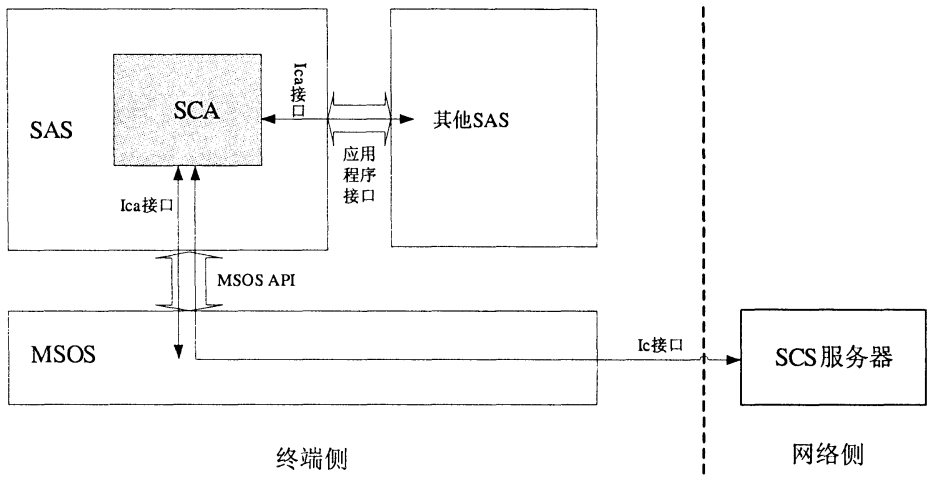


图15　SCA部署在SAS中

从图15可知，MSOS和SAS之间的接口是MSOS API或MSOS为上层应用开放的其他API。接口承载的消息内容为CRS中定义的Ica接口相关内容（参见5.5.3节），主要包括MSOS和SAS的安全相关信息。这样，MSOS API和应用程序接口就作为内容的承载通道在应用层面实现了Ica接口的功能。

— SCA嵌入到用户电信智能卡中

SCA作为一个可更新应用程序内嵌在电信智能卡中的情况如图16所示。

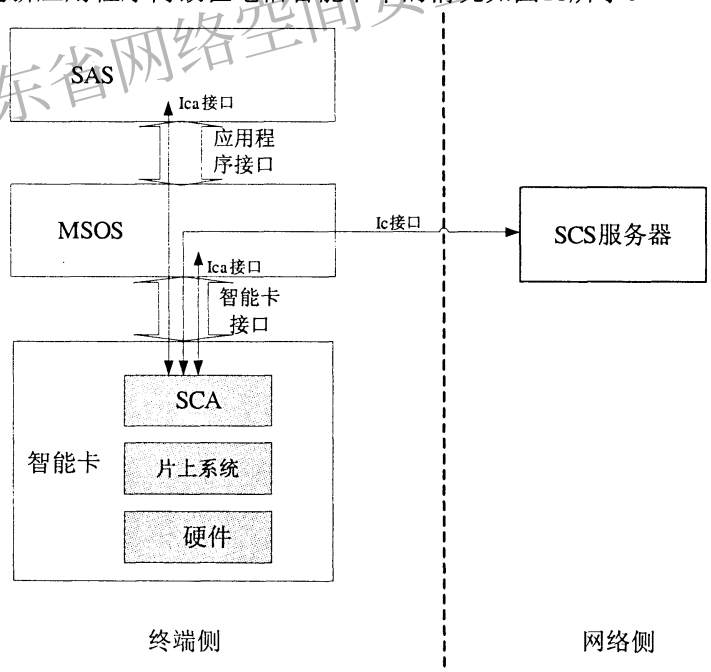


图16　SCA部署在电信智能卡中

从图16可知，MSOS与智能卡、SAS与MSOS之间的实际接口为智能卡接口和MSOS为上层应用开放的MSOS API。接口作为Ica消息的承载通道，承载的内容为CRS定义的Ica接口相关内容（参见5.5.3节）。通过ETSI TS 102.223标准定义的传输独立协议（Bearer Independent Protocol），可以实现智能卡与终端通过TCP/IP协议进行数据交换。

12.2 SCS 服务器的部署

SCS服务器与移动台、核心网的接入控制设备、核心网的网关设备、Internet/PDN上的服务器进行通信，SCS可以通过其协议栈中核心网的IP层直接与核心网的通信对端通信，也可以将通信内容封装到GTP隧道中，通过GTP隧道传输通信内容。

— SCS服务器与移动台、Internet/PDN上的服务器通信

SCS和移动台、Internet/PDN上的服务器进行通信的数据被封装成GTP报文在核心网内传输，在核心网边缘，GTP报文被解封装成普通IP报文在核心网外传输；IP报文被封装成GTP报文在核心网内传输。

— SCS服务器与接入控制设备、网关设备通信

SCS服务器与核心网的接入控制设备（例如CRS体系结构中的NAC）和网关设备通信，通信数据可以被封装成核心网IP层的载荷直接在核心网IP层之上传输，也可以被封装成GTP载荷，由核心网的GTP隧道传输。

在CRS（关联反应系统）中，SCS服务器的部署方式主要有两种：

— 在一个PLMN/核心网内，只部署一套SCS服务器，这套SCS服务器为接入每个PDN的MS提供服务。

— 为每个核心网/PLMN只部署一套SCS服务器时，PLMN系统的结构如图17所示，虚线表示SCS服务器为接入哪个PDN的MS服务。

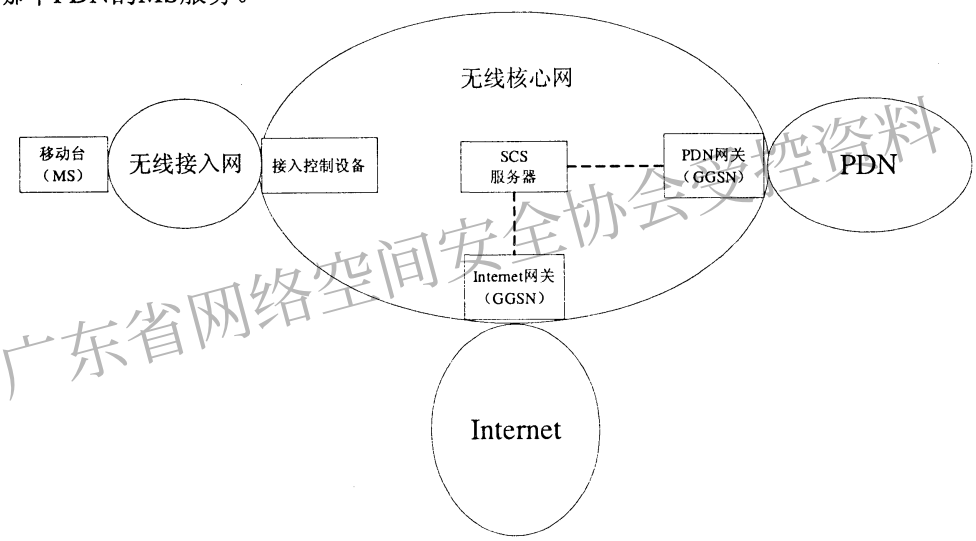
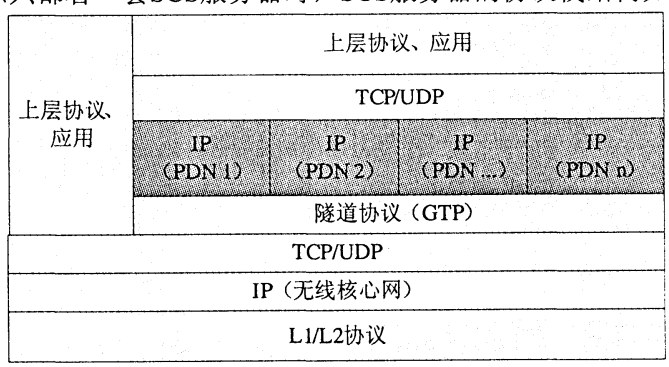


图17 每个核心网/PLMN只部署一套SCS服务器

为每个核心网/PLMN只部署一套SCS服务器时，SCS服务器的协议栈结构如图18所示。



SCS服务器协议栈

图18 每个核心网/PLMN部署一套SCS服务器时SCS服务器协议栈结构

SCS服务器拥有一个核心网内的静态IP地址——IP（核心网），这个IP地址在被SCS服务器用于在核心网内通讯。

在GTP协议层之上，与PLMN/核心网相连接的每一个PDN，SCS服务器都拥有一个相应PDN内的静态地址IP（IP PDN 1、IP PDN 2…… IP PDN n），用于同访问这个PDN的MS、同这个PDN中的其他网元进行通信。这类通信的报文被封装在GTP隧道中在核心网内传输，并被解封装成普通IP报文在核心网外传输。

— 在一个PLMN/核心网内，为每个与PLMN/核心网相连的PDN部署一套SCS服务器，每套SCS服务器为接入特定PDN的MS提供服务。

为每个与PLMN/核心网相连的PDN部署一套SCS服务器时，PLMN系统的结构如图19所示，虚线表示SCS服务器为接入哪个PDN的MS服务。

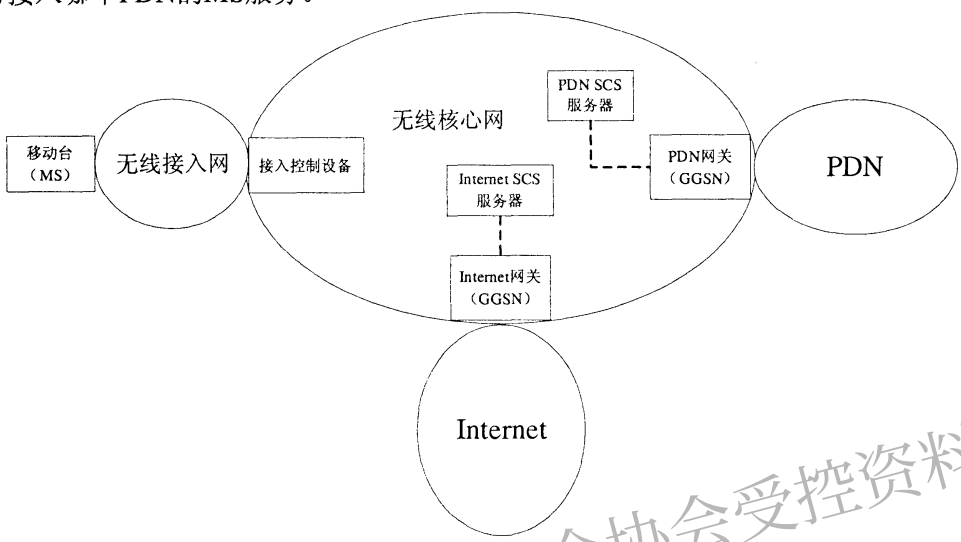
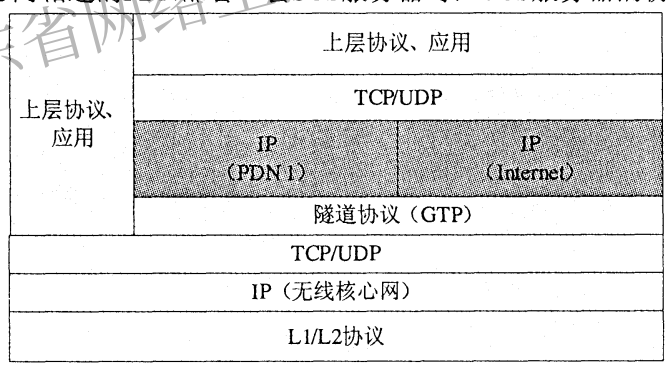
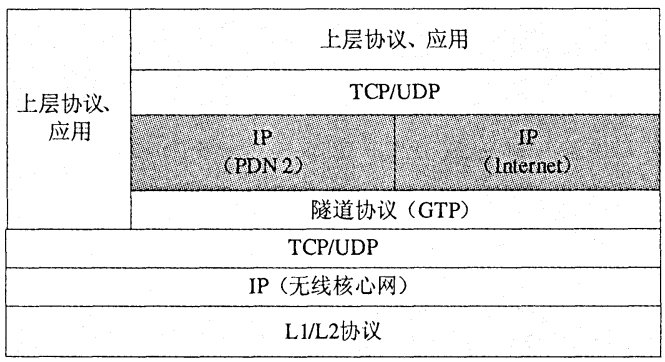


图19 每个PDN部署一套SCS服务器

为每个与PLMN/核心网相连的PDN部署一套SCS服务器时，SCS服务器的协议栈结构如图20所示。



PDN1 SCS服务器协议栈



PDN2 SCS服务器协议栈

图20 为PLMN/核心网连接的每个PDN部署一套SCS服务器时SCS服务器协议栈结构

当为PLMN/核心网连接的每个PDN部署一套SCS服务器时，每个SCS服务器在GTP层之上拥有一个静态IP地址（IP for PDN）和PDN相关。此IP地址被SCS服务器（为相应的PDN服务）用于同连接到相应PDN的移动台和相应PDN中的网元通信。SCS服务器在GTP层之上也可能拥有一个Internet静态IP地址，用于SCS服务器访问Internet资源。

上述的PDN指包交换数据网，所以PDN也包含Internet，为了便于理解，上述图中把Internet从PDN中单独列出来描述；一套SCS服务器指功能和协议栈结构相同的一个或者多个SCS服务器，一套SCS服务器至少包括一个处于正常工作状态的SCS服务器，并可能包含若干个处于备份状态的SCS服务器。

12.3 CRS 系统和移动 IP 的结合

如果CRS系统和移动IP共同部署，CRS的工作方式有以下两种考虑。

（1）由于移动IP主要解决的是移动节点在移动的过程中，应用不断开，IP地址可以不变化，移动节点可以被寻址的问题，移动节点感觉自己就像连接在原来的归属网络链路上一样。因此，移动台可以仍然使用归属网络环境的各种配置，包括SCS服务器和NAC，移动台的安全等级评估由其归属网络SCS服务器完成，对移动台用户的所有控制都由归属网络的NAC来执行。

（2）如果考虑到移动网络的使用效率，移动台可以使用拜访网络的转交地址和拜访网络的SCS服务器通信，移动台的安全等级评估由拜访网络SCS服务器完成，对移动台用户的所有控制都由拜访网络的NAC来执行。

参 考 文 献

〔1〕ITU-T X.800 国际电报电话咨询委员会应用的开放系统互联安全体系结构（1991）
〔2〕ITU-T X.805 提供端到端通信的系统的安全体系结构（2003）
〔3〕ITU-T X.1125 关联响应系统（2008）
〔4〕3GPP TS 23.060 V7.0.0 GPRS服务描述，阶段2（2006）
〔5〕3GPP TS 23.002 V7.1.0 3G网络结构（2006）
〔6〕3GPP TR 21.905 V7.0.0 3GPP规范词汇表（Vocabulary for 3GPP Specifications（2005））
〔7〕IETF RFC 2132 动态主机配置协议可选项和启动协议扩展
〔8〕IETF RFC 4261 基于传输层安全协议的通用开放策略服务

YD/T 2036-2009

*

人民邮电出版社出版发行

北京市崇文区夕照寺街14号A座

邮政编码：100061

北京新瑞铭印刷有限公司印刷

*

开本：880×1230　1/16　　2010年1月第1版

印张：2.75　　2010年1月北京第1次印刷

字数：82千字

ISBN 978-7-115-1975/10-37

定价：25元