第33卷 第20期 计 算 机 工 程 2007年10月
Vol.33 No.20 Computer Engineering October 2007
·安全技术· 文章编号：1000—3428(2007)20—0153—03 文献标识码：A 中图分类号：TP393

3GPP框架下的UMTS核心网安全体系研究

闻英友[1,2]，陈书义[1]，赵大哲[1,2]，赵 宏[1,2]
(1. 东北大学信息科学与工程学院，沈阳 110004；2. 东软集团研究院，沈阳 110187)

摘 要：3GPP UMTS网络是第3代移动通信系统的重要组网技术之一。UMTS核心网安全问题还没有受到充分的重视，缺乏完整的安全体系。为此，在3G网络安全分析的基础上，重点关注3G核心网面临的新的安全威胁和防护需求，建立了适用于3GPP UMTS网络的核心网络安全体系，划分了安全平面和安全层次，明确了核心网络安全目标，建立了未来研究的基础框架。
关键词：3GPP UMTS；安全体系；核心网；信令

Security Architecture of 3GPP UMTS Core Network

WEN Ying-you[1,2], CHEN Shu-yi[1], ZHAO Da-zhe[1,2], ZHAO Hong[1,2]
(1. School of Information Science and Engineering, Northeastern University, Shenyang 110004; 2. Neusoft Group Research, Shenyang 110187)

【Abstract】UMTS is one of the most important networking technologies of the third generation mobile communication system. Security in UMTS core network is lack of attention, and no integral security architecture is defined. To solve this problem, security of the third generation communication system is analyzed, and security architecture applied to 3GPP UMTS core network is proposed. This architecture provides a basis to security study of 3G core network in future.
【Key words】3GPP UMTS; security architecture; core network; signaling

3G网络的安全问题既不同于传统的蜂窝无线通信网络(如GSM)，也不同于传统的IP网络[1]。随着3G网络中IP技术的引入，一方面，整个网络提供了更多的对外接口，网络具有了充分的开放性，原有体系的不安全因素完全暴露并成为重要的安全威胁。另一方面，IP网络固有的一些安全威胁和漏洞同样会被引入到3G网络特别是3G核心网中。

针对3G核心网络中存在的安全问题，国内外众多学者已经开展了相关方面的探索。文献[2]讨论了3GPP UMTS网络的基础设施安全。文献[3]对UMTS网络安全问题进行了较全面的综述，阐述了基于MAPSec的7号信令移动应用部分(MAP)安全防护，基于IPSec的IMS系统SIP安全保障以及基于WTLS的应用数据保护，但没有提及UMTS核心网的安全体系及安全域划分。文献[4]重点讨论了基于IP的核心网络DoS攻击问题以及隐私暴露问题，但没有对整个网络底层协议安全性支持作系统分析。文献[5]讨论了基于IP的信令协议会话归属安全性问题。从国内的研究进展来看，目前针对3GPP UMTS网络安全问题的研究还主要集中在接入网安全方面，对于核心网环境下的安全问题，还没有系统的研究。上述国内外研究现状分析表明，对于3GPP UMTS核心网络的安全问题目前没有形成完整的安全体系，因此，对于核心网安全问题的研究也缺乏明确的定义。本文针对3GPP UMTS核心网所面临的安全威胁，提出了一种多维的UMTS核心网安全体系，以期为3GPP UMTS核心网安全问题的深入研究提供一个基础框架。

1 3GPP框架下的UMTS网络结构

3GPP UMTS网络从结构上分为无线接入网(RAN)和核心网(CN)[6]，其中核心网包括电路域(CS)和分组域(PS)两个部分。国际标准化组织3GPP针对WCDMA网络制定了R99、R4、R5以及R6等不同发展阶段的相应规范，以利于3G网络的平滑过渡和演进，其最终目标无疑是3G网络接入和业务承载的全面IP分组化。其中，3GPP UMTS R5结构如图1所示。

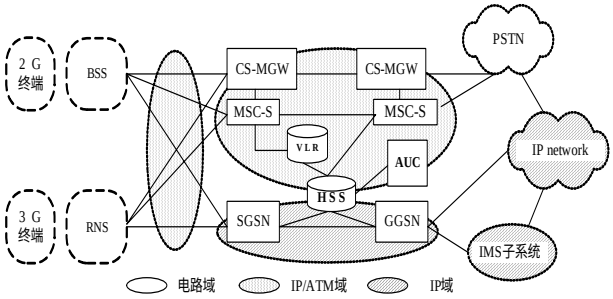

图1 3GPP UMTS R5结构

R99[7]网络通过引入分组域实现了原有2G网络的平滑过渡，R4[8]网络引入了NGN软交换概念，建议实现核心网的完全分组化。

R5[6,9]版本在接入网中引入全IP接入网(IP UTRAN)和高速下行分组接入(HSDPA)，在核心网引入了IP多媒体子系统(IMS)。IMS的引入大大提升了3G网络的业务应用提供能力。

2 UMTS安全问题及安全体系

2.1 无线接入网安全

无线通信系统中，应用数据是通过开放的无线信道进行传输，因而很容易受到攻击。3G网络的无线信道接入也存在

基金项目：国家“863”计划基金资助项目(2003AA712032)；国家博士后科研基金资助项目
作者简介：闻英友(1974－)，男，博士后，研究方向：网络安全，移动通信技术；陈书义，博士研究生；赵大哲，教授；赵 宏，教授、博士生导师
收稿日期：2006-10-29 **E-mail：**wenyy@neusoft.com

着同样的威胁。3G 系统提供了相对于 GSM 更强的安全接入控制。然而移动无线检测设备能力的增强给恶意攻击者创造了条件。IP 技术的应用也使得恶意节点易于伪装成核心网节点从而利用欺骗等手段获取终端的信息进而非授权入网。另一方面，传统 IP 网络的一些攻击模式(如拒绝服务攻击)给接入网的安全带来了新的挑战。终端自身的安全问题也会对接入网甚至核心网造成巨大的威胁。由于移动终端的功能越来越依赖于软件技术，虽然这在一定程度上提高了终端功能的灵活性，但是也使得恶意者可以利用伪“移动代码”或“病毒”攻击终端软件。同时终端上 IP 能力的提高，使恶意用户可以利用相应手段形成对系统资源的恶意占用进而使系统瘫痪，甚至通过某种蠕虫的形式实现 DDoS 攻击。

2.2 核心网安全

随着业务应用的发展，核心网安全逐渐受到广泛的关注。3G 核心网面向全 IP 网过渡，因而它必然要面对 IP 网所固有的一系列问题。核心网安全问题分析将在后续进行深入讨论。

针对第 3 代移动通信网络的安全，相关国际标准化组织进行了安全体系方面的研究，发布了相关的规范。3GPP在WCDMA网络规范TS33.102[10]中对 3G网络整体安全体系进行了描述，如图 2 所示。

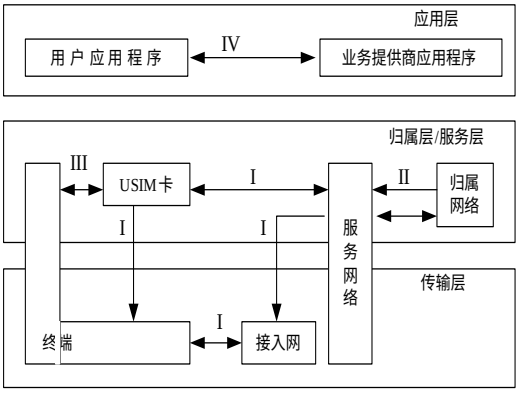

图 2　3GPP UMTS 网络安全体系结构

安全体系从 5 个方面描述了 3GPP UMTS 网络面临的安全问题及研究领域。网络接入安全(Ⅰ)定义了用户的网络接入安全，特别强调无线链路的攻击；网络域安全(Ⅱ)定义了核心网设备节点信令交换的安全需求，防止来源于外部 IP 网络的攻击及安全威胁；用户域安全(Ⅲ)定义了用户与移动终端设备间的安全特性；应用程序域安全(Ⅳ)定义了用户应用与业务服务之间数据交换的安全；安全的可见度与可配置性(Ⅴ)定义了用户如何对安全选择自行配置。

3　GPP UMTS 核心网安全威胁分析

网络安全体系的建立必须针对网络的业务特点和安全威胁。3GPP UMTS 核心网特别是核心网分组域具有丰富的对外接口，因此受到的安全威胁也更大。

采用IP技术的 3G核心网络中，流量类型复杂多样，既包括信令数据，又包括IP语音和业务数据。一些最初在电信网络中使用的信令(如SS7)在设计之初并没有着手安全方面的考虑，本身具有很多安全缺陷。尽管随着IPv6 协议的引入以及IPSec机制的采用，信令协议的安全传输可以在一定程度上加强，但对于未来网络及应用发展的需要，这种安全保障是极其有限的。SIP[11]协议作为IETF提出的在NGN架构中最重要的IP信令协议也被 3GPP明确引入到IMS子系统。目前已经出现了大量基于SIP协议的IMS业务应用和产品，如PoC等。然而，SIP协议本身基于文本的特点决定了其较差的安全性。在最初的VOIP应用中，很多安全漏洞被暴露出来。SIP协议安全漏洞和威胁主要分为两类：消息类攻击，如利用"BYE", "CANCEL", "REFER", "RE-INVITE", "INFO", "UPDATE", "DNS"等SIP协议消息发动的攻击。另一类是协议解析类攻击。目前国外已经开展了一些关于SIP的安全性分析及研究，但对于 3G网络环境中SIP的应用安全性分析还远未达到让人满意的程度。

实际上核心网络的安全所涉及的不仅仅是信令协议，也包括重要的IP承载协议。例如，在WCDMA R99/R4 版本 3G 核心网分组域中的Gn,Gp和Gc接口上采用了GPRS隧道协议(GTP)[12]作为分组数据的关键传输协议，实际是连接接入网和外部IP网络的通道，涉及到网络的计费和漫游等很多方面。但GTP协议本身几乎没有任何安全考虑，存在着大量的安全漏洞和安全威胁，可以被利用作为对整个网络进行攻击的手段，包括最简单的“过度计费”到“节点攻击”。GTP协议的安全问题可以分为以下几大类：

(1)协议异常。协议异常攻击包括异常或破坏的 PDU 数据包，也包括不符合协议设计规范的 PDU。属于这种类型的安全威胁包括“保留字段问题”、“GTPoverGTP 攻击”、“GTP 包封装非标准协议逃避检测”以及“错误长度问题”等。这些安全威胁有可能导致 DoS 攻击和其他远程攻击。包括利用程序实现上的缺陷远程入侵，及逃避相关的安全匹配和过滤。

(2)基础设备攻击(GTP 欺骗)。包括非法访问受限设备，如 SGSN、GGSN 节点，网络管理系统以及移动终端。例如，通过修改自己的源或目的地址，实现与内网连接，终端可以将攻击包封装进入 GTP 协议，经过 GGSN 路由进而攻击任何移动网络内的其他终端以及网络外部的目标。

(3)资源占用攻击。这类攻击可以从移动终端发起，也可以从外部网络发起。例如，基于特定的实现，终端可以发起类似于 SYN 的攻击，造成 GGSN 不能分配新的 PDP 上下文(分组数据协议上下文)，从而造成拒绝服务攻击。SGSN 在移动性切换和路由的过程中也需要相互之间进行类似于 TCP 的 3 次握手协议，在握手完成后，新的 SGSN 开始代替旧的 SGSN 转发用户数据。如果存在恶意或被俘获的 SGSN，就有可能不完成握手过程，从而造成 SGSN 的服务资源耗尽。

3G 核心网络涉及的重要信令和传输协议还有很多，如 SS7 中的 MAP 以及软交换结构中的 H.248、RTP 等。必须针对 3G 核心网络的结构以及业务应用特点，建立起完善的 3G 核心网安全体系结构，以便清晰描述 3G 核心网络所面临的安全威胁及必须实现的安全目标。

4　3GPP UMTS 核心网安全体系

在 3GPP 制定的相关规范中，TS33.102 对于 3G 网络总体的安全体系做出了定义。虽然此安全体系从总体上描述了 3G 网络的安全框架，但对于各部分的具体安全功能和需求描述并没有给出相应的阐述，特别是对于安全体系中第 2 部分的核心网络安全并没有给出更详细的描述和扩展。实际上 3G 核心网络的安全相对于接入网络的安全来说更具复杂性，因此也更需要一个完善的安全体系来对其可能受到的安全威胁以及安全问题的研究领域给予清晰描述。

3GPP UMTS网络核心网中采用了基于IP的承载技术和服务接入手段，因此网络具有了与以往移动通信网络不同的特点，以WCDMA网络为例，其R4 及R5 版本中，MSC和GMSC节点采用了软交换技术，并且引入了面向NGN的IP多媒体子

系统，因此核心网组网结构趋于扁平化。其服务提供以及连接控制也更具有P2P网络的特点。因此，考虑在UMTS核心网安全体系的定义中必须参考现有的相关标准。ITU-T X.805[12]是ITU-T针对P2P网络建立的一个安全体系标准。基于其描述的主要结构，结合 3G网络的组网和服务提供特点，对UMTS核心网安全体系定义如图 3 所示。

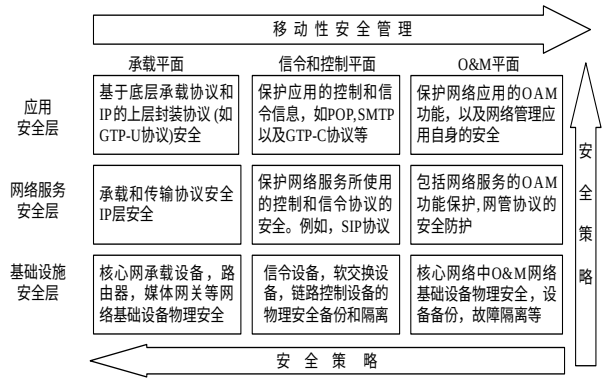

图 3　3GPP UMTS 核心网安全体系框架

整个UMTS核心网安全体系定义为3个层次和3个平面，并引入了多维的安全策略和移动性管理。

承载平面的内容包括 UMTS 核心网中的承载设备，交换和路由设备，媒体网关等关键节点以及节点间的通信连接。承载平面负责 UMTS 核心网络中业务分组数据的传递和转发，也完成传统电路信号到分组数据的拆装功能，因此是必须考虑的安全防范目标。针对核心网承载平面，具体划分为 3 个层面的防护。基础设施安全层针对承载设备的物理安全进行防护；网络服务安全层是核心网中需要重点考虑的安全目标，主要针对 IP 层。包括对于所有传统 IP 网络的安全威胁和攻击手段的防范；应用安全层主要确保基于 IP 的上层封装协议数据和应用数据安全，如 GPRS 隧道用户面协议(GTP-U)以及业务提供商的应用服务数据等。

信令和控制平面的内容包括网络中的信令点设备、软交换控制设备、信令转换网关以及这些设备节点间的信令和控制连接。信令和控制平面是 3G 网络中最为关键和重要的逻辑子系统，也是 UMTS 核心网安全的关键。同样对于信令和控制平面也分为 3 个层次。基础设施安全层确保物理设备节点的安全备份和故障隔离。网络服务安全层确保 3G 网络服务本身所使用的控制和信令协议数据以及通信连接的安全，如 SIP 用来建立和维护 IMS 子系统的多媒体通信连接以及软交换设备间的信息传递以维护网络通信的正常进行，它是需要在这个层次上重点保护的目标。信令和控制平面的应用安全层主要保护具体应用的控制和信令信息，这种具体应用既包括业务应用的控制信息，也包括承载应用的控制和信令服务。例如 POP 和 SMTP 协议从 3G 网络服务的角度看属于具体业务应用的控制协议。而 GTP-C 协议用于承载面 GTP-U 连接的建立控制协议，因此是在这一层次上需要重点关注的防范对象。

O&M 系统是电信运营网络中至关重要的维护平台。由于 IP 技术的大量应用，O&M 系统与核心网承载和控制系统具有了更多通信手段和交互的可能，因此其所具有的安全漏洞及面临的安全威胁将对整个 UMTS 核心网的安全带来重要的影响，是核心网安全体系中不能忽视的安全目标。实际上，在3G 核心网络中 O&M 平面的安全内容与传统电信网络安全没有更多区别，重点在于管理协议及管理应用，分别体现在本文提出的安全体系 O&M 平面服务安全层和应用安全层。其最终目标是实现“ 安全的网络管理 ”和“ 网络管理的安全 ”。

5　结论

3G UMTS 核心网络中既有承载网络，又有信令控制网络以及 O&M 网络，安全问题也更加复杂，需要对安全目标及安全研究的基础框架做出明确的定义。为此，在 3GPP UMTS 网络安全问题分析的基础上，针对 3G 核心网面临的新的安全威胁和防护需求，建立了适用于 UMTS 网络的核心网络安全体系，提供了安全问题研究基础框架。下一步工作，将基于安全体系的定义，开展系统的核心网关键信令协议安全性分析及安全防护技术研究。

参考文献

1 3GPP TS 21.133 V4.1.0-2002 Security Threats and Requirements[S/OL]. (2002-01-07). http://www.3gpp.org.

2 Prasad A, Wang H, Schoo P. Infrastructure Security for Future Mobile Communications System[C]//Proc. of WPMC’03, Yokosuka, Japan. 2003: 19-22.

3 Boman K, Horn G, Howard P, et al. UMTS Security[J]. Electronics & Communication Engineering Journal, 2002, 14(5).

4 Schäfer G. Research Challenges in Security for Next Generation Mobile Networks[C]//Proc. of Workshop on Pioneering Advanced Mobile Privacy and Security, Egham, Surrey, United Kingdom. 2002.

5 Fu Xiaoming, Tschofenig H. Security Implications of the Session Identifier[R]. Institute for Informatics, University of Goettingen, Germany, Technical Report: TB-IFI-2005-08, 2005-11.

6 3GPP TS 23.101 v5.0.1-2004 General UMTS Architecture[S/OL]. (2004-01-07). http://www.3gpp.org.

7 3GPP TS 23.101 v3.0.1-1999 General UMTS Architecture[S/OL]. (1999-06-23). http://www.3gpp.org.

8 3GPP TS 23.101 v4.0.0-2001 General UMTS Architecture[S/OL]. (2001-04-11). http://www.3gpp.org.

9 3GPP TS 23.228 v5.13.0-2005 IP Multimedia Subsystem[S/OL]. (2005-01-06). http://www.3gpp.org.

10 3GPP TS 33.102 v5.7.0-2005 Security Architecture[S/OL]. (2005-12-19). http://www.3gpp.org.

11 SIP: Session Initiation Protocol[S/OL]. (2002-07). RFC 3261, http://www.IETF.org.

12 ITU-T Recommendation X.805-2003 Security Architecture for Systems Providing End-to-End Communications[S/OL]. (2003-09-25). http://www.itu.int/itudoc/itu-t/aap/sg17aap/history/x805/.