NSIS框架下UMTS核心网动态防御系统研究

陈书义[1] 孙锦山[1] 闻英友[1,2] 赵 宏[1,2]
(东北大学计算机软件国家工程研究中心 沈阳 110004)[1] (东软集团研究院 沈阳 110179)[2]

摘 要 基于NSIS(Next Steps in Signaling)技术设计并实现了安全设备控制信令协议,提出了NSIS框架下的UMTS核心网动态防御系统。系统基于多源安全信息的融合和聚类分析,实时发现攻击,并依照安全策略,利用NSIS安全设备控制协议动态阻止针对核心网的攻击。NSIS信令技术的引入,保障了安全设备联动消息传输的安全性、可靠性,解决了目前动态防御系统联动协议存在的问题。基于UMTS核心网试验平台,测试验证了NSIS动态防御系统的可行性。

关键词 UMTS,核心网,安全信息融合,NSIS,实时响应
中图法分类号 TP309 **文献标识码** A

Research on NSIS-based Dynamic Defensive System in UMTS Core Network

CHEN Shu-yi[1] SUN Jin-shan[1] WEN Ying-you[1,2] ZHAO Hong[1,2]
(The Software Center of Northeastern University, Shenyang 110004, China)[1] (Neusoft Research, Shenyang 110179, China)[2]

Abstract The control signaling protocol of secure equipments was designed and implemented based on the NSIS (Next Steps in Signaling) technology, and a NSIS based dynamic defensive system in UMTS core network was proposed. Defensive system was based on multi-source information integration and cluster analysis. The attacks against core network were detected and prevented real time with NSIS control signaling protocol according to security policies. The security linkage information was safely and reliably transmitted, and problems of existed linkage protocols were resolved based on the introduction of NSIS signaling mechanism. The feasibility of NSIS dynamic defensive system was tested and verified based on UMTS core network test platform.

Keywords UMTS, Core network, Security information fusion, Next steps in signalling, Real-time response

1 引言

随着网络融合的发展,UMTS网络的安全问题亟待解决。一方面,融合使得UMTS网络具有了充分的开放性,UMTS体系原有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网络固有的安全威胁和漏洞也被引入到UMTS网络,特别是UMTS核心网中。

目前UMTS网络安全的研究主要集中在接入网领域[1,2],针对核心网安全问题的研究还处在起步阶段。A. Prasad等[3]讨论了3GPP UMTS网络的基础设施安全。K. Boman等[4]对UMTS网络安全问题进行了较全面的综述,但没有提及UMTS核心网的安全体系及安全域划分。ünter Schäfer等人[5]在文献中重点讨论了基于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做系统分析。总之,国内外针对3GPP UMTS核心网安全问题的研究成果还不能满足UMTS核心网络防御的需求。

UMTS核心网安全涉及G_n,G_p,G_i和计费接口等多个安全域,用户面、控制面和管理面多个层面。因此UMTS核心网安全防护需要不同安全域、不同层面的设备协同工作,构建不同设备联动的动态防御系统。传统IP网络的动态防御技术的研究已经取得了一定的成果。Check Point和天融信等公司推出了OPSEC (Open Platform for Security),TOPSEC (Talent Open Platform for Security)等技术,但是由厂商提出的设备间联动协议很难得到广泛的认可,缺乏通用性;也有人提出基于SNMP等方式的网络安全联动方案,但这些方案过于复杂、效率不高[6]。UMTS核心网动态安全防御问题的关键是需要一个安全、高效的设备联动协议。

下一代信令NSIS (Next Steps in Signalling)机制安全、可靠、灵活的特点非常适用于融合网络的设备控制,这种基于IP的信令协议框架必然对UMTS网络的发展带来深远的影响。国外研究机构已经提出了基于NSIS的QoS和NAT/FW控制信令应用[7,8],但是远远不能满足UMTS网络的安全需求。本文将基于NSIS设计网络安全设备控制信令协议,并研究和实现UMTS核心网动态防御系统。

到稿日期:2008-04-16 本文受国家自然科学基金(60602061),国家高技术研究发展计划(2006AA01Z413)资助。
陈书义 博士研究生,主要研究方向为网络与信息安全,下一代网络,E-mail:chen-sy@neusoft.com;**孙锦山** 博士研究生,主要研究方向为网络与信息安全、下一代网络;**闻英友** 博士,主要研究方向为网络与信息安全、下一代网络;**赵 宏** 教授,博士生导师,主要研究方向为网络与信息安全、网络管理。

2 NSIS 框架下的 UMTS 核心网络动态防御系统

2.1 NSIS 信令技术

为了满足下一代网络中信令应用的需要，IETF 成立了 NSIS 工作组，致力于新一代信令技术的研究[9,10]。NSIS 的主要思想是将信令协议分成两层，即 NSIS 传输层(NTLP)和 NSIS 信令层(NSLP)[11]。1)NTLP 独立于上层特定的信令应用，运行在标准的传输和控制协议之上，为上层应用信令提供安全、可靠、灵活的信令传输平台和通用的接口。NTLP 只维护自己的内部状态和下层传输及安全相关协议的管理，提供基于连接的传输模式(如 TCP)和非连接的传输模式(如 UDP) 两种信令传输模式。可以根据需要选择传输层协议，对于较长的、不能丢包或者对安全性要求较高的信令消息，采用基于连接的传输模式；对于长度较短、不常出现并且对时延要求不高的信令消息，采用非连接的传输模式。NTLP 还通过传输层和 IP 层的相关安全机制对信令的传输提供保护[12]。2)NSLP 层包含不同的 NSIS 信令协议，不同的信令实现不同的功能，信令消息通过 NTLP 提供的接口实现信令的传输。目前提出的 NSLP 包括用于保证服务质量的 QoS NSLP 以及用于 NAT/FW 穿越的 NAT/FW NSLP 等。

这种分层的设计方法将信令的具体实现与信令的传输分开，增强了信令系统的通用性。针对不同的信令可以提供不同的传输服务，具有一定灵活性。利用 IP 层和传输层的安全机制，为应用层信令的传输提供了安全保障。

2.2 基于 NSIS 的 UMTS 核心网动态防御系统

UMTS 分组域核心网中有 GTP 和普通 IP 两类节点，其可能受到的安全威胁也可能来自 GTP 攻击和普通的 IP 攻击[13,14]。由于 GTP 协议缺乏真实性、机密性和完整性保护，因此 GTP 节点容易受到来自移动终端或者 Internet 的攻击。而传统 Internet 上的 IP 攻击同样存在于核心网的 IP 节点[15]。如图 1 所示，核心网内的攻击主要有以下 5 种：1)Internet 到核心网络节点的攻击；2)漫游伙伴到核心网络节点的攻击；3)移动节点到核心网络节点的攻击；4)移动节点到移动节点的攻击；5)Internet 到移动节点的攻击。这些攻击可以分为针对移动节点的攻击和针对核心网络节点的攻击。

我们在深入分析这些安全威胁的基础上，开发了基于 NSIS 的安全设备控制信令协议，构建以防火墙、入侵检测为中心，多种安全技术和产品协同工作的核心网动态防御系统。系统中的防火墙、GGSN 等核心设备部署了 NSIS 信令组件，具有分布式和集中式相结合的控制方式。通过集中式管理，可以从更大范围内对攻击进行关联、分析，提高攻击检测的精确度，从全局的角度防御攻击；集中式管理能够将用户、控制和业务关联，有助于规则优化，冲突检测等。而分布式控制能够提高响应速度，提高系统效率。如基于分布式方式，当用户结束 PDP 上下文时，GGSN 可以直接通知 G_i 防火墙并要求防火墙删除所有相关的规则，关闭该通道。

如图 1 所示，为了防御上面分析的攻击，在核心网相应的接口部署了防火墙，这些防火墙设备能够与策略服务器和 GGSN 等节点联动，动态部署访问控制规则。审计服务器负责对来自网络测量节点和网络安全设备的多源数据进行融合，完成威胁信息的聚集、校验和告警关联等分析功能。根据分析结果，并结合上下文信息对系统的威胁进行评估，将评估结果存放到审计库并通告策略服务器。策略服务器根据攻击情况，查询策略库生成相应的响应动作，这些动作经 NSIS 协议封装传输给访问控制设备进行部署。而在分布式工作方式下，防火墙、GGSN 等节点可以根据安全需求，基于 NSIS 访问控制信令协议直接同其他 NSIS 实体进行联动，实时、高效地部署访问控制规则。

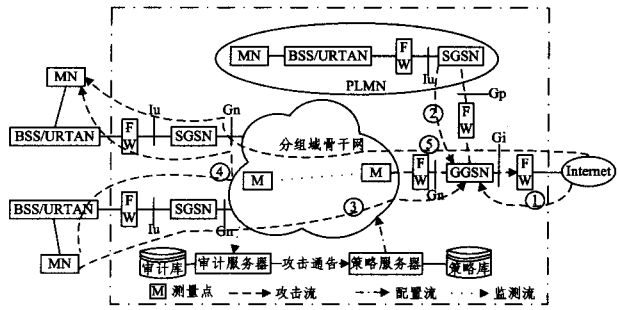


图 1 NSIS 框架下 UMTS 核心网动态防御系统

3 UMTS 核心网动态防御系统关键技术

3.1 通用访问控制 NSIS 信令层协议

设计通用访问控制 NSIS 信令层协议 UAC_NSLP(Universal Access Control NSIS Signaling Layer Protocol)的目的是充分利用 NSIS 框架安全、可靠、灵活的优势，弥补现有访问控制技术的不足，达到对网络中的访问控制设备进行动态、灵活的配置。UAC_NSLP 定义了配置请求消息 REQ、配置应答消息 REP 和错误消息 ERR 三种消息类型。REQ 用来给访问控制设备部署不同的访问控制策略。REP 是对 REQ 消息的响应，分为简单响应和详细响应，详细响应可以携带一些协商结果信息。ERR 消息主要是在鉴权失败或者检查到信令消息错误的时候返回出错的原因，为错误恢复提供参考。

协议的执行流程如图 2 所示。没有上层应用产生的时候，节点处于空闲状态。若收到上层应用的访问控制请求，则节点变为 NI(NSIS Initiator)，生成并发送 REQ。如果 REQ 达到 NSIS 转发节点 NF(NSIS Forward)，NF 根据需要对 REQ 进行处理，例如进行鉴权、策略配置等，并转发 REQ。如果 REQ 达到 NSIS 响应节点 NR(NSIS Responder)，NR 接收到 REQ，则产生一个应答消息 REP，并沿逆路径返回 NI。如果 NF 接收到 REP，则根据需要进行处理，并沿逆路径转发 REP。如果是 NI 接收到 REP，则访问控制配置请求完成。操作结果有成功和失败两种情况，NF 或者 NR 对 REQ 或者 REP 进行鉴权、错误检查等处理。如果鉴权失败或者检查到错误，则返回错误应答消息 ERR。错误情况的处理过程如图 2 所示。

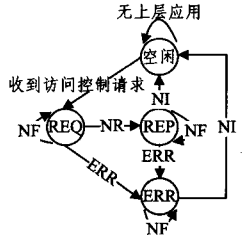


图 2 UAC_NSLP 的操作流程

访问控制配置实体的内部结构如图 3 所示。输入处理模

块接收输入分组，如果是 NSIS 消息，则转交给 GIST 处理器；GIST 处理器负责解析 NSIS 消息，得到 NSLP 层消息，如果是 UAC_NSLP，则将 NSLP 消息转给 UAC_NSLP 处理器；UAC_NSLP 处理器解析 UAC_NSLP 信息，并根据配置选择对象中的内容决定该节点是否需要进行配置操作。如果需要进行配置操作则将解析消息转给 UAC_NSLP 应用代理；安全策略模块决定请求是否被授权；如果允许进行本地策略配置，UAC_NSLP 应用代理根据配置策略信息进行处理，并为访问控制模块部署相应的规则。

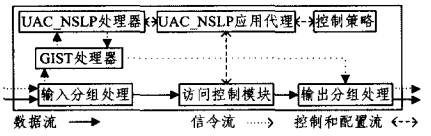


图 3　UAC_NSLP 节点内部结构

3.2　基于多源信息融合的安全事件分析

NSIS 框架下的核心网动态防御系统采集以 IDS 为主的多种安全部件和关键网络节点的安全信息，基于采集的信息进行聚集、校验和关联。

多源信息分析程序由安全信息采集模块、告警聚集、告警校验、告警关联等多个相对独立的模块组成。理想的告警聚集应该将所有同一个网络事件触发的告警合并为一条。但是，为了防止有效信息丢失，本文采用的是具有相同的源 IP、目的 IP、源端口、目的端口、协议、安全部件类型的事件，如果它们的时间间隔小于一定的范围，则将它们合并为一条告警。告警校验也就是行为推测，借助规则指定一种攻击成功发生所必需的上下文条件。最终的校验结果有 4 个可能的取值：未校验、正确告警、误告警、无法校验。本系统中的告警关联采用的是因果关联的方法[16]。该方法的输入是一系列告警，输出是一个告警关联后的有向图。

3.3　基于策略的自适应防御技术

为了实现核心网动态安全防御，必须将安全审计同策略管理相结合，将审计结果作为策略规则的触发事件，根据不同的状况执行相应的动作。策略的执行信息基于 NSIS 访问控制信令协议封装并传输到 NSIS 安全设备，实现动态规则配置。

策略是规则和事件的组合，根据策略事件触发相应规则，执行规则中定义的动作。本文中的策略特指用于对各安全部件进行配置和管理的安全策略，结合核心网动态防御的需求，给出了安全策略的如下定义。

定义 1　策略是一个七元组，记为

$Policy \Leftrightarrow \langle policyID, Subject, [Target], Event, Rule\langle Condition, Action\rangle, Lifetime\rangle$

其中 $Policy$ID 为策略的唯一标识号，用于策略的存储和查询；$Lifetime$ 为策略的生存时间，超过生存时间的策略将被自动删除；$Event$ 为策略的触发事件，能够触发相应的策略规则；$Rule$ 是安全规则集合，包括当前状况和对应的策略行为；$Subject$ 为策略的行为执行者集合；$Target$ 为策略作用目标集合，可以没有作用目标。策略中的 $Event$，$Rule$ 等是复合对象，可由一些元对象组成，如图 4 所示。

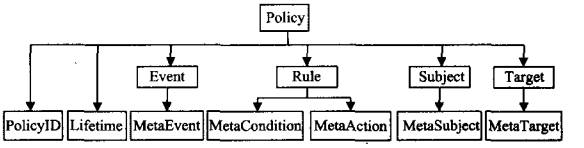


图 4　策略组成

这些元对象支持一些简单的操作，比如假设 E 为事件，e_i 表示元事件，对于 $\forall e_i, e_i \in E, i$ 是自然数，定义以下表示方式：

$$e_1 \wedge e_2 \wedge e_3 \wedge \cdots \wedge e_n \begin{pmatrix} \text{表示 } n \text{ 个事件} \\ \text{同时发生} \end{pmatrix}$$

$$e_1 \vee e_2 \vee e_3 \vee \cdots \vee e_n \begin{pmatrix} \text{表示 } n \text{ 个事件} \\ \text{至少有一个发生} \end{pmatrix}$$

$\neg e_i$（表示事件 e_i 没有发生）

根据这些规则，用户可以定制复合事件，扩展事件表述能力。

安全联动的过程是安全事件触发策略规则，策略规则根据当前的状态触发对应策略行为的过程，如下式所示：

$$E_i \rightarrow R_i \rightarrow \begin{cases} \text{if } coudition_1 \text{ then } action_1 \\ \text{if } coudition_2 \text{ then } action_2 \\ \text{if } coudition_n \text{ then } action_n \end{cases}$$

4　系统测试分析

基于 UMTS 核心网测试平台，对动态防御系统进行了测试。测试场景如图 5 所示，主要包括应用服务器、数据库服务器、防火墙、攻击机、SGSN 和 GGSN 等 6 个节点。应用服务器实现图 1 中审计和策略响应两方面的功能，部署了数据采集器、事件分析器和控制台程序。数据库服务器上部署了审计库和策略库。GGSN 和 SGSN 是按照 3GPP 标准实现的测试节点。NSIS 防火墙设备使用 Netfilter 防火墙。攻击机上部署了 Syn Flood Attack 工具，对目标机 SGSN 的 80 端口进行 Syn 攻击。除了数据库服务器和攻击节点外，其他节点都部署了 NSIS 协议栈。

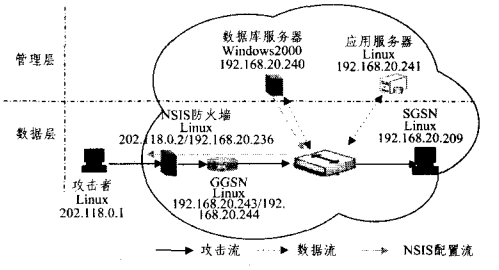
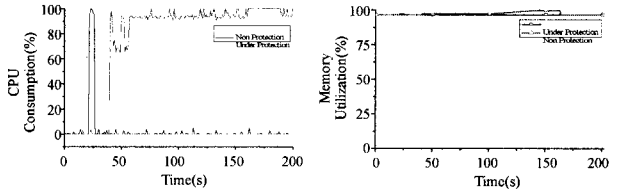


图 5　测试环境

测试步骤如下：1）安全审计。系统运行后启动 Snort、NetEye IDS 和漏洞扫描等程序，采集网络流量进行分析。如果发现具有攻击特征的流量，则生成告警。经过规范化处理后的告警转发给事件分析器，进行告警的关联、聚集、校验、写审计库等操作。2）动态响应。在攻击者节点使用 SYN Flood Attack 工具对 SGSN 进行大量的 SYN 攻击，攻击信息被入侵检测设备实时收集，并经过威胁评判后通告控制模块，控制模块根据当前配置情况产生对应的策略行为，封装到 NSIS 消息中，发送到 NSIS 防火墙进行相应的配置，实时阻断攻击。

在 SGSN 上使用 Vmstat 记录了资源占用情况，结果如图

6 所示，分为没有启动动态保护和启用动态保护两种测试情况。没有启动动态保护情况下，系统的 CPU 占用率大部分时间在 90%以上。而在启动动态防御系统情况下，在 Vmstat 启动约 20s 后开始 Syn 攻击，系统实时检测到攻击并自动阻断了攻击，CPU 占用率明显恢复到正常状态，如图 6(a)所示。而没有启动动态防御措施情况下的内存使用率也较启用动态防御情况下的使用率高，如图 6(b)所示。由此可知，基于 NSIS 的动态防御系统较好地实现了 UMTS 核心网防御的目的。



(a)CPU 使用情况　　(b)内存使用情况

图 6

结束语　将 NSIS 信令技术引入到 3G 网络安全中，设计和实现了 NSIS 框架下的 3G 核心网动态防御系统。NSIS 的引入不仅解决了传统网络安全联动协议缺乏通用性的问题，而且继承了 NSIS 信令技术安全、可靠的优点，为新一代融合网络核心网的安全防护提供了有效的手段。下一步的工作是完善入侵检测系统，支持对核心网 GTP 等关键信令协议攻击的检测，优化完善防御系统各个模块性能。

参 考 文 献

[1] Peter L, Martin L, Krzysztof P. Efficient Protection of Mobile Devices by Cross Layer Interaction of Firewall Approaches // Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2006, 3970: 155-165

[2] 郑宇，何大可，梅其祥. 基于自验证公钥的 3G 移动通信系统认证方案. 计算机学报，2005，28(8)：1327-1332

[3] Prasad A, Wang H, Schoo P. Infrastructure Security for Future Mobile Communications System // Proceedings of WPMC 2003. Yokosuka, Japan, 2003: 186-190

[4] Boman K, Horn G, Howard P, et al. UMTS security. Electronics & Communication Engineering Journal, 2002, 14(5): 191- 204

[5] Günter S. Research Challenges in Security for Next Generation Mobile Networks // Proceedings of Workshop on Pioneering Advanced Mobile Privacy and Security (PAMPAS). Egham, Surrey, United Kingdom, 2002

[6] 王文奇. 入侵检测与安全防御协同控制研究. 学位论文. 西安：西北工业大学，2006

[7] IETF Draft ietf-nsis-nslp-natfw-18. NAT/Firewall NSIS Signaling Layer Protocol (NSLP). 2008

[8] IETF Draft ietf-nsis-qos-nslp-16. NSLP for Quality-of-Service signaling. 2008

[9] Fu Xiaoming, Schulzrinne H, Bader A, et al. NSIS: A New Extensible IP Signaling Protocol Suite. IEEE Communications Magazine, Internet Technology Series, 2005: 133-141

[10] Fu Xiaoming, Tschofenig H, Hogrefe D. Beyond QoS signaling: A new generic IP signaling framework. Computer Networks, 2006, 50(17): 3416-3433

[11] IETF RFC 4080. Next steps in signaling (NSIS): framework. 2005

[12] IETF Draft ietf-nsis-ntlp-15. GIST: general Internet signaling transport. 2008

[13] 3GPP TS 33. 102 v5. 7. 0. Security architecture. 2008

[14] Gopal R L, Tat Chan, Ti-Shiang W. User plane firewall for 3G mobile network // Proceedings of 58th IEEE Vehicular Technology Conference. Orlando, USA, 2003: 2117-2121

[15] Xenakis C, Merakos L. Vulnerabilities and Possible Attacks Against the GPRS Backbone Network // Proceedings of Critical Information Infrastructures Security First International Workshop. CRITIS 2006, LNCS. 2006, 4347: 262-272

[16] Ning P. Techniques and tools for analyzing intrusion alerts. ACM Transactions on Information and System Security (TISSEC), 2004, 7(2): 274-318

(上接第 8 页)

[35] Santos J R. Inoperability input-output modeling of disruptions to interdependent economic systems. J. Syst. Eng., 9(1): 20-34

[36] Haimes Y Y, Horowitz B R, Lambert J H, et al. Inoperability input-output model (IIM) for interdependent infrastructure sectors. II: Case study. J. Infrastructure. Syst., 11(2): 80-92

[37] Haimes Y Y, Horowitz B R, Lambert J H, et al. Inoperability input-output model (IIM) for interdependent infrastructure sectors. I: Theory and methodology. J. Infrastructure. Syst., 11 (2): 67-79

[38] Jiang P. Input-output inoperability risk model and beyond: a holistic approach // Ph. D. dissertation. Systems and Information Engineering Dept., Univ. of Virginia, Charlottesville, Va

[39] Los Alamos National Laboratory presentation on the Interde - pendent Energy Infrastructure Simulation System (IEISS), NISAC Capabilities Demonstrations

[40] Houck D J, Kim E, O'Reilly G P, et al. A Network Survivability Model for Critical National Infrastructures. Bell Labs Tech. J., 2004, 8(4): 153-172

[41] O'Reilly G, Uzunalioglu H, Conrad S, et al. Inter-Infrastructure Simulations Across Telecom, Power, and Emergency Services // Proc. 5th Internet Workshop on Design of Reliable Commun. Networks (DRCN '05), Ischia, It., 2005

[42] Conrad S H, LeClaire R J, O'Reilly G, et al. Critical National Infrastructure Reliability Modeling and Analysis. Bell Labs Technical Journal, 11(3): 57-71

[43] Brown T, Beyeler W, Barton D. Assessing Infrastructure Interdependencies: The Challenge of Risk Analysis for Complex Adaptive Systems. Int. J. Critical Infrastructures, 2004, 1(1)

[44] Beyeler W, Conrad S, Corbet T, et al. Inter- Infrastructure Modeling-Ports and Telecommunications. Bell Labs Technical Journal, 2004, 9(2): 91-105