NSIS下通用访问控制信令协议的设计与验证

陈书义[1]，孙锦山[1]，闻英友[1,2]，赵宏[1,2]
(1. 东北大学计算机软件国家工程研究中心，110004，沈阳；2. 东软研究院，110179，沈阳)

摘要：在深入研究设备穿越和动态防御需求的基础上，提出了基于下一代信令(NSIS)技术的通用访问控制协议.协议实体由7个不同的功能模块组成，并定义了协议的消息类型、数据对象和执行流程.其中，消息类型包括请求消息、应答消息和错误.请求消息将为访问控制设备部署不同的访问控制策略，而错误消息主要是在鉴权失败或者检查到信令消息出错时返回出错的原因.最后，对协议进行了测试、验证，结果表明所提协议具有逻辑正确性，且性能开销较小.通过引入NSIS信令机制，保障了访问控制信令信息安全、可靠传输.

关键词：访问控制；下一代信令；设备穿越；动态防御
中图分类号：TP309 **文献标志码**：A **文章编号**：0253-987X(2009)04-0034-05

Design and Validation of Universal Access Control Signaling Protocol Based on Next Steps in Signaling

CHEN Shuyi[1], SUN Jinshan[1], WEN Yingyou[1,2], ZHAO Hong[1,2]
(1. State Engineering Research Center of Software, Northeastern University, Shenyang 110004, China;
2. Neusoft Research, Shenyang 110179, China)

Abstract: An access control protocol is proposed based on the NSIS technology after studying the demands of equipments traversal and dynamic defense. The protocol consists of seven modules with different functions. Message types, data objects and operation process of the protocol are presented. The message types include request, response and error message. The request message is mainly for setting up different access policies, and the error message is mainly for returning error when authentication failure or message error occurs. Performance of the protocol is tested and verified, and the results show that the proposed protocol has the advantages of logical validity with acceptable cost. The access control information is safely and reliably transmitted based on the use of NSIS signaling mechanism.

Keywords: access control; next steps in signaling; device traversal; dynamic defense

安全网关、防火墙等访问控制设备是网络的重要组成部分，对访问控制设备进行管理是目前研究的热点.国内外学者针对访问控制需求进行了大量的研究，并且取得了一定的成果.针对访问控制设备穿越问题，互联网工程工作小组(IETF)曾提出了一些中间盒穿越方案[1-3]，Pan等人分析了移动IPv6环境中防火墙穿越的方法[4]，Mihai Aurel分析了SIP(会话发起协议)通信穿越中间盒的问题及其解决方案[5]，但是这些技术在可靠性、安全性、可扩展性等方面存在着缺陷.针对安全防御的需求，产业界和学术界分别提出了基于开放式安全平台(OPSEC)、开放安全智能平台(TOPSEC)和简单网络管理协议(SNMP)的联动技术[6]，旨在通过安全设备联动实现动态防御.然而，由厂商提出的联动协议缺乏通用性，而基于SNMP的方案过于复杂.

综上所述，目前访问控制领域的研究成果在安

收稿日期：2008-07-29. 作者简介：陈书义(1972—)，男，博士生；赵宏(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60602061)；国家高技术研究发展计划资助项目(2006AA01Z413).

全性、通用性等方面还存在一些问题，它们还处于独立的层面，用于穿越的技术不适用于防御，而用于防御的技术却不适用于穿越. 由于穿越和防御都是针对访问控制设备的操作的，所以有必要统一起来，以构筑穿越和防御通用平台.

本文设计、实现了穿越与防御统一的访问控制信令协议，它满足新一代网络的需求.

1　NSIS 访问控制信令协议设计

为了满足融合网络中 QoS、安全和业务等方面管理控制的需求，IETF 成立了下一代信令(NSIS)工作组，以研究通用、可靠、可扩展的 NSIS 体系结构以及协议实现方法[7].

NSIS 将信令协议分为 2 层，即 NSIS 传输层(NTLP)和 NSIS 信令层(NSLP)[8]. 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接口[9]；NSLP 层包含了不同的 NSIS 信令协议，这些信令协议实现不同的功能. 信令消息通过 NTLP 提供的接口进行传输.

NSIS 可为控制信息提供安全、可靠的传输. 本文所设计的通用访问控制 NSIS 信令层协议(UAC_NSLP)的目的是，充分利用 NSIS 框架安全、可靠、灵活的优势来弥补现有访问控制技术的不足，同时将访问控制设备的穿越和阻止等操作统一起来，实现对网络中访问控制设备动态、灵活的配置管理.

UAC_NSLP 定义了协议的消息类型、数据对象和执行流程，其中消息类型包括配置请求消息 REQ、配置应答消息 REP 和错误消息 ERR. 配置请求 REQ 用来给访问控制设备部署不同的访问控制策略；配置应答 REP 是对 REQ 消息的响应；ERR 消息主要是在鉴权失败或者检查到信令消息出错时返回出错的原因. 为了对协议进行描述，首先将协议中用到的标识符加以说明，见表 1.

表 1　协议标识符说明

符号	含义
NI	NSIS 消息发起节点
NF	NSIS 消息转发节点
NR	NSIS 消息响应节点
$Cert_A$	节点 A 的证书
REQ	配置请求消息
REP	配置应答消息
ERR	错误报告消息
MAC	消息认证码

协议的执行流程如图 1 所示. 未产生上层应用，节点处于空闲状态. 收到上层应用的访问控制请求，则节点变为 NI 节点，生成并发送 REQ. 如果 REQ 到达 NF 节点，NF 根据需要对 REQ 进行处理，如进行鉴权、配置策略等，并转发 REQ. 如果 REQ 到达 NR 节点，NR 则产生一个应答消息 REP，并沿逆路径将 REP 返回 NI 节点. 如果 NF 节点接收到 REP，则根据需要进行处理，并沿逆路径转发 REP. 如果是 NI 节点接收到 REP，则访问控制配置请求完成. 操作结果有成功和失败 2 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 ERR 消息.

协议实体的内部结构如图 2 所示. 输入处理模块接收输入分组，如果是 NSIS 消息，则转交给通用互联网信传信令传输协议(GIST)处理器. GIST 处理器负责解析得到的 NSLP 层消息，如果是 UAC_NSLP，则转给 UAC_NSLP 处理器. UAC_NSLP 处理器解析 UAC_NSLP 信息，如果需要进行配置操作，则将解析消息转给 UAC_NSLP 应用代理. 控制策略模块决定请求是否被授权，且需经本地配置策略许可，如果允许进行配置，则通过 UAC_NSLP 代理为访问控制模块部署相应的规则.

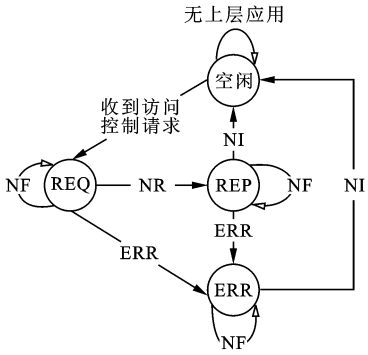

图 1　UAC_NSLP 的操作流程

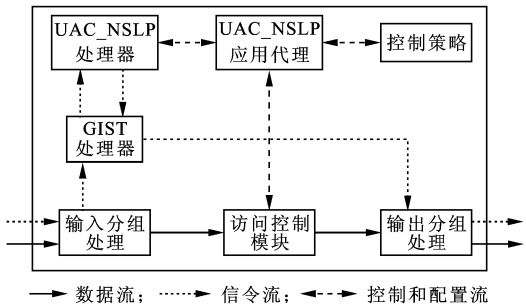

图 2　UAC_NSLP 节点内部结构

2 UAC_NSLP 协议描述和验证分析

2.1 UAC_NSLP 的 Petri 网描述和分析

基于 Petri 网的协议形式化分析方法具有精炼、简洁等特性，因此在该领域受到了广泛应用[10]. 利用 Petri 网对 UAC_NSLP 协议进行描述和验证分析，首先需定义 Petri 网中库所和变迁的标识，如表 2 所示.

表 2 Petri 网中库所和变迁的标识符说明

标识符	库所/变迁含义
P_1	NI 等待发送 REQ
P_2	NI 等待接收 REP
P_3	REQ 在信道中
P_4	失败 REP 在信道中
P_5	成功 REP 在信道中
P_6	NF 等待接收 REQ
P_7	NF 等待验证 REQ
P_8	NF 等待接收 REP
P_9	REQ 在信道中
P_{10}	失败 REP 在信道中
P_{11}	成功 REP 在信道中
P_{12}	NR 等待接收 REQ
P_{13}	NR 等待验证 REQ
T_1	NI 发送 REP
T_2	NI 接收到接受的 REP
T_3	NI 接收到失败 REP
T_4	NF 接收到 REQ
T_5	NF 转发 REQ
T_6	NF 接收到成功 REP
T_7	NF 发送失败 REP
T_8	NF 收到失败 REP
T_9	NR 接收到 REQ
T_{10}	NR 发送接受的 REP
T_{11}	NR 发送失败 REP

利用表 2 中的库所和变迁，可以得到 UAC_NSLP 的 Petri 网描述，如图 3 所示. 系统开始执行时，NI、NF 和 NR 处于空闲状态(P_1, P_6, P_{12})，当 NI 需要发送 REQ 消息的时候，通过 T_1 触发访问控制过程.

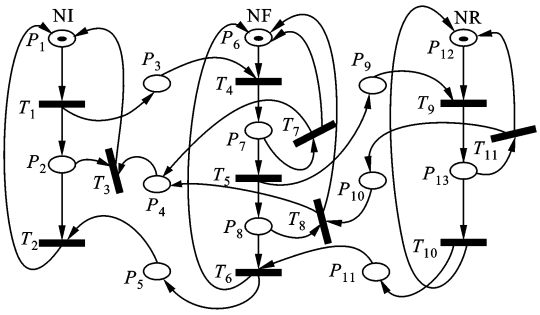

图 3 UAC_NSLP 的 Petri 网描述

利用可达树生成算法，可以获得 UAC_NSLP 的可达树，再通过可达树分析可知 UAC_NSLP 具有有界性、灵活性、完整性和前进性.

根据 Petri 网描述，可得到 UAC_NSLP 模型 Petri 网描述的关联矩阵，基于关联矩阵，可以对 UAC_NSLP 进行不变量分析.

利用 $\boldsymbol{C}^{\mathrm{T}} \cdot \boldsymbol{X}=\boldsymbol{\theta}_{\boldsymbol{T}}$，其中 $\boldsymbol{\theta}_{\boldsymbol{T}}$ 是分量全为 0 的 $\boldsymbol{T}$_向量，$\boldsymbol{C}$ 为关联矩阵，从而得到下面 3 个 $\boldsymbol{S}$_不变量

$$\boldsymbol{S}_1 = (1,1,0,0,0,0,0,0,0,0,0,0,0)^{\mathrm{T}}$$
$$\boldsymbol{S}_2 = (0,0,0,0,0,1,1,1,0,0,0,0,0)^{\mathrm{T}}$$
$$\boldsymbol{S}_3 = (0,0,0,0,0,0,0,0,0,0,0,1,1)^{\mathrm{T}}$$

即

$$m(P_1)+m(P_2)=1$$
$$m(P_6)+m(P_7)+m(P_8)=1$$
$$m(P_{12})+m(P_{13})=1$$

3 个库所不变量表明，NI、NF 和 NR 各自对应的所有库所的 Token 数等于常数 1，从而保证了协议的可靠性，而在协议运行过程中的库所总量没有发生变化，故体现出协议的守恒性.

利用 $\boldsymbol{C} \cdot \boldsymbol{X}=\boldsymbol{\theta}_{\boldsymbol{S}}$，其中 $\boldsymbol{\theta}_{\boldsymbol{S}}$ 是分量全为 0 的 $\boldsymbol{S}$_向量，从而得到下面的 $\boldsymbol{T}$_不变量

$$\boldsymbol{T}_{-1} = (1,1,0,1,1,1,0,0,1,1,0)$$
$$\boldsymbol{T}_{-2} = (1,0,1,1,0,0,1,0,0,0,0)$$
$$\boldsymbol{T}_{-3} = (1,0,1,1,1,0,0,1,1,0,1)$$

对所有从初始状态 $\boldsymbol{M}_0(m(P_1)=1, m(P_6)=1, m(P_{12})=1)$ 出发的激发序列 Q_K，由可达标识方程 $\boldsymbol{M}_K=\boldsymbol{M}_0+\boldsymbol{W}Q_K$ 从 $\boldsymbol{M}_0=(1,0,0,0,0,1,0,0,0,0,0,1,0)^{\mathrm{T}}$ 出发，分别在激发序列 $Q=\{\boldsymbol{T}_{-1}, \boldsymbol{T}_{-2}, \boldsymbol{T}_{-3}\}$ 的作用下，网系统都可以回到系统初始状态，这反映出协议系统的循环性.

2.2 UAC_NSLP 协议性能分析

在 Linux 环境下，基于 NSIS 协议栈对 UAC_NSLP 协议的性能进行了测试分析. 测试中，将 NTLP 层会话刷新率设置为 180 s，NSLP 层刷新率设

置为 90 s. 测试的性能参数包括：①CPU 使用率，即协议进程占用 CPU 的比率；②内存使用率，即协议进程消耗内存的大小；③处理时间，即 NF 节点对 NSLP 信令消息的处理时间；④平均会话建立时间，即从 NI 发送会话、建立请求消息到收到 NR 的应答消息之间的时延.

测试场景为 3 个节点，顺序是：NI↔NF↔NR. 为了分析协议的可行性，本文与最为典型的 NSIS 信令协议 NAT/FW_NSLP 进行了性能比较. 在对 UAC_NSLP 协议和 NAT/FW_NSLP 协议测试时，发送了 2 500 条不同的会话建立请求，并相应发送了 2 500 条 UAC_NSLP 协议 REQ 消息和 NAT/FW_NSLP 协议的 CREATE 消息.

CPU 利用率测试结果如图 4 所示，内存利用率测试结果如图 5 所示. 从图 4、图 5 可以看出，CPU 的利用率并没有因为会话数量的增加而显著增大. 随着会话数量的增加，内存的使用率有所上升，这主要是因为需要为每一条不同的会话维持相应状态的缘故.

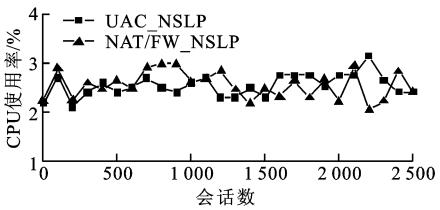

图 4　NF 节点的 CPU 使用情况

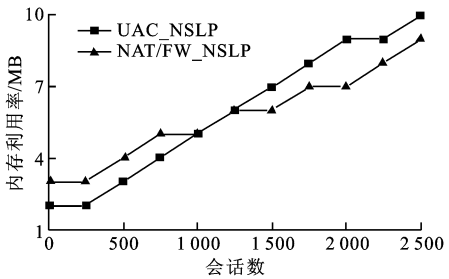

图 5　NF 节点的内存使用情况

消息处理时间如图 6 所示，平均会话建立时间如图 7 所示. 从图 6、图 7 看出：NF 节点对 NSLP 信令消息的处理时间并没有随会话数量的增加而加大，仅在 36 ms 附近略有波动；随着会话数量的增加，平均会话建立时间呈缓慢上升趋势，这主要是 NTLP 层为维护每个会话的状态而进行会话刷新导致 NSIS 消息排队产生延迟. 还可以看出，UAC_NSLP 协议同 NAT/FW_NSLP 协议的性能并没有显著的区别，这表明 UAC_NSLP 协议的性能开销是可以接受的.

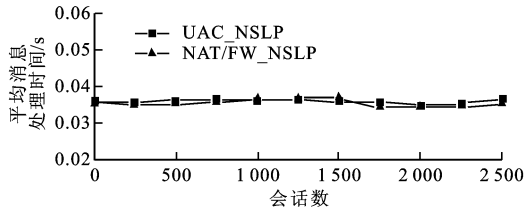

图 6　平均消息处理时间

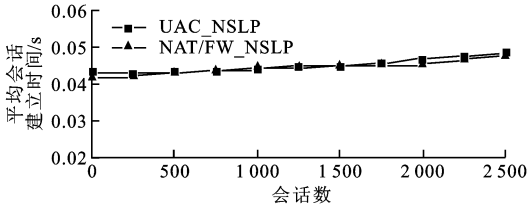

图 7　平均会话建立时间

3　结　论

将 NSIS 技术应用到网络设备的访问控制中，保障了网络访问控制信令的安全、可靠传输. 基于 NSIS 机制的访问控制管理构筑了设备穿越与安全防御统一的信令平台，提供了可扩展、通用、高效的网络设备访问控制管理. 基于 Petri 网验证了协议的正确性，最大限度地消除了协议设计潜在的错误，性能测试分析也表明了协议的可行性. 下一步的工作是，利用访问控制协议设计和实现新一代网络动态防御系统.

参考文献：

[1] ROSENBERG J, WEINBERGER J, HUITEMA C, et al. STUN — simple traversal of user datagram protocol (UDP) through network address translators (NATs), RFC 3489[R]. Reston, VA, USA: Internet Society. IETF, 2003.

[2] ROSENBERG J, MAHY R, HUTIEMA C, et al. Traversal using relay NAT (TURN), draft-rosenberg-midcom-turn-08[R]. Reston, VA, USA: Internet Society. IETF, 2006.

[3] ROSENBERG J. Interactive connectivity establishment (ICE): a methodology for network address translator (NAT) traversal for offer/answer protocols, draft-ietf-mmusic-ice - 15 [R]. Reston, VA, USA: Internet Society. IETF, 2007.

[4] PAN Jianli, CHEN Shanzhi. A mobile IPv6 firewall traversal scheme integrating with AAA[C]// 2006 International Conference on Wireless Communications, Networking and Mobile Computing. Piscataway, NJ, USA: IEEE, 2007:414-420.

[5] MIHAI A, CERNAIANU D O. NAT/firewall traversal for SIP: issues and solutions[C]// Proceedings of International Symposium on Signals, Circuits and Systems. Piscataway, NJ, USA: IEEE,2005: 521-524.

[6] 王文奇. 入侵检测与安全防御协同控制研究 [D]. 西安:西北工业大学信息科学与技术学院,2006.

[7] FU Xiaoming, TSCHOFENIG H, HOGREFE D. Beyond QoS signaling: a new generic IP signaling framework [J]. Computer Networks, 2006, 50(17):3416-3433.

[8] HANCOCK R, KARAGIANNIS G, LOUGHNEY J, et al. Next steps in signaling (NSIS): framework, IETF RFC 4080 [R]. Reston, VA, USA: Internet Society. IETF, 2005.

[9] SCHULZRINNE H, COLUMBIA U, HANCOCK R, et al. GIST: general internet signalling transport [EB/OL]. [2008-06-10]. http://www.ietf.org/internet-drafts/draft-ietf-nsis-ntlp-15.txt.

[10] 高磊, 张德运, ALAM M J, 等. 基于 Petri 网的 TCP 协议异常检测模型 [J]. 西安交通大学学报, 2006, 40(6): 659-662.
GAO Lei, ZHANG Deyun, ALAM M J, et al. Anomaly detection model based on Petri net for TCP protocol [J]. Journal of Xi′an Jiaotong University, 2006,40(6): 659-662.

(编辑 苗凌)