基于可信网络连接的多级涉密网安全接入方案

王 浩 陈泽茂 李 铮 黄碧翼
(海军工程大学信息安全系 武汉 430033)

摘 要 分析多级涉密网安全接入的需求,提出了基于可信网络连接的多级涉密网安全接入模型。模型通过引入安全属性检查规则,检查接入设备和设备中客体的安全属性,以确保其接入不会造成敏感信息的泄露;通过引入完整性度量规则,实现多级涉密网与接入设备双向完整性度量。在可信网络连接架构的基础上增加认证信息库,提出了一种多级涉密网安全接入架构,设计了对应的安全接入认证协议,协议以先完整性度量后用户认证的顺序实现了接入双方安全可靠的互认证。对比分析表明,该协议的效率比其他接入认证协议的高。

关键词 多级涉密网,可信网络连接,接入认证,安全属性
中图法分类号 TP393.08 **文献标识码** A

Secure Access Scheme Based on TNC for Multi-level Classified Network

WANG Hao CHEN Ze-mao LI-Zheng HUANG Bi-yi
(Information Security Department, Naval University of Engineering, Wuhan 430033, China)

Abstract According to the admission control requirements of multi-level classified network (MLCN), a secure access model based on trusted network connection was proposed. By introducing security attribute checking rule, the security attribute of accessing device and its objects were checked in order to ensure that they would not lead to sensitive information leakage. By introducing integrity measurement rule, mutual measurement between the network and the device can be achieved. Based on the access security model, an access system framework for MLCN and an accompanying authentication protocol were put forward. The protocol performs integrity measurement before authenticating user authentication to achieve reliable mutual authentication. Comparative analysis indicates that the protocol is relatively more efficient.

Keywords Multi-level classified network, Trusted network connection, Access authentication, Security attribute

1 引言

多级涉密网(Multi-Level Classified Network, MLCN)是一类由多种安全等级信息和设备组成的信息系统。如同其它网络系统,MLCN易遭受病毒和木马程序的攻击,但MLCN还存在敏感信息泄露的威胁。若不可信终端接入MLCN,易将恶意代码引入MLCN,并可能因终端安全级别较低而导致失泄密事件的发生。现有的安全措施多为防范来自安全边界外的攻击,对于安全边界以内的设备缺乏有效的管理和控制。因此,对MLCN中的接入设备进行可信度量、实施网络接入控制显得非常必要。但MLCN不同于其它信息系统,除关注接入设备是否可信外,还关注接入设备的安全属性是否满足安全接入要求。

为解决网络的安全接入问题,国内外学者相继开展了一些深入研究。Dave等研究设计了分布式网络接入系统[1],系统包括可编程的接入装置和一个外部处理器,实现了网络接入控制,但未对接入设备的可信性和安全属性进行检查;Vanessa等人提出了基于行为轮廓的网络接入控制机制[2],该机制可自动创建行为簇,并通过引入学习算法自动更新接入控制策略,以提高网络接入控制效率,但同样对接入设备是否可信、安全属性是否满足要求未做说明;自2004年至今,可信计算组织(Trusted Computing Group, TCG)一直致力于可信网络连接[3](Trusted Network Connection, TNC)的研究工作,而且学者对TNC的改进工作和对其它接入认证方法的探索一直没有中断过,如颜菲等人针对客户终端缺乏安全保护的问题,提出了一种基于TNC结构的安全认证协议[4],该协议将完整性度量和PKI相结合,可实现终端与网络的互认证;王佳慧等人提出的一种可信网络接入与认证协议[5],在完整性验证中采用服务器和客户端的双向认证;邱罡等人采用智能卡和可信计算技术结合的VPN接入认证方案[6]提供了用户和平台的双重认证,杜绝了终端平台成为入侵者的跳板的可能性。如上研究都解决了接入设备的可信度量问题,但就MLCN而言,依然不能完成对接入终端安全属性的检查。

本文第2节对MLCN环境进行描述;第3节引入安全属性检查函数,设计安全属性检查规则,建立了一个基于可信网络连接的多级涉密网安全接入模型(Security Access Model

到稿日期:2012-02-14 返修日期:2012-07-24 本文受中国博士后特别基金项目(201003757)资助。
王 浩(1988-),男,硕士生,主要研究方向为信息安全,E-mail:wanghao821@yahoo.cn;陈泽茂(1975-),男,博士,副教授,主要研究方向为信息安全;李 铮(1989-),男,硕士生,主要研究方向为信息安全;黄碧翼(1989-),男,硕士生,主要研究方向为网络安全。

Based on Trusted Network Connection for MLCN, TNC-MLCN 模型)；第 4 节基于 TNC-MLCN 模型研究设计了 MLCN 安全接入方案和接入认证协议；最后总结全文。

2 MLCN 环境

定义 1(客体集合 O) $O=\{o_1,o_2,o_3,\cdots,o_i\}$，为 MLCN 中的系统配置文件、程序代码、文本、图像等。

定义 2(隶属关系) $a\propto b$ 表示 a 为隶属于 b 的一个实体。其中 a 可以是客体、网络节点或网络域，b 可以是网络节点或网络域。如 o_i 为某个网络节点中的客体，则称 o_i 隶属于该节点。

定义 3(节点集合 T) $T=\{t_1,t_2,t_3,\cdots,t_i\}$为 MLCN 中设备的集合。

定义 4(安全级别集合 L) $L=\{(lc,lk),lc\in Lc,lk\subseteq Lk\}$，其中 $Lc=\{lc_1,lc_2,lc_3,\cdots,lc_i\}$为安全等级集合，$Lc$ 是大小可比较的线性序列；$Lk=\{lk_1,lk_2,lk_3,\cdots,lk_i\}$表示安全范畴的集合，$Lk$ 中的范畴是非等级的应用领域或类别集合。设 $l_m=(lc_m,lk_m)$，$l_n=(lc_n,lk_n)$，安全级别 l_m 支配 l_n，当且仅当 $lc_m\geqslant lc_n$，$lk_m\supseteq lk_n$，记作 $l_m\mathrm{dom}\ l_n$。

定义 5(安全标记函数 F) $F=\{(f_t,f_o,f_n)\}$，其中：

(a) $f_t:T\to L$，节点的安全标记函数；

(b) $f_o:O\to L$，客体的安全标记函数；

(c) $f_n:Net\to L$，安全域(见定义 8)的安全标记函数。

定义 6(单安全等级域集合 $SNet$) $SNet=\{snet_1,snet_2,snet_3,\cdots,snet_i\}$，$\forall\ snet\in SNet$，令 $f_n(snet)=l$，对于 $snet$ 中的任意节点，即 $\forall\ t'\propto snet$，有 $f_t(t')=l$。

定义 7(多安全等级域集合 $MNet$) $MNet=\{mnet_1,mnet_2,mnet_3,\cdots,mnet_i\}$，$\forall\ mnet\in MNet$，令 $f_n(mnet)=l$，对于 $mnet$ 中任意单安全等级域，即 $\forall\ snet\propto mnet$，有 $l\ \mathrm{dom}\ f_n(snet)$；且 $\exists\ snet_1、snet_2\propto mnet$，$f_n(snet_1)\neq f_n(snet_2)$。

MLCN 是由多个安全域组成的广域网络，其基本架构如图 1 所示。

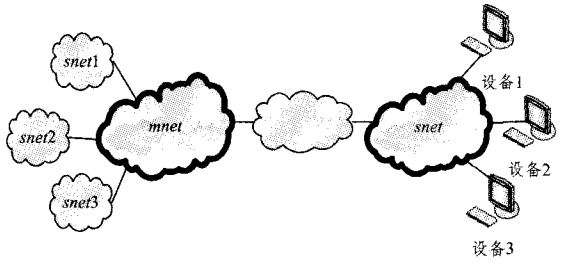

图 1 MLCN 基本架构

由 $SNet$、$MNet$ 的定义和 MLCN 架构可知，不同安全级别的设备不可随意接入 MLCN 的安全域中，如 $snet_1\in SNet$ 只允许与之安全级别相同的设备接入。为防止敏感信息泄露，MLCN 中规定，对于 $\forall\ o\propto t'$，$f_t(t')\ \mathrm{dom}\ f_o(o)$。

3 TNC-MLCN 模型

3.1 元素定义

定义 8(安全域集合 Net) $Net=\{net_1,net_2,net_3,\cdots,net_i\}$，为 MLCN 中所有安全域的集合，包括 $SNet$ 中的元素和组成 $MNet$ 的单安全等级域。

定义 9(用户集合 U) $U=\{u_1,u_2,u_3,\cdots,u_n\}$，为设备的使用者。$U=U_t\cup U_u$，其中 U_t 为可信用户集合，U_u 为不可信用户集合。

定义 10 集合 $A=\{c,d\}$为节点接入属性，其中 c 为接入操作，d 为断开连接操作。对 $x\in A$，$rq(t,net,x)$表示 t 对安全域 net 的 x 操作请求。

定义 11(安全属性集合 $Attr$) 对于节点 $t'\in T$，其安全属性为 $Attr_t=\{(f_t(t'),F_o)\mid F_o$ 为节点 t' 中客体安全属性的集合$\}$。对于安全域 $net\in Net$，$Attr_n=\{Attr_t\mid f_t(t')=f_n(net)$，$f_n(net)$ 支配 F_o 中的元素$\}$，表示安全域 net 期望接入节点所具有的安全属性。

定义 12(安全属性检查函数 M_1) $\langle O,Net\rangle\to Z_1$，其中 $Z_1=\{security,insecurity\}$，

$$M_1(o_i)=\begin{cases}security, & \text{if } Attr_t\subseteq Attr_n\\ insecurity, & \text{if } Attr_t\not\subset Attr_n\end{cases}$$

令 $O_s\subset O$ 为完整性安全保护的客体集合，如系统模块、配置文件等，其预期的完整性度量值为集合 $S=\{So_1,So_2,\cdots,So_n\mid o_i\in O_s\}$。

定义 13(完整性信息集合 W) 在某一时刻 k，对于 $\forall\ o\in O$，其完整性信息为 W_{ko}。

定义 14(完整性度量函数 M_2) $O\to Z_2$，其中 $Z_2=\{unmodified,modified,unfounded\}$，

$$M_2(o_i)=\begin{cases}unmodified, & \text{if } o_i\in O_s\cap W_{ko_i}\in S\\ modified, & \text{if } o_i\in O_s\cap W_{ko_i}\notin S\\ unfounded, & \text{if } o_i\notin O_s\end{cases}$$

定义 15(系统状态 V) $V=Net\times T\times B\times F$ 表示系统状态集合，B 表示 $T\times Net\times A$ 的幂集，为 $MLCN$ 中的接入关系。系统状态 $v=\{(Net,T,b,f)\mid b\in B,f\in F\}$。

定义 16(系统状态转换) $R\times V\to D\times V$，其中 R 为请求集，D 为判定函数，其输出为 yes 或 no，yes 表示允许执行请求的动作，no 表示不允许执行请求的动作。

3.2 安全接入规则

规则 1(完整性度量规则) 系统在(Net,T,b,f)安全状态下，对于 $t_j\in T$，$net_i\in Net$，$O_s^i\propto t_j$，$O_s^i\propto net_i$，有请求操作 $rq(t_j,net_i,c)$。对请求 $rq(t_j,net_i,c)$的处理如下：

(1) $D(rq,v)=no$，若 $\exists\ o\in O_s^i\cup O_s^i$，有 $M_2(o)=modified$；

(2) $D(rq,v)=yes$，并构造 $T^*=T\cup t_j$，$v^*=(Net,T^*,b,f)$，若对于 $\forall\ o\in O_s^i\cup O_s^i$，都有 $M_2(o)=unmodified$。

由完整性度量函数 $M_2()$检查节点和安全域的完整性，使节点和安全域检查彼此的完整性，以确保节点和安全域中完整性安全保护的客体未被恶意篡改。

规则 2(安全属性检查规则) 系统在(Net,T,b,f)安全状态下，对于 $t_j\in T$，$net_i\in Net$，有请求操作 $rq(t_j,net_i,c)$，其中 $f_n(net_i)=l_i$，$f_t(t_j)=l_j$，且 $l_i,l_j\in L$。对请求 $rq(t_j,net_i,c)$的处理如下：

(1) $D(rq,v)=no$，若下述条件至少有一个成立：

(a) $l_i\neq l_j$；

(b) $\exists\ o'\propto t_j$，有 $f_o(o')\ \mathrm{dom}\ l_j$ 成立。

(2) $D(rq,v)=yes$，并构造 $T^*=T\cup t_j$，$v^*=(Net,T^*,b,f)$，若下述条件都成立：

(a) $l_i=l_j$；

(b)对于$\forall o' \propto t_j$,都有 l_j dom $f_o(o')$成立。

规则 2 描述了 MLCN 对节点安全属性的要求,一是节点的安全级别等于安全域的安全级别;二是节点的安全级别支配其所有客体的安全级别。

规则 3(用户认证规则) 系统在(Net,T,b,f)状态下,对于$t_j \in T, net_i \in Net$,有请求操作$rq(t_j,net_i,c)$,用户为$u \in U$。对请求$rq(t_j,net_i,c)$的处理如下:

(1)$D(rq,v)=no$,若$u \in U_u$;

(2)$D(rq,v)=yes$,并构造$T^*=T \cup t_j, v^*=(Net,T^*,b,f)$,若$u \in U_t$。

规则 3 要求只有可信用户才可接入安全域中。

3.3 模型安全性证明

安全公理 1 一个系统状态 v 为安全状态,如果$net_i \in Net, t_j \in T$,则有(t_j,net_i,c)操作,且$M_1(o_m)=security \cap M_2(o_n)=unmodified$,其中$(t_j,net_i,c)$表示节点 t_j 接入安全域$net_i, o_m \propto t_j, o_n \in O_s^1 \cup O_s^2, O_s^1 \propto t_j, O_s^2 \propto net_i$。

由安全公理 1 表明,系统状态为安全状态,当网络接入行为满足如下条件时:(1)接入设备通过安全属性检查;(2)网络和接入设备完整性度量都成功通过。

命题 1 若节点接入 MLCN 同时满足规则 1—规则 3,则该节点的接入满足安全公理 1。

证明:

(1)若 $D(rq,v)=no$,系统保持原有状态,因此满足安全公理 1。

(2)若 $D(rq,v)=yes$,系统状态由 $R \times V \rightarrow D \times V^*$,$V^*-V=T^*-T=\{t_j\}$。

根据规则 1,对于$\forall o \in O_s^1 \cup O_s^2$,其中$O_s^1 \propto t_j, O_s^2 \propto net_i$,有$M_2(o)=unmodified$,满足安全公理 1 中的条件"$M_2(o_n)=unmodified$"。

根据规则 2,$Attr_t=(f_t(t_j),F_o)$,$f_n(net_i)=f_t(t_j)$,且对于$\forall o' \propto t_j$,有 $f_t(t_j)$ dom $f_o(o')$成立,可得 $Attr_t \subseteq Attr_n$,因此满足安全公理 1 中的条件"$M_1(o_m)=security$"。

规则 3 对用户身份进行认证,限制不可信用户接入网络,不会破坏安全公理 1。

综上,命题 1 得证。

命题 2 规则 1、规则 2 和规则 3 保持了系统状态的安全性。

证明:

令(t,o,r)和(t,o,w)为节点 t 对客体 o 的读和写操作。

(1)若 $D(rq,v)=no$,系统状态没有发生改变,因此保持了安全状态。

(2)若 $D(rq,v)=yes$,系统状态由 $R \times V \rightarrow D \times V^*$,$V^*-V=T^*-T=\{t_j\}$。

规则 1 和规则 3 分别是完整性检查和用户可信性认证,不会破坏系统的安全状态。

依据规则 2,由 $l_i=l_j$ 可推出,对$\forall t' \propto net_i$,有 $f_t(t')=l_j$;对于所有的$o \propto t'$,有 l_j dom $f_o(o)$成立,由此可得,对$\forall o' \propto net_i$,有 $f_t(t')$ dom $f_o(o')$。因此,在 net_i 中,$\forall t \in T, \forall o \in O$,操作$(t,o,w)$和$(t,o,r)$都满足 BLP 模型[7]的 ss-属性和*-属性。

综上,命题 2 得证。

4 MLCN 安全接入方案

根据 TNC-MLCN 模型,设计 MLCN 安全接入方案,通过扩展 TNC 架构和设计安全接入认证协议,实现对接入 MLCN 的设备进行完整性度量和安全属性检查。

4.1 安全接入架构

MLCN 接入架构汲取了 TNC 的三步认证思想,即用户身份认证、平台认证和完整性度量。平台可信是用户可信的前提,只有保证平台未被恶意程序入侵,才可认为后续认证是可信的。因此,将 MLCN 接入认证设置为平台身份认证和完整性度量、平台安全属性检查、用户认证的顺序进行操作。图 2 为 MLCN 接入架构。

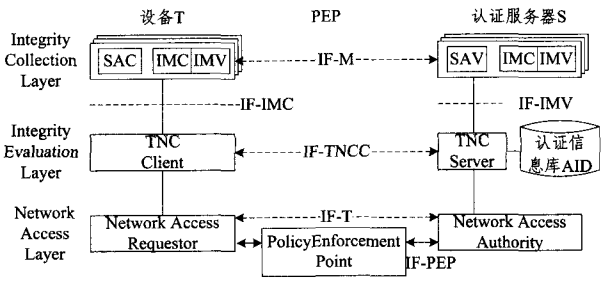

图 2 MLCN 安全接入架构

如图 2 所示,接入设备 T 和认证服务器 S 分别对应于 TNC 基础架构的 NAR 和 PDP。MLCN 在 TNC 架构的基础上增加了一个新的实体,即认证信息库(Authentication Information Database,AID)。AID 主要为接入认证提供策略支持和认证信息服务,同时还记忆 PEP 实施接入控制的结果,以避免对同一设备进行反复认证而增加系统开销。此外,MLCN 接入架构还扩展了 TNC 安全接入的功能,一是在设备 T 和认证服务器 S 中同时部署完整性度量收集器(Integrity Measurement Collector,IMC)和完整性度量验证器(Integrity Measurement Verifier,IMV);二是提供平台安全属性检查,在完整性度量层增加了安全属性收集器(Security Attribute Collectors,SAC)和安全属性验证器(Security Attribute Verifiers,SAV),其中,SAC 用于搜集平台安全属性信息发送给认证服务器 S,由 SAV 检查其是否满足策略。

在 MLCN 中,每一次接入认证都充分信任之前所做的认证,包括平台安全属性检查。本次的平台安全属性检查建立在前一次成功认证的基础上,因此,仅检查平台在之前成功认证后新引入的和被修改的静态信息即可,如此,可提高检查效率。

4.2 安全接入认证协议

假定 AID 中没有接入设备的认证记录或记录无效,且所有认证都可通过。下面对 MLCN 安全接入认证协议进行详细描述。

令 $i \in \{T,S\}$,PK_i、SK_i 为实体的公私钥对;$Certi$ 为实体的身份证书;W_{ki} 为实体的完整性信息;$Sig()$和 $H()$分别为消息签名和消息验证码;$Rec(T)$为设备 T 的接入认证记录,$Time$ 为记录生存期;N 为随机数;$E_k\{\}$为密钥 k 的加密信息($k=\{PK_i,SK_i\}$);SID 为会话标识。图 3 为 MLCN 安全接入认证协议。

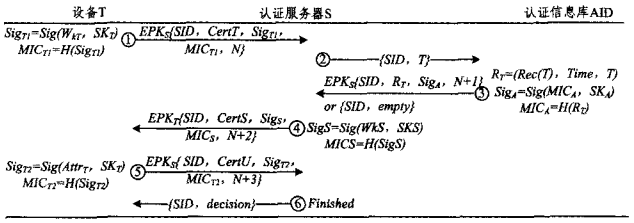

图 3　MLCN 安全接入认证协议

(1)在认证开始之前，设备 T 对每一个 IMC、IMV 和 SAC 进行初始化，同时认证服务器 S 也要初始化所有的 IMC、IMV 和 SAV。

(2)设备 T 收集自身完整性信息 W_{kT}，并产生一个随机数 N，连同平台身份证书 $CertT$ 和消息验证信息 MIC_{T1} 一起发送给认证服务器 S，请求接入网络，请求消息由 S 的公钥 PK_S 加密。

(3)S 首先判断签名消息 $Sig(W_{kT}, SK_T)$ 在传输途中是否遭篡改，然后验证 $CertT$ 和 W_{kT}，若有一个验证失败，则拒绝 T 接入网络。假定验证都成功，发送查询消息给 AID，查询是否有 T 的接入记录。

(4)若 AID 中包含设备 T 的接入记录且在生存期内，则返回接入记录给 S。若 AID 中没有设备 T 的接入认证记录或记录已过期，则返回消息 $empty$。

(5)假定 AID 返回消息 $empty$。S 搜集自身的平台认证信息，包括身份证书 $CertS$ 和完整性信息 W_{kS}，并用自身的私钥对完整性信息进行签名。由 T 的公钥加密平台认证信息并将其发送给设备 T。

(6)T 首先判断签名 $Sig(W_{kS}, SK_S)$ 是否被篡改；然后继续验证 W_{kS} 和 $CertS$。假定上述认证都成功完成，T 搜集自身平台的安全属性信息 $Attr_T$，用私钥签名并连同用户身份证书 $CertU$ 和消息验证信息 MIC_{T2} 一起发送给 S。

(7)S 首先验证签名 $Sig(Attr_T, SK_T)$ 在传输途中是否遭篡改，然后验证 $Attr_T$ 和 $CertU$ 是否满足安全接入策略，若有一个验证失败，则拒绝 T 接入网络。

(8)S 依据安全接入策略产生接入认证决策，并将决策实施结果保存于 AID 中。至此，此次 MLCN 接入认证过程结束。

4.3　协议分析

(1)协议效率分析

MLCN 安全接入认证协议的效率主要体现在交互的轮次上，对于没有接入记录或记录过期的设备只需 6 条消息即可完成接入认证；考虑到 MLCN 中设备接入的频繁性，本文引入了 AID，对于在接入记录生存期内再次接入的设备，仅 3 条消息即可。表 1 为几种认证协议消息交互次数的比较。

表 1　几种认证协议消息交互次数

认证协议	①	②	③	安全接入认证协议	
				有记录	无记录
消息数	7+	8	13	3	6

注：①、②、③分别为文献[4,5,8]中提到的接入认证协议；7+表示多于 7 条消息。

(2)协议安全性分析

接入认证协议的安全性能主要表现在抗冒充、篡改和重放的能力。为提高认证的安全性和可靠性，本文综合运用了公钥密码体制、消息验证码和随机数等多种安全认证技术。下面对 MLCN 安全接入认证协议的安全性进行分析。

假定有一攻击者 A，攻击者的能力表现在两个方面：攻击者已掌握的密钥集合和攻击者根据已知消息构造新消息。K_p 表示攻击者已知的密钥集合，包含所有公钥和攻击者的私钥以及与其他主体的对称密钥。M_k 表示攻击者已知的知识和通过已知知识生成的消息集合，包括通过 $k \in K_p$ 的加密或签名消息。攻击者可以接收、发送和使用已知密钥解密消息，其能力简要表示如下：

$S[m]$：〈$+m$〉表示攻击者可以发送一个消息；

$F[m]$：〈$-m$〉表示攻击者截获一个消息；

$T[-m,+n]$：表示攻击者接收到一个消息 m，然后发送消息 n。

式中，“+”表示发送项，“−”表示接收项。根据攻击者所具有的攻击能力，对 MLCN 安全接入认证协议中的每一条消息进行抗中间人攻击分析。为描述方便，以 $m_1, m_2, \cdots, m_6$ 表示 MLCN 安全接入认证协议的 6 条消息。由于 m_1、m_4 和 m_5 消息的构造相似，其安全性势必相同，因此将 m_1、m_4 和 m_5 消息的安全性一并证明。

命题 3　攻击者无法伪造、篡改和重放 m_1、m_4 和 m_5。

证明：由于 m_1、m_4 和 m_5 的安全性相同，只对 m_1 的安全性进行证明。假定 A 截获到消息 $F[EPK_S\{m_1\}]$，因 m_1 由 S 的公钥 PK_S 加密，解密密钥 $SK_S \notin K_p$，所以 $m_1 \notin M_k$；又由于 $SK_T \notin K_p$，$CertT \notin M_k$，A 无法伪造消息 $Sig(W_{kT}, SK_T)$ 和冒充 T，同时，对于任意信息 $M_x \neq Sig(W_{kT}, SK_T)$，$MIC_x \neq MIC_{T1}$，因此 $Sig(W_{kT}, SK_T)$ 可防篡改。并由于随机数 $N \in m_1 \notin M_k$，消息接收者可识别重放攻击。综上，命题 3 得证。

命题 4　消息 m_2、m_3 可防止伪造、篡改和重放攻击。

证明：攻击者 A 可以实现 $T[-m_2,+n_2]$，假设 $T' \in n_2$，则 AID 返回 $Sig(H(RT'), SK_A) \in m_3$ 或 $empty$，其中 $R_T' = (Rec(T'), Time, T')$，显然，认证服务器 S 可识别 m_3 中并非其所需的记录，因此伪造 m_2 不会影响 MLCN 的安全性；又由于 $SK_A \notin K_p$，A 无法伪造 Sig_A；对于任意信息 $M_x \neq R_T$，$MIC_x \neq MIC_A$，因此 A 无法对 R_T 实施篡改而避过消息完整性验证；同命题 3，$N+1 \notin M_k$，消息可防范重放攻击。综上，命题 4 得证。

上述协议的安全性分析表明，MLCN 安全接入认证协议运用多种安全认证技术，认证信息均未以明文的形式在信道上传输，有效防范了冒充、篡改和重放攻击，确保了认证消息在传输信道上的安全性和认证的真实性。

结束语　本文分析了 MLCN 的安全接入需求，设计了 TNC-MLCN 模型，模型通过引入安全属性检查函数和定义安全属性检查规则，实现了对接入设备安全属性的检查，并经过了模型安全性证明，结果表明 TNC-MLCN 模型具有很好的安全性。同时在 TNC 架构的基础上，构建了 MLCN 安全接入架构，并基于 TNC-MLCN 模型和 MLCN 安全接入架构设计了 MLCN 安全接入认证协议，实现了 MLCN 与接入设备的双向完整性度量和用户认证，分析表明该协议具有较好的认证效率和安全性。

参 考 文 献

[1]　McDysan D, Lee T H, Yao Lei. Network Access System Inclu-

ding a Programmable Access Device Having Distributed Service Control[P]. US:7499458B2,2009-03-03

[2] Frias-Martinez V,Sherrick J,Stolfo S J,et al. A Network Access Control Mechanism Based on Behavior Profiles[C]// Annual Computer Security Application Conference. ACSAC'09. Honolulu,2009:3-12

[3] TCG. Trusted Computing Group Timeline [EB/OL]. http://www.trustedcomputinggroup.org/files/resource_files,2011-02

[4] 颜菲,任江春,戴葵,等.基于 TNC 的安全认证协议设计与实现[J].计算机工程,2007,33(12):160-162

[5] 王佳慧.可信网络连接全生命周期接入与授权模型设计[D].西安:陕西师范大学,2010

[6] 邱罡,王玉磊,周利华.一种基于可信计算的 VPN 接入认证方案[J].计算机科学,2009,36(7):76-78

[7] Bell D E,LaPadula L J. Secure Computer System:Unified Exposition and Multics Interpretation[R]. Bedford,MA:The MITRE Corporation,1976

[8] 张俊伟,马建峰,文相在.通用可组合的可信网络连接模型和 IF-T 中的 EAP-TNC 协议[J].中国科学 E 辑,2010,40(2):200-215

(上接第 41 页)

端口对异常的影响不大;在缩减目的端口后,由异常引起的毛刺已经清晰地从正常流中隔离出来(见图 6(d))。

3.2.3 人工注入异常的识别准确性

为了评估 ECATI 流识别算法的准确率,采用异常注入的方式完成受控实验,其优点在于能学习算法的敏感度(如注入不同强度的异常、不同类型的异常)。表 3 给出了数据集 C 中注入的 3 种异常类型,数据集 C 本身是干净的(不包含异常),对每个检测的时间间隔(即 5 分钟),模拟每个间隔内异常对流的影响。若 ECAD 算法检测到注入异常,则运行 ECATI 识别算法。异常情况:1)链路失败,即通过去除给定持续时间内跨越链路的所有流量来仿真[10],设定 20 秒的链路失败时间;2)恶意流量为 DDoS 攻击和网络扫描时,为了使终端主机异常更为真实,可根据相同链路中发现的相似异常流的特征(IP 地址、端口和 AS 号等)来模拟产生流。

表 3 注入异常的类型

异常类型	异常描述
链路失败	去除间隔内流经被监测链路的所有流
DDoS	增加来自不同网络多个源 IP 地址到单一目的 IP 地址或单一目的端口的流
网络扫描	增加从单个源 IP 地址到单个 IP 目的地址的多个目的端口的流

图 7 给出了链路失败与恶意攻击的丢失流和额外流的 CDF。在 20 秒的链路失败中 ECATI 算法的识别错误率少于 2%,且几乎没有引入额外流。对于 DDoS 攻击和网络扫描,算法在识别率超过 82%的情况下能够精确地输出触发的异常流的特征值及完备异常候选集,丢失的流仅为 1%。经分析发现,这些注入的异常至少有一个终端主机有单一的流特征的值。因此,一旦算法识别出唯一的受害机(如 DDoS 和端口扫描)或使用单一的易受攻击的端口(如网络扫描),在间隔内大多数拥有这些特定特征值的流都可能是异常的一部分。

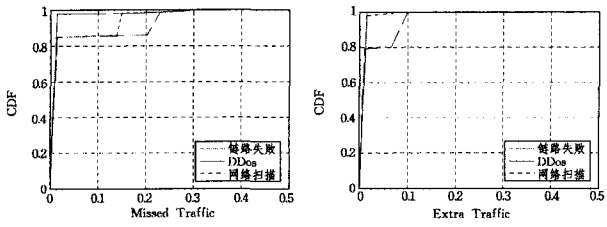

图 7 ECATI 算法对人工注入异常的识别性能

结束语 异常流识别是确保网络安全的重要研究课题,对根源分析、攻击缓解和异常检测器的测试都是必不可少的。ECATI 是一种自动异常流识别算法,算法采用特征熵来衡量流量特征参数的分布变化,用一次指数平滑法对正常流量进行预测来检测异常,在异常间隔内通过分析间隔内的流量来重复地排除类似正常的流,从而识别引发异常的根源流,关键在于利用检测器得到的反馈来确定哪些更像未被异常影响的流。经过真实异常数据集与人工注入异常数据集的实验评估,证实 ECATI 算法能够精确隔离出异常流,在平均识别率 89.5%的情况下识别的丢失流非常少甚至没有。ECATI 算法能有效减少网络管理员的工作,其识别结果能够为异常的正确分类、根源分析做准备。已证实大多数 ECATI 算法的误差是由小型路由事件引起的。尽管本文采用离线数据集来完成仿真实验,但 ECATI 算法能够足够快速地处理数据集以满足在线部署。例如,即使在普通 PC 机的常用硬件条件下,搜集时间为 3 个月的数据集 B 能够使用 ECATI 算法在 4 小时之内完成全部处理。算法依赖于异常检测器的输入,但不使用任何假设,可以不加修改地与任何异常检测器(如 Kalman[9]、PCA[10]与小波等[11])一起使用。本文提出的异常流量检测及识别技术能够用于监测网络,为网络的安全提供保障。

参 考 文 献

[1] Chandolav, Banerjeea, Kumarv. Anomaly Detection: A Survey [J]. ACM Computing Surveys,2009,41(3):1-58

[2] Brauckhoff D,Dimitropoulos X,Wagner A,et al. Anomaly Extraction in Backbone Networks using Association Rules [C]// IMC'09. November. Chicago,Illinois,USA,2009

[3] Krishnamurthy B,Sen S,Zhang Y,et al. Sketch-based change detection:methods,evaluation,and applications[C]// IMC'03:Proceedings of the 3rd ACM SIGCOMM Conference on Internet Measurement. NewYork,NY,USA,2003:234-247

[4] Lakhina A,Crovella M,Diot C. Diagnosing network-wide traffic anomalies[C]//Proceedings of SIGCOMM. 2004:219-230

[5] Lakhina A,Crovella M,Diot C. Mining Anomalies Using Traffic Feature Distributions[C]//Proceedings of SIGCOMM. August 2005:217-228

[6] Nychis G,Sekar V,Andersen D G. An Empirical Evaluation of Entropy-based Anomaly Detection[C]// Proceedings of IMC. Vouliagmeni,Greece,2008:151-156

[7] Guo R-S, Chen J-J. An EWMA-based process mean estimator with dynamic turning capability[J]. IIE Transactions,2002

[8] Thatte G,Mitra U,Heidemann J. Parametric Methods for Anomaly Detection in Aggregate Traffic[J]. IEEE/ACM Transactions on Networking,2011,19(2)

[9] Silveira F,Diot C,Taft N,et al. ASTUTE:Detecting a Different Class of Traffic Anomalies[C]// Proceedings of ACM SIGCOMM. New Delhi,India,2010

[10] Kandula S,Katabi D,Vasseur J. Shrink:A tool for failure diagnosis in IP networks[C]// Proceedings of ACM SIGCOMM MineNet Workshop. August 2005