第 35 卷 第 2 期 计 算 机 工 程 2009 年 1 月
Vol.35 No.2 Computer Engineering January 2009
·安全技术· 文章编号：1000—3428(2009)02—0172—03 文献标识码：A 中图分类号：TP309

危险信号协同作用的自适应 IPS 研究与设计

徐 慧，徐 晨，程学云，彭志娟
(南通大学计算科学与技术学院，南通 226019)

摘 要：入侵防御系统是网络安全领域为弥补防火墙及入侵检测系统的不足而发展起来的一种计算机信息安全技术。其嵌入式的工作方式，使其面临许多挑战，如数据流检测瓶颈、误报和漏报等。该文陈述基于粗糙集理论的危险评测方法和该信号的协同作用下防御及检测器的进化机制。提出以通过评估保护对象所受危险并以此信号协同检测的防御方法，可以提高检测效率和防御效果，降低误报和漏报。
关键词：入侵防御；危险检测；自适应

Research and Design of Adaptive Intrusion Prevention System for Co-stimulated by Danger Signals

XU Hui, XU Chen, CHENG Xue-yun, PENG Zhi-juan
(School of Computer Science and Technology, Nantong University, Nantong 226019)

【Abstract】 Intrusion prevention system is a new information security technology which can supply a gap of the firewall and the intrusion detection system in the information security domain. As work in-line, IPS faces with many challenges, such as bottleneck of data detection, false negative and false positive. This paper proposes a new way trying to solve these problem, which is called Adaptive Intrusion Prevention System co-stimulated by Danger Signal(DSAIPS). Experiments show the primary effects.
【Key words】 intrusion prevention; danger detection; adaptation

1 概述

2002 年下半年国际上的一些网络信息安全研究组织在入侵检测系统(Intrusion Detection System, IDS)难以胜任动态防护重任[1]时，提出了入侵防御系统(Intrusion Prevention System, IPS)的概念[2]。入侵防护不但能检测入侵的发生，而且能通过一定的响应方式，实时地中止入侵行为的发生和发展，实时地保护信息系统不受实质性攻击的一种智能化的安全技术[3]。相比于IDS，IPS则倾向于提供主动防护，其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才发出警报[4]。作为弥补防火墙和IDS的不足而发展起来的一种新型计算机信息安全技术[2]，IPS目前面临如下挑战[5-6]：

(1)瓶颈问题。由于 IPS 设备必须保持与数千兆或者更大容量的网络流量同步，因此设计不够完善的 IPS 嵌入设备无法支持很短的网络响应时间。

(2)高误报和漏报问题。由于 IPS 设备一旦拦截了攻击性数据包，就会对来自可疑攻击者的所有数据流进行拦截，因此如果入侵签名编写得不完善，“误报”就可能导致合法流量也能被拦截。

如何高效、准确地识别数据流是解决上述问题的关键所在。传统的识别方法是误用检测和异常检测，这些方法或把“非正常”统归为“异常”或把“非异常”统归为“正常”，因而引起高误报和漏报。本文提出了危险信号协同检测的入侵防护(Adaptive Intrusion Prevention System co-stimulated by Danger Signal, DSAIPA)方法，通过危险测定，协助入侵识别和启动防御措施。目标明确的检测，可以有效降低数据过滤量、提高检测的准确率、降低误报和漏报及防御措施的适时实施。

2 危险检测

2.1 相关定义

定义 1 危险。指由于违反访问控制、运行不恰当程序或硬件故障、软件设计的不完整和不正确等使保护对象受到损害的可能性。

对于特定的应用系统，因保护目标的确定性和保护属性的有限性决定了危险的有限性、可识别性和可响应性。

定义 2 危险信号。指入侵行为对被监控对象的局部的、极小的受损迹象，且该信号可以被迅速、自动测量，其强度反映受损程度的大小。危险是由多个因素综合反映出来的，可以把其中每一个因素称为危险因子。

定义 3 危险因子。反映计算机信息系统或其资源毁坏、泄露和拒绝服务的可测量的属性，称为危险因子。如 CPU 的利用率、处理器队列中的线程数、现使用的缓冲数、实际可用物理内存尺寸、在 1 s 内 NIC 上的被收送信的比特数等。

本文考虑由危险因子构成的危险信号，有 3 种可能的情况：

Case 1：由单一危险因子组成危险信号。

Case 2：多个相互无关危险因子同时出现。

Case 3：由多个相互关联危险因子组成危险信号。

2.2 危险评定

Case 1：危险信号只有一个危险因子组成。如特定端口

基金项目：江苏省高校自然科学基础研究基金资助项目(07KJD520177)；南通大学博士启动基金资助项目(03080107)；南通大学自然科学基金资助项目(07Z054)
作者简介：徐 慧(1965－)，女，副教授、博士，主研方向：网络与信息安全；徐 晨，教授；程学云，讲师；彭志娟，讲师、硕士研究生
收稿日期：2008-05-05 **E-mail：**xu.h@ntu.edu.cn

流量对端口阻塞的危险。

设危险因子$\boldsymbol{df}$=<s_{df}, v_{df}>，其中，s_{df}为危险因子标识；v_{df}为危险因子值。危险信号$ds=f(v_{df}), f: s_{df}\times v_{df}\rightarrow ds$为风险模型函数。多数情况下，$f$可定义为

$$f(x)=\frac{1}{1+e^{-s(x-t)}},\ s>0,\ t>0$$

其中，s 决定函数的上升速度，称为风险系数。系统越脆弱，s 越大；t 决定函数的水平位移，称为风险态度系数，其取值取决于决策者承担风险的态度，即与设定的安全等级有关。

由于瞬间的危险值往往不能表示攻击，因此危险信号不仅与风险因子某一时刻的值有关，还与该值持续时间有关，以风险信号强度 dd 反映，dd 计算如下：

```
…
if (ds(i) > safegate)；//safegate=g(s)，安全告警值取决于风险态
//度系数 s。
    dd(i)=dd(i-1)+1；
  else
    dd(i)=0；/*一旦危险值小于安全告警值，dd 恢复为 0。*/
  if ( dd > alert)  ；/*alert 为安全警戒值。*/
    take urgent action；/*触发防御措施*/
…
```

Case 2：多个彼此无关的风险因子同时出现。

设风险因子为$\boldsymbol{df}=\{df_1, df_2,\cdots\},df_1,df_2,\cdots$，彼此无关，则风险信号$ds=\max\{f(df_1),f(df_2),\cdots\}$；相应地，其危险强度$dd=\max\{dd_1, dd_2,\cdots\}$。

Case 3：有多个彼此相关的危险因子。

设彼此相关的危险因子组成向量$\boldsymbol{df}=\{df1,df2,\cdots\},df1, df2,\cdots$，共同确定危险程度，危险信号$ds=\sum w_i ds_i,\ ds_i=f(df_i)$，$w_i$ 为该因子的权重，由该因子在该危险决策中的重要性决定。用粗糙集理论的相关知识来计算该权重。危险相关的数据组成决策表见表 1，条件属性为各危险因子对应的危险值，决策属性为危险程度。表中数据为原始属性值的离散值，每一属性值被分为几个等级，每个等级代表一个数据区间。

表 1　关于危险信息的决策表

U	条件属性		…		…		…	决策属性
	c_1(cpu%)	c_2(memory%)	…	c_k(lines)	…	c_m(read operation)	…	d(danger)
x_1	1	2		1		1		0
x_2	3	4		3				3
…	…	…	…	…	…	…	…	…
x_n	5	1		2				1

条件属性来自 3 个方面：(1)被保护对象赖以生存的物理对象的状态属性，如CPU使用率、内存使用率等；(2)保护对象生存以来相关的操作、进程等；(3)被保护对象的属性，如：文件读写允许设定等。如果该属性是受保护的，但被侵犯了，则取值 1/*True*；否则，取值 0/*False*。决策属性 1 个，即该对象x_i对监控对象安全性产生的危协程度。由决策表，根据各条件属性对决策重要性来决定各属性权重的计算步骤如下：

Step1　计算决策分类各子集Di对各属性子集$C_j(=C\backslash c_j)$的正域 $POS_{C^j}(D_i)$。

对于危险决策表$S=<U, A, V, f>, A=C\cup d, C=\{c_1,c_2,\cdots,c_n\}$是条件属性集，$d$为决策属性集。设$C_j=C\backslash cj$是去除属性$c_j$之外的条件属性子集；$D=U/IND(\{d\})=\{D_1,D_2,\cdots,D_m\}$是关于决策的分类。决策分类子集$D_i$ 对属性子集C_j 的正域为

$$POS_{C^j}(D_i)=\cup\{Y_k\mid(Y_k\in U\mid IND(C^j)\wedge Y_k\subseteq D_i)\}$$

Step2　计算各属性子集 Cj 对决策的近似分类的质量 $r_{C^j}(D)$：

$$r_{C^j}(D)=\sum_{i=1}^{m}|POS_{C^j}(D_i)|/|U|$$

Step3　计算各属性对决策D的重要性$SGF(c_j)$：

$$SGF(c_j)=1-r_{C^j}(D)$$

Step4　计算各属性权重：

$$w_i=\frac{SGF(c_i)}{\sum_{j=1}^{n}SGF(c_j)}$$

各属性的权值组成向量$\boldsymbol{W}=(w_1, w_2,\cdots,w_n)$

Step5　加权综合

设各种危险因素组成向量$\boldsymbol{S}=(s_1,s_2,\cdots,s_n)$，则：

$$Signal2=\boldsymbol{S}\bullet\boldsymbol{W}^{\mathrm{T}}=\sum_{i=1}^{n}w_i s_i$$

3　系统设计

3.1　逻辑结构

本文构建的 IPS 在逻辑上分为包过滤引擎、识别引擎、危险评定、响应引擎几个部分，如图 1 所示。

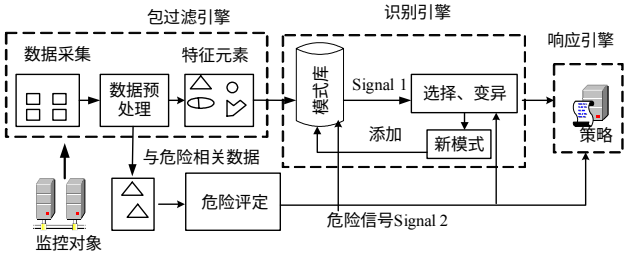


图 1　由危险信号协同刺激的 IPS 逻辑结构图

包过滤引擎完成数据采集和包特征提取。IPS 通常含有多个包过滤器，分级过滤。这里采集的数据分为 2 类：一类是异常数据流，用于提取入侵特征；另一类是与危险评定相关的数据。

识别引擎实现网络行为异常的确认。从包过滤获取的特征数据将与模式库中检测器进行匹配操作，匹配程度形成 Signal 1；危险评定相关数据，经过危险测定运算，综合成 Signal 2；在 Signal 1, Signal 2 共同作用下，模式库中的检测器被激活。对于未知有害攻击，在 Signal 2 引导下将朝着匹配程度不断提高的方向变异，最终形成新检测器，加入到模式库中；而对于已知攻击，变异过程缺省。

响应引擎触发针对危险行为的防御措施。若为已知攻击，则触发与识别结果相对应的某一预安排措施；若为未知攻击，则根据 Signal 2 所确定的危险特征，实施防御，作为初步响应；当然，防御措施也可由两者协作触发。可供选择的防御方式有直接丢掉包、阻断相应的网络流量、发送 SNMP 命令或反击攻击源等。

3.2　检测器及其进化

IPS模式库是一个决策表$S=<U, A, V, f>, A=C\cup\{d\}$，决策类$D=U|IND(\{d\})=\{D_1, D_2,\cdots\}$，$D_i\in D$为一个入侵模式；$D_i=\{r_{i1},r_{i2},\cdots\}$是一个规则的集合，其中，每一个规则$r_{ij}$为一个检测器。入侵特征由一至多个特征基组成，对应的检测模式是由多个规则组成。

(1)一个入侵行为会有多种特征，识别该入侵行为的将是多个检测器。

(2)一个检测器，可能被一种以上的入侵激活。

设：采集到的数据经预处理后提取的一特征基$CAg=\{g_1, g_2,\cdots\}$，g_i为特征基的组成成份。记$CAb=\{b_1,b_2,\cdots\}$为检测器的条件属性集，b_i为一个检测器的条件属性。CAg与CAb匹配

关系有 2 种基本关系，如图 2 中的Case1, Case2，其他情况都可表达成这 2 种情况，如图 2 中的other1, other2。

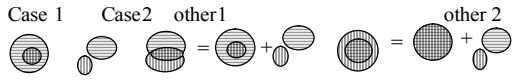


图 2　*CAg* 与 *CAb* 的匹配关系

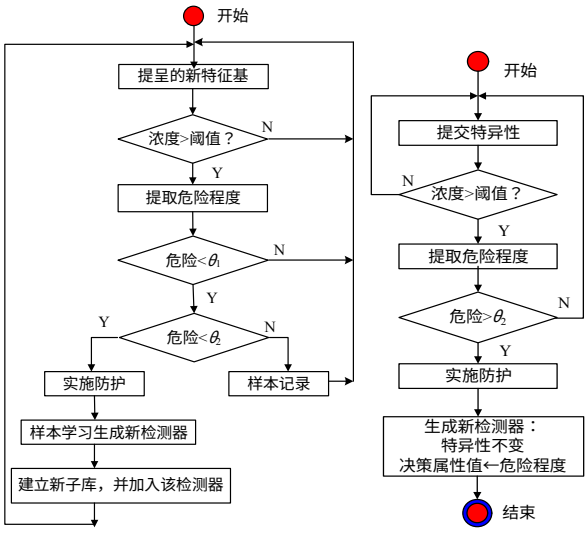
Case 1：$CAg \subseteq CAb$，$m(CAg,CAb)=\dfrac{|CAg \cap CAb|}{|CAb|}$，并记 $y_{i1}=\Phi$。

Case 2：$CAg \cap CAb=\phi$，$m(CAg,CAb)=0$，$y_{i2}=CAg$。

other 1,2 其他情况，可用 Case1 与 Case2 表示。

提呈的特征属性分为 2 个部分，$CAg=x_i \cup y_i, x_i=CAg \cap CAb$ 是能与CAb匹配的属性；$y_i=CAg \backslash x_i$ 是不能与CAb匹配的属性，这可能是由于攻击变形或未知攻击引起的。

检测器进化有 2 种可能情况过程如图 3(a)、图 3(b)所示，其中，θ_1为危险警示阈值；θ_2为危险警戒阈值。θ_1,θ_2为紧急防御措施信号，$\eta=m(CAg, CAb)$。



(a)Case 1　　(b)Case 2

图 3　检测器进化流程

Case 1：出现了无法识别的特征基

当新特征基浓度超过阈值时，提取危险信号。如果是有害攻击，必有危险信号dd发出，在危险小于防御警戒时，即：$\theta_1<dd<\theta_2$时，进行数据采样；一旦$dd>\theta_2$，采取防御措施。危险解除或成功报警后，进行样本学习，生成新的检测器。新检测器的特异性由提呈的新特征基决定，检测器的决策部分由危险类型及危险程度决定。

Case 2：因为特征基的值变异引起的进化

在样本训练中，不可能包含所有可能情况，必然带来检测器不仅在特异性上的不完备性(Case 1)，而且还会带来值上的不完备性，这是形成 Case 2 的主要原因。此时，要识别当前特征基，必须对当前检测器进行变异。变异的结果是生成这样的一个新检测器，其特异性不变(即规则的条件属性不变)，特异性的属性值取当前特征基的相关特征因子的值，规则的决策属性不变，属性取值取决于危险信号的程度，即如果危险信号是“ high ”，则决策属性值取“ high ”。

4　实验

4.1　攻击与防御设置

在自组小型局域网上攻击实验，设置如表 2 所示。

表 2　实验所用攻击类型其及分布

Class	Sub-Class
Normal	
U2R	buffer_overflow
DOS	back, land, surmf, SYN Flood
PRB	ipsweep，portsweep

采取的紧急防御措施为：(1)阻断攻击源，如丢包、关闭端口等；(2)杀死当前进程相关的非系统线程。

4.2　危险信号选取

采集 4 个数据作为危险检测信号，即 CPU 使用率、内存使用率、与进程相关的线程数、端口流量。其中，端口流量与端口一一对应，作为端口阻塞危险信号；CPU 使用率、内存使用率、与线程数共同决定系统资源耗尽的危险。部分样例数据如表 3 所示。

表 3　资源耗尽危险的样例

U	$a_{1(\text{CPU})}$	$a_{2(\text{Memoruy})}$	$a_{3(\triangle\text{lines})}$	danger
1	4	2	2	0
2	4	3	3	3
3	3	3	4	3
4	3	2	3	2
5	4	2	4	2
6	2	4	2	3
7	4	4	4	3
8	3	3	3	2
9	3	2	1	0
10	2	2	2	0

根据 2.2 节给出算法与表 3 数据，可得属性a_1,a_2,a_3对决策的重要性$SGF(a_1)$，$SGF(a_2)$，$SGF(a_3)$分别为：$SGF(a_1)$=1-8/10=0.2, $SGF(a_2)$=1-4/10=0.6, $SGF(a_3)$=1-4/10 =0.6。各属性的权重为：w_1=0.2/(0.2+0.6+0.6)=1/7, w_2=3/7, w_3=3/7, w=(1/7 3/7 3/7)

如果ds=(0.9,0.8,0.5)，则signal 2=$ds \cdot \boldsymbol{w}^{\mathrm{T}}$=0.6，表明此时资源耗尽危险程度为 60%。

4.3　性能分析

对于已知攻击，检测率为 100%。出现非已知攻击时，漏报率、误报率随危险阈值θ_2(触发紧急防御措施的危险信号值)变化，如图 4 所示。

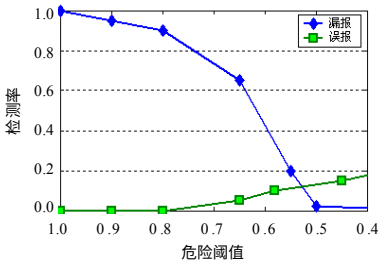


图 4　危险域值对检测性能的影响

(1)误报率。由于采用的是异常检测，因此总体上误报率很低。但是当危险警戒过低，即检测响应过早时，可以引起误报。

(2)漏报率。总体上，漏报率随着θ_2的减小而减小。1)θ_2=1，即没有危险协同作用，则不能识别非已知攻击，漏报率接近于 1。2)θ_2越小，即安全警戒越高，漏报率越小。3)$\theta_2 \leq 0.5$，漏报率≈0。θ_2越大，表示危险警戒线越低，攻击成功的可能性就越大，所以，漏报率就越高。

5　结束语

本文提出了以危险信号协同检测的入侵防御方法。入侵防御目的除了惩戒攻击者，更多地是保护网络用户的利益。相对于攻击的动态性、不可预测性和无穷性，被保护者的利益即需要规避的危险却是明确的、有限的。因此，通过危险

(下转第 186 页)