受免疫原理启发的Web攻击检测方法

曾金全，赵 辉，刘才铭，彭凌西

(四川大学计算机学院 成都 610065)

【摘要】随着Internet应用的不断深入，Web服务器成为了黑客的主要攻击目标。为克服传统误用入侵检测系统无法识别未知Web攻击和异常入侵检测系统误报率高等缺陷，受生物免疫系统启发，该文提出了一种基于免疫原理的Web攻击检测方法。给出了自体、非自体、抗原、抗体基因库、免疫细胞等的数学定义，描述了免疫学习算法。对比实验结果表明该方法较传统的基于神经网络和ID3算法的Web攻击检测技术能有效检测未知Web攻击，具有检测率和分类率高、误报率低和实时高效等特点，是检测Web攻击的一种有效新途径。

关 键 词 异常检测； 人工免疫； 网络安全； Web攻击
中图分类号 TP393 文献标识码 A

Immune Principles Inspired Approach to Detection of Web Attacks

ZENG Jin-quan，ZHAO Hui，LIU Cai-ming，PENG Ling-xi

(School of Computer Science, Sichuan University Chengdu 610065)

Abstract Internet and Web servers become the core infrastructure for companies and institutes. Simultaneously, Web servers also become a popular target for attackers. However, misuse Intrusion Detection Systems (IDSs) are only effective in detecting known attacks and it is difficult to keep up with the daily exploitation of novel and Web-related vulnerabilities; anomaly IDSs often produce a high false alarm rate. To get over the limitations of misuse and anomaly IDSs, this paper inspired by immune principles presents a novel anomaly detection approach to detect unknown Web attacks. In our proposed approach, which is referred to the immune principles Inspired Approach to Detection of Web attacks (IADW), mathematical formulas of self, non-self, antigen, library of antibody genes, immunocyte, and etc., are given, and immune-learning algorithm is described. Experiment results show that our approach can detect unknown attacks with lower false alarm rate, missing alarm rate, and higher detection rate and identification rate than the technique based on neural network and ID3. Thus, it provides an effective novel solution to detection of Web attacks.

Key words anomaly detection; artificial immune system; network security; Web attacks

由于在Web应用系统的设计开发过程中没有严格遵从安全设计与编程规范等原因，导致Web应用系统存在许多安全漏洞和隐患，使得Web服务器成为黑客和网络蠕虫病毒攻击的主要目标[1-2]。

目前，针对Web攻击检测的方法较少，文献[2-3]通过分析Web日志发现Web攻击，但不能检测未知Web攻击以及已知Web攻击的变种。文献[4]提出将攻击检测与应用系统集成在一起并采取多种分析手段相结合的方法。由于这种入侵检测方法嵌入在应用系统内，入侵检测的性能将受到影响，并且这种方法只能专用于Apache Web服务器。误用入侵检测[2-5]，虽然误报率较低，但不能检测未知Web攻击。为检测未知Web攻击，文献[6]采用ID3算法在训练阶段建立一棵决策树以检测并分类Web攻击。但这种检测方法存在检测率和分类率低的缺点。

计算机网络的安全问题与人体免疫系统所遇到的问题具有惊人的相似性，两者都要在不断变化的环境中维持系统的稳定性[7]。基于免疫原理的网络安全技术研究已引起了国内外学者的广泛关注并取得了一些成果[8-12]。本文受生物免疫系统能成功识别未知病原体原理启发，提出了一种基于免疫原理的Web攻击检测方法(Immune-based Approach to Detection of Web attacks，IADW)。

1 模型理论

生物免疫系统中，在进行一次应答时，采用克隆选择原理和高频变异机制进行学习识别，最后留下一定数量的记忆免疫细胞，用来进行二次应答[7]。

收稿时间：2007 – 09 – 07
作者简介：曾金全(1973 –)，男，博士生，主要从事网络安全、人工免疫方面的研究.

受此原理启发，本文提出了一种基于免疫原理的Web攻击检测方法。该方法把从Web攻击数据进行编码，形成抗原集合，将抗原集合提交给免疫学习系统进行学习以产生免疫记忆细胞来检测Web攻击。

1.1 模型架构

IADW模型主要由抗体基因库生成模块、免疫学习模块和检测模块组成，体系架构如图1所示。

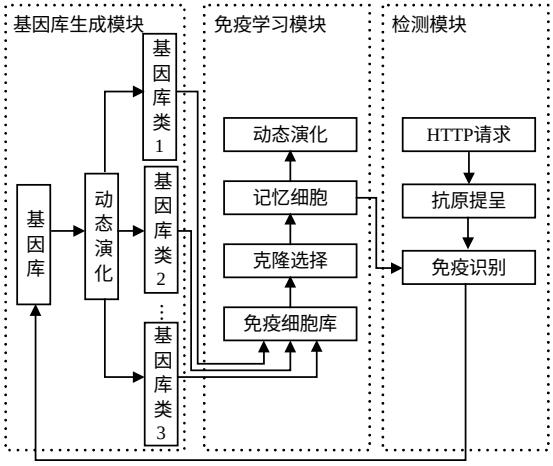

图1 IADW体系架构

抗体基因库是产生优良免疫细胞的基础，抗体基因库的构建一方面可以通过计算机管理员人工输入，另一方面可以通过系统将新识别的Web攻击基因添加到基因库中；免疫学习模块通过克隆选择和高频变异机制促进免疫细胞学习Web攻击模式，生成高亲和力的记忆细胞；检测模块将HTTP请求经过抗原提呈，交由记忆细胞进行识别。

1.2 模型的免疫理论

1.2.1 抗原提呈

模拟免疫系统中的抗原提呈是对HTTP请求进行特征提取，获得抗原的特征。HTTP请求特征分为保留特征和用户特征。在抗原提呈的过程中将HTTP请求中的用户特征用“@”取代，而保留特征不变。如“B?var1=123&var2=25&var3=../dir”转化为“@?@=@&@=@&=../@”，其中“?”，“&”，“=”和“..”是保留特征。

设Ω为HTTP请求特征组成的集合：$\Omega=\bigcup_{i=1}^{\infty}\{<k,w>\}$，其中$k$是HTTP请求特征；$w$是该特征的权重。权重的计算方法为：

$$f(k)=\sigma\lg\left(N\frac{\lambda}{\lambda+\beta}\right) \tag{1}$$

式中 σ是该特征在本条HTTP请求中出现的次数；N是总的HTTP请求数；λ是该特征在同类HTTP请求中出现的次数；β是该特征在其他类HTTP请求中出现的次数。定义抗原集合Ag为：

$$\mathrm{Ag}=\{<a,t>|\,a\in D_1,|\,a\,|=l,t\in D_2\} \tag{2}$$

式中 $D_1=\{<k,w>\}^l$，l为常自然数；a为从HTTP请求中抽取出的由l个请求特征组成的字符串，为抗原决定基；D_2为Web攻击类型集合。

定义正常的HTTP请求为$\mathrm{Self}\subset\mathrm{Ag}$，攻击HTTP请求为$\mathrm{Nonself}\subset\mathrm{Ag}$，满足：

$$\mathrm{Self}\cup\mathrm{Nonself}=\mathrm{Ag},\ \mathrm{Self}\cap\mathrm{Nonself}=\Phi \tag{3}$$

1.2.2 抗体基因库

定义HTTP请求中的特征为抗体基因。定义抗体基因库$\mathrm{Agd}\subseteq\Omega$，不同类的HTTP请求组成了不同的抗体基因库：

$$\mathrm{Agd}=\mathrm{Agd}_1\cup\mathrm{Agd}_2\cup\cdots\cup\mathrm{Agd}_n \tag{4}$$

抗体基因库用于产生检测Web攻击的免疫细胞，为产生更优良的检测已知和未知Web攻击的免疫细胞，需要将新的抗体基因添加到抗体基因库中，其动态演化过程为：

$$\mathrm{Agd}(t)=\begin{cases}\mathrm{Agd}_1(0)\cup\mathrm{Agd}_2(0)\cdots\mathrm{Agd}_n(0) & t=0\\ \mathrm{Agd}(t-1)\cup\mathrm{Agd}_{\mathrm{new}}(t) & t\geq 1\end{cases} \tag{5}$$

式中 $\mathrm{Agd}_i(0)$为初始基因；$\mathrm{Agd}_{\mathrm{new}}(t)$为$t$时刻新增加的基因。

1.2.3 免疫细胞

定义免疫细胞B为：

$$\begin{aligned}B=\{<d_1^k,d_2^k,\cdots,d_l^k,\mathrm{age},\mathrm{aff},t>|\,d_i^k\in\mathrm{Agd}_k,\\ 1\leq k\leq n,1\leq i\leq l,\mathrm{age}\in N,\\ 0\leq\mathrm{aff}\leq 1,0\leq\mathrm{off}\leq 1,t\in D_2\}\end{aligned} \tag{6}$$

式中 d_i^k为免疫细胞抗体基因；Agd_k为抗体基因库；l为基因长度；age为免疫细胞年龄；aff为免疫细胞亲和力；N为自然数；t为免疫细胞能检测的Web攻击类型。

由不同的基因库可以产生不同的免疫细胞：

$$B=B_1\cup B_2\cup\cdots\cup B_n \tag{7}$$

定义记忆细胞集合$M\subset B$为：

$$M=\{m\,|\,m\in B,m.\mathrm{aff}\geq\delta,0\leq\delta\leq 1\} \tag{8}$$

式中 δ为记忆细胞亲和力阈值。为检测未知Web攻击，应从抗体基因库中不断产生新的免疫细胞；同时，不能有效检测Web攻击的免疫细胞应被淘汰，其动态演化过程为：

$$B(t)=\begin{cases}B(0) & t=0\\ B(t-1)\cup B_{\mathrm{new}}(t)-B_{\mathrm{dead}}(t) & t\geq 1\end{cases} \tag{9}$$

$$M(t)=\begin{cases}M(0) & t=0\\ M(t-1)\cup M_{\mathrm{new}}(t)-M_{\mathrm{dead}}(t) & t\geq 1\end{cases} \tag{10}$$

式中 $B_{\mathrm{new}}(t)$是t时刻从抗体基因库中新产生的免疫

细胞；$M_{new}(t)$是t时刻亲和力大于记忆细胞亲和力阈值δ的免疫细胞；$B_{dead}(t)$、$M_{dead}(t)$分别代表免疫细胞和记忆细胞的死亡。式(9)、(10)分别表示免疫细胞和记忆细胞的演化过程。

定义免疫细胞$b^k \in B_k$亲和力函数$f_{aff}(b^k)$为：

$$f_{aff}(b^k)=\frac{\sum_{x^k\in B^k, x^k\neq b^k}\cos(x^k,b^k)}{|B^k|}-f_{pun}(b^k) \quad (11)$$

免疫细胞b^k的亲和力为在同类免疫细胞集合B^k中的平均余弦值，平均余弦值越大，则其代表本类免疫细胞的能力越强，检测Web攻击的能力也越强。同时，为避免免疫细胞检测到其他Web攻击或误报，免疫细胞的惩罚函数$f_{pun}(b^k)$为：

$$f_{pun}(b^k)=\frac{\gamma}{m}\sum_{x^i\in B-B^k,\cos(b^k,x^i)\geq\omega}\cos(b^k,x^i) \quad (12)$$

式中　m是免疫细胞b^k与其他免疫细胞$x^i \in B^i(i\neq k)$的余弦值大于相似性阈值ω的免疫细胞数；γ是惩罚系数。定义免疫细胞$x^i,y^j \in B$的相似性函数为：

$$\cos(x^i,y^i)=\frac{\sum_{h=1}^{l}(x^i.d_h^i.w\times y^j.d_h^j.w)}{\sqrt{\sum_{h=1}^{l}(x^i.d_h^i.w)^2}\sqrt{\sum_{h=1}^{l}(y^j.d_h^j.w)^2}} \quad (13)$$

式中　$x^i.d_h^i.w$和$y^j.d_h^j.w$是免疫细胞x^i和y^j的第h个基因的权重。

1.3　免疫学习

免疫学习分为克隆选择和生成记忆细胞过程。

1.3.1　克隆选择

对免疫细胞$x^k \in B$依据其亲和力大小进行克隆，克隆的数目为：

$$f_{clone\_number}(x^k)=\theta f_{aff}(x^k) \quad (14)$$

对克隆后的免疫细胞x^k以概率$1-x^k$.aff进行变异，高亲和力的免疫细胞由于具有较优良的基因，故变异率较小，反之，变异率较大。将发生了变异的免疫细胞和x^k一起加入到B细胞集合中。

克隆选择算法描述如下：输入：免疫细胞集合B_k大小为m、终止条件Γ；输出：免疫细胞。

```
Begin
随机从基因库 Agd_k 中产生m个免疫细胞并添加到集合B_k中；
计算B_k中免疫细胞的平均亲和力f；
While f<Γ do
  Begin
    For 每个免疫细胞x^k do
      Begin
        clonenumber=f_clone_number(x^k)；
        For i=1 to clonenumber do
          Begin
            mutate^k=x^k
            If 1–mutate^k.aff>Random() Then
              Begin
                对免疫细胞mutate^k基因进行变异；
                将变异后的免疫细胞mutate^k添加到B_k中；
              End
          End
        将免疫细胞x^k添加到B_k中；
      End
    计算B_k中每个免疫细胞的亲和力；
    选择m个免疫细胞组成下一代免疫细胞 B_k′ ；
    //依据免疫细胞亲和力采用轮盘赌的方式选择
    计算B_k中免疫细胞平均亲和力f；
End
```

1.3.2　生成记忆细胞

将免疫细胞集合B中亲和力大于记忆细胞亲和力阈值δ的免疫细胞添加到记忆细胞集合M中。记忆细胞用于检测Web攻击，检测的方法为：将HTTP请求经抗原提呈后，输入到学习好的系统中，检测的结果由ρ个最大亲和力的记忆细胞投票决定。

2　实　验

为检测IADW的性能，将IADW与基于神经网络的IDS-ANN[6]和基于ID3算法的ID3-ids[6]等技术进行对比。为便于比较分析，实验数据集采用文献[6]中的数据集。该实验数据集包括正常HTTP请求和四类攻击HTTP请求：SQL injection、cross site scripting、directory transversal和code injection。在本文的实验中，各参数设置为：免疫细胞集合大小m为50，进化终止条件Γ为0.75，惩罚亲和力阈值ω为0.5，惩罚系数γ为1，记忆细胞亲和力阈值δ为0.5，投票数ρ为3。

表1为IADW与基于神经网络和ID3算法的异常Web攻击检测方法的比较。表1的比较结果表明，本文的方法IADW的性能优于其他异常入侵检测方法。如IADW的检测率为96.61%，高于IDS-ANN的90.44%和ID3-ids的93.65%。与此同时，本文的方法还有较高的分类Web攻击的能力，达到了80.56%，均高于IDS-ANN和ID3-ids的分类能力。在IADW的具体应用中，可将IADW置于HTTP请求代理服务器中，在HTTP请求被Web服务器执行前先执行WEB攻击检测，因此IADW较通过分析Web日志的方法[2-3]，

具有更好的实时性。

表1 IADW与其他异常入侵检测方法比较

方法	检测率/(%)	错误告警率/(%)	漏检率/(%)	分类率/(%)
IDS-ANN	90.44	2.78	6.78	78.50
ID3-ids	93.65	1.64	4.70	77.25
IADW	96.61	2.78	2.78	80.56

从实验结果可以看出，IADW较传统的基于神经网络和ID3算法的Web攻击检测方法，具有更好的学习识别能力和自适应能力，同时也具有很好的实时性。

3 结 论

IADW吸取了生物免疫系统快速学习并识别新病原体之优点，能有效检测针对Web服务器的攻击，克服了传统Web攻击检测方法不能检测未知Web攻击和误报率高、实时性差等缺陷，具有高检测率、高分类率、低漏检率和实时性好等特性，是检测Web攻击的一种有效新途径。

本文的研究工作得到了四川大学青年教师基金(JS20070411506428)的资助，在此表示感谢！

参 考 文 献

[1] KLEIN D. Defending against the wily surfer: web-based attacks and defenses[C]//Proceedings of the USENIX Workshop on Intrusion Detection and Network Monitoring. California, USA: [s.n], 1999.

[2] ADEVA J J G, ATXA J M P. Intrusion detection in web application using text mining[J]. Engineering Applications of Artificial Intelligence, 2007, 20(4): 555-566.

[3] ALMGREN M, DEBAR H, DACIER, M. A lightweight tool for detecting web server attacks[C]//Proceedings of Network and Distributed Systems Security. [S.l.]: [s.n.], 2000: 157-170.

[4] ALMGREN M, LINDQVIST U. Application-integrated data collection for security monitoring [C]//RAID 2001, LNCS 2212. Berlin: Springer-Verlag, s2001: 22-36.

[5] VIGNA G, ROBERTSON W, KHER V, et al. A stateful intrusion detection system for World-Wide Web servers[C]//Proceedings of the Annual Computer Security Applications Conference. [S.l.]: [s.n.], 2003: 34-43.

[6] GARCIA V H, MONROY R, QUINTANA M. Web attack detection using ID3[C]//Proceedings of the 2nd IFIP International Symposium on Professional Practice in AI. [S.l.]: [s.n.], 2006: 323-332.

[7] 李 涛. 计算机免疫学[M]. 北京: 电子工业出版社, 2004.

[8]焦李成, 杜海峰. 人工免疫系统进展和展望[J]. 电子学报, 2003, 31(10): 1540-1548.

[9] LI T. An immune based dynamic intrusion detection model [J]. Chinese Science Bulletin, 2005, 50(17): 1912-1919.

[10] DASGUPTA D. An immunity-based technique to characterize intrusions in computer networks[J]. IEEE Transactions on Evolutionary Computation, 2002, 6(3): 281-291.

[11] HARMER P K, WILLIAMS P D, GUNSCH G H, et al. An artificial immune system architecture for computer security applications[J]. IEEE Transactions on Evolutionary Computation, 2002, 6(3): 252-280.

[12] FORREST S, HOFMEYR S, SOMAYAJI A. Computer immunology[J]. Communications of the ACM, 1997, 40(10): 88-96.

编 辑 漆 蓉

(上接第1205页)

参 考 文 献

[1] PHAM V A, KARMOUCH A. Mobile software agents: An overview[J]. IEEE Communications Magazine, 1998, 36(7): 26-37.

[2] GREENBERG M S, BYINGTON L C, HARPER D G. Mobile agents and security [J]. IEEE Communications Magazine, 1998, 36(7): 76-85.

[3] TARDO J, VALENTE L. Mobile agent security and telescript[C]//In: Proceedings of COMPCON Spring '96. Santa Clara: IEEE Computer Society press, 1996.

[4] WALSH T, PACIOREK N, WONG D. Security and reliability in Concordia TM[C]//Proceedings of the Thirty-First Hawaii International Conference on System Sciences. Hawaii: [s.n.], 1998.

[5] JANSEN W A. Countermeasures for mobile agent security [J]. Computer Communications, 2000, 23(17): 1667-1676.

[6] KARJOTH G, LANGE D, OSHIMA M. A security model for aglets[J]. IEEE Internet Computing, 1997, 1(4): 68-77.

[7] 王汝传, 徐小龙, 郑晓燕, 等. 移动代理安全机制的研究[J]. 计算机学报, 2002, 25(12): 1294-13011.

[8] 杨 博, 杨 鲲, 刘大有. 面向网络管理的移动主体安全设施[J]. 软件学报, 2003, 14(10): 1761-1767.

[9] 狄晓龙, 庄镇泉, 张仕山. 移动主体技术的安全机制研究[J]. 小型微型计算机系统, 2004, 25(4): 493-496.

[10] GONG Li. Java 2平台安全技术-结构、API设计和实现[M]. 机械工业出版社, 2000.

编 辑 熊思亮