

云模式下基于危险理论的网络攻击态势察觉模型

孙飞显^{1, 2}, 李 涛²

(1 中原工学院 计算机学院, 河南 郑州 450007; 2 四川大学 计算机学院, 四川 成都 610065)

摘 要: 为探索大规模、复杂网络的安全态势要素获取新途径, 提出了一种云模式下基于危险理论的网络攻击态势察觉模型. 效仿“细胞受损或非正常死亡产生危险信号, 并由危险信号诱发免疫应答”机理, 在定义计算机网络到危险模式映射后, 用云模型的不确定性推理方法, 通过构造云图和设计规则发生器, 建立计算机网络定量安全状态参数转化为定性危险级别的云模型; 依据危险等级生成危险信号, 并由其激活由云端实现的基于免疫危险理论的网络攻击态势察觉. 理论分析和验证实验结果表明该模型有效, 为大规模、复杂计算机网络的安全态势感知提供了新思路.

关键词: 人工免疫; 危险理论; 网络攻击; 态势察觉; 云模式

中图分类号: TP393; TP18

文献标识码: A

文章编号: 1000-7180(2014)04-0006-04

Danger Theory Based Model for Network Attacks Situation Perception with Cloud Method

SUN Fei-xian^{1, 2}, LI Tao²

(1 School of Computer Science, Zhongyuan University of Technology, Zhengzhou 450007, China;

2 School of Computer Science, Sichuan University, Chengdu 610065, China)

Abstract: To explore new ways of getting security situational factors for complex large-scale networks, a danger theory based model for network attacks situation perception with cloud method is proposed. The proposed model follows the danger model principles of cells dying unnaturally or distressed may release an alarm signal, and the adaptive immune response stimulated by danger signal. With the establishment of mapping the computer networks to immune danger model, the model is built by using the uncertainty reasoning method of cloud computing. Within the model, the quantitative safety state parameters, such as resource occupancy rate, network traffic are translated into different qualitative risk levels by cloud generators. Network attacks' detection is activated by danger signal, which is generated by different risk level. Theoretical analysis and simulation results show that the presented model is valid. Thus, it provides a good solution to large-scale computer network security situation awareness.

Key words: artificial immunity; danger theory; network attack; situation awareness; cloud method

1 引言

当今, Internet 规模日益膨胀, 获取、理解、评估和呈现大规模、复杂的计算机网络中设备运行状况、网络及用户行为的当前状态, 并据此预测未来安全状况, 成为网络安全态势感知的研究热点^[1-3]. 同时, “棱镜门”事件再次触痛网络安全. 为探索大规模、复杂网络的安全态势要素获取新途径, 受人类自然免

疫机理启发, 提出了一个云模式下基于危险理论的网络攻击态势要素察觉模型(danger theory based model for network attacks situation perception with cloud method, dtcm-NASP).

2 模型理论

2.1 设计思想

依照危险理论“细胞受损或非正常死亡产生危

收稿日期: 2013-07-28; 修回日期: 2013-09-20

基金项目: 国家自然科学基金项目(61173159); 河南省教育厅科学技术研究重点项目(13B520305)

险信号并由危险信号诱发免疫应答”机理建立计算机网络到免疫危险理论的映射,基于网络方式部署的分布式云端通过人工免疫识别方法实时检测网络攻击,并依据资产重要性、攻击类别、攻击强度、持续时间、危害程度等定量的安全参数计算并发出不同级别的定性危险信号,通过接收、存储、融合各云端的危险信号进而察觉大规模网络正在遭受的攻击,并在此基础上建立云模式下基于危险理论的网络攻击态势察觉模型。

2.2 相关映射

dctm-NASP 中定义的计算机网络到危险理论的映射如表 1 所示。

表 1 Idtm-NASP 到 DT 的映射

危险理论	计算机网络
细菌/病毒	计算机网络攻击
细胞非正常死亡/凋亡	网络瘫痪或拒绝服务
危险信号	网络活动的异常参数
危险区域	遭受威胁的网络空间
抗原	经过提呈的 IP 数据包
抗体	网络攻击检测器
抗原提呈细胞 APC	IP 包捕获与分析单元

2.3 术语定义

定义 1 在 dctm-NASP 中,定义人工免疫抗体 (antibody, ab) 为形如 $ab = ab_1 + ab_2 + ab_3 + \dots + ab_n$ 的二进制串,其中“+”表示连接, ab_i 表示抗体 ab 的第 i 个片段, n 表示片段的总数。

定义 2 在 dctm-NASP 中,将抗原 (antigen, ag) 定义为从 IP 包中抽取而且结构与 ab 一致的二进制位序列。

定义 3 dctm-NASP 中的危险信号是指计算机网络遭受威胁而临近瘫痪或拒绝服务时所发出的可监测的信号,模拟危险理论中免疫细胞受损或非正常死亡时的免疫触发条件。

定义 4 dctm-NASP 中的云端 (记为 s) 定义为与时间 t 相关的二元组 $s = (d, \text{dangersignal}(t))$,检测器 $d = (ab, \text{age}(t), \text{matchnum}(t_0, t), \text{ds}(t))$,云端 s 在 t 时刻产生的危险信号记为 $s, \text{danger signal}(t)$ 。其中, $\text{age}(t)$ 、 $\text{matchnum}(t_0, t)$ 、 $\text{ds}(t)$ 分别表示云端 s 中检测器 d 在 t 时刻的年龄、 $t - t_0$ 时间段内检测到网络攻击的次数、危险信号大小。

定义 5 设 S 是一个用数值表示的定量论域空

间, C 是 S 上的定性概念,如果存在 $x \in S$, 且 x 是 C 的一次随机实现, x 对 C 的确定度 $\mu(x) \in [0, 1]$ 是有稳定倾向的随机数: $\mu: S \rightarrow [0, 1], \forall x \in S \quad x \rightarrow \mu(x)$, 则 x 在 S 上的分布称为云 (Cloud), 每一个 x 称为一个云滴, 且 x 的属性通过其数学期望 (Ex)、熵 (En) 和超熵 (He) 来表示。

定义 6 为定性描述计算机网络的危险级别, 定义五元组 $SVC = (f_{T-n}(s_i), Ex, En, He, \sigma)$, 其中 $f_{T-n}(s_i)$ 表示云端 s 的第 i ($1 \leq i \leq N$) 个安全参数的采样值, n, T 和 σ 分别表示采用次数、采样间隔和隶属度阈值。

2.4 模型体系

在大规模、复杂的计算机网络中, 表征计算机网络安全状态的特征信息包括被监视网络的延迟时间、丢包率、带宽、流量以及被监视主机的 CPU 占用率、内存占用率、可用交换空间的数量、I/O 使用情况等, 这些安全参数都以定量方式存在, 且参数来源范围广、数量多。

为将上述定量安全参数转换为“很危险”、“危险”、“较危险”、“较安全”、“安全”的定性态势级别, dctm-NASP 利用云模型的不确定性推理思想及逆向云发生器将计算机网络中定量的安全参数转化成定性的危险级别, 模型的体系结构如图 1 所示。

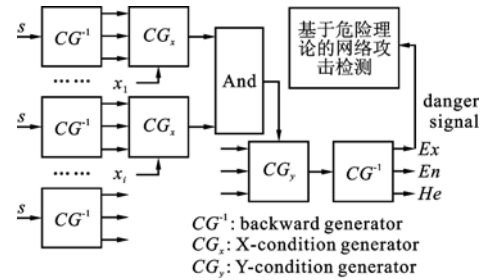


图 1 dctm-NASP 的体系结构

在图 1 中, CG^{-1} 表示逆向云发生器, 其输入端来自云端 s , CG_x 、 CG_y 分别表示前件云发生器和后件云发生器, 期望值 Ex 用于提升安全参数的粒度, 进而满足网络安全态势感知的需要。

2.5 粒度提升

设 $f(s(t))$ 表示 t 时刻云端 s 感知到的安全状态参数, σ_s 表示云端 s 的隶属度阈值, dctm-NASP 中定义的隶属度 $\mu(f(s(t)))$ 如式 (1) 所示。

$$\mu(f(s(t))) = e^{-\frac{(f(s(t)) - Ex)^2}{2En^2}} \quad (1)$$

为适合大规模、复杂的计算机网络安全态势察

觉需要, dtcm-NASP 中定义 t 时刻云端 s 是否发出危险信号的条件如下:

$$dc(s(t)) = \begin{cases} \text{True} & \mu(f(s(t))) > \sigma_s \\ \text{False} & \mu(f(s(t))) \leq \sigma_s \end{cases} \quad (2)$$

在式(2)中, $dc(s(t)) = \text{True}$ 表示 t 时刻云端 s 要发出危险信号。

在 dtcm-NASP 中, 连续采样宏观网络的延迟时间、丢包率、带宽、流量等安全参数, 用 Ex 作为安全参数的代表值, 并采用算法 1 进行安全参数粒度的提升。

算法 1 dtcm-NASP 的安全参数粒度提升算法。

输入: t 时刻之前云端 s 采样到的 n 组延迟时间、丢包率、带宽、流量(记为 $f(s([t] - i * T), i \in [0, n-1])$).

输出: Ex 、 En 和 He .

Begin

Step 1. for ($i = 0$; read $f(s([t] - i * T); i$ ++);

Step 2. $Ex = \frac{1}{n} \sum_{i=1}^n f(s([t] - i * T));$

Step 3. $En = \sqrt{\frac{\pi}{2}} \times \frac{1}{n} \sum_{i=1}^n |f(s([t] - i * T) - Ex|;$

Step 4. 计算 $k^2 = \frac{1}{n-1} \sum_{i=1}^n (f(s([t] - i * T) - Ex)^2;$

Step 5. $He = \sqrt{k^2 - En^2};$

End.

2.6 检测流程

dtcm-NASP 的网络攻击检测流程如图 2 所示。

在图 2 中, δ 表示亲和力阈值, 亲和力计算函数 af 的计算方法如式(3)。

$$af(s, d, ab, ag) = 1 - \frac{\sqrt{\sum_{i=1}^n (s, d, ab_i - ag_i)^2}}{n} \quad (3)$$

式中 s, d, ab_i 、 ag_i 分别表示抗体 s, d, ab 和抗原 ag 的

第 i 个片段(共 n 个片段), $\sqrt{\sum_{i=1}^n (s, d, ab_i - ag_i)^2}$ 表示 s, d, ab 和 ag 之间的欧氏距离。

2.7 危险信号计算

在 dtcm-NASP 中, 攻击网络的危险状况与网

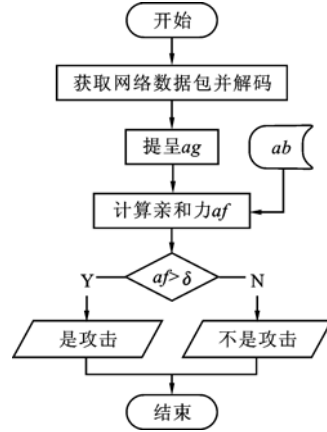


图 2 网络攻击检测流程

络攻击种类、攻击强度和攻击的持续时间等因素相关。据此, dtcm-NASP 中单个抗体 s, d, ab 及云端 s 在 t 时刻的危险信号的生成及量化计算方法分别如式(4)、(5)所示。

$$s, d, ds(t) = \frac{s, d, \text{matchnumber}(t_0, t)}{s, d, \text{age}(t) - s, d, \text{age}(t_0)} \quad (4)$$

$$s, \text{dangersignal}(t) = \sum_{i=1}^m (\varphi(s, d_i, ab) \times s, d_i, ds(t)) \quad (5)$$

式中, m 表示云端 s 中抗体的数量, $\varphi(s, d_i, ab)$ 表示第 i 个检测器对应抗体所检测到的网络攻击的危险程度。

在 dtcm-NASP 中, 云端 s 中的检测器 s, d_i 在 t 时刻的年龄 $\text{age}(t)$ 和 $t - t_0$ 时间段内检测成功次数 $\text{matchnum}(t - t_0)$ 的计算方法分别如式(6)和式(7)所示。

$$s, d_i, \text{age}(t) = s, d_i, \text{age}(t-1) + 1$$

$$\text{iff } af(s, d_i, ab, ag) = \text{any} \quad (6)$$

$$s, d_i, \text{matchnumber}(t) = s, d_i, \text{matchnumber}(t-1) + 1$$

$$\text{iff } af(s, d_i, ab, ag) > \delta \quad (7)$$

式(6)说明只要检测器 s, d_i 中的抗体进行了一次抗原识别, 无论是否检测到网络攻击 s, d_i 的年龄均增加 1; 式(7)表示只有在 s, d_i 的检测到网络攻击情况下 s, d_i 的匹配次数才增加 1。

3 模型分析与实验验证

3.1 模型分析

该模型在理论上是可行的, 原因在于: 第一, 模型通过抽取 IP 包的特征字段而得到抗原, 这种结构与由基因片段组成的自然免疫抗体的结构相似, 进

行匹配是可行的. 第二,模型中人工免疫抗体的注入过程相当于疫苗接种,这不仅符合现实,而且真实可行. 第三,该模型是基于人类自然免疫系统的原理而设计的,抗体的变异特性可以保证本文所设计的模型在理论上具有识别未知网络攻击的能力. 第四,文中式(3)给出的 s 、 d 、 ab 与 ag 用欧氏距离计算亲和力的途径满足人工免疫系统的设计要求. 第五,文中式(4)、(5)给出的危险信号的定量计算办法不仅考虑到了网络攻击的类别(由参数 φ 实现),而且将攻击强度和攻击持续的时间(分别由 $matchnumber$ 和 age 决定),符合真实网络攻击环境的需要. 最后,模型中危险信号数值大,表明该区域为“网络疫情”的重灾区;定量的危险信号还可以为动态呈现某一种网络攻击或全部网络攻击的态势图提供了数据支持.

3.2 实验验证

为验证 dtcm-NASP 的可行性和效率,作者在经典的 kddcup99 数据集上进行了测试实验. 在实验中,作者依据入侵检测系统 Snort 检测规则,提取可用的字段形成本模型中抗体的基因片段,并将最后得到的人工免疫抗体通过人工注入的方式加载到原型系统中进行实验验证.

为了进行有针对性的验证实验,我们在开启路由器广播功能、调整路由器的网络出口过滤功能、允许网络主机对 IP 广播请求进行响应的前提下,分别对普通 PC、FTP 和 WWW 服务器进行了 smurf 和 land 攻击验证实验. 可以看出 dtcm-NASP 察觉到的结果与网络攻击实际情况相符,即针对网络的攻击强度和持续时间越长,产生的危险信号就越大;当

攻击强度迅速变弱时,网络面临的风险也会变小,但下降的幅度要相对慢于攻击强度变化趋势,这符合自然免疫系统的一般规律,利于网络对短时间内再次发生的同类攻击敏感.

4 结束语

本文将人类自然免疫系统的危险理论用于网络安全领域,完善了以往基于 SNS 的识别机制,理论分析和实验结果表明该模型有效,弥补了基于误用和基于异常的网络入侵检测技术的不足,对健全信息安全保障体系,有积极的理论指导意义和实用价值.

然而,该模型尚存在一定的不足,如抗体的数量及抗体的完备性会影响察觉结果的准确性. 同时,模型中 af 函数中的权重、阈值的选取也需更深入地实验.

参考文献:

- [1] 席荣荣, 云晓春, 金舒原, 等. 网络安全态势感知研究综述 [J]. 计算机应用, 2012, 32(1): 1-4, 59.
- [2] Brancik K, Ghinita G. The optimization of situational awareness for insider threat detection [C]//Proceedings of the 1st ACM Conference on Data and Application Security and Privacy. San Antonio: ACM, 2011: 231-235.
- [3] 龚正虎, 卓莹. 网络态势感知研究 [J]. 软件学报, 2010, 21(7): 1605-1619.

作者简介:

孙飞显 男, (1970—), 博士, 副教授. 研究方向为网络安全技术与应用、人工免疫.