

层次化网络安全威胁态势评估技术研究^{*}

朱丽娜¹, 张作昌¹, 冯 力²

(1. 广西财经学院 计算机与信息管理体系, 南宁 530003; 2. 武汉数字工程研究所, 武汉 430074)

摘 要: 为了评估大规模网络系统的安全状态, 针对机密性、完整性和可用性, 采用层次化分析方法, 建立一种网络安全威胁态势量化评估模型。该模型包括一套分为服务、主机、子网、全网四层的安全威胁态势指标和各项指标的量化计算方法。实验结果表明, 该模型具有较好的可操作性, 能够准确、直观地刻画网络系统的安全演化过程。

关键词: 网络安全威胁态势; 态势评估; DREAD 模型; Markov 模型; D-S 证据理论

中图分类号: TP309 **文献标志码:** A **文章编号:** 1001-3695(2011)11-4303-04

doi:10.3969/j.issn.1001-3695.2011.11.082

Research on hierarchical network security threat situation assessment

ZHU Li-na¹, ZHANG Zuo-chang¹, FENG Li²

(1. Dept. of Computer & Information Management, Guangxi University of Finance & Economics, Nanning 530003, China; 2. Wuhan Digital Engineering Institute, Wuhan 430074, China)

Abstract: In order to estimate the security situation of large-scale network, this paper aimed at confidentiality, integrality and availability, adopted hierarchical analysis, and put forward a quantitative evaluation model for network security threats situation. This model included a suit of security threat situation indices composed of service, host, subnet and whole network, and quantitative calculation method for each index. Experimental results show the easy operation of this model, and it depicts the safety evolution process of network system accurately and intuitively.

Key words: network security threat situation; situation assessment; DREAD model; Markov model; D-S evidence theory

随着攻击技术的变异提升, 仅仅对已经发生的攻击进行报警和拦截不再满足人们对网络安全的需求, 需要对黑客攻击、恶意代码等安全威胁进行分析, 对网络的安全状况进行评估, 对网络安全状况的变化趋势进行预测, 以争取在大规模攻击的产生或准备阶段就实施安全防护。在这种形势下, 网络安全态势评估技术应运而生, 它是新型网络安全防御体系的重要组成部分, 也是目前网络安全领域的研究热点之一。网络安全态势是对网络运行状况的宏观反映, 它的原始数据来源于被评估网络的网管设备、网络安全设备、网络监管设备等, 通过对这些数据进行数学处理、整合, 产生可以反映网络运行状况的数值或图表。

1 相关研究

Ortalo 等人^[1] 基于 COPS 数据采用权限图理论建模系统漏洞, 使用 Markov 模型计算攻击者击败系统安全目标需要付出的代价, 定量给出系统安全的演化过程; Bass^[2] 应用多传感器数据融合技术建立了网络空间态势感知框架, 通过推理识别出入侵者身份、速度、威胁性和入侵目标; Bruce 等人^[3] 开发了基于问卷调查方式的态势评估系统 SSARE, 实现了入侵检测、态势评估和响应评估的有机结合, 但信息获取方式较单一; Porras 等人^[4] 充分考虑了攻击发生的网络环境因素, 提出 Mission-Impact 方法实时评估安全事件的威胁程度; Hariri 等人^[5] 基于

网络性能度量指标, 评估网络攻击对系统安全的影响, 仅适用于 DoS 类攻击; Gorodetsky 等人^[6] 提出了基于异步数据流的态势评估方法, 利用多代理检测异常的数据流并进行分析, 但忽略了网络本身的特性; Yegneswaran 等人^[7] 提出了基于 Honey-nets 评估网络安全态势的方法, 根据报警构建态势曲线, 但只在大规模病毒或蠕虫爆发时才能呈现明显的效果; Mehta 等人^[8] 使用贝叶斯网络计算攻击图中各安全状态的转换概率, 对攻击场景进行威胁评估; Arnes 等人^[9] 使用隐马尔可夫模型描述主机的安全状态和转换关系, 通过状态转换概率评估攻击的威胁程度。

国内有关网络安全态势评估的研究起步较晚。中科院软件所冯登国等人^[10] 对信息安全风险评估领域的安全模型、评估标准、评估方法、评估工具等进行了综述, 主要关注通过漏洞扫描等技术、依据评估标准或依赖量化漏洞因素的评估指标进行评估; 华中科技大学肖道举等人^[11] 基于服务在系统中所占的比重和漏洞威胁度给出了一个综合评估模型, 评估目标系统所提供服务的风险, 定量分析目标系统的安全状况, 但其侧重于安全隐患评估; 西安交通大学李辉等人^[12] 根据攻击报告结合历史态势数据, 分析当前系统遭受入侵的严重程度; 西安交通大学陈秀真等人^[13] 基于 IDS 报警和网络性能指标, 结合服务、主机的重要性及网络系统结构, 提出自下而上、先局部后整体的层次化安全威胁态势量化评估方法, 但没有考虑攻击间的

收稿日期: 2011-04-28; **修回日期:** 2011-05-26 **基金项目:** 国防“十一五”预研资助项目 (C0820061362-06); 广西教育厅科研资助项目 (201012MS116)

作者简介: 朱丽娜 (1981-), 女, 安徽淮北人, 讲师, 博士, 主要研究方向为入侵检测与网络安全态势评估 (zhulina81@gmail.com); 张作昌 (1976-), 男, 讲师, 硕士, 主要研究方向为信息系统与信息安全; 冯力 (1974-), 男, 高级工程师, 博士, 主要研究方向为入侵检测与网络预警。

关联;北京邮电大学汤永利等人^[14]用信息熵度量信息系统风险,引入故障树分析法把定性分析与定量计算相结合来评估系统风险;中国科学技术大学韦勇等人^[15]使用改进的 D-S 证据理论融合多源信息计算网络安全态势,通过时间序列分析得到安全趋势,但没有考虑系统日志间的关系,不适用于 DoS 类攻击。

上述工作在安全隐患态势评估方面,局限于单个主机范围,不适用于大规模网络系统;在安全威胁态势评估方面,没有关联报警,或虽然提出了安全态势感知的概念,建立了安全态势感知框架,但没能给出具体的系统实现,无法提供直观的态势变化曲线,态势评估的精度也有待提高。

2 层次化网络安全威胁态势量化评估

2.1 安全威胁态势指数定义

依据 CC 涉及的三种保护类型(机密性、完整性、可用性),提出一套分层安全威胁态势指标,重点评估安全事件对于信息的机密性、完整性和服务的可用性所造成的威胁。

定义 1 服务层态势指数(service-level situation, SS)。它是指某种服务在一定时间内遭受攻击,主机信息的机密性和完整性被破坏的程度。使用微软提出的 DREAD(damage potential & reproducibility & exploitability & affected users & discoverability)模型^[16]评估单次攻击造成的威胁严重程度。服务层态势指数的取值范围为[0,1]。

定义 2 主机层机密完整性态势指数(host-level confidentiality & integrity situation, HS_{CI})。它是指单台主机在一定时间内遭受攻击,主机信息的机密性和完整性被破坏的程度。由于攻击步骤之间存在依赖关系,这里基于服务层报警关联的结果,使用 Markov 模型来评估复合攻击造成的威胁严重程度。主机层态势指数的取值范围为[0,1]。

定义 3 主机层可用性态势指数(host-level availability situation, HS_A)。它是指单台主机在一定时间内遭受攻击,主机所提供服务的可用性被破坏的程度。采用 D-S 证据推理理论融合网络带宽耗用、响应时延等网络性能参数得到^[17]。主机层可用性态势指数的取值范围为[0,1]。

定义 4 主机层态势指数(host-level situation, HS)。它是指单台主机在一定时间内遭受攻击,主机信息的机密性、完整性和服务的可用性被破坏的程度。该指数由主机层机密完整性态势指数和主机层可用性态势指数加权综合得到。假设信息机密性、完整性对应的权重为 ω_{CI} ,服务可用性的权重为 ω_A ,其中, $\omega_{CI} \in [0,1]$, $\omega_A \in [0,1]$,且 $\omega_{CI} + \omega_A = 1$,则主机层态势指数的计算如式(1),取值范围为[0,1]

$$HS = \omega_{CI} HS_{CI} + \omega_A HS_A \quad (1)$$

定义 5 子网层态势指数(LAN-level situation, LS)。它是指子网在一定时间内遭受攻击,子网信息的机密性、完整性和服务的可用性被破坏的程度。由主机层态势指数加权综合得到,假设子网中有 m 台主机,对应的权重为 $\alpha_i (i=1,2,\dots,m)$, $\alpha_i \in [0,1]$ 且 $\sum \alpha_i = 1$,则子网层态势指数的计算如式(2),取值范围为[0,1]

$$LS = \sum_{i=1}^m (\alpha_i \times HS_i) \quad (2)$$

定义 6 全网层态势指数(WAN-level Situation, WS)。它是指全网在一定时间内遭受攻击,全网信息的机密性、完整性

和服务的可用性被破坏的程度。由子网层态势指数加权综合得到,假设全网由 n 个子网组成,对应的权重为 $\beta_i (i=1,2,\dots,n)$, $\beta_i \in [0,1]$ 且 $\sum \beta_i = 1$,则全网层态势指数的计算如式(3),取值范围为[0,1]

$$WS = \sum_{i=1}^n (\beta_i \times LS_i) \quad (3)$$

2.2 层次化网络安全威胁态势评估模型

按照规模和拓扑结构,网络系统可分解为全网、子网、主机和服务四层,而绝大多数攻击都针对主机所提供的特定服务发起的。层次化网络安全威胁态势评估模型如图 1 所示。该模型采取“自下而上、横向关联、先局部后整体”的评估策略。以 IDS 报警和漏洞扫描结果作为原始数据,在服务层评估单次攻击对信息的机密性和完整性造成的威胁严重程度。DoS 类攻击造成的危害动态地表现在主机层,因此,主机层的态势指数由两个部分组成,一个结合发生在单台主机上的攻击路径,评估攻击对信息的机密性和完整性造成的威胁严重程度;一个评估攻击对服务的可用性造成的威胁严重程度。子网层态势指数等于各主机层态势指数的加权和。全网层态势指数等于各子网层态势指数的加权和。

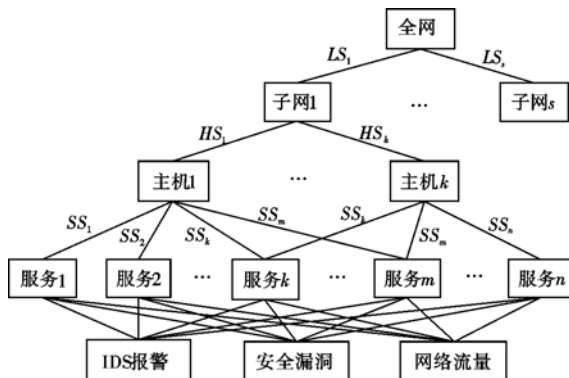


图1 层次化网络安全威胁态势评估模型

2.3 评估参数赋值

在计算各层安全威胁态势指数的过程中,需要确定主机权重、主机层机密完整性态势权重、主机层可用性态势权重、子网权重等四个参数。参数的确定涉及服务器类型、服务器数据的重要性等诸多因素,没有统一的标准,需要网络安全管理员根据具体的环境,制定合适的评价准则。

1) HS_{CI}和 HS_A 的权重

由于工作内容存在差异,各主机关注的安全属性可能不同,由网络管理员根据主机的实际工作特点分配 ω_{CI} 与 ω_A 。

2) 主机的权重

确定主机的重要性属于资产评估的范畴,需要依据特定的标准来划分主机的等级,如密级、设备角色、访问量等。

3) 子网的权重

子网的重要性由其内部主机的重要性决定,重要程度高的主机数量越多,相应子网在全网中的地位就越高,即子网越重要。假设全网被划分为 n 个子网,全网的主机被划分为 m 个等级,用 N_{ij} 表示子网 i 中等级为 j 的主机个数,则子网 i 的权重计算如式(4):

$$\beta_i = \frac{\sum_{j=1}^m (\alpha_j N_{ij})}{\sum_{i=1}^n \sum_{j=1}^m (\alpha_j N_{ij})} \quad (4)$$

2.4 态势指数计算

2.4.1 服务层态势指数

采用 DREAD 模型评估服务面临的威胁。结合主机系统存在的漏洞和安全设备的响应,参照 $D、R、E、A、D$ 五项指标对报警打分(取值只能为 1、2、3),按照式(5)计算攻击造成的威胁严重程度。以两次尝试获取数据库服务器上信息为例,第一次端口访问被防火墙阻止,而第二次未被阻止,两次攻击的 DREAD 分值及服务层态势指数取值如表 1。由于 DREAD 模型的总分值在 $[6,54]$ 之间,而服务层态势指数的取值范围为 $[0,1]$,采用线性函数转换进行归一化。

Risk = Probability of Occurrence × Business Impact =
$$(R + E) \times (D + A + D)$$

表 1 DREAD 应用实例

攻击描述	D	R	E	A	D	Risk	SS
端口访问被阻止	1	1	1	3	3	14	0.167
端口访问未被阻止	2	3	2	3	3	40	0.708

虽然上述两次攻击的类型相同,但第一次失败,第二次成功。表 1 说明 DREAD 模型不仅能定量地描述攻击的威胁严重程度,而且能区别对待成功和失败的攻击,使评估结果更加合理。基于 DREAD 模型得到的服务层态势为准确评估主机和网络系统的安全威胁态势奠定了良好的基础。

2.4.2 主机层机密完整性态势指数

采用 Markov 模型计算攻击路径的累积威胁严重程度。从安全目标的初始正常状态沿攻击路径到攻击结束的末状态,计算主机层机密完整性态势,存在下述三种情况:

a) 不存在攻击路径,则

$$HS_{CI} = 0$$

b) 存在一条包含 n 步攻击的攻击路径,则

$$HS_{CI} = \frac{\sum_{i=1}^n SS_i}{n}$$

(7)

c) 存在多条攻击路径,则

$$\begin{cases} HS_{S_j} = \frac{\sum_{S_i \in \text{Into}(S_j)} [P_{S_i S_j} \times (SS_{ij} + HS_{S_i})]}{|\text{Into}(S_j)|} \\ P_{S_i S_j} = \frac{SS_{ij}}{\sum_{S_k \in \text{Into}(S_j)} SS_{kj}} \end{cases}$$

(8)

其中: HS_{S_j} 表示主机状态为 S_j 时的主机层机密完整性态势; $\text{Into}(S_j)$ 表示主机状态转换到 S_j 的前一刻所处的状态集合; $|\text{Into}(S_j)|$ 表示集合中的主机状态个数; $P_{S_i S_j}$ 表示主机状态从 S_i 转换到 S_j 的概率,假设攻击者优先选择威胁程度高的攻击; SS_{ij} 表示主机状态从 S_i 转移到 S_j 所受攻击的 DREAD 分值;初始正常状态时, $HS_{S_0} = 0$ 。

2.4.3 主机层可用性态势指数

基于网络带宽耗用 C_{bw} 、响应时间延迟 C_{rt} 等网络性能参数,使用 D-S 证据推理综合评估服务可用性被破坏的严重程度。 C_{bw} 和 C_{rt} 从不同的角度衡量主机对合法用户请求的服务可用性,取值越大,说明主机所提供服务的可用性越差。把 C_{bw} 和 C_{rt} 作为两条服务可用性证据,经过 D-S 证据推理理论融合得到的评估结果比依赖单条证据更加准确。定义判别框 $\Omega = \{\text{Safe}, \text{Unsafe}\}$,分别表示系统的安全、不安全状态,基本概率分配函数如式(9):

$$m_1(\{\text{Safe}\}, \{\text{Unsafe}\}) = (1 - C_{bw}, C_{bw})$$
$$m_2(\{\text{Safe}\}, \{\text{Unsafe}\}) = (1 - C_{rt}, C_{rt})$$

(9)

经过证据合并,得到主机层可用性态势是上述局部证据的函数,如式(10):

$$HS_A = m(\{\text{Unsafe}\}) = \frac{\sum_{X \cap Y = \{\text{Unsafe}\}} m_1(X) m_2(Y)}{\sum_{X \cap Y \neq \emptyset} m_1(X) m_2(Y)} = \frac{C_{bw} C_{rt}}{C_{bw} C_{rt} + (1 - C_{bw})(1 - C_{rt})}$$

(10)

3 实验与分析

3.1 实验设计

1) 实验环境

实验网络由三个网段组成,主机被划分为非密、秘密、机密和绝密四个等级,各网段的主机等级分布如表 2,如图 2 所示。其中,5 网段 IP 地址为 133 的主机是态势评估服务器,装有 SQL Server 2000、Winpcap 和 Snort,通过分析来自路由器的 Netflow 镜像检测各网段遭受的攻击;所有主机均装有漏洞检测代理,定期检测系统漏洞,并把结果上传至服务器的数据中心;使用 Spirent ThreatEx/2700 发起攻击。

表 2 全网主机等级分布

主机数	$\alpha_1 = 0.1$	$\alpha_2 = 0.2$	$\alpha_3 = 0.3$	$\alpha_4 = 0.4$
5 网段	0	0	4	0
6 网段	7	0	0	0
7 网段	0	0	1	2

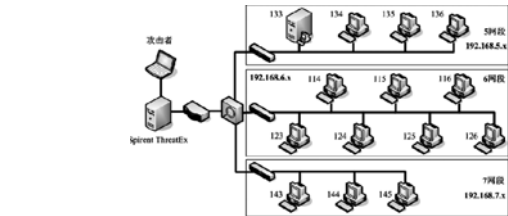


图2 层次化安全威胁态势评估实验网络

2) 攻击案例

模拟两个攻击:a) MSsqlDoS 攻击;b) Nmap ICMP Netmask Request Probe 和 Nmap ICMP Ping 攻击。其中,案例 a) 与服务的可用性相关,是单步攻击;案例 b) 由两个攻击步骤组成,属于简单的复合攻击。同一攻击对不同主机造成的威胁程度可能不同。例如,5 网段 IP 地址为 133 的主机提供 SQL Server 服务,而遭受相同攻击的 6. 123 和 7. 143 主机不提供该服务,因此,MSsqlDoS 攻击对于前者的 DREAD 分值要大一些。各次攻击的 DREAD 分值如表 3 所示。

表 3 实验攻击案例

攻击名称	目标类型	攻击描述	受害主机	DREAD 值
MSsqlDoS	Database	伪造源地址,向服务器的 1434 端口发送大量 UDP 包,服务器的回复得不到响应而造成拒绝服务	5. 133	0.778
			6. 123	0.185
			7. 143	0.185
Nmap ICMP Netmask Request Probe	Protocol	由 Nmap 端口扫描程序发送 ICMP 子网掩码请求,查找在线主机	全网主机	0.444
Nmap ICMP Ping	Protocol	由 Nmap 端口扫描程序发送 ping 包,发现在线主机的脆弱端口	全网主机	0.556

3.2 结果分析

3.2.1 MSsqlDoS 攻击

部分主机遭受攻击,由于提供的服务不同,同一攻击造成的威胁程度可能不同。MSsqlDoS 攻击持续 20 min,每 12 s 采样一次,攻击数据包的发送时间间隔服从指数分布。受害主机的带宽耗用和响应时间延迟如图 3 所示。由于带宽使用上限非常大,在模拟攻击的前 20 min 内,带宽耗用的百分比变化不明显;由于服务器 Ping Reply 得不到响应,数据包缓冲区可用资源减少,服务器对外界正常连接的响应时间增加。

1) 主机层态势

根据式(7)(10)计算 HS_{Ci} 和 HS_A ,受害主机 5.133 的 HS_{Ci} 为 0.778、6.123、7.143 的 HS_{Ci} 为 0.185。三台主机的 HS_A 相同。随着攻击持续,受害主机的 HS_A 恶化,主要因为 MSsqlDoS 造成主机响应延迟增加,影响了 HS_A 。由主机密级的分布情况可知,5、7 网段关注信息的机密性和完整性,6 网段关注服务的可用性,三台受害主机的 HS_A 如图 4,5.133 的 HS_A 介于 0.7002~0.70117 间,7.143 的 HS_A 介于 0.1665~0.16747 间,取值区间非常小,近似地表现为一条直线。

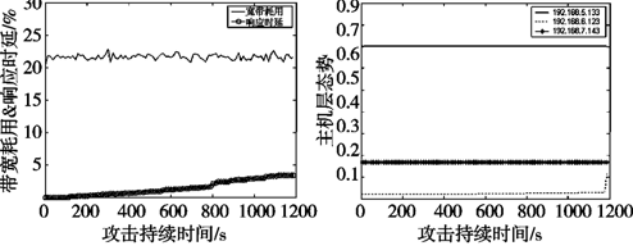


图3 MSsqlDoS攻击的 C_{bw} 和 C_a

图4 MSsqlDoS攻击的 HS

2) 子网层态势

三台受害主机的权重分别为 0.4、0.1、0.3,其余主机的 HS 为 0,加权求和得到 LS ,如图 5 所示。其中,5 网段的 LS 最大,说明该网段受到的安全威胁最严重,其次是 7 网段,6 网段受到的安全威胁相对小一些。

3) 全网层态势

由式(4)计算得到三个子网权重分别为 0.413 8、0.206 9、0.379 3,加权求和得到 WS ,如图 6 所示。

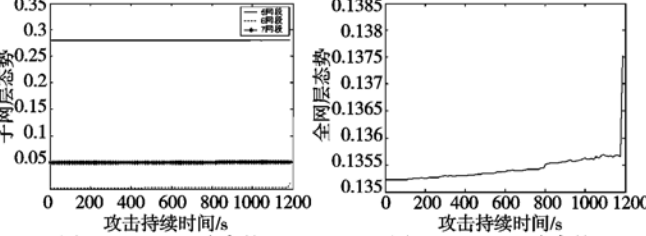


图5 MSsqlDoS攻击的 LS

图6 MSsqlDoS攻击的 WS

3.2.2 端口扫描复合攻击

Nmap ICMP Netmask Request Probe 攻击持续 10 min,随后发起 Nmap ICMP Ping 攻击,也持续 10 min。受害主机带宽耗用和响应时延如图 7 所示。攻击包的发送时间间隔服从指数分布,前 10 min 平均每秒发送 100 个攻击包,后 10 min 平均每秒发送 25 个攻击包。在图 8 中,由于攻击包的发送速率在 600 s 时骤减,造成网络带宽耗用降低;端口扫描复合攻击不消耗主机资源,也不会大量消耗带宽资源,所以在攻击的前 20 min,响应时间延迟近似为 0。

1) 主机层态势

在端口扫描复合攻击的前期,全网主机受到 probe 攻击, HS_{Ci} 为 0.444;在实验进行到 600 s 时,全网主机受到 Ping 攻

击, HS_{Ci} 增至 0.5。由于受害主机的 C_a 在整个攻击过程中始终为 0,故 HS_A 也为 0。对于 5、7 网段的主机, $HS = 0.9HS_{Ci}$;而对于 6 网段的主机, $HS = 0.1HS_{Ci}$ 。 HS 的变化情况如图 8 所示。可以看出,多步攻击的威胁程度逐渐增加,如 5、7 网段的 HS 在 600 s 时发生突变;由于不同主机关注的安全属性不同,故相同攻击对它们造成的威胁程度可能不同,如 6 网段的 HS 比 5、7 网段的 HS 小一些。

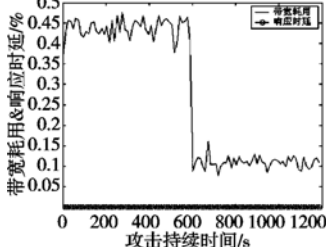


图7 端口扫描攻击的 C_{bw} 和 C_a

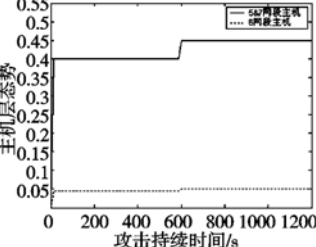


图8 端口扫描攻击的 HS

2) 子网层态势

5 网段主机的权重均为 0.3,6 网段主机的权重均为 0.1,7 网段有一台主机的权重为 0.3,其余两台为 0.4。 LS 等于各个 HS 的加权求和,如图 9 所示。虽然 5、7 网段的 HS 相同(图 8),但由于这两个网段中的主机权重不同,计算得到的 LS 不同,5 网段的 LS 大于 7 网段,如图 9 所示。

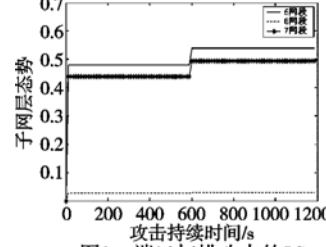


图9 端口扫描攻击的 LS

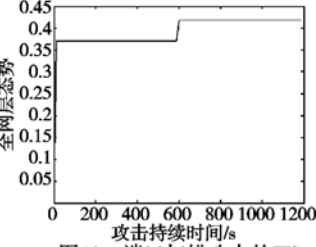


图10 端口扫描攻击的 WS

3) 全网层态势

5、6、7 网段的子网权重分别为 0.4138、0.2069、0.3793, WS 等于各 LS 的加权求和,如图 10 所示

4 结束语

本文根据网络的拓扑结构,结合机密性、完整性和可用性三种主要安全属性,提出一套包括服务、主机、子网和全网四层的网络安全威胁态势指标,并给出了各项指标的量化计算方法,在真实的网络环境中模拟攻击验证了该模型的可行性。本文实现了对网络当前的安全状态进行评估,下一步将基于历史数据或专家知识预测网络安全的发展趋势。

参考文献:

[1] ORTALO R, DESWARTE Y, KAA NICHE M. Experimenting with quantitative evaluation tools for monitoring operational security [J]. IEEE Trans on Software Engineering, 1999, 25(5): 633-650.

[2] BASS T. Intrusion systems and multisensor data fusion: creating cyberspace situational awareness [J]. Communications of the ACM, 2000, 43(4): 99-105.

[3] BRUCE D, MASAMI T, DANIEL U, et al. Security situation assessment and response evaluation [C]// Proc of the 2nd DARPA Information Survivability Conference & Exposition. Los Angeles, CA: IEEE, 2001: 387-394.

[4] PORRAS P A, FONG M W, VALDES A. A mission-impact-based approach to INFOSEC alarm correlation [C]// Proc of the 5th International Symposium on Recent Advances in Intrusion Detection. Berlin: Springer-Verlag, 2002: 95-114.

hash 值的绝对差异度,其中 e_i 和 e'_i 分别是原始 hash 值和新的 hash 值的第 i 个 ASCII 码字符,而函数 $t(*)$ 将 ASCII 码字符转换为它们相应的十进制数值。做了 2 048 次这样的实验, d 的最大,最小和平均值等列在表 2 中。

表 2 两个 hash 值的绝对差异度

最大值	最小值	平均值	平均值/字符
2 148	650	1 384.4	86.52

可以看出,两个 hash 值的绝对差异度值平均值是 86.52,比较接近理论值 85.333 3。

3.5 算法性能比较

选取当前国内外发表的比较安全的 hash 函数算法与本文的算法在绝对差异度和统计性能等方面进行比较,以体现本文算法在这两方面的优劣性,如表 3 所示。

表 3 Hash 算法性能比较

算法	绝对差异度	算法的混乱与扩散统计性能($N=2\ 048$)			
		$\overline{B}$	$P/\%$	ΔB	$\Delta P/\%$
Xiao ^[4]	94.125	63.850 1	49.88	5.789 8	4.52
Wang ^[6]	95.375	63.98	49.98	5.53	4.33
邓绍江 ^[7]	88.78	63.82	49.62	5.88	4.54
Xiao ^[8]	87.562 5	64.177 7	50.14	5.585 9	4.36
康小培 ^[9]	81.786 3	63.70	49.77	4.97	3.89
Li ^[10]	89.51	63.807 6	49.849 7	5.756 3	4.497 1
本文	86.52	63.880 9	49.91	5.640 6	4.41

从表 3 可以看出,在绝对差异度方面,与其他算法相比本文算法均值 86.52,最接近理论值 85.333 3;在算法的混乱与扩散统计性能方面,本文算法的平均变化比特数 $\overline{B}=63.880\ 9$ 和每比特平均变化概率 $P=49.91$ 与其他算法的 $\overline{B}$ 和 P 相比,除了 Wang 的之外,最接近理想状况下的 64 bit 和 50%,说明本算法有较好的混乱与扩散性能,而本算法的 ΔB 和 ΔP 也相对较小,体现了较好的混乱与扩散的稳定性。

4 结束语

本文提出了基于提高运行速度的并行结构和增强安全性

的可变参数的混沌 hash 函数算法。通过明文扩展将并行处理的明文消息矩阵元素信息关联起来,实现了并行性。由矩阵元素位置标号决定的可变参数以及矩阵元素相应的 ASCII 码值作为混沌分段线性映射的参数和迭代次数来生成相应的中间 hash 值。最终的 128 bit 的 hash 值由中间 hash 值的异或而得到。计算机模拟表明本算法满足单向 hash 函数的各项性能要求。

参考文献:

[1] RIVEST R L. RFC 1321, The MD5 message digest algorithm request for comments [S]. Cambridge: MIT and RSA Data Security, 1992.

[2] NITS F P. FIPS PUB 180, Secure hash standard [S]. Washington DC: U. S. Department of Commerce, 1993.

[3] WONG K W. A combined chaotic cryptographic and hashing scheme [J]. *Physics Letters A*, 2003, 307(5-6):292-298.

[4] XIAO Di, LIAO Xiao-feng, DENG Shao-jiang. One-way hash function construction based on the chaotic map with changeable-parameter [J]. *Chaos Solitons and Fractals*, 2005, 24(1): 65-71.

[5] WANG Yong, LIAO Xiao-feng, XIAO Di, et al. One-way hash function construction based on 2D coupled map lattices [J]. *Information Sciences*, 2008, 178(5): 1391-1406.

[6] AKHSHANI A, BEHNIA S, AKHAVAN A, et al. Hash function based on hierarchy of 2D piecewise nonlinear chaotic maps [J]. *Chaos Solitons and Fractals*, 2009, 42(4):2405-2412.

[7] 邓绍江, 李艳涛, 张岱国, 等. 基于混沌查找表的单向 hash 函数构造算法[J]. *计算机工程*, 2010, 36(10):29-31.

[8] XIAO Di, FRANK Y S, LIAO Xiao-feng. A chaos-based hash function with both modification detection and localization capabilities [J]. *Communications in Nonlinear Science and Numerical Simulation*, 2010, 15(9): 2254-2261.

[9] 康小培, 李艳涛, 邓绍江, 等. 基于双混沌映射的文本 hash 函数构造[J]. *计算机应用研究*, 2010, 27(7):2636-2637.

[10] LI Yan-tao, DENG Shao-jiang, XIAO Di. A novel hash algorithm construction based on chaotic neural network[J]. *Neural Computing and Applications*, 2011, 20(1):133-141.

(上接第 4306 页)

[5] HARIRI S, QU G Z, DHARMAGADDA T, et al. Impact analysis of faults and attacks in large-scale networks [J]. *IEEE Security & Privacy*, 2003, 1(5): 49-54.

[6] GORODETSKY V, KARSAEV O, SAMOILOV V. On-line update of situation assessment based on asynchronous data streams [C]// Proc of International Conference on Knowledge-based Intelligent Information & Engineering Systems. Berlin: Springer-Verlay, 2004: 1136-1142.

[7] YEGNESWARAN V, BARFORD P, PAXSON V. Using honeynets for Internet situation awareness [C]// Proc of ACM/USENIX Hotnets IV. [S. l.]: ACM, 2005: 1-6.

[8] MEHTA V, BARTZIS C, ZHU H, et al. Ranking attack graphs [C]// Proc of the International Symposium on the Recent Advances in Intrusion Detection. Berlin: Springer-Verlay, 2006: 127-144.

[9] ARNES A, VALEUR F, VIGNA G, et al. Using hidden Markov models to evaluate the risk of intrusions [C]// Proc of the International Symposium on the Recent Advances in Intrusion Detection. Berlin: Springer-Verlay, 2006: 145-164.

[10] 冯登国, 张阳, 张玉清. 信息安全风险评估综述 [J]. *通信学报*, 2004, 25(7): 10-18.

[11] 肖道举, 杨素娟, 周开峰, 等. 网络安全评估模型研究 [J]. *华中科技大学学报: 自然科学版*, 2002, 30(4): 37-39.

[12] 李辉, 郑庆华, 韩崇昭, 等. 基于多假设跟踪的入侵场景构建研究 [J]. *通信学报*, 2005, 26(4): 70-79.

[13] 陈秀真, 郑庆华, 管晓宏, 等. 层次化网络安全威胁态势量化评估方法 [J]. *软件学报*, 2006, 17(4): 885-897.

[14] 汤永利, 徐国爱, 钮心忻, 等. 基于信息熵的信息安全风险分析模型 [J]. *北京邮电大学学报*, 2008, 31(2): 50-53.

[15] 韦勇, 连一峰, 冯登国. 基于信息融合的网络安全态势评估模型 [J]. *计算机研究与发展*, 2009, 46(3): 353-362.

[16] OLZAK T. A practical approach to threat modeling [EB/OL]. (2008-03-20) [2010-04-16]. http://www.infosecwriters.com/text_resources/pdf/.

[17] CHEN Xiu-zhen, ZHENG Qing-hua, GUAN Xiao-hong. Multiple behavior information fusion based quantitative threat evaluation [J]. *Computers and Security*, 2005, 24(3): 218-213.