基于动态攻击图的网络安全实时评估

陈 靖 王冬海 彭 武
(中国电子科技集团公司电子科学研究院 北京 100041)

摘 要 针对网络安全评估对实时性及可视化的需求,提出了一种基于动态攻击图的实时评估方法。首先通过采集网络的脆弱性、网络拓扑、资产价值等安全属性信息,同时提取入侵检测系统的报警信息、防火墙策略、安全管理等动态攻防对抗信息,生成动态攻击图,并实时调整防御手段对网络进行及时、有效的保护,实时地对网络系统的安全状态进行评估,并采用可视化的方法展现评估结果,在此基础上给出整体安全策略调整建议。最后通过实验证明了本方法的可行性和有效性。

关键词 动态攻击图,实时评估,攻防对抗信息
中图法分类号 TP393.08 **文献标识码** A

Real-time Network Security Assessment Based on Dynamic Attack Graph

CHEN Jing WANG Dong-hai PENG Wu
(China Academy of Electronics and Information Technology, Beijing 100041, China)

Abstract In order to evaluate the network security, a real-time security assessment method based on dynamic attack graph was presented. At first, network security related information such as network vulnerabilities, topology information, asset value, IDS alerts, and firewall rules was fused into attack graph. Then network security situation was evaluated and results were shown through visualization method, on this basis, some corresponding suggests were given to improve security. Finally, the feasibility and validity of this method were proved through some experiments.

Keywords Dynamic attack graph, Real-time assessment, Confront information of attack and defense

1 引言

网络安全评估是依据有关信息安全技术与管理标准,对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程[1]。对整个网络的安全状况进行准确的评估,能够帮助网络管理员掌握整个网络中存在的安全弱点和运行风险,提高网络的防护能力,具有重要的应用价值,是网络安全领域的研究热点。

在网络安全评估领域,基于攻击图的网络安全量化评估已取得一定的研究成果。Swiler 等[2]首先应用图论中的节点、边及其关系来描述网络安全属性之间的关系。通过网络中漏洞的关联关系,发现攻击者可能利用的攻击路径。根据已有的攻击模板,采用深度优先的搜索策略生成网络攻击图,对网络安全状况作出较全面的评价,但是攻击图的生成过程完全依靠手工,评估效率低且无法适应规模稍大的网络。Sheyner 等[3]在模型检测方法基础上,提出了一种自动生成攻击图的方法,但该方法生成的攻击图规模过大。Ammann 等[4]采用基于图论的方法并引入单调性假设,其在一定程度上解决了攻击图的状态爆炸问题,但其仍难以适用于规模稍大的网络。Lippmann 等[5]采用主机为节点、漏洞为边的攻击图,每种网络状态只在图中出现一次,这样虽然降低了图的规模,但不利于后期的量化分析。国内的相关研究[6-9]也提出了各自独到的见解,但是在处理攻击图规模或评估方法的实用性、实时性上仍有可提升的空间。

针对现有的评估方法存在的不足,以及对网络安全评估实时性、结果可视性的需求,本文提出了一种针对网络安全属性的实时评估方法。该方法针对现在网络极强的时效性和日渐增强的互动性,结合攻防对抗信息对网络系统采用动态评估的方法多层次多角度地展示网络的安全状态和发展趋势,并根据历史评估数据分析网络的安全等级。

2 评估建模

2.1 实时评估模型

保密性、完整性及可用性是网络安全状态中最重要、最受关注的3个属性,将保密性、完整性及可用性统称为网络系统的CIA安全属性,并且针对这3种属性进行安全评估。

图1为网络安全属性实时评估架构图。首先,将生成动态攻击图所需预处理的信息分为静态信息和动态信息。静态信息主要包括漏洞信息、主机资产价值、主机CIA属性量化分值以及网络拓扑结构,该类信息的更新相对缓慢,被认为是静态的;动态信息主要包括防火墙防护规则信息、入侵检测系统给出的攻击信息以及网络管理工具的配置信息,该类信息

收稿日期:2012-04-09 返修日期:2012-07-07 本文受国防基础科研项目(A0420110006)资助。
陈 靖(1986—),男,硕士生,主要研究领域为信息安全与风险评估,E-mail:evasa1986@sina.com;王冬海(1968—),男,硕士,高级工程师,主要研究领域为网络与信息安全;彭 武(1979—),男,博士,工程师,主要研究领域为网络安全与风险评估。

的更新对实时性要求相对较高，被认为是动态变化的。静态信息和动态信息的传递分别采用实线和虚线来表示。然后，将经过预处理的信息分别存入数据库中，利用开源制图软件得到攻击图，并对攻击图加以量化分析，得到各主机的安全属性威胁值。最后，按照主机在网络系统中所占的资产价值比对各主机的安全属性威胁值进行加权求和，得到整个系统的安全属性威胁值。采用可视化及数理统计的方法长期观察评估结果，以为管理员调整安全防护策略提供依据。从攻防对抗的角度，根据动态攻击图的分析结果，实时地调整防火墙规则，及时采取有效的防御措施。该方法直接针对网络的核心安全属性进行评估，细化了评估结果，在实时评估的同时能够对存在严重安全隐患的主机进行及时有效保护，并考量长期的评估结果，得到一个对网络整体安全性的全面评价。

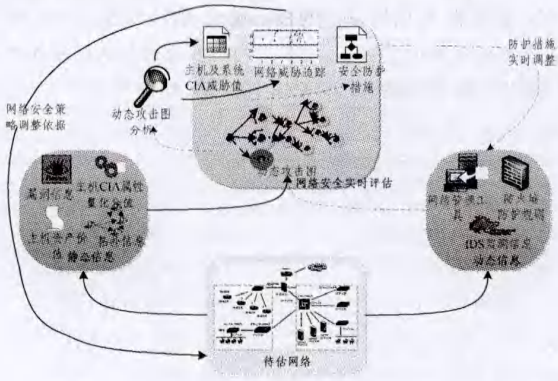


图 1　网络实时评估架构

2.2　动态攻击图生成

定义 1　动态攻击图 $G(H,V)$ 是一个有向图。H 是主机集，是网络中的核心设备与被攻击的主机集合。V 是漏洞集，表示主机在被入侵过程中可被利用的漏洞，攻击者在目标主机上的权限由低到高依次为 none、user、root。动态攻击图经可视化处理，如图 2 所示。

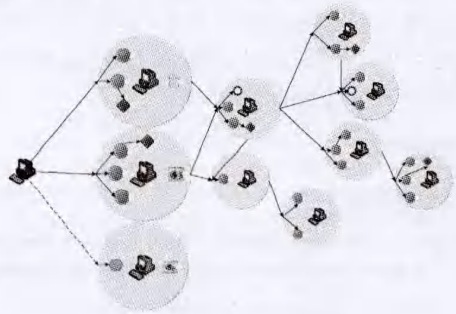


图 2　动态攻击图

在攻击图中，共有两种不同状态的主机，分别用红色和绿色标识，代表该主机处于被入侵及受保护状态，主机的被入侵状态指攻击者在该设备上获得权限的提升，绿色表示主机暂时处于受保护状态。共有 4 种不同种类的漏洞，●表示可远程获得目标主机 user 权限的漏洞，简称为远程-用户类（remote-user）漏洞；◆表示攻击者只有在获得本地 user 权限的前提下才可以获得 root 权限的漏洞，简称为本地-管理员类（local- administrator）漏洞；○表示可远程获得目标主机 root 权限的漏洞，简称远程-管理员类（remote-administrator）漏洞；⬬表示从攻击者角度不可达或者被修复的漏洞。有向边指向漏洞，表示不同主机或同一主机内部的漏洞关联关系。主机背景圆面积与该设备的资产价值成正比。攻击图中的节点表示网络受到攻击的主机和该主机上的漏洞以及资产价值较高可能会被攻击的主机。

实时网络安全评估时，需要通过快捷的手段来生成攻击图，限制生成攻击图的规模。为此首先引入单调性假设，即认为攻击者都是智能的主体，在攻击网络的时候不会为了获取已经得到的权限而发动攻击。其次，将攻击图的生成过程分为两个阶段，第一个阶段是评估系统初次生成攻击图，在该阶段中完整运行生成算法，得到攻击图；在第二个阶段，评估系统定时刷新，根据输入的攻防信息及网络中漏洞信息的更新情况，利用 AJAX 技术完成对攻击图的刷新，将更新的信息反映到攻击图中，从而大大节省了系统的开销。

动态攻击图自动生成算法描述如下：

输入：主机集 H，主机脆弱性集 V，主机间的连接关系集 C，权限集 P，主机资产价值集 Val。

输出：攻击图 G(H,V)

1）对 $\forall h\in H$，在主机 h 的脆弱性集合 V 中，从权限 none 出发查找所有可获得权限提升的本地漏洞 vul_{j+1}，以及 vul_{j+1} 的前提条件漏洞 vul_j，将 vul_j 与 vul_{j+1} 添加到顶点集，边 $vul_j \rightarrow vul_{j+1}$ 添加到边集。直到达到 root 权限或 user 权限，即生成该主机 h 内部的以脆弱性为节点的攻击图。

2）从主机 h_i 的 user 或 root 权限出发，满足 $(h_i, h_{i+1}, port)\in C$，且通过主机 h_i 利用 h_{i+1} 的漏洞 vul_j 能获得 h_{i+1} 的 user 或 root 权限，则 h_i 与漏洞 vul_j 是节点，边 $h_i \rightarrow vul_j$ 是有向边，其中 $h_i, h_{i+1}\in H$，$vul_j \in V$。

3）将满足 $Val_i > Val_0$ 的主机 h_i 以及 h_i 上的漏洞加入攻击图节点，其中 $h_i\in H$，$Val_i\in Val$，Val_0 为管理设定的主机资产价值阈值。

采用广度优先算法搜索，将满足(a)、(b)和(c)的节点和边添加到节点集 H、V 以及边集中，生成攻击图。

3　实时评估

加强对网络系统的安全防护，对网络安全状况作出准确评估，仅仅了解网络系统本身的特点和存在的漏洞并不全面，网络安全是一个攻防对抗的动态过程，只有掌握了攻防双方的信息才能在评估过程中不失偏颇。

网络静态信息、网络动态信息以及基于二者生成的动态攻击图是实时评估的基础。网络静态信息中包含了评估所需的系统脆弱性信息、主机资产价值信息和主机 CIA 属性量化分值，而网络动态信息包括攻防双方的信息，动态攻击图正是将这两者有机地结合到一起，并以此作为评估的模型。

3.1　网络静态信息

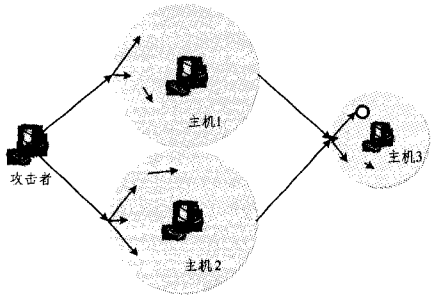
采取自下而上的分析方法，首先计算单台主机所受到的威胁值大小，再按该主机的 CIA 属性量化分值计算攻击者对每一种安全属性的威胁，最后按主机在整个网络中所处的地位对各主机的 3 种安全属性威胁值进行加权求和，得到攻击者对整个网络 3 种安全属性的威胁值大小。

3.1.1　漏洞被利用难易度信息

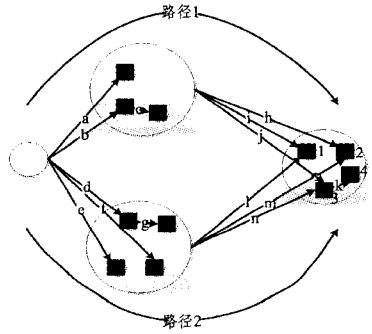
定义 2　主机漏洞利用复杂度是网络系统中某台主机上

各漏洞被攻击者成功利用的难易度量化值集合，可以用列向量$\overrightarrow{V_{hx}}=[V_1,V_2,\cdots,V_n]^{\mathrm{T}}$表示，其中，$hx$为主机编号，$V_n$表示该主机第$n$个漏洞的利用难易度量化值。

在实际网络环境下，攻击者往往需要将多台主机作为跳板，采用多步攻击的方法获得目标主机的权限。攻击者的多步攻击，实际上就是每个单步攻击的有机组合。由动态攻击图可以得到攻击者所能选取的所有攻击路径，分析路径间的关系，结合单步攻击的难易度，可以得到针对该主机上每个漏洞的多步攻击难易度，进而可以得到主机漏洞利用复杂度集合。它的具体计算方法如图3所示。



(a) 攻击图



(b) 攻击图计算模型

图3

图3(a)是图2所示攻击图的一部分，图3(b)是它的计算模型，以计算主机3上的漏洞利用复杂度集合为例说明$\overrightarrow{V_{h3}}=[V_1,V_2,V_3,V_4]^{\mathrm{T}}$的计算方法。

图3(b)中a到k表示漏洞单步利用难易度，由CVSS可得其具体取值。对于主机3的漏洞V_1而言，攻击者有路径1和路径2两种选择，这两条路径间是逻辑或的关系；而对于其中一条路径而言，以路径1为例，攻击者必须首先获得主机1的一定权限并以此为跳板才能成功利用V_1。攻击者→主机1→主机3上的V_1，这一过程是逻辑与的关系。通过分析可以得到，攻击者通过路径1成功利用V_1的难易度为$(a+b+b*c)*i$，通过路径2利用V_1的难易度为$(d+e+f+d*g)*l$，因为两条路径间是逻辑或的关系，求得$V_1=(a+b+b*c)*i+(d+e+f+d*g)*l$。同理可得$V_2,V_3,V_4$。

由以上方法，可以得到：

$$\overrightarrow{V_{hx}}=[V_1,V_2,\cdots,V_\beta]^{\mathrm{T}} \tag{1}$$

式中，hx为主机编号，β为该主机上所存在的所有漏洞总数。

3.1.2 资产价值信息

资产价值在很大程度上体现了设备在网络中的重要性以及攻击者对该设备进行攻击的可能性。在本文所述的评估方法中，网络服务器设备按其在网络系统中所处的地位及被攻击者攻击得手后可能造成的后果，采用专家打分法给每台网络设备一个资产价值量化值S_i(其中，i取1至网络中所有设备数)，而客户机的资产价值采用调查问卷的方式从用户手中获得。在动态攻击图中，资产价值通过面积大小的不同加以区分。

定义3 主机资产价值比为网络中各主机的资产价值占所在网络资产总价值的比例，用下式表示：

$$\eta_i=\frac{S_i}{\sum_{hx=1}^{n}S_{hx}} \tag{2}$$

式中，S_i为第i台主机资产价值，n为网络中所有设备数。

3.1.3 主机安全属性量化分值

在实际的网络防护中，不同的网络设备核心具有不同的安全属性，安全需求有差异，安全策略也不尽相同，比如对于Web服务器，可用性是它的核心安全属性，保密性和完整性处在相对次要的位置，这就要求网络安全评估的过程能体现出各设备在安全属性上的差异。本文采用层次分析法(AHP法)来确定不同网络设备的CIA属性量化分值。

定义4 主机CIA属性量化分值是不同主机的机密性、完整性及可用性所处地位的量化表示，可用如下行向量表示：

$$\overrightarrow{\lambda_{hx}}=[\lambda_{chx},\lambda_{ihx},\lambda_{ahx}],\lambda_{chx}+\lambda_{ihx}+\lambda_{ahx}=1 \tag{3}$$

式中，hx为主机编号，λ_{chx}、λ_{ihx}、λ_{ahx}分别为该主机的机密性、完整性、可用性量化分值。

3.2 网络动态信息

3.2.1 攻击者行为信息

定义5 攻击行为是攻击者利用网络漏洞导致主机或网络安全状态发生转移的一个过程。利用入侵检测系统(IDS)可以检测到网络攻击行为。但是IDS存在的一个较明显缺点就是虚警多、报警量大。因此，采用基于标志的检测技术，维护一个攻击行为知识库，筛选对网络安全威胁大的、易于发动的攻击行为录入库中，发现匹配时报警。

针对网络中某台主机的一组攻击行为可以表示成攻击行为威胁级别向量，如下所示：

$$\overrightarrow{A_{hx}}=[A_1,A_2,A_3,\cdots,A_\alpha] \tag{4}$$

式中，hx为该主机的编号，A_α表示其中一个攻击行为对该主机的威胁级别，可以由IDS报警信息得到，α为针对该主机所有攻击行为的数量。因为不同时刻网络或网络中某台设备受到的攻击行为不同，所以$\overrightarrow{A_{hx}}\propto t$，即攻击行为随时间变化。

3.2.2 防御行为信息

定义6 防御行为是网络管理员采用防火墙、网络管理工具软件等手段对网络攻击进行抵制的过程。通过防火墙访问控制表(ACLs)、网络地址转换(NAT)控制网络可达性的方法来进行网络防御。

某一时刻针对网络中某台设备的防御行为信息可以用矩阵D_{hx}来描述：

$$D_{hx}=\begin{bmatrix}d_{11} & \cdots & \cdots\\ \vdots & \ddots & \vdots\\ \cdots & \cdots & d_{\alpha\beta}\end{bmatrix} \tag{5}$$

式中，$d_{\alpha\beta}$为该主机遭受到的第α个攻击利用其上的第β个漏洞对其进行攻击时的防御情况，它的具体取值见表1。

表中防御效果指网络的防御体系对攻击的抵制效果，并按不同的防御原理分成5个防御级别。

表 1　防御效果量化

防御级别	防御成功率	描述
1	0	攻击无法利用某漏洞。
2	0.3	攻击可能成功利用某漏洞，但通过控制防火墙访问列表，攻击不可达。
3	0.5	攻击可能成功利用某漏洞，但通过防火墙静态 NAT 机制，攻击不可达。
4	0.7	攻击可能成功利用某漏洞，但通过防火墙动态 NAT 机制，攻击不可达。
5	1	攻击可达且可被利用。

在进行实时评估时，评估系统定时刷新，以动态攻击信息和防御信息的实时变化为基础，更新动态攻击图，并通过实时数据库将信息反馈给防火墙等网络防御体系，以及时更新防御措施。

3.3　量化评估

引入最坏情况假设：网络中某台设备存在漏洞并且该主机从攻击者的视角可达，则认为该设备被攻击成功。

定义 7　主机威胁值 Rhx 为某台主机被攻击者获得权限提升的可能性。由前文分析可知，主机的安全状况取决于黑客攻击、网络防御以及主机上存在的脆弱性，主机威胁值 R_{hx} 是在这 3 者的共同作用下确定的，式(1)、式(4)及式(5)分别给出了攻击威胁级别信息、防御信息及脆弱性利用难易度，这 3 者的积可表征网络中某台主机的威胁值 R_{hx}：

$$R_{hx}=\overrightarrow{A_{hx}} * D_{hx} * \overrightarrow{V_{hx}}$$

$$=[A_1,A_2,A_3\cdots A_\alpha]\begin{bmatrix} d_{11} & \cdots & \cdots \\ \vdots & \ddots & \vdots \\ \cdots & \cdots & d_{\alpha\beta} \end{bmatrix}[V_1,V_2,\cdots,V_\beta]^{\mathrm{T}} \tag{6}$$

式中，α 为针对该主机所有的攻击行为数，β 为该主机上所存在的漏洞数。

主机安全属性威胁值为某台主机由于被攻击者成功攻击而带来的对保密性、完整性及可用性的损害程度。利用式(6)以及式(3)说明的主机 CIA 属性量化分值，可以进一步得到该主机的安全属性威胁值：

$$R_{hx} * \overrightarrow{\lambda_{hx}}=R_{hx} * [\lambda_{chx},\lambda_{ihx},\lambda_{ahx}]$$

$$=[R_{hx}\lambda_{chx},R_{hx}\lambda_{ihx},R_{hx}\lambda_{ahx}] \tag{7}$$

式中，$R_{hx}\lambda_{chx}$、$R_{hx}\lambda_{ihx}$、$R_{hx}\lambda_{ahx}$ 分别为针对该主机保密性、完整性及可用性的威胁值。

定义 8　网络安全属性威胁值为整个网络系统由于被攻击者成功攻击而带来的对保密性、完整性及可用性的损害程度。按主机在网络系统中的地位，即主机资产价值比，结合各主机安全属性威胁值，得到网络安全属性威胁值。利用式(2)以及式(7)可以得到网络安全属性威胁值 $\overrightarrow{P}$：

$$\overrightarrow{P}=[P_c,P_i,P_a] \tag{8}$$

其中，

$$P_c=\sum_{hx=1}^{n}(\eta_{hx} * R_{hx}\lambda_{chx}) \tag{9}$$

$$P_i=\sum_{hx=1}^{n}(\eta_{hx} * R_{hx}\lambda_{ihx}) \tag{10}$$

$$P_a=\sum_{hx=1}^{n}(\eta_{hx} * R_{hx}\lambda_{ahx}) \tag{11}$$

P_c，P_i，P_a 表示网络保密性、完整性及可用性威胁值。

4　实验与结果

为验证提出的评估方法，搭建如图 4 所示的网络环境。

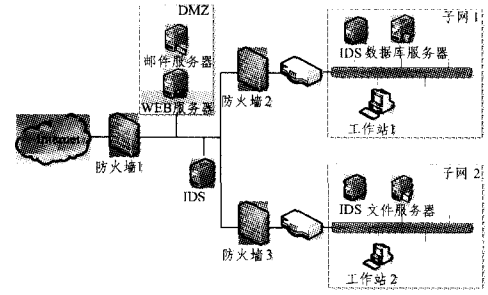


图 4　实验网络拓扑结构图

网络分成 3 个区域，分别是 DMZ 区、子网 1 及子网 2。可达性设置如下：DMZ 区中的 Web 服务器由防火墙 1 保护并连接互联网，且只能直接访问子网 1 中的数据库服务器和子网 2 中的文件服务器，各子网内部主机可互相访问，子网 1 中的工作站 1 可以访问子网 2 的文件服务器。各区域的 IDS 系统负责各区域中的攻击监测。主机资产价值信息 S_i 由专家打分法获得，主机安全属性量化分值由层次分析法求得。

各主机信息及其所含漏洞信息如表 2 所列，主机信息栏包括主机类型、使用的操作系统以及开放的服务或存在的软件，漏洞利用前提及效果栏表示利用该漏洞时攻击者在源主机上所必须拥有的最低权限以及成功利用该漏洞后在目标主机上获得的权限。

表 2　主机及其漏洞信息

主机编号	主机信息	漏洞编号	CVE 编号	漏洞描述	漏洞利用前提及后果
H1	Web 服务器，Windows2000	V1	CVE-2002-0364	IIS 缓冲区溢出攻击，远程	SrcP=user，RstP=root
H2	数据库服务器，Redhat8.0，LICQ	V2	CVE-2001-0439	LICQ 的 URL 解析功能，远程	SrcP=user，RstP=user
		V3	CVE-2002-0004	本地缓冲区溢出，本地	SrcP=user，RstP=root
		V4	CVE-2001-1030	可绕过 ACLs 机制，对主机进行扫描等非法操作，远程	SrcP=user，RstP=user
H3	工作站 1，Windows2000，IE6.0，Funk Proxy v3.0	V5	CVE-2002-0193	脚本漏洞，远程	SrcP=user，RstP=user
		V6	CVE-2002-0065	弱口令，本地	SrcP=user，RstP=root
H4	文件服务器，Redhat8.0，RPC	V7	CVE-2003-0252	利用 RPC 进行 Dos 攻击，远程	SrcP=user，RstP=root
		V8	CVE-2001-1030	可绕过 ACLs 机制，对主机进行扫描等非法操作，远程	SrcP=user，RstP=user
		V9	CVE-2002-0004	本地缓冲区溢出，本地	SrcP=user，RstP=root
H5	工作站 2，Windows2000，IE6.0	V10	CVE-2002-0193	脚本漏洞，远程	SrcP=user，RstP=user
		V11	CVE-2002-0065	弱口令，本地	SrcP=user，RstP=root

利用 2.2 节给出的动态攻击图生成算法生成攻击图，并提取出如图 5 所示的计算模型。

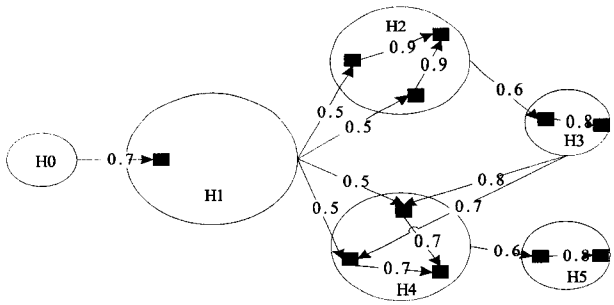


图 5　实验网络的攻击图计算模型

箭头数字表示漏洞单步利用难易度，攻击者单步攻击的难易度可以由文献[8]给出的漏洞利用的复杂度标准结合CVSS漏洞评分系统得到，而主机漏洞被利用难易度由攻击者到攻击目标的多步攻击难易度量化。利用 3.1.1 节中的方法，得到各主机漏洞被利用难易度信息：$\overrightarrow{V_{h1}}=[0.7]^{T}$、$\overrightarrow{V_{h2}}=[0.35,0.35,0.625]^{T}$、$\overrightarrow{V_{h3}}=[0.42,0.336]^{T}$、$\overrightarrow{V_{h4}}=[0.69,0.64,0.85]^{T}$、$\overrightarrow{V_{h5}}=[0.386,0.309]^{T}$。

攻击行为信息可以由各区域中设置的 IDS 检测系统得到，针对实时评估对处理速度的需求，采用基于标志的检测方法，维护一个知识库，将威胁大、易发动的攻击特征提取出来放到库中，发现匹配时报警。

表 3 为实验过程中遇到的针对不同主机存在漏洞的攻击行为信息。攻击源表示某次攻击发动的位置，威胁级别表示攻击成功对目标主机造成的危害程度，从 IDS 报警信息及知识库提取得到。由此，可以得到针对各主机的攻击行为威胁级别向量：

$\overrightarrow{A_{h1}}=[0.86,0.92]$

$\overrightarrow{A_{h2}}=[0.83,0.77,0.82,0.93]$

$\overrightarrow{A_{h3}}=[0.87,0.63,0.94]$

$\overrightarrow{A_{h4}}=[0.84,0.82,0.87,0.84,0.82,0.93]$

$\overrightarrow{A_{h5}}=[0.84,0.93,0.94]$

表 3　攻击行为信息

攻击编号	攻击时间	攻击源	攻击目标	相关漏洞	攻击后果量化
1	03/10-08:44:16	H0	H1	CVE-2004-0040	0.86
2	03/10-08:45:53	H0	H1	CVE-2002-0364	0.92
3	03/10-08:46:33	H1	H2	CVE-2001-0439	0.83
4	03/10-08:48:06	H1	H2	CVE-2006-2379	0.77
5	03/10-08:49:22	H1	H2	CVE-2001-1030	0.82
6	03/10-08:50:35	H2	H2	CVE-2002-0004	0.93
7	03/10-08:56:12	H2	H3	CVE-2002-0193	0.87
8	03/10-09:05:53	H2	H3	CVE-2004-0575	0.63
9	03/10-09:10:43	H3	H3	CVE-2002-0065	0.94
10	03/10-09:15:03	H3	H4	CVE-2002-0064	0.87
11	03/10-09:18:41	H3	H4	CVE-2003-0252	0.84
12	03/10-09:26:21	H3	H4	CVE-2001-1030	0.82
13	03/10-09:27:13	H4	H4	CVE-2002-0004	0.93
14	03/10-09:29:12	H1	H4	CVE-2003-0252	0.84
15	03/10-09:30:21	H1	H4	CVE-2001-1030	0.82
16	03/10-09:31:47	H4	H5	CVE-2003-0193	0.84
17	03/10-09:35:54	H4	H5	CVE-2008-0702	0.93
18	03/10-09:46:35	H5	H5	CVE-2002-0065	0.94

防御行为信息矩阵 D_{h1} 至 D_{h5} 可以由 2.2.2 节所述方法结合表 2 得到，其具体取值如下：$D_{h1}=\begin{pmatrix}0\\0.5\end{pmatrix}$、$D_{h2}=\begin{pmatrix}1&0&0\\0&0&0\\0&0&1\\0&1&0\end{pmatrix}$、$D_{h3}=\begin{pmatrix}0.7&0\\0&0\\0&1\end{pmatrix}$、$D_{h4}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\\1&0&0\\0&1&0\\0&0&1\end{pmatrix}$、$D_{h5}=\begin{pmatrix}1&0\\0&0\\0&1\end{pmatrix}$。此时实时评估系统由获取到的攻防信息及时反应，调整防火墙规则，隔离受攻击主机或者及时对漏洞进行修补。

由式(6)即各主机威胁值 R_{hx} 等于 $\overrightarrow{A_{hx}}*D_{hx}*\overrightarrow{V_{hx}}$，再利用式(7)—式(11)得到整个网络安全属性威胁值，如图 6 所示。

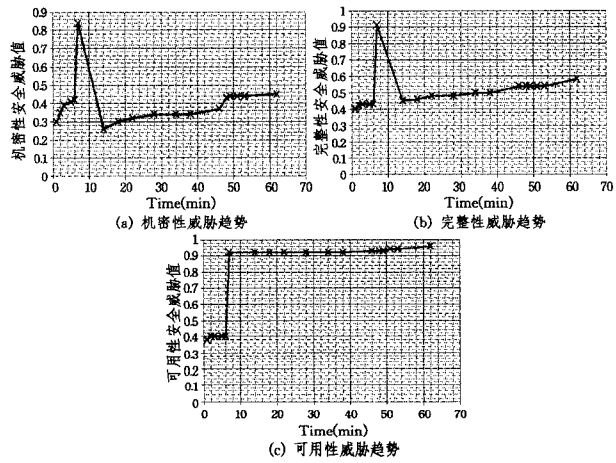


图 6

由图可看出，攻击者在攻击的第六步对 H2 数据库服务器构成严重威胁，由于该设备资产价值高，导致对整个网络的安全属性构成严重威胁。评估系统采取实时措施，通过防火墙策略调整暂时隔断了 Web 服务器对该设备的访问，所以在机密性和完整性趋势图中，对网络的这两个属性威胁大大减小了，但是由于数据库服务器的暂时不可用，整个网络的可用性依然被大大限制。从图 6(c)可以看出在整个攻击过程中，可用性威胁值在很长一段时间内处于较高位置，这就需要管理员采取漏洞修补、软件更新等进一步措施。

结束语　本文在基于攻击图的网络安全量化评估的基础上，提出了一种基于动态攻击图的网络安全实时评估方法。该方法能较好地体现出攻击对网络 3 大安全属性的影响，实时地调整网络防御策略来有效保护网络，并根据攻防对抗信息实时调整评估结果，帮助管理员有效判断当前网络安全状况。

对网络进行实时的保护，不仅要求评估系统能客观、完整地体现攻防双方的行为信息，在此基础上对网络安全状况作出准确评估，还应该对攻击者的攻击行为进行预测，识别攻击者的入侵意图，提前采取有效措施保护，这将是下一步研究工作的重点。

参 考 文 献

[1] 信息安全技术信息安全风险评估规范[S]. GB/T 20984-2007. 2007

[2] Phillips C, Swiler L. A Graph-based System for Network Vulnerability Analysis[C]//Proceedings of the New Security Para-

digms Workshop. Charlottesville, VA, USA: [s. n.], 1998

[3] Sheyner O, Haives J, Jha S. Automated generate on and analysis of attack graphs[C]// Proc 2002 IEEE Symposium on Security and Privacy. Oakland, California, USA, 2002: 254-265

[4] Ammann P, Wijesekera D, Kaushik S. Scalable, graph-based network vulnerability analysis [C]// Proc the 9th ACM Conference on Computer and Communications Security. Wa-shington, DC, USA, 2002: 217-224

[5] Lippmann R, Ingols K, Scott C, et al. Validating and Restoring Defense in Depth Using Attack Graphs[C]// Proc the 2006 Military communications Conference. Washington, DC, USA, IEEE Press, 2006: 1-10

[6] 汪渊, 蒋凡, 陈国良. 基于图论的网络安全分析方法的研究与实现[J]. 小型微型计算机系统, 2003, 24(10): 1865-1869

[7] 张涛, 胡铭曾, 云晓春, 等. 计算机网络安全性分析建模研究[J]. 通信学报, 2005, 26(12): 100-109

[8] 张维明, 毛捍东, 陈锋. 一种基于图论的网络安全分析方法研究[J]. 国防科技大学学报, 2008, 30(2)

[9] 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

(上接第 97 页)

行初始化，其中数据安全程度阈值(θ,σ)中，取$\theta=\sigma=\sum_{i=1}^{n}\min(card(x)_i^F)=\sum_{i=1}^{n}\max(card(x)_i^-)$，伪装不良信息判定阈值$\phi$取$\phi=0.99$，伪装不良信息模板向量为$\{P|P_1,P_2,\cdots,P_n\}$。

利用传统的基于敏感词汇的方法、文献[9]的算法和本文算法对实验目标数据集进行不良伪装信息检测，具体仿真效果图如图 1 所示。

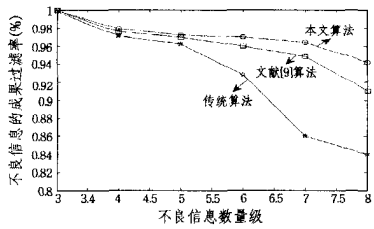


图 1　3 种算法的不良信息检测效果对比仿真图

通过图 1 可以看出，随着敏感词汇数据集合信息量级数的增加，文献[9]算法的过滤效果要优于传统效果，这是由于基于语义分析的物联网云存储数据伪装不良信息更能从语义关联的角度对信息量进行检测，检测面更广，效果更优。但同时可以看到，文献[9]的算法依赖于对词汇语义关联关系的提取，其提取信息的正确率和敏感词汇语义矩阵的抽取直接影响着其语义关联度的计算，且其算法基于先验概率来进行敏感词汇关联度的计算。与本文基于 B-ISVM 算法相比，本文的算法基于序列风险最小化，将信息量样本集基于均值和标准差的 K 均值方法进行聚类分析，并以数据安全度阈值和不良伪装信息相似度阈值的计算为参数在增量模式下进行信息量判定识别，其效果要优于传统的基于敏感词汇的算法和文献[9]的算法。具体的统计结果如表 1 所列。

表 1　3 种算法的检测效果对比

算法	敏感词汇数	检测个数
传统算法	195	98
文献[9]算法	195	177
本文算法	195	192

通过计算，3 种算法的漏检率如表 2 所列。

表 2　3 种算法的漏检率对比

算法	漏检率
传统算法	3
文献[9]算法	0.62
本文算法	0.13

通过漏检率可以看出，本文提出的基于 B-ISVM 算法的物联网云存储数据伪装不良信息检测算法对敏感词汇的检测效果要优于传统算法和文献[9]的算法，其不仅通过信息量样本空间分类构造对信息量进行真伪识别和伪信息中不良信息判别，而且利用增量模式进行尺度检测，在确保检测精度的同时提高了 SVM 的训练速度和不良伪装信息的检测效率，有利于物联网云存储数据伪装不良信息的检测。

结束语　通过对物联网云存储数据信息量的伪装与筛选原理进行基础知识定义，对信息量真伪信息筛选的定理进行了研究，并对信息量的伪信息发生不良信息的概率进行了探讨，以此为基础进行了数据安全度阈值计算和不良伪装信息模板向量集的相似度阈值计算。基于此，提出了基于 B-ISVM 算法的物联网云存储数据伪装不良信息检测算法，以样本信息量空间最优分割面构造为目的对信息量进行基于邻界区和增量模式的 SVM 算法检测，在相似度阈值范围内对各样本集进行不良伪装信息分类，从而得到不良信息向量集。实验证明该算法具有较好的检测效果和准确率。下一步的研究将集中于对阈值的修正和初始参数的统计验证，以确保算法检测效率的最佳与优化。

参 考 文 献

[1] 彭昱忠, 元昌安, 王艳. 基于内容理解的不良信息过滤技术研究[J]. 计算机应用研究, 2009, 26(2): 433-438, 447

[2] 季秀兰, 熊拥军. 基于网络安全的网页过滤模型及其关键算法[J]. 中南林业科技大学学报, 2011, 12: 197-201

[3] 李连, 朱爱红, 苏涛. 一种改进的基于向量空间文本相似度算法的研究与实现[J]. 计算机应用与软件, 2012, 2: 282-284

[4] 袁鼎荣, 钟宁, 张师超. 文本信息处理研究述评[J]. 计算机科学, 2011, 2: 9-13

[5] 唐云, 罗俊松. 基于粗糙集和 BP 神经网络的文本分类研究[J]. 计算机仿真, 2011, 6: 219-222, 283

[6] 耿红琴, 张冠宇, 史开泉. F-信息伪装与伪装-还原辨识[J]. 计算机科学, 2011, 38(2): 241-245

[7] 牟琦, 陈艺坤. 一种基于快速增量 SVM 的入侵检测方法[J]. 计算机工程, 2012, 12: 92-94

[8] 丁文军, 薛安荣. 基于 SVM 的 Web 文本快速增量分类算法[J]. 计算机应用研究, 2012, 4: 1275-1278

[9] 邵听, 徐倩漪. 物联网云存储数据伪装不良信息检测方法的研究与仿真[J]. 计算机仿真, 2012, 29(2): 135-138

[10] 邬贺铨. 物联网的应用与挑战综述[J]. 重庆邮电大学学报: 自然科学版, 2010, 22(5): 526-531