

基于攻击模式识别的网络安全态势评估方法

王 坤, 邱 辉*, 杨豪璞

(信息工程大学, 郑州 450001)

(* 通信作者电子邮箱 pioneerqh@126.com)

摘 要: 通过对已有网络安全态势评估方法的分析与比较, 发现其无法准确反映网络攻击行为逐渐呈现出的大规模、协同、多阶段等特点, 因此提出了一种基于攻击模式识别的网络安全态势评估方法。首先, 对网络中的报警数据进行因果分析, 识别出攻击意图与当前的攻击阶段; 然后, 以攻击阶段为要素进行态势评估; 最后, 构建攻击阶段状态转移图(STG), 结合主机的漏洞与配置信息, 实现对网络安全态势的预测。通过网络实例对所提出的网络安全态势评估模型验证表明, 随着攻击阶段的不断深入, 其网络安全态势值也随之增大, 能够更加准确地反映攻击实情; 且在态势预测中无需对历史序列进行训练, 具有更高的预测效率。

关键词: 因果分析; 状态转移图; 态势评估; 模式识别; 多阶段攻击

中图分类号: TP393.08 **文献标志码:** A

Network security situation evaluation method based on attack pattern recognition

WANG Kun, QIU Hui*, YANG Haopu

(Information Engineering University, Zhengzhou Henan 450001, China)

Abstract: By analyzing and comparing the existing network security situation evaluation methods, it is found that they can not accurately reflect the features of large-scale, coordination, multi-stage gradually shown by network attack behaviors. Therefore, a network security situation evaluation method based on attack pattern recognition was proposed. Firstly, the causal analysis of alarm data in the network was made, and the attack intention and the current attack phase were recognized. Secondly, the situation evaluation based on the attack phase was realized. Lastly the State Transition Diagram (STG) of attack phase was created to realize the forecast of network security situation by combining with vulnerability and configuration information of host. A simulation experiment for the proposed network security situation evaluation model was performed by network examples. With the deepening of the attack phase, the value of network security situation would increase. The experimental results show that the proposed method is more accurate in reflecting the truth of attack, and the method does not need training on the historical sequence, so the method is more effective in situation forecasting.

Key words: causal analysis; state transition diagram; situation evaluation; pattern recognition; multi-stage attack

0 引言

随着网络规模的不断扩大, 传统行业与互联网的结合越来越广泛, 人们的生活已高度依赖于网络。目前网络环境不容乐观, 网络攻击日益频繁, 造成的威胁与损失也越来越大。而传统的安全产品只能单一地反映网络状况一项或某几项指标, 已经无法满足管理人员对及时掌握网络整体安全状况的需求。网络安全态势感知技术融合了入侵检测系统(Intrusion Detection System, IDS)、防火墙、病毒检测系统(Virus Detection System, VDS)等网络安全设备的防护数据, 是对网络安全状况与趋势的一个整体反映, 能够作为网络预警与响应的重要参照, 因此, 网络安全态势感知技术近年来也逐渐成为网络安全领域的研究热点。

态势感知技术首先源于航天飞行领域的研究, 随后在军事、交通监管以及医疗应急调试等领域都被广泛应用。1999年, Bass^[1]首次提出网络安全态势感知的概念, 他结合入侵检测系统的现状与网络攻防的发展, 指出融合分布式网络中的

多源传感器的态势感知研究必然成为未来发展的趋势。

Information Extraction & Transport^[2]开发的SSARE (Security Situation Assessment and Response Evaluation) 系统, 实现了入侵检测、态势评估和响应的融合, 但该系统信息获取方式单一, 自动化程度较低, 具体实施时需要大量的人工参与, 无法实现及时评估与响应。

Abad等^[3]通过对网络安全报警数据进行关联分析, 综合评估网络安全态势, 并开发设计了态势评估系统, 该系统能够发现新型安全事件、分析不可信主机、找出攻击源等功能, 但是该方法选取的网络安全报警数据不够全面, 且只是定性地对网络安全态势进行分析, 无法直观地给出网络当前的安全态势。

陈秀真等^[4]提出了层次化网络安全威胁态势量化评估方法, 分别对服务、主机、系统3个层次进行量化评估, 采取“自下而上, 先局部后整体”的评估策略, 逐层评估。该方案能够对网络安全威胁态势给出一个量化评估值, 并得到直观的安全态势。该方案因其易行性, 得到了许多学者的关注与

收稿日期: 2015-08-05; 修回日期: 2015-09-15。 基金项目: 国家自然科学基金资助项目(61309013)。

作者简介: 王坤(1975-), 男, 河南周口人, 副教授, 博士, 主要研究方向: 网络安全、数据挖掘; 邱辉(1990-), 男, 河南永城人, 硕士研究生, 主要研究方向: 网络安全、态势感知; 杨豪璞(1993-), 女, 河南封丘人, 硕士研究生, 主要研究方向: 网络安全、攻击检测。

研究,文献[5-6]等都在该方案上做了许多改进工作。

韦勇等^[7]提出了基于信息融合的网络安全态势评估方法,将多源数据信息进行融合,利用漏洞信息和服务信息,经过态势要素融合和节点态势融合计算网络安全态势,绘制安全态势曲线。文献[8]又通过融合环境信息、资产价值,对安全态势进行修正,得到更加准确的评估结果。经过信息融合,该方法较好地解决了数据源的模糊与不确定性。

张勇等^[9]与席容容等^[10]提出了基于博弈模型的网络安全态势评估方法,通过分析安全防护手段与攻击威胁规律,利用博弈理论,在网络攻防两端建立博弈模型,从而对网络安全态势进行有效评估,但该方法状态空间很大、效率较低,无法提供实时评估。

近年来网络攻击行为逐渐呈现出大规模、协同、多阶段等特点,网络攻击不再是一个个孤立事件。根据国家计算机网络应急技术处理协调中心的年度网络安全工作报告中对攻击按类型进行统计的结果,大部分攻击尤其是危害巨大的攻击几乎都是多步攻击。而以上评估方法没有去发现攻击间的关联,忽略了攻击间的协同性。文献[11]提出了基于时空关联分析的网络态势评估方法,通过对多角度安全信息的融合,挖掘出攻击间的因果关联;文献[12]提出了基于挖掘攻击场景的态势评估方法,通过还原攻击路径,实现网络安全态势的评估。以上方法进行了攻击间的因果关联,但该方法均以攻击图为基础,其无法实现对攻击阶段的识别评估。为解决该问题,本文提出了基于攻击模式识别的网络安全态势评估方法,从攻击者的角度进行评估,依据建立的攻击模式库,通过对攻击间的因果分析识别出攻击所处的阶段,并将攻击阶段作为态势评估要素,经过态势要素融合和节点态势融合得到网络整体安全态势。在此基础上,依据构建的攻击阶段状态转移图(State Transition Diagram, STG),结合漏洞与服务信息,实现对网络安全态势的预测。

1 网络安全态势评估模型

随着网络规模的不断扩大,网络中的安全传感器数量也在不断增多,产生海量、多源、异构的安全报警数据。该数据存在着大量的错报误报,且分散独立,无法对网络攻击作出及时的防护响应,因此通过关联攻击事件内部的逻辑关系,可还原出攻击场景,从而提高网络攻击的检测能力,实现对网络安全态势的实时评估与预测。

下面首先对评估模型中出现的术语进行定义。

定义1 攻击发生概率。是指将多个网络检测设备的报警数据进行信息融合,得到的某种攻击已经发生的可能性,以 $m(h)$ 表示。

定义2 攻击阶段支持概率。是指已发生攻击在整个攻击意图中所处的某个阶段状态的可能性,以 $s(h)$ 表示。

定义3 攻击阶段转移概率。是指攻击从目前所处的阶段转移到攻击意图中的下一个阶段的可能性,以 $ns(h)$ 表示。

定义4 攻击威胁。是指攻击所处的阶段状态所带来的影响,是专家对攻击破坏性的评估打分,以 $t(h)$ 表示。

本文提出的网络安全态势评估模型首先对网络中的多源数据进行信息融合,对融合后的结果进行因果分析,识别出攻击意图与当前的攻击阶段,并将攻击阶段作为态势要素进行节点评估。在计算整个网络的安全态势时,采取自下而上、先局部后整体的策略,其评估框架如图1所示。

依据上述评估模型,基于攻击模式识别的网络安全态势评估方法的实施步骤如下所示。

步骤1 信息融合。对网络中的多源报警数据进行信息融合,以减弱数据的冗余与误报,得到更加准确的攻击发生概率 $m(h)$ 。

步骤2 攻击阶段识别。对已经发生的攻击进行关联分析,得到攻击阶段支持概率 $s(h)$ 。

步骤3 节点态势评估。根据攻击阶段与其相对应的攻击威胁,计算节点的安全态势。

步骤4 网络整体态势评估。将节点态势依据其权重进行融合,得到网络的安全态势。

步骤5 网络态势预测。依据攻击阶段状态转移所依赖的漏洞信息与本节点的漏洞信息,得到攻击意图转移概率 $ns(h)$,并依此对网络安全态势进行预测。

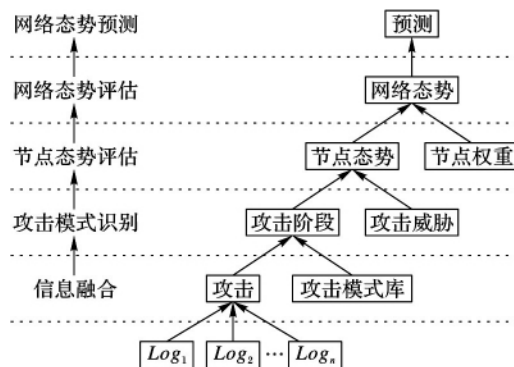


图1 基于攻击模式识别的网络安全态势评估模型

根据上述评估模型,对网络安全态势进行如下建模。

1) 报警信息 Log, 包括入侵检测系统、防火墙、系统日志等传感器检测到的报警日志,使用一个六元组 $(id, time, type, content, id_s, id_d)$ 来表示。其中: id 是报警信息的唯一标识符; $time$ 是该报警的产生时间; $type$ 是报警信息的类型, $type \in \{Sys, IDS, Firewall\}$; $content$ 是报警信息的内容; id_s 是报警信息产生的节点; id_d 是该报警信息检测的目标节点。

2) 融合后的安全事件 Alert, 使用一个七元组 $(id, time, Sip, Dip, Sport, Dport, AttackType)$ 来表示。其中: id 是该事件的唯一标识符; $time$ 是该事件的发生时间; Sip 是攻击者的源地址; Dip 是攻击的目标地址; $Sport$ 是攻击者的源端口; $Dport$ 是攻击的目的端口; $AttackType$ 是本次安全事件使用的攻击类型。

3) 网络攻击模式 AttackPattern, 使用 (s_i, s_j) 来描述攻击模式 $s_i, s_j \in S$, S 为一系列的攻击者状态集合。 s_i, s_j 分别为攻击的前提状态与后续状态,即 $s_i = pre(s_j)$, $s_j = post(s_i)$ 。在现实网络中完成一次完整的攻击场景,需要多个攻击序列组合在一起,按照因果关系形成网络攻击模式。

4) 主机信息 hostInf, 使用一个五元组 $(HostIp, Services, SoftV, Vuls, Weight)$ 来表示。其中: $HostIp$ 标识主机的网络地址; $Services$ 是主机上运行着的服务/端口列表; $SoftV$ 是主机上的软件列表; $Vuls$ 是该主机上的脆弱性列表; $Weight$ 是该主机在网络中的重要程度。

2 基于攻击模式识别的网络态势评估算法

2.1 数据融合

网络多源传感器源源不断地产生海量异构报警信息,来

自入侵检测系统、防火墙、系统日志的报警信息在不同的层面上反映着网络的安全状况,但其无法直接应用于攻击模式识别。其一,不同的安全产品一般定义了不同的报警格式,造成海量的异构报警处理上混乱;其二,现有安全产品由于设计上固有的缺陷,其报警信息存在着大量的冗余与误报,因此必须对报警信息进行数据融合,使多源异构报警相互补充、相互印证,以融合成更加准确可信的报警信息。

首先对报警信息进行预处理。先对数据进行清洗,通过设置过滤规则,将不符合规范的数据过滤掉。例如字段缺省、参数错误、超出设定范围,视此类报警为非法信息,将被直接过滤掉。其次为方便后续报警信息的处理,对多源异构数据统一格式,转化为通用的可扩展标记语言(Extensible Markup Language, XML)公共数据模型。

面对海量冗余的报警信息,为减轻后续整体融合的负担,避免造成网络阻塞,并增加报警信息的可读性,便于管理员对网络状况的及时了解,需对报警信息进行聚类,将在属性上重复或相似的多条报警聚合成同一条报警。其具体算法详见文献[8]。

最后对聚类后的报警进行数据融合,以减少单个传感器的漏报与误报,从而进一步精简安全报警信息的数量、提高安全报警信息的质量。统计传感器得到的报警信息 Log_i 与该传感器对相应攻击的检测率 w_i ,然后将各传感器的报警信息经过 D-S(Dempster-Shafer)证据理论合成,得到更加精确的攻击发生概率 $m(h)$ 。其具体算法详见文献[13]。

2.2 攻击阶段识别

定义 5 攻击关联度。是指两个攻击间的关联程度,用于确定两个攻击属于同一攻击场景的可能性,记为 $cor(a, b)$ 。a, b 是两个安全事件,它们之间的关联度函数为:

$$cor(a, b) = \frac{[\sum_{k=1}^n \alpha_k Feature_k(a, b)]}{[\sum_{k=1}^n \alpha_k]} \quad (1)$$

其中 $Feature_k(a, b)$ 和 α_k 分别表示第 k 个特征属性之间的关联度和相应的权重。其中特征值与相应权重的选取参考文献[14]。

在攻击阶段识别中,首先将数据融合后的安全事件与攻击模式数据库中的模板进行匹配,并通过计算攻击间的关联性来确定攻击所处的具体阶段。其具体算法如下所示。

算法 1 攻击阶段识别算法。

Input: $Alter_i$ 表示融合后的报警信息; $AttackPattern$ 表示攻击模式库; δ 表示设置攻击关联度阈值。

Output: $s(h)$ 表示攻击阶段支持概率; $TPList$ 表示实时攻击场景。

Method:

```
for each new received  $Alter_i$  do
    Match the alert in  $AttackPattern$ 
    if alert match success then
        Create a new node for  $Alter_i$  in  $TPList$ 
    end if
    Calculate  $cor(Alter_i, pre(Alter_i))$ 
    if  $cor(Alter_i, pre(Alter_i)) < \delta$  then
        Delete  $Alter_i$  from  $TPList$ 
    else
        Calculate  $s(h)$ 
    end if
end for
```

攻击阶段识别算法将每收到的一个报警信息与攻击模式库进行匹配,并将匹配的记录放到实时攻击场景中,并计算该

报警与其在实时攻击场景中前提报警之间的攻击关联度,通过阈值判断是否对其剪枝。对通过阈值的安全事件,计算其攻击阶段支持概率 $s(h)$ 。本文给出攻击阶段支持概率的计算方法如下所示:

$$s(h) = \prod_{i=1}^n m(T_i) \cdot \prod_{i=1}^n cor(T_i, T_{i+1}) \quad (2)$$

其中: T_i 为第 i 个攻击阶段的攻击信息, n 为当前攻击所处的攻击阶段。

2.3 网络安全态势评估量化

网络安全态势评估采取自下而上、先局部后整体的策略,通过对节点态势与其相应权重的融合,来评估网络安全态势。

首先,对节点态势进行评估。将攻击阶段支持概率 $s(h)$ 结合该攻击阶段所对应的攻击威胁 $t(h)$,得到该攻击阶段对节点态势的影响 e :

$$e = s(h) \cdot t(h) \quad (3)$$

如果在同一阶段检测到该节点受到多个攻击,则节点安全态势 SA 为多个攻击对态势影响的累加和:

$$SA = \sum_{i=1}^n e_i \quad (4)$$

其中 i 为检测到的攻击个数。

得到网络节点安全态势后,根据网络各个节点的重要程度 w_i ,计算整个网络的安全态势 NSA:

$$NSA = \sum_{i=1}^n SA_i \cdot w_i \quad (5)$$

其中 i 为网络中节点的个数。

3 基于状态转移图的网络态势预测算法

首先需要构建攻击阶段状态转移图(STG), $STG = (S_0, A_i, E)$,如图 2 所示。 S_0 表示尚未发起任何攻击的初始状态, $A_i = \{A_1, A_2, \dots, A_n\}$ 表示网络攻击模式, S_0 与 A_i 中的攻击阶段构成了攻击图中所有的节点集合 $E \subset (S_0 \times A_i) \cup A_i$ 表示边的集合,代表节点之间的关联关系,即为能够成功实施下一阶段所需的漏洞与主机配置信息。 $e_i = \{n_1 \& n_2 \& \dots \& n_i \mid n_1 \& n_3 \& \dots \& n_j \mid \dots \mid n_x \& n_y \& \dots \& n_z\} \subset E$ 其中 n_i 表示一个漏洞或主机配置信息;与关联 $n_1 \& n_2 \& \dots \& n_i$ 表示只有 n_1, n_2, \dots, n_i 都满足时,才能够达到下一阶段;或关联 $n_1 \& n_2 \& \dots \& n_i \mid n_1 \& n_3 \& \dots \& n_j$ 表示只要任意一个与关联满足时,即可达到下一阶段。该图类似于传统的攻击状态转移图,但其却具有明显的差别。该图从攻击者的角度进行构建,图中状态节点不是防护主机的安全状态,而是攻击者的攻击阶段。而且攻击者的攻击手段有限,该方法能够有效避免传统状态转移图状态空间爆炸的问题。

网络安全态势预测算法依据构建的攻击阶段状态转移图,结合攻击意图的识别与当前所处的攻击状态,来预测攻击者下一时刻可能实施的攻击动作,以此对网络安全态势值进行预测评估。该算法是通过各个节点态势的预测来判断整个网络未来的发展趋势,其具体步骤如算法 2 所示。

算法 2 网络安全态势预测算法。

Input: 当前检测到的攻击阶段 $s(h)$ 、攻击阶段状态转移图 STG。

Output: 网络安全态势预测值 NSA。

Method

```
for each  $host_i$  do
     $SA_i = 0$ 
    Get the  $hostInf$  of  $host_i$ 
    for each attack state do
```

```

if hostInf satisfy  $e[h \rightarrow post(h)]$  then
     $ns(h) = 1$ 
else
     $ns(h) = 0$ 
end if
 $s(post(h)) = s(h) \cdot ns(h)$ 
 $SA_i += s(post(h)) \cdot t(post(h))$ 
end for
end for
 $NSA = \sum_{i=1}^n SA_i \cdot w_i$ 

```

算法2中,首先对网络中的各个节点进行漏洞扫描,得到漏洞信息,并统计主机的配置信息;对节点中检测到的各个攻击的阶段转移概率进行计算,通过在攻击阶段状态转移图STG中找出相应攻击当前阶段的状态转移条件,使之与本主机的漏洞与配置信息进行匹配,如果能够满足转移条件, $ns(h) = 1$,否则 $ns(h) = 0$;根据状态转移概率得到后续阶段的发生概率,再结合后续阶段的攻击威胁,可得到节点的安全态势预测值为:

$$SA = \sum_{i=1}^n s(h) \cdot ns(h) \cdot t(post(h)) \quad (6)$$

最后结合各节点的权重,得到整体网络的安全态势预测值。

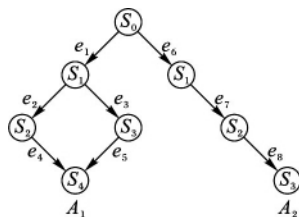


图2 攻击阶段状态转移图

4 实验与结果分析

为验证本文模型及算法的可行性与有效性,搭建了一个实验网络,其网络拓扑结构如图3所示。网络中包括防火墙、交换机、入侵检测系统、Web服务器、文件服务器、工作站以及一台攻击主机。其中:IDS安装SNORT入侵检测系统,Web服务器和工作站均安装Windows操作系统,文件服务器安装Linux操作系统。在数据采集上选用网络运行中IDS、防火墙产生的报警数据,以及各主机的安全审计日志。

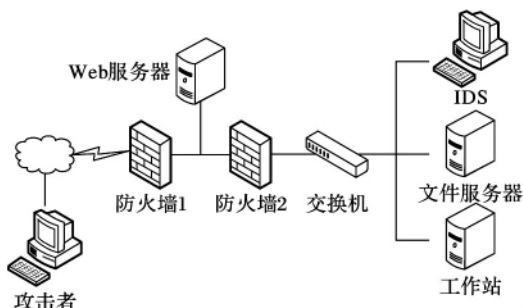


图3 实验环境网络拓扑

攻击者对该网络实施了一次特洛伊木马攻击。攻击者首先对目标网络进行IPsweep攻击,扫描搜寻有效主机;发现有效主机Web服务器,并利用Apache Web Server分块编码远程溢出漏洞对其进行缓存溢出攻击,从而获得本地访问权限;然后攻击者利用文件服务器上的网络文件系统(Network File System, NFS)导出表的设置不当,使用NFS Shell程序,通过NFS协议修改文件服务器上的文件。随后在文件服务器上查

找由工作站安装的可执行二进制代码,并在其中安装一个特洛伊木马程序。最后攻击者通过工作站运行该二进制代码执行程序,激活木马,从而获得对这台工作站的控制权。

假设该攻击步骤为已知方法,则根据攻击模式与它所依赖的漏洞与主机配置信息可以构建攻击阶段状态转移图,该攻击模式记为A1,如图4所示。其中状态转移条件 e_1 到 e_5 分别为网络控制报文协议设置不当、Apache Web Server分块编码远程溢出漏洞、NFS导出表设置不当、 \emptyset 、 \emptyset 。

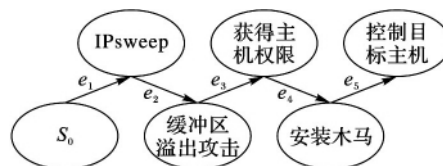


图4 攻击阶段状态转移图

结合入侵检测报警数据和审计日志,依据第3章提出的态势评估方法,对网络中各节点依次进行数据融合、攻击阶段识别、网络安全态势评估,从而得到实时的网络安全态势值。以主机Web服务器为例,在检测到该主机受到缓冲区溢出攻击时,经过数据融合得到攻击发生概率,计作 $m(a) = 0.923$;而在之前检测到该主机受到IPsweep攻击,并且 $m(b) = 0.907$,两个攻击同属于Attack Model A1中,计算两个攻击之间的关联度 $cor(a, b) = 1$,因此可以得到当前攻击者处于A1攻击模式的第2个阶段的攻击阶段支持概率 $s(A1_state2) = m(a)m(b)cor(a, b) = 0.923 \times 0.907 \times 1 = 0.837$ 。再结合该攻击阶段的攻击威胁 $t(A1_state2) = 0.4$,得到该攻击对Web服务器节点的安全态势的影响 $e = s(A1_state2)t(A1_state2) = 0.837 \times 0.4 = 0.335$ 。而在此时仅仅检测到该攻击,因此Web服务器节点的安全态势只受到该攻击的影响,则此刻的安全态势值 $SA = e = 0.335$ 。最后结合各节点的权重便可计算出整个网络的安全态势值。其权重值的选取,依据各节点重要程度,设置Web服务器、文件服务器、工作站的权重分别为0.2 0.3 0.5。按照此方法得到网络的安全态势值如表1所示。

表1 网络安全态势值计算结果

攻击阶段	攻击发生概率	Web服务器	文件服务器	工作站	NSA
A1_state1	0.907	0.036	0	0	0.0072
A1_state2	0.923	0.335	0	0	0.0670
A1_state3	0.874	0	0.366	0	0.1098
A1_state4	0.890	0	0.456	0	0.1368
A1_state5	0.848	0	0	0.442	0.2210

根据上述计算结果,将网络安全态势值绘制成图,以更加直观的形式展现,如图5所示。其中横轴为时间,纵轴为态势值,而态势值越大表示此刻网络中受到的攻击危害程度越大。通过图5中可以看出,对权重越大的主机进行攻击,其对整体网络的影响就越大;而且随着攻击阶段的不断深入,攻击者逐渐实现攻击目的,相应的网络安全态势值也越来越大,其基本符合攻击实情。相比文献[7]仅仅考虑单个攻击的影响,没有考虑攻击的前后因果,其计算结果中A1_state4受到安装木马攻击时的网络安全态势值要明显高于后续的步骤,而本文的计算结果基本随着攻击阶段的深入逐渐增加,因此本文提出的方法更具合理性。其次文献[7]的方法只有当网络中出现攻击时,才能计算网络安全态势,其取值仅有离散的几个点,表现在图5中攻击发生时计算得到的几个拐点;而本文以

攻击阶段为评估要素,其取值具有连续性,因此本文所绘制的评估图更具实用参考价值。

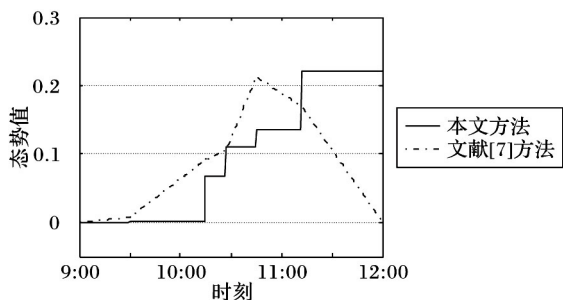


图5 网络安全态势评估

最后,本文对网络安全态势进行预测,按照所提出的方法,将各个节点依据攻击阶段状态转移图评估状态转移概率以预测下一时刻的安全态势。以节点 Web 服务器为例,在检测到该主机受到 IP sweep 攻击时,经过攻击模式识别匹配出攻击者正按照 A1 攻击模式实施攻击,经过漏洞扫描与统计主机配置信息,发现其包含 Apache Web Server 分块编码远程溢出漏洞,其能够满足状态转移条件 e_2 , 则 $ns(h) = 1$ 。该主机当前只受到该攻击模式的攻击,因此预测下一时刻 Web 服务器的安全态势 $SA = s(A1_state1) ns(h) t(A1_state2) = 0.0907 \times 1 \times 0.4 = 0.363$ 。最后结合各节点的权重便可预测出整个网络的安全态势值。按照此方法得到网络的安全态势预测值如图 6。

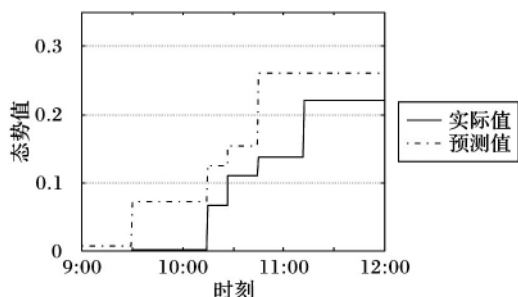


图6 网络安全态势预测

从图 6 可以看出,本文提出的方法能够准确地预测出网络攻击下一时刻的攻击行为,并能提前对网络安全态势值的变化作出预判,有利于管理员对网络中出现的安全状况及时作出相应的防护措施。本文方法虽然不是去预测下一时刻与真实值相近的态势,但是能通过阶段的转移较好地预测态势的发展趋势,且在与文献[7, 15]相比较中,该方法无需对历史序列进行训练,具有更高的预测效率。

5 结语

本文对现有的网络安全态势评估方法进行了分析比较,并结合目前网络攻击多步化、协同化的特点,提出了基于攻击模式识别的网络安全态势评估方法。首先,对网络中的多源数据进行信息融合,对融合后的结果因果分析,识别出攻击意图与当前的攻击阶段,并将攻击阶段作为态势要素进行节点评估,并采取自下而上、先局部后整体的策略,得到整个网络的安全态势;其次,构建攻击阶段状态转移图,结合主机的漏洞与配置信息,推算攻击者能够成功实施下一阶段的转移概率,以此预测网络安全态势的发展趋势;最后,通过网络实例进一步验证了本文提出方法的适用性与效率。本文的研究方法依赖于已知的攻击模式,因此日后的研究方向包括完善评

估模式,并加强对新型攻击场景还原的研究,进一步增强模型的通用性。

参考文献:

- [1] BASS T. Intrusion detection systems & multisensory data fusion: creating cyberspace situational awareness [J]. Communications of the ACM, 2000, 43(4): 99-105.
- [2] D'AMBROSIO B. Security Situation Assessment and Response Evaluation (SSARE) [C]// DISCEX01: Proceedings of 2001 DARPA Information Survivability Conference & Exposition. Washington, D. C.: IEEE Computer Society, 2001: 387-394.
- [3] ABAD C, YURCIK W. UCLog+: a security situational awareness system for incident storage, querying, and correlation [C]// ICTSM 2006: Proceedings of the 14th International Conference on Telecommunication Systems Modeling and Analysis. Washington, D. C.: IEEE Computer Society, 2006: 316-322.
- [4] 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): 885-997. (CHEN X Z, ZHENG Q H, GUAN X H, et al. Quantitative hierarchical threat evaluation model for network security [J]. Journal of software, 2006, 17(4): 885-997.)
- [5] 张建锋. 网络安全态势评估若干关键技术研究[D]. 长沙: 国防科学技术大学, 2013: 19-35. (ZHANG J F. Research on key technologies of network security assessment [D]. Changsha: National University of Defense Technology, 2013: 19-35.)
- [6] 李方伟,杨绍成,朱江. 基于模糊层次法的改进网络安全态势评估方法[J]. 计算机应用, 2014, 34(9): 2622-2626. (LI F W, YANG S C, ZHU J. Improved network security situational assessment method based on FAHP [J]. Journal of computer applications, 2014, 34(9): 2622-2626.)
- [7] 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. (WEI Y, LIAN Y F, FENG D G. A network security situational awareness model based on information fusion [J]. Journal of computer research and development, 2009, 46(3): 353-362.)
- [8] 席荣荣,云晓春,张永铮. 基于环境属性的网络威胁态势量化评估方法[J]. 软件学报, 2015, 26(7): 1638-1649. (XI R R, YUN X C, ZHANG Y Z. Quantitative threat situational assessment based on contextual information [J]. Journal of software, 2015, 26(7): 1638-1649.)
- [9] 张勇,谭笑彬,崔孝林,等. 基于 Markov 博弈模型的网络安全态势感知方法[J]. 软件学报, 2011, 22(3): 495-508. (ZHANG Y, TAN X B, CUI X L, et al. Network security situation awareness approach based on Markov game model [J]. Journal of software, 2011, 22(3): 495-508.)
- [10] 席荣荣,云晓春,张永铮,等. 一种改进的网络安全态势量化评估方法[J]. 计算机学报, 2015, 38(4): 749-758. (XI R R, YUN X C, ZHANG Y Z, et al. An improved quantitative evaluation method for network security [J]. Chinese journal of computers, 2015, 38(4): 749-758.)
- [11] 吕慧颖,彭武,王瑞梅,等. 基于时空关联分析的网络实时威胁识别与评估[J]. 计算机研究与发展, 2014, 51(5): 1039-1049. (LYU H Y, PENG W, WANG R M, et al. A real-time network threat recognition and assessment method based on association analysis of time and space [J]. Journal of computer research and development, 2014, 51(5): 1039-1049.)
- [12] ONWUBIKO C, OWENS T. Situational awareness in computer network defense principles, methods and applications [M]. Hershey: IGI Global Snippet, 2012: 125-137.

(下转第 226 页)

参考文献:

- [1] 田文君. 基于深度图像的三维人脸特征提取[D]. 北京: 北京交通大学, 2009. (TIAN W J. 3D face feature extraction based on depth image [D]. Beijing: Beijing Jiaotong University, 2009.)
- [2] 范文婕, 王命延, 杨文姬. 基于深度图像的指尖和掌心特征提取方法[J]. 计算机应用, 2015, 35(6): 1791 – 1794. (FAN W J, WANG M Y, YANG W J. Feature detection method of fingertip and palm based on depth image [J]. Journal of computer applications, 2015, 35(6): 1791 – 1794.)
- [3] CUI W, WANG W, LIU H. Robust hand tracking with refined CAMshift based on combination of depth and image features [C]// Proceedings of the 2012 IEEE International Conference on Robotics and Biomimetics. Piscataway, NJ: IEEE, 2012: 1355 – 1361.
- [4] ZHAO Y, LIU Z, CHENG H. RGB-depth feature for 3D human activity recognition [J]. China communications, 2013, 10(7): 93 – 103.
- [5] KARPUSHIN M, VALENZISE G, DUFAUX F. Local visual features extraction from texture + depth content based on depth image analysis [C]// Proceedings of the 2014 IEEE International Conference on Image Processing. Piscataway, NJ: IEEE, 2014: 2809 – 2813.
- [6] LU C, JIA J, TANG C. Range-sample depth feature for action recognition [C]// Proceedings of the 2014 IEEE Conference on Computer Vision and Pattern Recognition. Piscataway, NJ: IEEE, 2014: 772 – 779.
- [7] JALAL A, UDDIN M Z, KIM T S. Depth video-based human activity recognition system using translation and scaling invariant features for life logging at smart home [J]. IEEE transactions on consumer electronics, 2012, 58(3): 863 – 871.
- [8] LIU Y, LASANG P, SIEGEL V, et al. Geodesic invariant feature: a local descriptor in depth [J]. IEEE transactions on image processing, 2015, 24(1): 236 – 248.
- [9] DALAL N, TRIGGS B. Histograms of oriented gradients for human detection [C]// Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Piscataway, NJ: IEEE, 2005: 886 – 893.
- [10] SPINELLO L, ARRAS K O. People detection in RGB-D data [C]// Proceedings of the 2011 IEEE/RSJ International Conference on Intelligent Robots and Systems. Piscataway, NJ: IEEE, 2011: 3838 – 3843.
- [11] LIN Y, WEI S, FU L. Grasping unknown objects using depth gradient feature with eye-in-hand RGB-D sensor [C]// Proceedings of the 2014 IEEE International Conference on Automation Science and Engineering. Piscataway, NJ: IEEE, 2014: 1258 – 1263.
- [12] WANG N, GONG X, LIU J. A new depth descriptor for pedestrian detection in RGB-D images [C]// Proceedings of the 21st International Conference on Pattern Recognition. Piscataway, NJ: IEEE, 2012: 3688 – 3691.
- [13] BOYKOV Y, VEKSLER O, ZABIH R. Fast approximate energy minimization via graph cuts [J]. IEEE transactions on pattern analysis and machine intelligence, 2001, 23(11): 1222 – 1239.
- [14] DUAN F, WANG Y, YANG L, et al. Spatio-temporal consistency in stereoscopic video depth map sequence estimation [J]. Journal of information and computational science, 2014, 11(18): 6497 – 6508.
- [15] LEE S B, HO Y S. Temporally consistent depth map estimation for 3D video generation and coding [J]. China communications, 2013, 10(5): 39 – 49.
- [16] 张永库, 李云峰, 孙劲光. 基于多特征融合的图像检索[J]. 计算机应用, 2015, 35(2): 495 – 498. (ZHANG Y K, LI Y F, SUN J G. Image retrieval based on multi-feature fusion [J]. Journal of computer applications, 2015, 35(2): 495 – 498.)
- [17] RICHARDT C, ORRD D, DAVIES I, et al. Real-time spatiotemporal stereo matching using the dual-cross-bilateral grid [C]// Proceedings of the 2010 European Conference on Computer Vision. Berlin: Springer, 2010: 510 – 523.

Background

This work is partially supported by the National Key Technology Research and Development Program of the Ministry of Science and Technology of China (2012BAH37F02), the Science and Technology Innovation Project of Ministry of Culture of China (2014KJXXM08).

DUAN Fengfeng, born in 1982, Ph. D. candidate, lecturer. His research interests include image processing and retrieval, Internet media and new media.

WANG Yongbin, born in 1963, Ph. D., professor. His research interests include Internet media and new media, multimedia big data processing, information security.

YANG Lifang, born in 1984, Ph. D., engineer. Her research interests include image processing and retrieval, high-dimensional indexing.

PAN Shujing, born in 1991, M. S. candidate. Her research interests include image processing and retrieval.

(上接第 198 页)

- [13] 赖积保. 基于异构传感器的网络安全态势感知若干关键技术研究[D]. 哈尔滨: 哈尔滨工程大学, 2009: 54 – 73. (LAI J B. Research on some key technologies for heterogeneous sensors-based network [D]. Harbin: Harbin Engineering University, 2009: 54 – 73.)
- [14] KAVOUSHI F, AKBARI B. Automatic learning of attack behavior patterns using Bayesian networks [C]// IST2012: Proceedings of the 6th International Symposium on Telecommunications. Washington, D. C.: IEEE Computer Society, 2012: 999 – 1004.
- [15] 韦勇, 连一峰. 基于日志审计与性能修正算法的网络安全态势评估模型[J]. 计算机学报, 2009, 32(4): 763 – 772. (WEI Y, LIAN Y F. A network security situational awareness model based on log audit and performance correction [J]. Chinese journal of computers, 2009, 32(4): 763 – 772.)

Background

This work is partially supported by the National Natural Science Foundation of China (61309013).

WANG Kun, born in 1975, Ph. D. associate professor. His research interests include network security, data mining.

QIU Hui, born in 1990, M. S. candidate. His research interests include network security, situation awareness.

YANG Haopu, born in 1993, M. S. candidate. Her research interests include network security, attack detection.