

基于 EA-DS 证据理论的安全事件关联分析

龙 春^{1,2}, 申罕骥¹, 李 俊¹

(1 中国科学院 计算机网络信息中心, 北京 100190; 2 中国科学院大学, 北京 100190)

摘 要: 为了对多源安全事件进行关联分析, 提出了基于 EA-DS 证据理论的安全事件关联分析方法. 该方法结合所在网络环境将来自多个不同种类的安全传感器数据进行证据融合, 计算网络服务威胁状态置信度, 能够快速发现高威胁状态的服务并采取相应的措施进行响应. 通过在实际网络环境中进行实验和对比, 该方法有较好的高危攻击发现能力.

关键词: 安全事件; 报警日志; 关联分析聚合; EA-DS 证据理论

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2015)11-0046-07

Security Events Fusion Based on EA-DS Evidence Theory

LONG Chun^{1,2}, SHEN Han-ji¹, LI Jun¹

(1 Computer Network Information Center, Chinese Academy of Science, Beijing 100190, China;

2 University of Chinese Academy of Sciences, Beijing 100190, China)

Abstract: In order to correlate and analyze multi-source security events, this paper has proposed a security event correlation analysis method which is based on Environment Awareness Dempster-Shafer evidence theory (EA-DS). The method combined various security sensor data in the network environment for evidence fusion, computed threat state confidence of network service, and detected high threat state of the service rapidly. Extensive experiments show that EA-DS has good ability to find high risk threat in the real network environment.

Key words: security events; alert log; correlation analysis fusion; EA-DS evidence theory

1 引言

在大规模网络系统中, 存在多个不同类型的安全传感器, 这些传感器产生大量的安全事件数据. 把不同来源的传感器的安全数据进行关联能够有效解决安全数据孤岛问题, 大大提升安全事件管理能力. 另外, 由于安全监控设备本身的一些局限性, 产生的安全事件报警信息存在大量误报, 如入侵检测系统、防火墙系统以及恶意代码防护系统等, 这些报警信息本身就存在一定程度的不确定性. DS 证据理论^[1]能够处理不确定性信息, 所以采用 DS 证据理论对来自不同位置、不同类型的安全设备的安全信息进行关联分析是非常适合的. 同时将传感器和网络服

务所在拓扑环境结合起来, 本文提出了环境感知的 EA-DS 证据理论 (Environment Awareness Dempster Shafer Evidence Theory) 来进行多源安全传感器数据关联融合.

2 国内外研究现状

DS 证据理论在信息融合的应用中, 有着较强的理论基础, 不需要先验信息且算法结构简单, 但也存在两个问题: 一是证据获取的主观性; 二是高冲突证据合成的局限性.

DS 证据理论中的基本概率分配函数赋值主要依赖专家知识和经验存在有限性、主观性, 会导致证据合成结果偏差性和倾向性问题的出现. 在处理冲

收稿日期: 2015-01-22; 修回日期: 2015-03-17

基金项目: 国家科技支撑计划课题 (2012BAH01B03); 科技部“九七三”课题 (2012CB315803); 科技部“八六三”课题 (2013AA010601); 中科院战略性先导专项 (XDA06010306)

突证据时,DS 组合规则有时会导致结果有悖常理.采用 DS 组合规则时,对各证据的信任程度是等同的,没有区分每一个证据的重要性,这与实际情况不符.Zadeh 悖论^[2]显示,当冲突因子 K 过大时,DS 组合规则不能对证据进行好的组合.在冲突因子较大时,DS 组合规则的鲁棒性会变的很差.

对于产生违反直观结果原因,国内外研究者开展了很多相关研究,一些研究者认为产生问题的原因是由 DS 组合规则造成的,特别是其在处理冲突时的丢弃式处理方式.持该观点的研究者认为需要修改组合规则.Haenni R 等^[3]认为,反直观结果来自证据源而非证据组合规则,在组合之前应对证据进行修正,使其从数学和逻辑上更加合理.

此外,还存在一种观点,认为违反直观结果来自辨识框架的不完整.如 Smets 等^[4]提出开放世界假设,邓勇^[5]等设计非完备框架及相应组合方法.上述方法大都属于组合式证据融合方法.杨艺^[6]等利用多因素排序融合方式实现了证据的选择性融合.随着研究的深入,有关冲突证据组合问题的新思路、新方法将不断涌现.当前有关证据理论的研究主要集中在冲突证据组合方面.

导致冲突的原因主要来自于证据的不可靠,并且在证据合成过程中将所有证据同等看待,这与现实中网络和系统的复杂情况也不一致.本文根据不同的环境设定不同证据的接受程度,从而减少证据冲突.另外,在证据合成之前对证据冲突情况进行计算,对高冲突证据进行处理,通过判定,降低准确度和和相关度低的证据的置信度.

3 环境感知 DS 的安全事件关联系统设计

基于环境感知的 DS 证据理论安全事件关联系统架构如图 1 所示.

3.1 对安全传感器数据的预处理

3.1.1 入侵检测系统数据

入侵检测系统数据的预处理分为报警信息标准化、误报警信息去除、报警信息聚合等阶段.

报警信息标准化.为提高入侵检测系统的互操作性,IETF 的入侵检测工作组(Intrusion Detection Work Group)制订了入侵检测消息交换格式 ID-MEF(Intrusion Detection Message Exchange Format).为了开展后续的事件关联分析工作,本文选取该格式中的部分类用来进行后续的关联处理工作.

定义 1 入侵检测事件(IDS_Event)包括 sen-

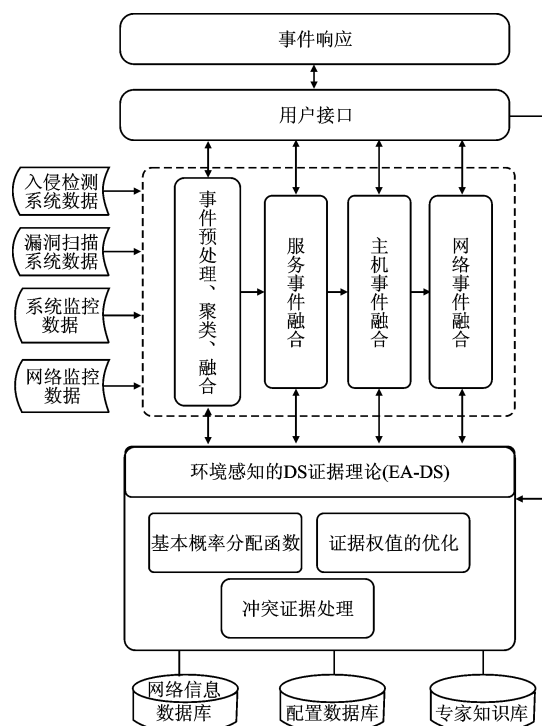


图 1 环境感知的 DS 理论的安全事件关联系统架构
sor 编号、报警事件号(用于 IDS 内部标识,每个唯一)、检测时间、源目的 IP 和端口、IP 层协议类型、报警特征、报警级别、CVE 等信息.入侵检测事件表示为一个多元组 $IDS_Event = \{SensorID, DetectTime, SrcIP, SrcPort, TargetIP, TargetPort, Protocol, Signature, Level, CVE_ID\}$.

误报警信息去除.对于不同的目标系统和不同网络服务类型,有些报警信息是误报或者无用信息,这类信息在预处理阶段需要进行去除.去除的方法主要是结合目标主机和服务的信息对 IDS_Event 按照规则进行筛选.

3.1.2 漏洞扫描系统数据

漏洞扫描系统利用已知的攻击手段对目标信息系统进行自动化的攻击,以检测目标系统是否有相应的漏洞.漏洞扫描系统对于系统威胁状态有着非常重要的作用.对系统漏洞的数据格式定义如下所示.

定义 2 系统漏洞事件(Vul_Event).系统漏洞事件包括漏洞扫描器编号、漏洞编号、漏洞类型、扫描对象 IP、服务端口、漏洞特征、漏洞危险程度、对象危险程度、CVE 等信息. $Vul_Event = \{Sensor_ID, Vul_ID, Vul_Type, Dst_IP, Dst_Port, Vul_Sig, Vul_Lev, Dst_Lev, CVE_ID\}$.

3.1.3 系统监控数据

系统监控传感器主要对系统的运行状态特征进

行监控,这类特征很多,这里主要提取一些和安全相关的指标,包括系统 CPU 利用率、内存利用率、服务响应延迟、非法访问记录次数、高危入侵报警等。

定义 3 系统监控事件(Sys_Event). 系统监控事件是指对系统监控信息进行抽取和预处理之后形成事件记录 $\text{Sys_Event} = \{\text{CPU_Usage}, \text{Mem_Usage}, \text{Service_Lag}, \text{IllAccess_Num}, \text{Intrusion_Alert}\}$

3.1.4 网络监控数据

系统所在网络带宽以及流量状态反映系统及服务的安全状态,网络监控传感器在判断威胁状态时也可以起到很重要的作用. 其中最重要的网络监控指标包括带宽和传输包数,这两项指标及其变化情况直接反应了网络的安全状态。

定义 4 网络监控事件(Network Event). 网络监控事件是指规定时间内网络带宽平均使用率和包传输速率, $\text{Network_Event} = \{\text{Band_Usage}, \text{Packet_Rate}\}$.

3.2 基于 EA-DS 理论的服务安全状态关联分析

服务安全状态的关联直接利用各安全传感器的原始事件报警信息来确定一个服务的安全威胁状态,其判断准确程度直接影响到后续的主机以及网络的威胁状态判断。

定义 5 网络服务. 这里的网络服务是指在网络系统中为用户提供特定的信息服务,例如 www 服务、FTP 服务以及 DNS 服务等。

定义 6 服务安全状态辨识框架. 服务安全状态辨识框架 $\Theta = \{\text{High}, \text{Other}\}$, 其中 High 指的是服务安全状态为高危,需要立即采取处理措施, Other 指除非高危状态。

定义 7 证据接受系数. 证据接受系数是根据服务所在的网络环境,传感器位置,传感器证据对特定服务的可信程度确定的证据接受程度, $\text{Accept_Lev} \in [0, 1]$.

对服务安全状态的证据融合过程如下所示。

(1)确定目标服务. 确定需要进行安全状态评估的主机和服务,一般情况下以 IP 和端口唯一定义一个服务。

(2)根据服务所在主机网络环境情况,选择和目标服务相关的传感器,标记为 $\text{Sensor}_1, \text{Sensor}_2, \dots, \text{Sensor}_n$ 。

(3)根据传感器所在网络拓扑中的位置,对目标服务安全状态的判断能力等因素确定传感器的证据接受程度。

(4)按照服务 IP 和端口从各个传感器中抽取和目标服务相关的安全事件信息;

(5)焦元 $H = \{\text{High}\}, O = \{\text{Other}\}, U = \{\text{High} \cup \text{Other}\}$ 表示不确定. 分别计算他们的初始基本概率分配函数. 记 Sensor_n 的初始基本概率分配函数为 $m'_n(H), m'_n(O)$ 和 $m'_n(U)$ 。

(6)根据各个 Sensor 的不同证据接受程度 Accept_Lev 计算 $m_n(H), m_n(O)$ 和 $m_n(U)$, 计算方法如下:

$$m_n(H) = m'_n(H) \cdot \text{Accept_Lev},$$

$$m_n(O) = m'_n(O) \cdot \text{Accept_Lev},$$

$$m_n(U) = 1 - m_n(H) - m_n(O).$$

(7)对 n 个 Sensor 的进行冲突证据计算,如果冲突因子 k 小于可接受的阈值则进行下一步,否则对冲突证据的接受度进行调整,再重新计算冲突因子。

(8)进行 DS 证据融合,计算 $m(H) = m_1(H) \oplus m_2(H), m_n(H), m(O) = m_1(O) \oplus m_2(O), m_n(O)$

由于算法中 $H = \{\text{High}\}$ 只有一个元素,所以这里 $\text{Bel}(H) = m(H)$. 当计算得到的信度函数高于一定的阈值时,则认为该服务处于高危状态,需要进行处理。

4 EA-DS 基本概率分配函数的实现

基本概率分配函数(BPA)决定每个证据对目标命题的判断,对 BPA 的计算是非常关键的环节. 目前没有适合各个应用环境的通用的 BPA 计算模式,一般是根据具体的应用情况来设定 BPA^[7]。

各种类型的传感器在判定数据来源、数据格式上都有比较大的区别,本文根据传感器类型采取不同的 BPA 确定方法。

4.1 入侵检测传感器 BPA

在计算入侵检测传感器的 BPA 时,本文认为决定服务安全威胁状态中最关键的是入侵攻击的方式而不是攻击尝试的次数,另外在计算过程中,对于长期存在的攻击报警多数情况下为扫描探测或无效攻击,所以在计算威胁状态时要将这部分安全事件排除. 具体计算方法如下所示。

(1)提取 Δt 时间范围内的 $\text{Dst_IP}, \text{Dst_Port}$ 和目标服务匹配的 IDS_Event 。

(2)将入侵检测报警数据中的例行攻击数据排除。

(3)采用入侵检测日志聚合算法进行告警事件聚合,聚合后形成聚合报警 Clustered_Event ;

(4) 统计计算 Δt 时间范围内发生级别分别为高、中、低三个等级的聚合报警攻击的数量 E_H 、 E_M 、 E_L 。

(5) 根据设备类型和检测能力设定设备对不确定性的基本概率分配函数 $m(U)$ 。

(6) 按照以下计算方法计算 $m'(H)$ 、 $m'(O)$ ：

$$m'(H) = \min((E_H + E_M/a + E_L/b)\Delta m, 1 - m'(U)),$$

$$m'(O) = 1 - (m'(H) + m'(U)).$$

式中, a 为中等威胁类型转换, b 为低威胁类型转换因子。 Δm 为每发生一起高危攻击增加的 BPA 值。

4.2 漏洞扫描传感器 BPA

漏洞扫描是对网络服务存在安全隐患的有效检测方法。相比入侵检测系统、网络监控等传感器,漏洞扫描传感器的事件信息更新速度一般不会太高。在评估系统安全状态时,采用最近一次漏洞扫描发现的未处理漏洞。

漏洞扫描类传感器的 BPA 计算方法如下：

(1) 提取最近一次漏洞扫描中 Dst_IP、Dst_Port 和目标服务匹配的 Vul_Event。

(2) 网络服务对应的高危、中危以及低危的漏洞数量分别为 V_H 、 V_M 、 V_L ；

(3) 根据设备类型和检测能力设定设备对不确定性的基本概率分配函数 $m(U)$ 。

(4) 按照以下计算方法计算 $m'(H)$ 、 $m'(O)$ ：

$$m'(H) = \min((V_H + V_M/a + V_L/b)V_m, 1 - m'(U))$$

$$m'(O) = 1 - (m'(H) + m'(U)).$$

式中, a 为中等威胁类型转换因子, b 为低威胁类型转换因子。 Δm 为每增加一种高危漏洞增加的 BPA 值。

4.3 系统监控传感器 BPA

系统监控类传感器的数据直接来自被监控的系统本身,系统资源使用情况的异常以及服务响应速度的异常变化很多时候直接反映了系统是否被攻击。但是由于系统性能和资源利用指标和服务的访问人数、服务作业的资源需求情况直接相关,所以直接以性能指标阈值来判定服务安全状态并不合适。利用统计预测对网络安全情况进行检测也是很多研究者采取的思路,例如李仰耀^[8]提出的基于统计预测的方法对网络进行预警的方法。本文采用统计异常方法给出系统监控类传感器的 BPA 值。

在过去 m 天的同一时间段 Δt 时间里的全部 n 个观测样本观测值为(例如过去 30 天里每天 8:00 到 9:00 的一个小时内每 5 分钟观测的平均 CPU 利

用率) $x_1, x_2, \dots, x_n$ 。全部样本的均值和标准差：

$$\text{样本均值: } \bar{x}_n = \frac{1}{n} \sum_{i=1}^n x_i, \text{ 样本标准差: } \sigma = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x}_n)^2}.$$

计算过程如下所示。

(1) 如果监控发现确定的入侵,例如系统文件被篡改、未授权的用户访问则 Intrusion_Alert = 1, 则 $m'(H) = 1, m'(O) = m'(U) = 0$;

(2) 提取 Δt 时间范围内平均 CPU 利用率 CPU_Usage、内存利用率 Mem_Usage、平均服务延迟 Service_Lag。

(3) 计算当前的观测值和平均观测值之间的偏差 $e_{n+1} = x_{n+1} - \bar{x}_n$, 如果 $x_{n+1} < \bar{x}_n$, 则取 $e_{n+1} = 0$ 。

(4) 通过下面的公式计算 $m'(H)$ 和 $m'(O)$ ：

$$m'(H) = \min((1 + \frac{e_{n+1}}{\sigma})\Delta m, 1 - m'(U));$$

$$m'(O) = 1 - m'(H) - m'(U).$$

(5) 分别计算 CPU 利用率、内存利用率以及平均服务延迟的 $m'(H)$, 取三者中最大的 $m'(H)$ 作为最终的基本概率分配函数。

4.4 网络监控传感器 BPA

网络带宽的使用情况能反映服务的安全状态,特别是服务可用性这一基本指标。当网络服务遭到分布式拒绝服务攻击时,在网络带宽以及包速率方面的指标在判断威胁程度时有比较高的可信度。

在一天的同一个时间段,流量的特征基本比较类似。如图 2 所示的某线路的一周带宽使用情况。

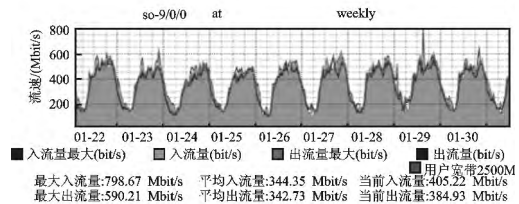


图 2 某线路一周带宽使用情况

图 2 显示样本符合正态分布特征,流量突变的情况可以作为遭受攻击的一个判断证据。和前面所述的服务主机性能监控指标一样,带宽和包速率指标来判断服务安全状态也采取基于统计分析的方法。

在过去 m 天的同一时间段 Δt 时间里的全部 n 个观测样本观测值为(例如过去 30 天里每天 8:00 到 9:00 的一个小时内每 5 分钟观测的带宽速率) $x_1, x_2, \dots, x_n$ 。全部样本的均值和标准差如下所示。

样本均值: $\bar{x}_n = \frac{1}{n} \sum_{i=1}^n x_i$;

样本标准差: $\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x}_n)^2}$;

样本均值: $\bar{x}_n = \frac{1}{n} \sum_{i=1}^n x_i$;

样本标准差: $\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x}_n)^2}$.

计算过程如下:

(1) 提取 Δt 时间范围内平均网络带宽平均使用率 Band_Usage 和包传输速率 Packet_Rate;

(2) 如果带宽超过可用带宽的 99%, 即 $\frac{\text{Band_Usage}}{\text{Avail_Band}} \geq 0.99$ 则 $m'(H) = 1, m'(O) = m'(U) = 0$;

(3) 计算当前的观测值和平均观测值之间的偏差 $e_{n+1} = x_{n+1} - \bar{x}_n$, 如果 $x_{n+1} < \bar{x}_n$, 则取 $e_{n+1} = 0$;

(4) 通过下面的公式计算 $m'(H)$ 和 $m'(O)$:

$$m'(H) = \min((1 + \frac{e_{n+1}}{\sigma})\Delta m, 1 - m'(U));$$

$$m'(O) = 1 - m'(H) - m'(U).$$

分别计算带宽使用率和包传输速率的 $m'(H)$, 取两者中最大的 $m'(H)$ 作为最终的基本概率分配函数.

5 EA-DS 对冲突证据的处理改进

上一节中对于冲突证据避免的方法中已经论述了根据传感器位置、准确度等环境信息来设定证据的接受程度, 从而在一定程度上避免证据之间的冲突. 这一节主要论述如果在根据证据接受程度修正证据之后仍然存在冲突的情况的处理办法. 由于本文提出的 EA-DS 证据理论安全事件合成方法中的焦元数量少, 出现冲突的情况只有 $m(H)$ 和 $m(O)$ 的冲突.

本文采取的方法是修正和其他证据冲突程度最高的证据接受程度来处理冲突.

(1) 如果存在传感器的 $m(H) = 1$, 则直接结束冲突处理过程以及后续的证据合成过程, 直接确定系统处于高危状态.

(2) 计算冲突因子 k , 如果 k 大于可接受的冲突阈值 k , 说明证据中存在高冲突证据.

(3) 找出 $m(H)$ 和 $m(O)$ 中最高的两个传感器 Sensor_MaxH 和 Sensor_MaxO.

(4) 计算除二者之外的高危和非高危支持度之和:

$$\text{sum}(H) = \sum_{i=1}^{n-2} m_i(H) \quad \text{sum}(O) = \sum_{i=1}^{n-2} m_i(O).$$

(5) 如果 $\text{sum}(H) \geq \text{sum}(O)$, 则 Sensor_MaxO 的接受系数临时降低 Δi , 反之如果 $\text{sum}(H) < \text{sum}(O)$ 则将 Sensor_MaxH 的接受系数临时减少 Δi ;

(6) 再次计算冲突因子, 如果 k 仍大于可接受的冲突阈值 k , 则重复步骤(2).

在之前的 BPA 计算中对于 $m(H) = 1$ 的情况是有严格要求确定发生高危安全事件才能确定, 所以对于出现 $m(H) = 1$ 时就可以结束上述判定和证据融合过程. 因为没有绝对安全的系统, 故 $m(O) = 1$ 的情况是不符合实际情况的. 当出现 $m_i(H) = 1$ 和 $m_j(O) = 1$ 的时候就直接判定 $m(H) = 1$, 这样就避免了 DS 证据理论失效的情况.

6 实验和分析

实验环境包括防火墙、服务器、入侵检测系统、漏洞检测系统, 交换机等. 网络拓扑结构如图 3 所示.

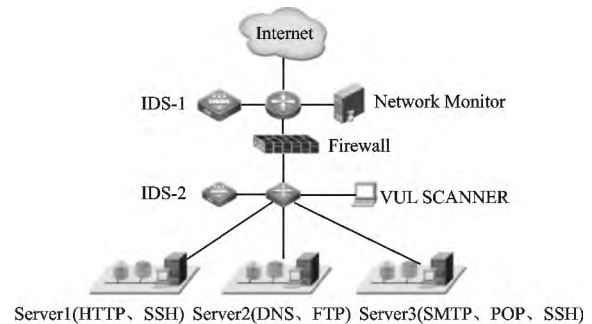


图 3 实验网络拓扑

在测试环境中, 网络连接类型为千兆以太网, 安全传感器包括入侵检测传感器 IDS-1、IDS-2, 网络监控传感器, 漏洞传感器以及系统监控传感器.

从各安全传感器中收集的一个月的原始事件数情况如表 1 所示.

表 1 传感器收集的原始事件

传感器类型	传感器	事件数	说明
入侵检测类	IDS-1	198 万	防火墙过滤之前的入侵检测报警事件数
入侵检测类	IDS-2	26 万	防火墙过滤之后的入侵检测报警事件数
漏洞扫描类		2156	在一个月的时间里每周都进行一次漏洞扫描
主机监控类	系统监控传感器	2.6 万	每 5 分钟一个记录, 为每 5 分钟平均的 CPU 利用率、内存利用率以及服务访问延迟
网络监控类	网络监控传感器	1.7 万	每 5 分钟一个记录, 为每 5 分钟平均的带宽速率和包速率

经过对原始数据的预处理形成可以进行下一步处理的安全事件. 这里取 Server1 的 HTTP 服务作为服务安全状态的关联分析对象. 为了便于证明关联方法的结果, 提取服务器的一次被进行 SQL 注入攻击前后各两小时的数据作为分析数据.

入侵检测传感器 IDS-1 计算的 $m'_1(H)$ 、 $m'_1(O)$, 考虑到入侵检测系统本身的误报率, 设 $m'_1(U) = 0.3, \Delta m = 0.1$. 根据入侵检测的安全报警事件处理之后计算得到的 $m'_1(H)$ 如图 4 所示.

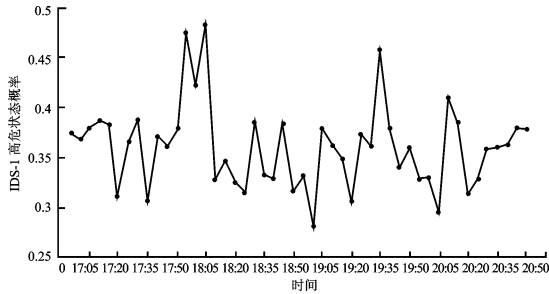


图 4 IDS-1 高危状态概率

入侵检测传感器 IDS-2 计算的 $m'_2(H)$ 、 $m'_2(O)$, 考虑到入侵检测系统本身的误报率, 设 $m'_2(U) = 0.3, \Delta m = 0.1$. 根据入侵检测的安全报警事件处理之后计算得到的 $m'_2(H)$ 如图 5 所示.

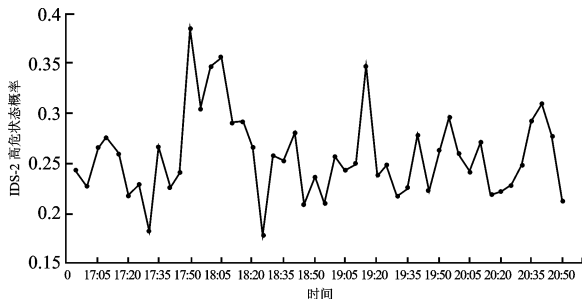


图 5 IDS-2 高危状态概率

对漏洞扫描传感器的基本概率分配函数计算时由于服务高危漏洞对系统安全有很大的影响, 所以设 $\Delta m = 0.2, m'_3(U) = 0.3$. 经过对最近的一次针对该服务器的安全扫描结果计算得到 $m'_3(H) = 0.468, m'_2(O) = 0.232$.

主机监控传感器的高危状态基本概率分配函数为 $m'_4(H)$, 由于主机性能异常是系统被攻击以后有可能发生的情况, 但是性能表现正常并不宜过高的设置系统安全状态的置信度, 所以这里设 $m'_2(U) = 0.5, m = 0.1$. 通过对主机性能和状态数据计算之后得到的 $m'_4(H)$ 如图 6 所示.

主机监控传感器的高危状态基本概率分配函数

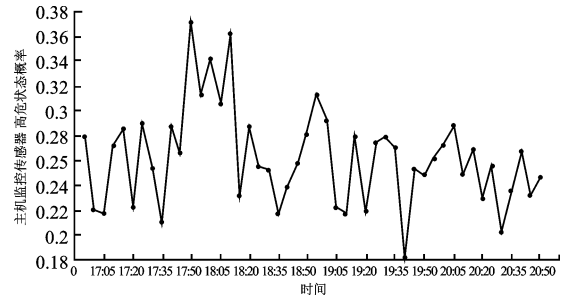


图 6 主机监控传感器高危状态概率

为 $m'_5(H)$, 网络流量异常是一个判定发生攻击和服务可用性的重要参考, 但是和主机监控参数一样, 流量指标正常不能认为系统安全, 所以设置 $m'_5(U) = 0.5, m = 0.1$. 通过对主机性能和状态数据计算之后得到的 $m'_5(H)$ 如图 7 所示.

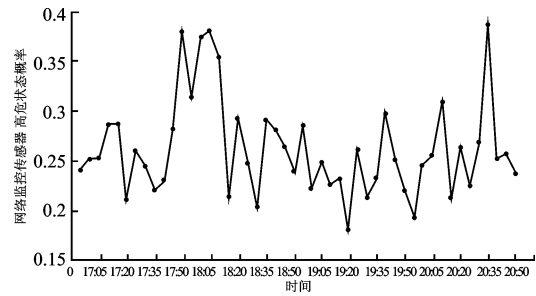


图 7 网络监控传感器高危状态概率

融合过程中首先要设定不同传感器的 $ACCEPT_Lev$, 根据网络环境和拓扑, 由于入侵检测传感器在防火墙外, 所以其证据接受程度要相应降低, $ACCEPT_Lev(1) = 0.4$, 而网络流量传感器所在位置采集到的网络数据并不是服务器的全部流量, 所以设置网络传感器的证据接受程度 $ACCEPT_Lev(5) = 0.8$, 其他证据接受程度为 1. 经过融合计算, 得出 Server1 的 HTTP 服务高危状态置信度曲线如图 8 所示.



图 8 HTTP 服务高危状态置信度曲线

从图 8 可以看出, 如果我们设置高危事件响应阈值为 0.6, 则可以检测出 18:00-18:20 发生的多起

高危 SQL 注入攻击.

以上是提取了一段时间内的基于 EA-DS 证据理论的安全事件关联过程和结果,从 2014 年 9 月到 12 月三个月内对于 Server1 的 HTTP 服务的安全监控系统报告的原始安全事件数的情况如表 2 所示.

表 2 原始报警事件攻击类型及数量

攻击类型	原始报警事件数
拒绝服务攻击	11 020
扫描探测	88 732
漏洞利用攻击	6 392
非法访问	12 267
其他	2 976

经过对三个月内实际的安全事件处理过程中,我们对针对这个系统的攻击事件处理进行了对比实验分析,基于 EA-DS 理论的安全事件关联对于需要处理的高危安全事件的检测情况如表 3 所示.

表 3 基于 EA-DS 的高危安全事件的检测情况

攻击类型	聚合后的安全事件数	高危安全事件	EA-DS 检测率/%	EA-DS 误报率/%
拒绝服务攻击	228	81	67.9	9.88
扫描探测	2 172	12	58.33	16.67
漏洞利用攻击	282	126	70.63	6.35
非法访问	32 298	41	53.66	9.76
其他	98	12	52.94	11.76

从表 3 可以看出,基于 EA-DS 理论的安全事件关联方法能够较高的检测出高危安全事件,误报率也在可以接受的范围内.

7 结束语

本文提出了基于 EA-DS 理论的安全事件关联方法,通过对来自不同安全监控设备和系统中的安

全事件数据通过数据预处理,提取针对特定重点网络服务的安全事件,计算后得到各个安全传感器对指定服务的高危状态置信度,EA-DS 理论进行证据融合,从而得出网络服务的高危状态判断的置信度,通过实验表明,该方法取得了比较高的高威胁事件检测率和较低的误报率.

参考文献:

- [1] Dempster A P. Upper and lower probabilities induced by a multivalued mapping[J]. The Annals of Mathematical Statistics, 1967, 38(2): 325-339.
- [2] Zadeh L A. A simple view of the dempster-shafer theory of evidence and its implication for the rule of combination [J]. AI Magazine, 1986, 7(2): 85-90.
- [3] Haenni R. Are alternatives to dempster's rule of combination real alternative?—comments on “about the belief function combination and the conflict management problem” [J]. Information Fusion, 2002, 3(4): 237-239.
- [4] Smets P, Kennes R. The transferable belief model [J]. Artificial Intelligence, 1994, 66(2): 191-234.
- [5] 邓勇, 蒋雯, 韩德强. 广义证据理论的基本框架[J]. 西安交通大学学报, 2010, 44(12): 119-124.
- [6] 杨艺, 韩德强, 韩崇昭. 基于多准则排序融合的证据组合方法[J]. 自动化学报, 2012, 38(5): 823-831.
- [7] 王连锋, 刘卫东. 一种新的基本概率函数构建方法及应用[J]. 指挥控制与仿真, 2009, 31(6): 98-100.
- [8] 李仰耀, 张国清, 何清, 等. 一种自适应的新型网络性能预警系统[J]. 计算机应用, 2004, 24(7): 82-84.

作者简介:

龙 春 男, (1979-), 博士研究生, 高级工程师. 研究方向为网络安全. Email: shenhanji@cstnet.cn

申罕骥 男, (1987-), 硕士. 研究方向为网络安全.

李 俊 男, (1968-), 博士, 博士生导师. 研究方向为互联网技术.