第 38 卷 第 3 期
Vol.38 No.3

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 安全技术 •

文章编号：1000—3428(2012)03—0150—03 文献标识码：A 中图分类号：TP309

局域网安全态势感知系统的研究

赵伯昕，卓秀然，郑潮宇

(福建省气象服务中心，福州 350001)

摘 要：针对局域网中存在的安全风险和统一威胁管理瓶颈问题，提出一种局域网安全态势感知系统，给出其体系结构，采用 DEMATEL 方法获取主要安全指标，利用模糊综合评价算法建立态势评估模型，在此基础上构建威胁评估模型，计算局域网的威胁程度。仿真结果证明，该系统能准确分析局域网的安全态势，增强网络安全性。

关键词：态势感知；DEMATEL 方法；模糊综合评价；统一威胁管理；马尔可夫预测模型

Research of LAN Security Situational Awareness System

ZHAO Bo-ting, ZHUO Xiu-ran, ZHENG Chao-yu

(Meteorological Service Center of Fujian Province, Fuzhou 350001, China)

【Abstract】This paper proposes the research of the security situational awareness system, aiming at solving the risk existed in the LAN and the bottleneck problem of United Threat Management(UTM). For the first time, it brings forward security situational awareness system architecture in the LAN combining UTM. The main security index is acquired through the DEMATEL method and the situational measurement model is built by adopting the fuzzy comprehensive evaluation algorithm. The threat measurement model is constructed to compute the threat degree in the LAN based on the security index and situational measurement model. The result proves that the system can analyze the security situation accurately and make the UTM strengthen the network security.

【Key words】situational awareness; DEMATEL method; fuzzy comprehensive evaluation; United Threat Management(UTM); Markov prediction model

DOI: 10.3969/j.issn.1000-3428.2012.03.051

1 概述

随着计算机技术的迅速发展，围绕着信息进行获取、控制、破坏的行为更加恶化和严重。要改变目前这种被动防御的现状，需要新的技术来实现网络的主动防御。网络安全态势感知技术[1]是一种对网络整体性、趋势性的评价技术。通过对网络安全状况进行实时监控和预警，发现潜在的恶意入侵行为，分析下一时段的安全趋势，使决策者提前修改安全策略，减少网络攻击造成的破坏。

态势感知概念源于航天飞行的人因(Human Factors)[2]研究，此后在军事战场、核反应控制、空中交通监管(ATC)及医疗应急调度等领域得到广泛的应用。网络安全态势感知就是在大规模的网络环境中，对能够引起网络安全态势发生变化的安全要素进行获取、理解及预测的过程。局域网态势感知综合了局域网内各种软硬件设施在时空、人为、环境上的安全信息，对攻击行为或攻击对象做出一致性的评估或描述。本文从“点”(主机)、“面”(子网)、“体”(局域网)3 层对局域网进行态势感知研究，阐述了局域网态势感知系统的全过程及解决统一威胁管理(United Threat Management, UTM)瓶颈问题的方法。

2 局域网安全态势感知系统体系结构

通过综合分析研究 JDL(Joint Directors of Laboratories Data Fusion Sub-Panel)和基于多传感器数据融合的入侵检测等网络安全态势感知系统的体系结构[3]，本文提出了一种结合 UTM 的局域网安全态势感知系统的体系结构，如图 1 所示。局域网安全态势感知系统体系结构是针对局域网安全性设计的，具有可扩展性、普遍性。从图 1 可知，该体系结构展现了从数据采集到可视化显示、响应与预警一系列过程。其传感器特指配置 SNMP 功能或捕获安全事件的网络设备，具有多源性、异构性及网络部署方式多样性的特征。

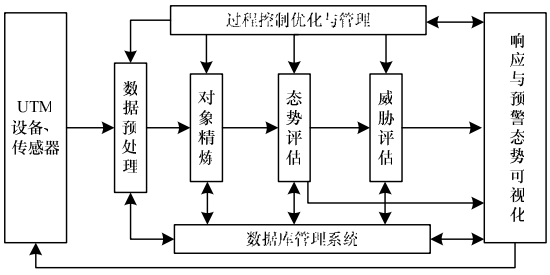

图 1 局域网安全态势感知系统体系结构

该系统体系结构较之其他态势感知体系结构更加灵活，不依赖于网络的拓扑结构，且可根据特定的网络环境和安全需求进行动态配置和裁剪功能模块。在数据源方面充分考虑了采集数据的多源、多维、海量等特性，并进行数据融合。在过程优化方面使得各个过程层层递进，相互补充，体现了“数据-信息-知识”的过程，能及时监控各功能模块，并对关键模块进行重点管理，对其信息通信过程实施加密保护。在态势可视化[4]方面做到结果清晰、易懂、动态显示，能够

基金项目：四川省科技厅科研基金资助项目“信息化网络安全机制的研究”(20082R0090)

作者简介：赵伯昕(1984－)，男，硕士研究生，主研方向：信息安全；卓秀然、郑潮宇，工程师

收稿日期：2011-07-11 **E-mail：**tzzbt@163.com

使其信息对 UTM 进行数据互补，解决了其单故障点、性能瓶颈、灵活性低等问题。

3　概念模型及指标体系建立

3.1　局域网安全态势感知概念模型

局域网安全态势感知系统概念模型共分为 5 层，分别为特征提取、态势评估、威胁评估、预警与响应、安全指标值预测。概念模型如图 2 所示，能对系统各功能模块在关联关系、时空关系上进行定性研究。从概念模型中可以看出，特征提取是态势感知的前提，态势评估是核心，威胁评估是关键，预警和响应是目的，安全指标值预测是保障。

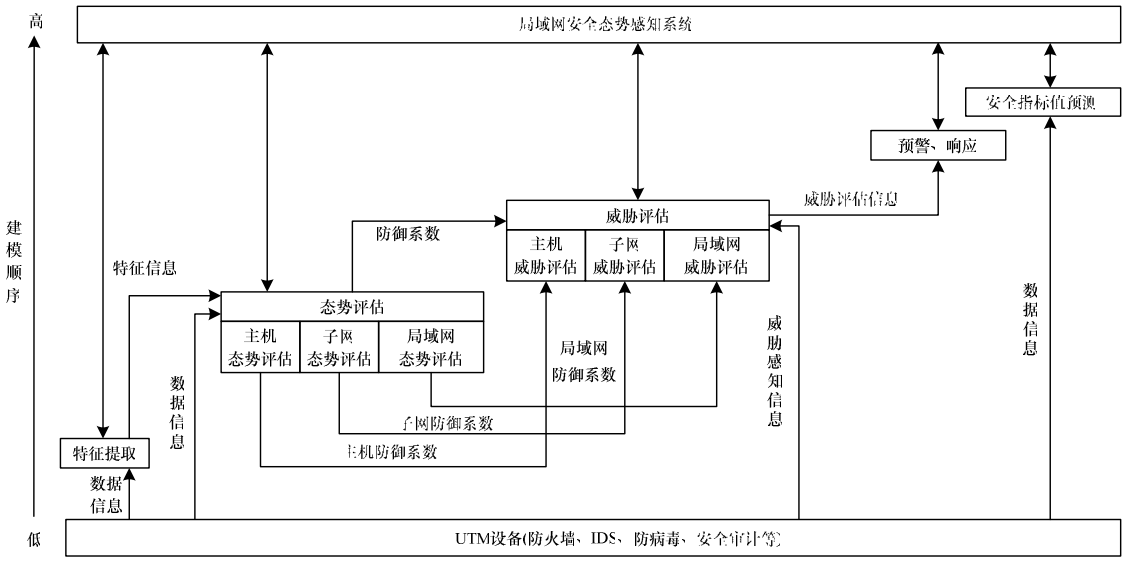

图 2　局域网安全态势感知系统概念模型

3.2　指标体系建立

系统的安全指标体系反映了整个动态复杂的网络安全状况，决定了态势感知的效果。本文系统采用主客观权重法(即基于安全指标之间的内在统计规律和专家经验)来处理多维、海量数据。通过层次化方式提取主机、子网、局域网层候选指标，进行态势评估、威胁评估、态势预测、态势可视化，其实质就是对指标的抽象、简化、可视化。

系统对安全指标体系的处理、检测原则是：(1)相似相近原则针对服务层的候选指标。(2)分层原则针对主机、子网端口流量安全性划分范围。(3)动静结合原则针对流量、内存使用率、拓扑结构。(4)服务共性原则针对服务的特性。(5)冗余性处理原则针对 2 个或多个候选指标的交叉、重复关系。

4　局域网态势感知模型

4.1　态势评估模型

态势评估是系统的核心，是威胁评估的基础，是对整个网络安全状况的分析。本文系统的态势评估步骤为：(1)利用 DEMATEL 方法对主机层、子网层、局域网层的候选指标进行综合分析，计算各层候选指标的综合影响指数，找出影响各层安全的深层次原因。(2)通过对各层候选指标中心度实施排序，选取影响各层安全的主要安全指标，构建模糊评价矩阵和判断矩阵。继而，通过判断矩阵求得各层主要安全指标的安全权重值，并进行一致性验证。(3)通过模糊评估运算计算各层的安全态势值。

4.1.1　主要安全指标获取

根据我国公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准 GB17859《计算机信息系统安全保护等级划分准则》和业界公认的 BS7799 标准，选取影响主机层、子网层、局域网层的安全候选指标。

利用 DEMATEL[5]方法对各层候选指标间的逻辑关系构建直接影响矩阵，计算影响主机、子网、局域网层候选指标的中心度 $A_{i,j}$，i=1,2,3, j=1,2,…,n。取得各层中心度排序前 m 位的主要安全指标，$\sum_{j=1}^{m} A_{i,j} / \sum_{j=1}^{n} A_{i,j} \geqslant 90\%$,$m<n$。

4.1.2　模糊综合评价模型

基于上述 DEMATEL 算法求得主机层、子网层、局域网层的主要安全指标，建立各层的因素集。对因素集进行模糊综合评价，建立模糊综合评价模型如下：

步骤 1 对主机、子网、局域网层的因素集 U，根据专家经验和统计法建立评语集 V，V={很安全, 安全, 基本安全, 不安全}。

步骤 2 根据专家经验和网络环境确定因素集中各个因素的评价向量，如 u_1 ={0.2, 0.2, 0.2, 0.4}。

步骤 3 根据因素的评价向量构造各层的模糊评价矩阵$\boldsymbol{R}$。

步骤 4 构造各层的判断矩阵，确定安全因素的权值。判断矩阵中的元素为 2 个安全因素的重要性比值。安全因素的重要性依据原则为：风险级别越高的因子，影响越大，权重越大。

步骤 5 根据正规化原则求判断矩阵的特征向量$\boldsymbol{W}$以及对应的最大特征根 $\lambda_{\max}$，用特征值法求该矩阵的最大特征值 λ。如果 $\lambda < \lambda_{\max}$，$|\lambda_{\max} - \lambda|$的值小于0.1，那么C.R.、C.I.验证矩阵的一致性通过，特征向量即安全因素集的权重模糊矩阵，否则，返回步骤4。

步骤 6 根据各层因素集的模糊综合评价矩阵 $\boldsymbol{R}$ 和权重模糊矩阵 $\boldsymbol{W}$，构建模糊综合评价模型 $\boldsymbol{L} = w_{i,k} \times R_{k,j}$。其中，$\boldsymbol{L}$ 向量经过加权法运算，得到各层的安全态势值，其值越大，安全性越好，其倒数为各层防御攻击的防御系数。加权法的权值向量为{3, 2, 1, 0}，并进行归一化处理。

4.2　威胁评估模型

威胁评估是在态势评估基础上评估恶意攻击对网络的威胁程度。局域网威胁评估通过对 UTM、内部各个防火墙、防病毒软件等攻击信息进行收集，分析各种服务遭受恶意攻击

时，网络所承受的危害性程度。

恶意攻击对服务的危害可以量化为危害严重度和攻击频率 2 个方面。通过 Snort 手册查询，各种恶意攻击的危害严重度可归结为高危、中危、低危，即 P_{high}、P_{medium}、P_{low}。考虑到网络遭受 1 次高危攻击造成的危害远大于承受 3 次低危攻击的危害，经协调检测，对各攻击种类的危害度进行量化，即[10^3 10^2 10^1]。对威胁评估建模，即：

(1)S 表示威胁评估中所有的服务总和，S_i 表示第 i 种服务。

(2)C 表示各种服务遭受的攻击次数，C_j 表示服务 S_i 受到第 j 种恶意攻击的次数。

(3) $T_{i,j}$ 表示某种恶意攻击的危害性。

(4) S_{S_i} 表示服务 S_i 的威胁评估度，S_{S_i} 越大，其目标服务受到的威胁程度越高。

(5)服务威胁评估模型为：

$$S_{S_i}=\sum_{j=1}^{m}10^{T_{i,j}}C_j$$

主机威胁评估模型为：

$$S_{H_k}=\frac{1}{P_{H_k}}\sum_{i=1}^{n}\beta_i S_{S_i}=\frac{1}{P_{H_k}}\sum_{i=1}^{n}\beta_i\left(\sum_{j=1}^{m}10^{T_{i,j}}C_j\right)$$

其中，P_{H_k} 表示主机 H_k 的防御能力，由主机态势评估得到；β_i (i=1, 2, …, n)表示 H_k 所提供网络服务的安全比重权值。

子网威胁评估模型为：

$$S_{F_l}=\frac{1}{P_{F_l}}\sum_{i=1}^{n}\beta_i S_{S_i}=\frac{1}{P_{F_l}}\sum_{i=1}^{n}\beta_i\left(\sum_{j=1}^{m}10^{T_{i,j}}C_j\right)$$

其中，P_{F_l} 表示子网 F_l 的防御系数，由子网态势评估得到；β_i (i=1, 2, …, n)表示 F_l 所提供网络服务 S_i 的安全比重权值。

局域网威胁评估模型为：

$$S_L=\frac{1}{P}\left(\sum_{i=1}^{n}\beta_i S_{S_i}\right)=\frac{1}{P}\left(\sum_{i=1}^{n}\beta_i\left(\sum_{j=1}^{m}10^{T_{i,j}}C_j\right)\right)$$

其中，P 表示局域网的防御系数，由局域网态势评估得到；β_i (i=1, 2, …, n)表示局域网 L 所提供网络服务 S_i 的安全比重权值。

4.3 安全指标安全程度向量预测

马尔可夫预测模型已用于网络安全入侵检测系统，且其“无后效性”原则符合动态变化的安全指标的特性，因此，采用该模型对各个动态变化的安全指标进行安全程度预测。其步骤如下：

步骤 1 确定安全指标的评语集 V。

步骤 2 统计 N 个时段各个评语的次数 M_i 以及各个评语变化的次数 $M_{i,j}$，其中，$M_{i,j}$ 为评语 i 跳转到评语 j 的次数，i,j=1, 2, …, n。

步骤 3 构建初始状态概念 P 和状态转移概率 $\boldsymbol{R}$，计算下一时段各评语的概率，即：

$$P(N+1)=P(N)\times\boldsymbol{R}=$$

$$\left(\frac{M_1}{N}\ \frac{M_2}{N}\ \frac{M_3}{N}\ \frac{M_4}{N}\right)\times\begin{bmatrix}\frac{M_{1,1}}{M_1} & \frac{M_{1,2}}{M_1} & \frac{M_{1,3}}{M_1} & \frac{M_{1,4}}{M_1}\\ \frac{M_{2,1}}{M_2} & \frac{M_{2,2}}{M_2} & \frac{M_{2,3}}{M_2} & \frac{M_{2,4}}{M_2}\\ \frac{M_{3,1}}{M_3} & \frac{M_{3,2}}{M_3} & \frac{M_{3,3}}{M_3} & \frac{M_{3,4}}{M_3}\\ \frac{M_{4,1}}{M_4} & \frac{M_{4,2}}{M_4} & \frac{M_{4,3}}{M_4} & \frac{M_{4,4}}{M_4}\end{bmatrix}$$

步骤 4 分析$\boldsymbol{R}$的稳态分布状态，求解下一时段各个评语的概率，即：

$$(x_1x_2x_3x_4)\times\begin{bmatrix}\frac{M_{1,1}}{M_1} & \frac{M_{1,2}}{M_1} & \frac{M_{1,3}}{M_1} & \frac{M_{1,4}}{M_1}\\ \frac{M_{2,1}}{M_2} & \frac{M_{2,2}}{M_2} & \frac{M_{2,3}}{M_2} & \frac{M_{2,4}}{M_2}\\ \frac{M_{3,1}}{M_3} & \frac{M_{3,2}}{M_3} & \frac{M_{3,3}}{M_3} & \frac{M_{3,4}}{M_3}\\ \frac{M_{4,1}}{M_4} & \frac{M_{4,2}}{M_4} & \frac{M_{4,3}}{M_4} & \frac{M_{4,4}}{M_4}\end{bmatrix}=(x_1x_2x_3x_4)$$

$$x_1+x_2+x_3+x_4=1$$

求解得到的 x_1、x_2、x_3、x_4 构成的向量，即该安全指标的安全向量。

步骤 5 将获得的下一时刻各个安全指标的安全向量代入态势评估模型，得到下一时段的安全态势值，分析局域网的安全状况。

5 系统仿真

利用信息工程大学网络攻防实验室的部分设备构造实验环境，对系统进行测试、仿真。其中，仿 UTM 功能的服务器安装了防火墙、IDS、防病毒软件。攻击类型主要针对 FTP、RPC、SMTP、SCOKET 和 HTTP 五种服务。

利用 DEMATEL 方法获取局域网安全因素集 U 为{子网 1 安全性，子网 2 安全性，目标机 3 安全性，UTM 服务器安全，态势感知服务器安全性，漏洞数及等级，蠕虫攻击，木马攻击次数，拒绝服务攻击次数，其他病毒攻击次数，报警数，端口总数，路由器端口流量}。

通过对局域网安全因素集 U 在 t_1~t_{10} 时刻各 10 次的测试统计，代入模糊综合评价模型，获得 t_1~t_{10} 时刻局域网的安全向量值。

继而将安全指标模糊矩阵和安全指标权重模糊矩阵求得安全态势值，如图 3 所示。

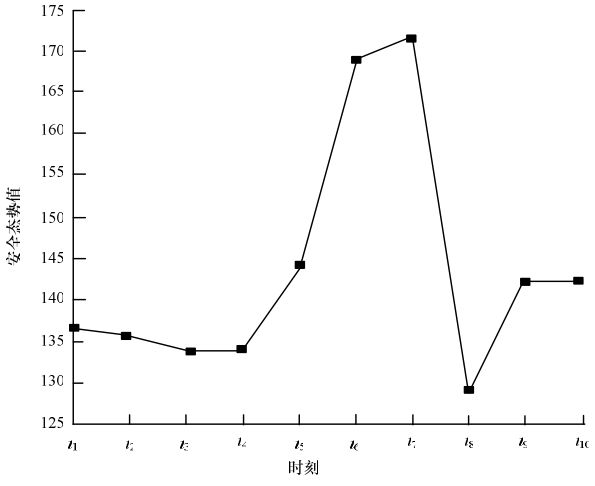

图 3 安全态势值

根据网络嗅探工具(Wireshark)监控得到的 5 种服务的平均访问量，利用网络服务重要性原则，计算 5 种服务的安全比重权重向量 $\boldsymbol{T}$={1/4, 1/4, 1/4, 1/6, 1/12}。利用 SNMP 数据流分析和监控软件监测 t_1 至 t_{10} 时刻主机、子网、局域网中服务遭受攻击次数，结合局域网在各个时刻的防御系数，即安全态势值的倒数，代入威胁评估模型，得到危害程度值，如图 4 所示。

(下转第 168 页)