

文章编号: 1001-9081(2012)01-0001-04

doi: 10.3724/SP.J.1087.2012.00001

## 网络安全态势感知研究综述

席荣荣\*, 云晓春, 金舒原, 张永铮

(中国科学院 计算技术研究所, 北京 100190)

(\*通信作者电子邮箱 [xirongrong@software.ict.ac.cn](mailto:xirongrong@software.ict.ac.cn))

**摘要:** 网络安全态势感知(SA)的研究对于提高网络的监控能力、应急响应能力和预测网络安全的发展趋势具有重要的意义。基于态势感知的概念模型,详细阐述了态势感知的三个主要研究内容:网络安全态势要素提取、态势理解和态势预测,重点论述各研究点需解决的核心问题、主要算法以及各种算法的优缺点;最后对各研究点的相关理论及其应用实现的发展趋势进行了分析和展望。

**关键词:** 态势感知;网络安全;数据融合;态势预测

**中图分类号:** TP393.08    **文献标志码:**A

### Research survey of network security situation awareness

XI Rong-rong\*, YUN Xiao-chun, JIN Shu-yuan, ZHANG Yong-zheng

(Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China)

**Abstract:** The research of network security Situation Awareness (SA) is important in improving the abilities of network detection, response to emergency and predicting the network security trend. In this paper, based on the conceptual model of situational awareness, three main problems with regard to network security situational awareness were discussed: extraction of the elements in the network security situation, comprehension of the network security situation and projection of future situation. The core issues to be resolved, and major algorithms as well as the advantages and disadvantages of various algorithms were focused. Finally, the opening issues and challenges for network security situation awareness concerning both theory and implementation in near future were proposed.

**Key words:** Situation Awareness (SA); network security; data fusion; situational prediction

### 0 引言

随着网络的飞速发展,安全问题日益突出,虽然已经采取了各种网络安全防护措施,但是单一的安全防护措施没有综合考虑各种防护措施之间的关联性,无法满足从宏观角度评估网络安全性的需求。网络安全态势感知的研究就是在这种背景下产生的。它在融合各种网络安全要素的基础上从宏观的角度实时评估网络的安全态势,并在一定条件下对网络安全态势的发展趋势进行预测。

网络安全态势感知研究是近几年发展起来的一个热门研究领域。它融合所有可获取的信息实时评估网络的安全态势,为网络安全管理员的决策分析提供依据,将不安全因素带来的风险和损失降到最低。网络安全态势感知在提高网络的监控能力、应急响应能力和预测网络安全的发展趋势等方面都具有重要的意义。

### 1 网络安全态势感知概述

1988年,Endsley首次明确提出态势感知的定义,态势感知(Situation Awareness, SA)是指“在一定的时空范围内,认知、理解环境因素,并且对未来的发展趋势进行预测”<sup>[1]</sup>,该定义的概念模型如图1所示。但是传统的态势感知的概念主要应用于对航空领域人为因素的考虑,并没有引入到网络安全

全领域。

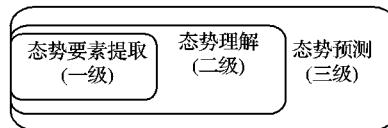


图1 态势感知的概念模型

1999年,Bass等<sup>[2]</sup>指出,“下一代网络入侵检测系统应该融合从大量的异构分布式网络传感器采集的数据,实现网络空间的态势感知(cyberspace situational awareness)”,并且基于数据融合的JDL(Joint Directors of Laboratories)模型,提出了基于多传感器数据融合的网络态势感知功能模型。如图2所示。

虽然网络态势根据不同的应用领域,可分为安全态势、拓扑态势和传输态势等,但目前关于网络态势的研究都是围绕网络的安全态势展开的。

Endsley<sup>[1]</sup>和Bass<sup>[2]</sup>为网络安全态势感知的研究奠定了基础。基于Endsley<sup>[1]</sup>态势感知的概念模型和Bass<sup>[2]</sup>的功能模型,后来的研究者又陆续提出了十几种网络安全态势感知的模型。不同的模型组成部分名称可能不同,但功能基本都是一致的。基于网络安全态势感知的功能,本文将其研究内容归结为3个方面:

1) 网络安全态势要素的提取;

收稿日期:2011-08-01;修回日期:2011-09-09。

基金项目:国家自然科学基金资助项目(60703021);国家863计划项目(2009AA01Z438, 2009AA01Z431)。

作者简介:席荣荣(1979-),女,山西洪洞人,博士研究生,主要研究方向:网络安全态势感知、安全评估; 云晓春(1971-),男,黑龙江哈尔滨人,教授,博士生导师,博士,主要研究方向:计算机网络、信息安全; 金舒原(1974-),女,黑龙江哈尔滨人,副研究员,博士,主要研究方向:安全测评、入侵检测、脆弱性分析; 张永铮(1978-),男,黑龙江哈尔滨人,副研究员,博士,主要研究方向:网络安全事件监控、网络安全分析、网络脆弱性评估。

- 2) 网络安全态势的评估;
- 3) 网络安全态势的预测。

下面将从这 3 个方面对网络安全态势的研究进行详细的阐述。

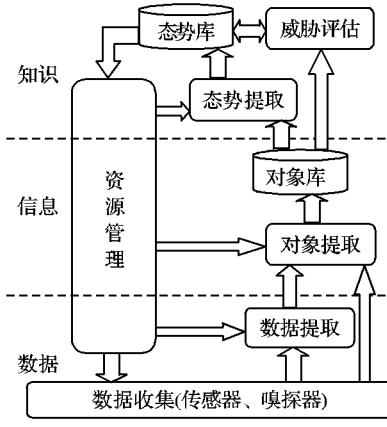


图 2 网络态势感知的功能模型

## 2 网络安全态势的提取

准确、全面地提取网络中的安全态势要素是网络安全态势感知研究的基础。然而由于网络已经发展成一个庞大的非线性复杂系统,具有很强的灵活性,使得网络安全态势要素的提取存在很大难度。

目前网络的安全态势要素主要包括静态的配置信息、动态的运行信息以及网络的流量信息等。其中:静态的配置信息包括网络的拓扑信息、脆弱性信息和状态信息等基本的环境配置信息;动态的运行信息包括从各种防护措施的日志采集和分析技术获取的威胁信息等基本的运行信息。

国外的学者一般通过提取某种角度的态势要素来评估网络的安全态势。如 Jajodia 等<sup>[3]</sup> 和 Wang 等<sup>[4-5]</sup> 采集网络的脆弱性信息来评估网络的脆弱性态势; Ning 等<sup>[6-7]</sup> 采集网络的警报信息来评估网络的威胁性态势; Barford 等<sup>[8]</sup> 和 Dacier 等<sup>[9]</sup> 利用 honeynet 采集的数据信息,来评估网络的攻击态势。

国内的学者一般综合考虑网络各方面的信息,从多个角度分层次描述网络的安全态势。如王娟等<sup>[10]</sup> 提出了一种网络安全指标体系,根据不同层次、不同信息来源、不同需求提炼了 4 个表征宏观网络性质的二级综合性指标,并拟定了 20 多个一级指标构建网络安全指标体系,通过网络安全指标体系定义需要提取的所有网络安全态势要素。

综上所述,网络安全态势要素的提取存在以下问题:1)国外的研究从某种单一的角度采集信息,无法获取全面的信息;2)国内的研究虽然力图获取全面的信息,但没有考虑指标体系中各因素之间的关联性,将会导致信息的融合处理存在很大难度;3)缺乏指标体系有效性的验证,无法验证指标体系是否涵盖了网络安全的所有方面。

## 3 网络安全态势的理解

网络安全态势的理解是指在获取海量网络安全数据信息的基础上,通过解析信息之间的关联性,对其进行融合,获取宏观的网络安全态势。本文将该过程称为态势评估,数据融合是网络安全态势评估的核心。

网络安全态势评估摒弃了研究单一的安全事件,而是从宏观角度去考虑网络整体的安全状态,以期获得网络安全的综合评估,达到辅助决策的目的。

目前应用于网络安全态势评估的数据融合算法,大致分为以下几类:基于逻辑关系的融合方法、基于数学模型的融合方

法、基于概率统计的融合方法以及基于规则推理的融合方法。

### 3.1 基于逻辑关系的融合方法

基于逻辑关系的融合方法依据信息之间的内在逻辑,对信息进行融合。警报关联是典型的基于逻辑关系的融合方法。

警报关联是指基于警报信息之间的逻辑关系对其进行融合,从而获取宏观的攻击态势。警报之间的逻辑关系分为:警报属性特征的相似性,预定义攻击模型中的关联性,攻击的前提和后继条件之间的相关性。Ning 等<sup>[6-7]</sup> 实现了通过警报关联,从海量警报信息中分析网络的威胁性态势的方法。

基于逻辑关系的融合方法,很容易理解,而且可以直观地反映网络的安全态势。但是该方法的局限性在于:1)融合的数据源为单源数据;2)逻辑关系的获取存在很大的难度,如攻击预定义模型的建立以及攻击的前提和后继条件的形式化描述都存在很大的难度;3)逻辑关系不能解释系统中存在的不确定性。

### 3.2 基于数学模型的融合方法

基于数学模型的融合方法,综合考虑影响态势的各项态势因素,构造评定函数,建立态势因素集合  $R$  到态势空间  $\theta$  的映射关系  $\theta = f(r_1, r_2, \dots, r_n), r_i \in R (1 \leq i \leq n)$  为态势因素,其中最具代表性的评定函数为加权平均。

加权平均法是最常用、最简单的基于数学模型的融合方法。加权平均法的融合函数通常由态势因素和其重要性权值共同确定。西安交通大学的陈秀真等<sup>[11]</sup> 提出的层次化网络安全威胁量化评估方法,对服务、主机本身的重要性因子进行加权,层次化计算服务、主机以及整个网络系统的威胁指数,进而分析网络的安全态势。

加权平均法可以直观地融合各种态势因素,但是其最主要的问题是:权值的选择没有统一的标准,大都是依据领域知识或者经验而定,缺少客观的依据。

基于逻辑关系的融合方法和基于数学模型的融合方法的前提是确定的数据源,但是当前网络安全设备提供的信息,在一定程度上是不完整的、不精确的,甚至存在着矛盾,包含大量的不确定性信息,而态势评估必须借助这些信息来进行推理,因此直接基于数据源的融合方法具有一定的局限性。对于不确定性信息,最好的解决办法是利用对象的统计特性和概率模型进行操作。

### 3.3 基于概率统计的融合方法

基于概率统计的融合方法,充分利用先验知识的统计特性,结合信息的不确定性,建立态势评估的模型,然后通过模型评估网络的安全态势。贝叶斯网络、隐马尔可夫模型(Hidden Markov Model, HMM)是最常见的基于概率统计的融合方法。

在网络态势评估中,贝叶斯网络是一个有向无环图  $G = \langle V, E \rangle$ ,节点  $V$  表示不同的态势和事件,每个节点对应一个条件概率分配表,节点间利用边  $E$  进行连接,反映态势和事件之间概率依赖关系,在某些节点获得证据信息后,贝叶斯网络在节点间传播和融合这些信息,从而获取新的态势信息。以色列 IBM 海法实验室的 Etzion 等<sup>[12]</sup> 在不确定性数据融合方面作了大量的研究工作,Etzion 等<sup>[12]</sup> 和 Gal<sup>[13]</sup> 提出利用贝叶斯网络进行态势感知。Oxenham 等<sup>[14]</sup>, Holsopple 等<sup>[15]</sup> 和 Sabata 等<sup>[16]</sup> 基于贝叶斯网络,通过融合多源数据信息评估网络的攻击态势<sup>[14-16]</sup>。李伟生等<sup>[17]</sup> 根据网络安全态势和安全事件之间的不同的关联性建立态势评估的贝叶斯网络模型,并给出相应的信息传播算法,以安全事件的发生为触发点,根据相应的信息传播算法评估网络的安全态势。

HMM 相当于动态的贝叶斯网络,它是一种采用双重随机

过程的统计模型。在网络态势评估中,将网络安全状态的转移过程定义为隐含状态序列,按照时序获取的态势因素定义为观察值序列,利用观察值序列和隐含状态序列训练HMM模型,然后运用模型评估网络的安全态势。Arnes等<sup>[18-19]</sup>和Ourston等<sup>[20]</sup>将网络安全状态的变化过程模型化为隐马尔可夫过程,并通过该模型获取网络的安全态势。

基于概率统计的融合方法能够融合最新的证据信息和先验知识,而且推理过程清晰,易于理解。但是该方法存在以下局限性:1)统计模型的建立需要依赖一个较大的数据源,在实际工作中会占有很大的工作量,且模型需要的存储量和匹配计算的运算量相对较大,容易造成维数爆炸的问题,影响态势评估的实时性;2)特征提取、模型构建和先验知识的获取都存在一定的困难。

#### 3.4 基于规则推理的融合方法

基于规则推理的融合方法,首先模糊量化多源多属性信息的不确定性;然后利用规则进行逻辑推理,实现网络安全态势的评估。目前D-S证据组合方法和模糊逻辑是研究热点。

D-S证据组合方法对单源数据每一种可能决策的支持程度给出度量,即数据信息作为证据对决策的支持程度。然后寻找一种证据合成规则,通过合成能得出两种证据的联合对决策的支持程度,通过反复运用合成规则,最终得到全体数据信息的联合体对某种决策总的支持程度,完成证据融合的过程。其核心是证据合成规则。Sabata等<sup>[16]</sup>提出了一个多源证据融合的方法,完成对分布式实时攻击事件的融合,实现对网络态势的感知。徐晓辉等<sup>[22]</sup>将D-S理论引入网络安全评估,对其过程进行了详细描述。

在网络态势评估中,首先建立证据和命题之间的逻辑关系,即态势因素到态势状态的汇聚方式,确定基本概率分配;然后根据到来的证据,即每一则事件发生的上报信息,使用证据合成规则进行证据合成,得到新的基本概率分配,并把合成后的结果送到决策逻辑进行判断,将具有最大置信度的命题作为备选命题。当不断有事件发生时,这个过程便得以继续,直到备选命题的置信度超过一定的阈值,证据达到要求,即认为该命题成立,态势呈现某种状态。

模糊逻辑提供了一种处理人类认知不确定性的数学方法,对于模型未知或不能确定的描述系统,应用模糊集合和模糊规则进行推理,实行模糊综合判断。

在网络态势评估中,首先对单源数据进行局部评估,然后选取相应的模型参数,对局部评估结果建立隶属度函数,将其划分到相应的模糊集合,实现具体值的模糊化,将结果进行量化。量化后,如果某个状态属性值超过了预先设定的阈值,则将局部评估结果作为因果推理的输入,通过模糊规则推理对态势进行分类识别,从而完成对当前态势的评估。Rao等<sup>[23]</sup>利用模糊逻辑与贝叶斯网络相结合的方法,对多源数据信息进行处理,生成宏观态势图。李伟生等<sup>[24]</sup>使用模糊逻辑的方法处理事件发生的不确定性,基于一定的知识产生对当前态势的假设,并使用D-S方法对获得的信息进行合成,从而构造一个对战场态势进行分析、推理和预测的求解模型。

基于规则推理的融合方法,不需要精确了解概率分布,当先验概率很难获得时,该方法更为有效。但是缺点是计算复杂度高,而且当证据出现冲突时,方法的准确性会受到严重的影响。

### 4 网络安全态势的预测

网络安全态势的预测是指根据网络安全态势的历史信息和当前状态对网络未来一段时间的发展趋势进行预测。网络

安全态势的预测是态势感知的一个基本目标。

由于网络攻击的随机性和不确定性,使得以此为基础的安全态势变化是一个复杂的非线性过程,限制了传统预测模型的使用。目前网络安全态势预测一般采用神经网络、时间序列预测法和支持向量机等方法。

神经网络是目前最常用的网络态势预测方法,该算法首先以一些输入输出数据作为训练样本,通过网络的自学习能力调整权值,构建态势预测模型;然后运用模型,实现从输入状态到输出状态空间的非线性映射。上海交通大学的任伟等<sup>[25]</sup>和Lai等<sup>[26]</sup>分别利用神经网络方法对态势进行了预测,并取得了一定的成果。

神经网络具有自学习、自适应性和非线性处理的优点。另外神经网络内部神经元之间复杂的连接和可变的连接权值矩阵,使得模型运算中存在高度的冗余,因此网络具有良好的容错性和稳健性。但是神经网络存在以下问题,如难以提供可信的解释,训练时间长,过度拟合或者训练不足等。

时间序列预测法是通过时间序列的历史数据揭示态势随时间变化的规律,将这种规律延伸到未来,从而对态势的未来做出预测。在网络安全态势预测中,将根据态势评估获取的网络安全态势值 $x$ 抽象为时间序列 $t$ 的函数,即: $x = f(t)$ ,此态势值具有非线性的特点。网络安全态势值可以看作一个时间序列,假定有网络安全态势值的时间序列 $x = \{x_i | x_i \in R, i = 1, 2, \dots, L\}$ ,预测过程就是通过序列的前 $N$ 个时刻的态势值预测出后 $M$ 个态势值。

时间序列预测法实际应用比较方便,可操作性较好。但是,要想建立精度相当高的时序模型不仅要求模型参数的最佳估计,而且模型阶数也要合适,建模过程是相当复杂的。

支持向量机是一种基于统计学习理论的模式识别方法,基本原理是通过一个非线性映射将输入空间向量映射到一个高维特征空间,并在此空间上进行线性回归,从而将低维特征空间的非线性回归问题转换为高维特征空间的线性回归问题来解决。张翔等<sup>[27]</sup>根据最近一段时间内入侵检测系统提供的网络攻击数据,使用支持向量机完成了对网络攻击态势的预测。

综上所述,神经网络算法主要依靠经验风险最小化原则,容易导致泛化能力的下降且模型结构难以确定。在学习样本数量有限时,学习过程误差易收敛于局部极小点,学习精度难以保证;学习样本数量很多时,又陷入维数灾难,泛化性能不高。而时间序列预测法在处理具有非线性关系、非正态分布特性的宏观网络安全态势值所形成的时间序列数据时,效果并不是不理想。支持向量机有效避免了上述算法所面临的问题,预测绝对误差小,保证了预测的正确趋势率,能准确预测网络安全态势的发展趋势。支持向量机是目前网络安全态势预测的研究热点。

### 5 结语

本文基于网络安全态势感知的概念模型,详细阐述了态势感知中三个主要的研究内容:安全态势要素提取、态势理解和态势预测,重点讨论各研究点需解决的核心问题、主要算法以及各种算法的优缺点。目前对于网络安全态势感知的研究还处于初步阶段,许多问题有待进一步解决,本文认为未来的研究方向有以下几个方面。

#### 1) 网络安全态势的形式化描述。

网络安全态势的描述是态势感知的基础。网络是个庞大的非线性的复杂系统,复杂系统描述本身就是难点。在未来的研究中,需要具体分析安全态势要素及其关联性,借鉴已有

的成熟的系统表示方法,对网络安全态势建立形式化的描述。其中源于哲学概念的本体论方法是重要的研究方向。本体论强调领域中的本质概念,同时强调这些本质概念之间的关联,能够将领域中的各种概念及概念之间的关系显式化,形式化地表达出来,从而表达出概念中包含的语义,增强对复杂系统的表示能力。但其理论体系庞大,使用复杂,将其应用于网络安全态势的形式化描述需要进一步深入的研究。

### 2) 准确而高效的融合算法研究。

基于网络攻击行为分布性的特点,而且不同的网络节点采用不同的安全设备,使得采用单一的数据融合方法监控整个网络的安全态势存在很大的难度。应该结合网络态势感知多源数据融合的特点,对具体问题具体分析,有针对性地对目前已经存在的各种数据融合方法进行改进和优化。在保证准确性的前提下,提高算法的性能,尽量降低额外的网络负载,提高系统的容错能力。另一方面可以结合各种算法的利弊综合利用,提高态势评估的准确率。

### 3) 预测算法的研究。

网络攻击的随机性和不确定性决定了安全态势的变化是一个复杂的非线性过程。利用简单的统计数据预测非线性过程随时间变化的趋势存在很大的误差。如时间序列分析法,根据系统对象随时间变化的历史信息对网络的发展趋势进行定量预测已不能满足网络安全态势预测的需求。未来的研究应建立在基于因果关系的分析之上。通过分析网络系统中各因素之间存在的某种前因后果关系,找出影响某种结果的几个因素,然后利用个因素的变化预测整个网络安全态势的变化。基于因果关系的数学模型的建立存在很大的难度,需要进一步深入的研究。另外,模式识别的研究已经比较广泛,它为态势预测算法奠定了理论基础,可以结合模式识别的理论,将其很好地应用于态势预测中。

### 参考文献:

- [1] ENDSLEY M R. Design and evaluation for situation awareness enhancement [ C ] // Proceeding of the 32nd Human Factors Society Annual Meeting. Santa Monica: Human Factors and Ergonomics Society, 1988: 97 - 101.
- [2] BASS T, ARBOR A. Multisensor data fusion for next generation distributed intrusion detection systems [ C ] // Proceeding of IRIS National Symposium on Sensor and Data Fusion. Laurel, MD: [ s. n. ], 1999: 24 - 27.
- [3] JAJODIA S, NOEL S, O'BERRY B. Topological analysis of network attack vulnerability [ M ] // KUMAR V, SRIVASTAVA J, LAZAREVIC A. Managing Cyber Threats: Issues, Approaches and Challenges. Dordrecht: Kluwer Academic Publisher, 2005: 247 - 266.
- [4] WANG LINGYU, SINGHAL A, JAJODIA S. Measuring network security using attack graphs [ C ] // Proceedings of the 2007 ACM Workshop on Quality of Protection. New York: ACM Press, 2007: 49 - 54.
- [5] WANG LINGYU, SINGHAL A, JAJODIA S. Measuring the overall security of network configurations using attack graphs [ C ] // Proceedings of the 21st IFIP WG 11.3 Working Conference on Data and Applications Security. Berlin: Springer-Verlag, 2007: 98 - 112.
- [6] NING PENG, CUI YUN, REEVES D S, et al. Techniques and tools for analyzing intrusion alerts [ J ]. ACM Transactions on Information and System Security, 2004, 7(2): 274 - 318.
- [7] XU DINGBANG, NING PENG. Alert correlation though trigger event and common resource [ C ] // Proceedings of the 20th Annual Computer Security Applications Conference. Washington, DC: IEEE Computer Society, 2004: 360 - 369.
- [8] BARFORD P, CHEN YAN, GOYAL A, et al. Employing honeynets for network situational awareness [ C ] // Proceedings of the Fourth Workshop on Hot Topics in Networks. Berlin: Springer-Verlag, 2005: 71 - 102.
- [9] THONNARD O, DACIER M. A framework for attack patterns' discovery in honeynet data [ C ] // Proceeding of the 8th Digital Forensics Research Conference. Baltimore: [ s. n. ], 2008: S128 - S139.
- [10] 王娟, 张凤荔, 傅琳, 等. 网络态势感知中的指标体系研究 [ J ]. 计算机应用, 2007, 27(8): 1907 - 1909.
- [11] 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.
- [12] WASSERKRUG S, ETZION O, GAL A. Inference and prediction of uncertain events in active systems: A language and execution model [ EB/OL ]. [ 2011-04-25 ]. <http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-76/wasserkrug.pdf>.
- [13] GAL A. Managing uncertainty in schema matching with top-k schema mappings [ J ]. Journal on Data Semantics VI, 2006, 4090: 90 - 114.
- [14] OXENHAM M, CHALLA S, MORELANDE M. Fusion of disparate identity estimates for shared situation awareness in a network-centric environment [ J ]. Information Fusion, 2006, 7(4): 395 - 417.
- [15] HOLSOOPPLE J, YANG S J, SUDIT M. TANDI: Threat assessment of network data and information [ EB/OL ]. [ 2011-04-20 ]. <https://ritdml.rit.edu/handle/1850/10737>.
- [16] SABATA B, ORNES C. Multi-source evidence fusion for cyber-situation assessment [ C ] // Proceedings of Multisensor, Multisource Information Fusion Conference. Bellingham: SPIE, 2006: 1 - 9.
- [17] 李伟生, 王宝树. 基于贝叶斯网络的态势评估 [ J ]. 系统工程与电子技术, 2003, 25(4): 480 - 483.
- [18] ARNES A, VALEUR F, VIGNA G, et al. Using hidden Markov models to evaluate the risks of intrusions [ C ] // Proceedings of the 9th Symposium on Recent Advances in Intrusion Detection, LNCS 4219. Berlin: Springer-Verlag, 2006: 145 - 164.
- [19] ARNES A, SALLHAMMAR K, HASLUM K, et al. Real-time risk assessment with network sensors and intrusion detection systems [ C ] // Proceeding of 2005 International Conference on Computational Intelligence and Security, LNCS 3802. Berlin: Springer-Verlag, 2005: 388 - 397.
- [20] OURSTON D, MATZNER S, STUMP W, et al. Applications of hidden Markov models to detecting multi-stage network attacks [ C ] // Proceedings of the 36th Hawaii International Conference on System Sciences. Washington, DC: IEEE Computer Society, 2003: 334.2.
- [21] QU ZHAO-YANG, LI YA-YING, LI PENG. A network security situation evaluation method based on D-S evidence theory [ C ] // Proceedings of the 2010 International Conference on Environmental Science and Information Application Technology. Washington, DC: IEEE Computer Society, 2010: 496 - 499.
- [22] 徐晓辉, 刘作良. 基于 D-S 证据理论的态势评估方法 [ J ]. 电光与控制, 2005, 12(5): 36 - 37.
- [23] RAO N P, KASHYAP S K, GIRIJA G. Situation assessment in air combat: A fuzzy-Bayesian hybrid approach [ C ] // Proceedings of 2008 International Conference on Aerospace Science and Technology. Bangalore: [ s. n. ], 2008: 26 - 28.
- [24] 李伟生, 王宝树. 基于模糊逻辑和 D-S 证据理论的一种态势估计方法 [ J ]. 系统工程与电子技术, 2003, 25(10): 1278 - 1280.
- [25] 任伟, 蒋兴浩, 孙锁锋. 基于 RBF 神经网络的网络安全态势预测方法 [ J ]. 计算机工程与应用, 2006, 42(31): 136 - 138.

行为进行认证,对不会被攻击的行为不必设计到信息基树中。服务器端可调节设计不同客户端的信息基树,客户端经过自度量扩展后 *root\_hash* 值和服务器端不一致,就认为该行为不可信。

验证行为节点是否完整,通过行为节点进行度量后按照 Merkle 哈希树方法生成 *root\_hash*,整个过程是对一次行为进行操作,相比文献[9]提出的每次度量,每次都计算 *root\_hash*,将预期 *root\_hash* 值放到本地比较的方法,本地计算机计算能力不需太强,且克服本地 *root\_hash* 值被攻击的不安全性,将可预期的根 Hash 值放到远程端,每次行为都通过计算本地当前的 *root\_hash*,和远程计算机进行验证更能保证行为的安全,而远程计算机不需要一系列的证书验证过程,不需要考虑 *root\_hash* 值是否受到攻击,可靠性更高,克服了基于属性认证的静态特性弱点。

#### 4 结语

本文基于可信计算平台,在软件行为学理论的基础上,根据可信计算动态度量的实际需求,定义了基于软件行为认证的动态度量相关概念,将 Merkle 哈希树引入行为树中,对行为进行动态度量。给出了创建 AM\_AIB 树过程,根据当前行为的度量值,得到该时刻的 *root\_hash* 值,并且将 *root\_hash* 用于远程认证,经过客户端 TPM 签名的 *root\_hash* 和服务器端 *root\_hash* 值一致,就表明该行为是可信的。利用 Merkle 哈希树计算时间短的特性,在验证过程中只验证客户端的 *root\_hash*,有效地保护了客户端的隐私,还可以根据行为不同粒度来设计 AM\_AIB,验证方式灵活。在可信平台上基于行为的验证克服了基于属性验证的静态特点,经过组合之后度量,确保了平台应用软件运行时的可信。

(上接第 4 页)

- [26] LAI JIBAO, WANG HUIQIANG, LIU XIAOWU, et al. A quantitative prediction method of network security situation based on wavelet neural network [C]// Proceedings of the First International Symposium on Data, Privacy, and E-Commerce. Washington, DC: IEEE Computer Society, 2007: 197–202.
- [27] 张翔,胡昌振,刘胜航,等.基于支持向量机的网络攻击态势预测技术研究[J].计算机工程,2007,33(11):10–12.
- [28] 王娟.大规模网络安全态势感知关键技术研究[D].成都:电子科技大学,2010.
- [29] 龚正虎,卓莹.网络态势感知研究[J].软件学报,2010,21(7):1605–1619.
- [30] 王慧强.网络安全态势感知研究新进展[J].大庆师范学院学报,2010,30(3):1–8.
- [31] RABINER L R. A tutorial on hidden Markov models and selected applications in speech recognition [J]. Proceedings of the IEEE, 1989, 77(2): 257–286.
- [32] ADI A, BOTZER D, ETZION O. The situation manager component of Amit — Active middleware technology [C]// Proceedings of the 5th International Workshop on Next Generation Information Technologies and Systems. Berlin: Springer-Verlag, 2002: 158–168.
- [33] VALEUR F. Real time intrusion detection alert correlation [D]. Santa Barbara: University of California, 2006.
- [34] ZHAI YAN. Integrating multiple information resources to analyzing intrusion alerts [D]. Raleigh: North Carolina State University, 2006.
- [35] PORRAS P A, FONG M W, VALDES A. A mission-impact-based approach to INFOSEC alarm correlation [C]// Proceedings of the

#### 参考文献:

- [1] Trusted Computing Group. TCG Specification architecture overview specification revision 1.2 [EB/OL]. [2011-04-15]. <http://www.trustedcomputinggroup.org/>.
- [2] Trusted Computing Group. TCG specification architecture overview [S]. Oregon, USA: Trusted Computing Group, 2007: 5–40.
- [3] STUMPF F, TAFRESCHI O, RÖDER P, et al. A robust integrity reporting protocol for remote attestation [C]// WATC 2006: Proceedings of the Second Workshop on Advances in Trusted Computing. Tokyo: [s. n.], 2006: 25–36.
- [4] SADEGHİ A R, STÜBLE C. Property-based attestation for computing platforms: Caring about properties, not mechanisms [C]// NSPW 2004: Proceedings of the 2004 Workshop on New Security Paradigms. New York: ACM Press, 2004: 67–77.
- [5] CHEN LIQUN, LANDFERMANN R, LÖHR H, et al. A protocol for property-based attestation [C]// Proceedings of the First ACM Workshop on Scalable Trusted Computing. New York: ACM Press, 2006: 7–16.
- [6] HALDAR V. Semantic remote attestation [D]. Irvine: University of California, 2006.
- [7] 李晓勇,左晓栋,沈昌祥.基于系统行为的计算平台可信证明[J].电子学报,2007,35(7):1234–1239.
- [8] 庄碌,蔡勉,李晨.基于软件行为的可信动态度量[J].武汉大学学报:理学版,2010,56(2):133–137.
- [9] 徐梓耀,贺也平,邓灵莉.一种保护隐私的高效远程验证机制[J].软件学报2011,22(2):339–352.
- [10] 屈延文.软件行为学[M].北京:电子工业出版社,2004.
- [11] MERKLE R C. A certified digital signature [C]// Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 1989: 218–238.

5th International Symposium on Recent Advances in Intrusion Detection. Berlin: Springer-Verlag, 2002: 95–114.

- [36] MORIN B, MÉ L, DEBAR H, et al. M2D2: A formal data model for IDS alert correlation [C]// Proceedings of the International Symposium on Recent Advances in Intrusion Detection. Berlin: Springer-Verlag, 2002: 115–137.
- [37] SMITH D, SINGH S. Approaches to multisensor data fusion in target tracking: A survey [J]. IEEE Transactions on Knowledge and Data Engineering, 2006, 18(12): 1696–1710.
- [38] HINMAN M L. Some computational approaches for situation assessment and impact assessment [C]// Proceedings of the Fifth International Conference on Information Fusion. Washington, DC: IEEE Computer Society, 2002: 687–693.
- [39] OXENHAM M, CHALLA S, MORELANDE M. Fusion of disparate identity estimates for shared situation awareness in a network-centric environment [J]. Information Fusion, 2006, 7(4): 395–417.
- [40] IVANSSON J. Situation assessment in a stochastic environment using Bayesian networks [D]. Linköping: Linköping University, 2002.
- [41] JAJODIA S, LIU P, SWARUP V, et al. Cyber situation awareness: Issue and research (advanced in information security) [M]. Berlin: Springer-Verlag, 2009.
- [42] LIGGINS M E, HALL D L, LLINAS J. Handbook of multi-sensor data fusion: Theory and practice [M]. Boca Raton: CRC Press, 2009.
- [43] RAOL J R. Multi-sensor data fusion: Theory and practice [M]. Boca Raton: CRC Press, 2009.