安全报警关联技术研究

伏 晓 谢 立
(南京大学计算机软件新技术国家重点实验室 南京 210093)

摘 要 安全报警关联技术是近年来安全领域中的热点之一,它能够有效地解决目前困扰安全管理者的海量报警以及误报、漏报报警等问题。近年来该领域出现了大量有价值的研究成果,但已有工作大多集中在个别子领域,整个领域的发展并不均衡。对这一技术的研究现状进行了综述,介绍了其处理过程及体系结构,重点总结比较了报警聚类及融合、攻击场景重建和攻击意图识别这3个关键阶段的已有算法,之后又总结评述了目前报警关联的主要应用、技术难点及现有解决方案,最后对该领域面临的问题加以分析,并展望了未来方向。

关键词 报警关联,报警聚类,报警融合,攻击场景重建,攻击意图识别
中图法分类号 TP393.08 **文献标识码** A

Security Alert Correlation: A Survey

FU Xiao XIE Li
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)

Abstract Alert correlation is a new promising technology and has drawn more and more attentions in recent years. It can efficiently solve many problems bothering security managers now, such as high false positives (i. e. alerts mistakenly triggered by benign events), high false negatives (i. e. intrusions mistakenly missed by security mechanisms), and large amounts of alerts created by security products per day. In the past several years, a lot of vulnerable researches were done in this field, but most of them only focused on few issues. And there are still many challenging problems that have not been addressed well, or even not been touched. Researchers of this field need put more efforts into them in the future. This paper gave an overview of the research progress in this area. Firstly, we introduced the common process and the popular architectures of current alert correlation systems. Then we summarized and compared the main algorithms of three key phases (i. e. alert aggregation and fusing, attack scenarios constructing, and attack plan recognition) in the common process. After these, the main applications of this technology were introduced, and the difficulties and corresponding methods were summarized. At the end of this paper, we analyzed the shortages of current work and the possible new directions in this field.

Keywords Alert correlation, Alert aggregation, Alert fusing, Attack scenarios constructing, Attack plan recognition

1 引言

当前复杂的安全形式要求诸如防火墙、防毒软件、入侵检测系统(IDS)等多种安全机制联合部署。这些安全产品常产生大量难以理解的低层报警,而且其中可能混杂着众多误报、漏报,为管理者理解、分析安全形势造成了极大的困难,更不利于对安全威胁的及时响应。

安全报警关联是为解决上述问题而产生的一种新技术。其基本思想是根据某种策略(例如报警对应攻击的因果关系)分析各类报警,通过识别及融合不同相关程度的报警来构造攻击场景,获得攻击策略和意图。该技术主要具备以下功能:①用更抽象、简明的攻击场景或攻击策略取代低层报警,从而减少报警数量,增强报警语意;②识别误报及其触发根源,提高报警准确度;③通过关联多个安全机制的互补报警获得关于安全威胁的全面信息,降低漏报率,提高报警可信度。对于安全报警关联技术的研究大约始于2000年。因为该技术具有重大现实意义和实用价值,所以它在近几年逐渐成为安全领域的研究热点。

本文综述了安全报警关联技术的研究现状。首先介绍了报警关联的基本原理和处理过程,然后分别总结比较了报警聚类及融合、攻击场景重建和攻击意图识别这3个处理阶段的各类算法,之后又介绍了报警关联的主要应用及其面临的挑战。最后,分析了该技术的现有问题和未来方向。

2 报警关联技术简述

报警关联技术的原理是通过分析各类报警依次发现不同

到稿日期:2009-06-02 返修日期:2009-09-01 本文受2005年国家信息安全重大专项基金项目和国家"八六三"高技术研究发展计划项目基金(2003AA142010)资助。

伏 晓(1979—),女,博士生,主要研究方向为网络安全、机器学习等,E-mail:fuxiao1225@hotmail.com;谢 立(1942—),男,教授,博士生导师,主要研究方向为信息安全、分布式计算和先进操作系统等。

程度的相关报警，最终揭示攻击者的策略和意图。相关报警根据关联程度可分为4类(见图1)：关系最密切的是同类安全产品发出的针对同一事件的重复报警(即同一报警)；第二类是针对同一攻击步骤的报警，它们一般来自不同类型的安全产品第三类是由同一攻击场景触发的报警。攻击场景是指入侵者的一次行动，包括多个相互关联的攻击步骤，因此其对应报警也彼此相关；最后，一个攻击计划可由多个攻击场景组成，因此属于同一计划的报警也具有一定相关性。

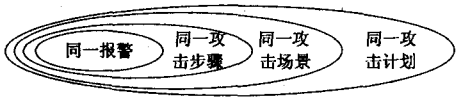

图1 报警关联层次

现有报警关联系统按其处理对象可分为3种：仅关联IDS报警的系统[1,2]，利用背景知识(如网络拓扑、组织安全策略等)辅助IDS报警关联的系统[3,4]，关联IDS、防火墙等多种安全机制报警的系统[5]。它们虽然在处理细节上略有差异，但其处理过程大致均可分为以下几个阶段(见图2)。

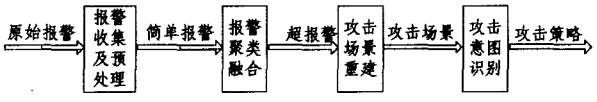

图2 报警关联处理过程

报警收集阶段负责从异构安全机制(即安全sensor)选择感兴趣的原始报警或辅助信息，转化成统一格式(例如IDMEF)后传递给关联系统。关联系统在接收到报警信息之后，通常还需对其做进一步的预处理，包括检查及补充重要的报警属性，将报警转化成关联算法可处理的格式(如属性元组)。不同关联算法需要的报警属性亦不同，但一般均需用到报警时间、攻击来源、攻击目标、攻击类型这几类。其中报警时间和攻击类型的预处理较为复杂：由于异构安全设施的时钟差异以及网络延迟等原因，各安全机制的报警时间常需预先同步(可利用全局逻辑时间或SNTP协议等实现[6])。而攻击类型属性则不是所有安全机制均能提供的，例如异常入侵检测(anomaly intrusion detection)即无法识别攻击的种类，此时关联算法应当与该属性无关[2]。

报警聚类及融合阶段的主要工作是将紧密相关的低层报警合并为超报警(hyper-alert)(亦称元报警或全局报警)，以便做关联分析。这一方面可以删除冗余信息，另一方面可提高报警的抽象层次、改善其语意。超报警可采用不同粒度及融合方式。一般的方法是首先聚类融合不同安全sensor的重复报警，然后进一步融合对应于同一攻击步骤的报警、对应于同一根源(root cause)的报警等。

攻击场景重建阶段的主要工作是分析报警聚类及融合得到的超报警，关联其中属于同一攻击过程的部分。最终得到的攻击场景可有多种描述方式，较为流行的包括超报警关联图[7](一种有向无环图，可直观地反映出报警间的依赖关系)、攻击场景描述规则[8]等。

对于易受攻击的大型网络，场景重建得到的将是大量独立的关联图或规则，它们对于管理者而言仍然难以理解。所以还需对其进一步分析，学习其中隐含的攻击策略，识别出攻击者的真实意图，以便管理者做出准确的安全形势评估，采取适当的响应措施。这即是意图识别阶段的主要工作。

上述处理过程中，后3个阶段是关键步骤。下面将详细介绍这几个阶段的相关算法。

3 报警聚类及融合

如前所述，报警聚类及融合阶段的作用是将单个报警组织成粗粒度的超报警，为进一步关联做准备。其中聚类是指按某种原则分组报警。融合则指对每组报警加以概括，得到一个可表示该分组的抽象报警。分组时可采用不同的原则，如攻击类型相似性、时间相似性、来源相似性、目标相似性[3]等。不同原则融合成的超报警，抽象程度亦不同。选择何种原则，取决于关联算法和关联目的。选择的宗旨应是在不丢失关联所需信息的前提下尽可能缩减数据量。

3.1 聚类及融合算法

目前用于报警聚类及融合的算法主要有以下3种。

(1)直接比较报警属性的方法

这类方法根据报警属性的相似度决定是否聚类融合报警。数据挖掘中的聚类分析(clustering)是其常用算法。属性相似度的计算方式可以是简单的string匹配，也可为不同属性设计不同的相似度计算策略[9]。目前许多关联系统采用了这种方法，例如最早提出超报警概念的Peng Ning等[7]即是将报警按攻击类型分组，每个超报警代表一组满足预定时间限制且具有相同类型的攻击实例。而文献[10]的方法是首先合并来自同一安全sensor的重复报警，再合并来自不同sensor且属性相同的报警，最后对上述结果应用某种clustering算法，并对每个聚类加以概括。文献[11]则提出了一种实时报警聚类算法，另外引入分类学习阶段来抽取报警所属的攻击类型。这样，即使IDS将某些报警误分为其它攻击类型，该算法仍能识别出同类攻击的报警。

(2)基于预定义pattern的方法

这类方法预先定义好每个报警分组的模式(pattern)，然后将报警流与已知pattern比较，实现聚类及融合。这些pattern用专用语言描述。例如文献[12]即用chronicle范式来描述报警pattern，完成紧密相关报警的集成。每个chronicle是一个事件集，事件间通过时间限制连接，事件的发生依赖于用断言描述的上下文。

(3)基于底层触发事件的方法

这种方法不是根据报警属性，而是根据触发报警的底层事件来融合报警。例如文献[13]即首先通过安全系统及领域知识获得每个报警的trigger event，然后根据trigger event的相似度聚类报警。

3.2 聚类及融合算法分析

直接比较报警属性是目前安全报警聚类及融合的主流方法。其原理简单，实现方便，一般无需关于攻击或系统本身的先验知识。但若异构安全sensor为同一触发事件产生的报警属性差异很大，这种方法将无法处理。

基于预定义pattern的方法准确度高，生成结果的语意也比较好，但这些优势依赖于pattern的良好定义。而这种定义目前大多人工完成，工作量大，容易出错，并且需要大量关于攻击和系统本身的先验知识，同时这种方法不能聚类未定义的报警分组。

基于底层触发事件的报警融合方法能够方便、准确地聚类异构安全产品的相关报警，即使这些报警的属性完全不同，或被赋予了不准确的取值。这类方法的难点在于每个报警触

发事件的识别。这不仅需要关于被保护系统的知识，有时还需了解安全产品的实现细节，而这些信息通常难以获得。

4 攻击场景重建

攻击场景重建阶段的目标是构造报警链，以揭示攻击者的行为方式。它是报警关联过程中最为关键的阶段，因此对场景重建算法的研究一直都是报警关联领域的重点。

4.1 攻击场景重建算法

现有的重建算法按实现原理可分为以下5种。

(1)基于属性相似度的方法

该算法也是根据属性间的相似度分组报警的，但它得到的报警分组抽象程度更高，而且处理的数据可为融合后的超报警。文献[14]是这类算法的典型，它为每个属性定义了一个相似度评估函数和一个作为权重的相似度期望值。整体相似度是各属性相似度的加权平均。另外，算法还为一些属性规定了最小相似度。只有当该值满足时，报警才能被关联。通过在不同属性上施加最小相似度限制，算法可以产生不同层次的关联结果。文献[15]则对属性间的比较策略加以扩充，除相等、相似关系外还增加了相等相异度和协方差关联关系。

(2)基于攻击前因后果的方法

在攻击者入侵过程中，某些步骤是为之后的步骤做准备，因此可根据这种准备关系来关联相应报警。即若在一定时间限制内，某先发生攻击的结果可使后发生攻击的前提得到满足，那么其对应报警即可被关联。这类算法的关键在于如何定义攻击的前提和结果，现有的方法主要有：①用被攻击系统的状态定义攻击的因果[16]。②用攻击者的能力定义攻击的因果[17]。③用输入输出资源定义攻击的因果[13]。定义完攻击的前提和结果之后，还需要用某种语言来描述它们，目前常用的描述方法是逻辑谓词。如文献[7]即将超报警类型描述为一个(事实，前提，结果)三元组，其中前提和结果均是谓词的逻辑范式。范式中的自由变元为事实中描述的报警属性名。逻辑谓词的定义常需手工完成，不但工作量大，而且难以统一。因此文献[18]又提出了一种自动构造攻击因果关系的方法。

(3)基于统计的方法

这类方法利用各种统计学算法来发现报警间的关联，并据此建立预测模型，然后用该模型来关联新输入的报警。这类算法的代表是Qin Xinzhou等提出的基于统计因果分析的关联方法[10]。算法使用GCT(Granger Causality Test)来关联报警。GCT是一种基于时间序列的统计分析方法，其目标在于通过执行"统计假设测试"来检验时间序列变量X与Y是否相关。GCT方法依赖于多个配置参数，而这些参数的设置通常只能依靠猜测，难以评估。因此文献[2]提出将报警建模为时间上的随机事件，并用两种更简单的统计测试来发现报警间的关联，但该方法只能构造简单的攻击场景。

(4)基于已知攻击场景的方法

这类算法的原理类似误用入侵检测，即首先定义所有已知或可能存在的攻击场景，然后比较输入报警和这些场景，根据匹配程度生成关联结果。攻击场景可由领域专家定义，也可从训练数据集中学习得到。在建模已知场景时，可采用多种方式，现有的方式包括基于预定义规则的方法[8]、基于网络攻击图的方法[19]、基于策略因果网的方法[3]、基于case-based learning的方法[20]等。

(5)基于Data Mining的方法

这类方法利用数据挖掘技术发现相关的报警。常用的数据挖掘算法包括分类、关联规则挖掘、frequent episode挖掘等。需要注意的是，数据挖掘技术必须与知识发现过程的其它步骤(即应用域理解、数据集成及选择、结果pattern评估、知识表示)联合使用，否则得到的可能是无意义的结果[21]。这类方法的典型是文献[22]，它用关联规则挖掘自动学习攻击场景的描述规则。规则生成有两种方式：基于攻击特征的方法首先选择与指定特征有关的报警数据，然后对其应用关联规则挖掘；基于攻击源的方法则首先将报警按照来源分组，再对每组挖掘关联规则。文章还提出了一种connected-component算法来过滤无关数据、缩减挖掘的数据集。基于数据挖掘的关联算法还有文献[5]，它提出了一种采用RIPPER分类技术的日志关联方法，用来改善入侵检测。

4.2 攻击场景重建算法分析

虽然已出现了众多场景重建算法，但目前对于算法的评估尚无公认的标准，算法之间难以比较。这导致关联系统的设计者常常对选择何种算法感到无所适从。针对这一现状，下面首先定义了"关联能力"这一概念，希望能从定性的角度为各种算法的比较提供一个依据。然后从准确度和效率方面比较了现有算法。

4.2.1 算法关联能力评估

将场景重建算法的"关联能力"定义为"识别能力"和"描述能力"两个方面。"识别能力"指能否识别出某个等级的关联报警，"描述能力"指能否描述报警之间如何相关。报警的相关程度从高到低可定义为4个等级，即实体等价、逻辑相关、统计相关和意图相关。实体等价指报警描述的是重复信息或对应同一个攻击步骤。逻辑相关指报警对应的攻击之间存在可明确描述的直接/间接因果关联。统计相关指报警对应的攻击没有直接的逻辑关联，报警属性也有较大差异，但报警却存在某种统计联系，例如总是同时发生。意图相关则表示报警对应的攻击看似无关，实则属于同一个攻击计划。

现有的场景重建算法具有不同的关联能力(见表1)：基于属性相似度的方法能够识别及描述对应同一实体(即报警或攻击步骤)的报警。通过比较源/目标地址等属性，也可能识别出逻辑相关的报警，但它无法描述报警之间如何逻辑相关。基于攻击前提和结果的方法仅能识别逻辑相关的报警，但它可以给出报警间逻辑关系的具体描述。基于统计的方法与基于数据挖掘的方法均能识别实体等价、逻辑相关和统计相关的报警，但数据挖掘方法的描述能力更强。基于已知攻击场景方法的关联能力取决于预定义的场景Pattern，即该Pattern描述的是何种关联等级，算法就能达到何种关联等级。

通过表1可以看出，基于已知攻击场景的方法关联能力最强，但该方法存在许多难以克服的缺点，如不能处理未定义的攻击场景、无法关联新型攻击。另外，攻击场景的描述通常比较复杂。若由专家定义，则工作量大且容易出错，而采用自动学习方法则需准备合适的训练数据集，但这种训练数据通常很难获得。其它几种算法均无需关于攻击场景的先验知识，能够关联新出现的攻击，但它们在关联能力上却有一定局

限。因此近年来一些研究者提出通过合并互补关联方法来获得更强的关联能力。例如文献[23]即是将基于攻击的前因后果的方法和基于统计的方法相结合，首先在超报警集上应用基于 Bayesian 网络的因果关联生成一组独立的关联图，再用基于 GCT 的关联方法连接独立的关联图。类似的还有文献[24-26]。

表 1　场景重建算法关联能力比较

关联度	基于属性相似度的方法		基于攻击前因后果的方法		基于统计的方法		基于已知攻击场景的方法		基于数据挖掘的方法	
	识别能力	描述能力	识别能力	描述能力	识别能力	描述能力	识别能力	描述能力	识别能力	描述能力
实体等价	√	√	×	×	√	×	√	√	√	√
逻辑相关	√	×	√	√	√	×	√	√	√	√
统计相关	×	×	×	×	√	√	√	√	√	√
意图相关	×	×	×	×	×	×	√	√	×	×

注：√代表肯定，×代表否定。

4.2.2　算法准确度及效率比较

在算法的准确度和效率方面（见表 2），基于属性相似度的方法实时性较好，但准确性依赖于设计者的经验和大量实验。例如它需要设计者为每个属性设计恰当的相似度比较函数，以及在不同属性间合理地分配权重。基于攻击前因后果的方法若因果关系定义适当则准确度很高，但前提结果的说明和匹配是耗时而易出错的工作，所以算法的实时性较差。基于统计的方法实现复杂，预测模型（关联规则）需要离线生成，这在一定程度上影响了算法的实时性。该算法的准确性取决于采用何种统计模型及模型的参数选择，后者通常只能靠经验决定，难以评估。基于已知攻击场景方法的准确性取决于模型本身：高质量的模型必然可以生成准确的关联结果，而且一旦模型定义完毕即可有效地实时关联报警。但其模型库需要及时更新才能处理新的攻击场景，这难免会影响其效率。基于数据挖掘的方法一般只能离线分析报警，实时性不够好，其准确性则取决于是否采用了有效的 KDD 过程。

表 2　场景重建算法准确度及效率比较

	基于属性相似度的方法	基于攻击前因后果的方法	基于统计的方法	基于已知攻击场景的方法	基于数据挖掘的方法
准确度	依赖于经验及实验	依赖于前因后果定义	依赖于统计模型及参数	依赖于场景定义	依赖于有无 KDD 过程
实时性	好	一般	一般	一般	一般

5　攻击意图识别

场景重建的结果是一些彼此独立的攻击场景。它们虽描述了攻击步骤之间的联系，但仍难以揭示攻击者的真实意图。这主要是因为：一方面，同一攻击策略可以有不同实现方式，而同一行为模式（攻击场景）也可能为不同意图的攻击者所采纳，所以攻击场景与攻击意图之间并非简单的一一映射。另一方面，为实现一个目的，攻击者可能会采取多次攻击行动，仅凭借其中个别场景难以推测攻击者的整体意图。而且，一旦处于报警密集的环境中，场景重建算法就会生成大量低层次的攻击场景，致使管理者很难从中推断攻击者的真实策略，更无法做出及时响应。因此，继续分析攻击场景，自动从中识别攻击者的策略和意图十分必要。目前这方面的研究才刚刚起步，现有的尝试主要是基于以下两种思想：

（1）自底向上归纳的方法

这类方法对独立的攻击场景继续进行关联分析，并抽象关联结果以得到攻击者的意图。文献[27]是其典型，它对关联算法生成的超报警关联图做进一步抽象，合并同类且相邻的超报警，在尽量不丢失信息的前提下得到更为简洁的关联图。这种关联图即是最终输出的攻击策略图。

（2）自顶向下分解的方法

这类方法先根据攻击者可能的策略分析出相应的攻击场景，然后将其与实际场景比较，以便识别攻击者意图。人工智能领域的“规划识别”（plan recognition）是其经常借鉴的技术。这类方法的典型是文献[28]，它首先用攻击树定义攻击规划库，然后据此关联独立的攻击场景。在得到关联结果之后，再用 probabilistic reasoning 技术来识别攻击规划。

现有的攻击意图识别方法还比较简单，无论是准确性还是效率均有待提高。可以改善意图识别算法准确性的一个有用思想是根据攻击的效果而非攻击的行为来判断攻击者意图。另外，其它领域的一些方法对于攻击意图识别也有很好的借鉴作用。例如文献[29]即提出用经济学领域的博弈理论来建模和推理攻击者的策略与意图。由于攻击者与识别者存在竞争关系，因此他们可能故意采用一些隐蔽或欺骗步骤来干扰识别。这是攻击意图识别领域在未来必须解决的难题。

6　报警关联技术的应用

根据报警关联的结果可以开发出各种应用。现有的应用主要包括攻击预测、攻击取证和攻击响应等。

基于关联得到的攻击策略，管理者可方便地预测出即将到来的攻击并尽早采取行动。近年来出现的“主动入侵检测”（Proactive/Anticipatory Intrusion Detection）技术即属此类应用。所谓主动入侵检测是指一旦检测到攻击准备步骤的标志事件（亦称攻击先兆），即立刻发起报警或阻断攻击[30]。该技术的关键在于从历史数据中发现入侵的先兆规则，而这些规则实质上就是攻击场景的变体。

计算机取证（computer forensics）是近几年兴起的一个新领域，其主要工作是研究如何利用科学的推理方法来预测、发现及重构由计算机犯罪引起的一系列事件，以便采取法律措施[31]。攻击取证/入侵取证（intrusion forensics）是其中的一个重要研究分支，其目的是在已知攻击发生的情况下如何恢复攻击的路径。这实际是报警关联技术的一种离线应用。

在发现攻击之后，除报警之外还可以做出主动的响应，包括重新配置安全机制、修复发现的漏洞、调整系统安全策略等。报警关联技术对于这些响应有很大帮助，例如根据识别出的攻击意图，可以更有针对性地调整相关安全机制的配置和整体安全策略；根据识别出的报警触发根源，可以更有效地修复系统漏洞。

7　报警关联技术的主要挑战

目前安全报警关联技术的难点问题主要包括误报过滤、漏报推理、报警与背景知识的结合以及关联系统本身的安全性等几个方面。

7.1　误报过滤

安全 sensor 产生的报警中常含有大量误报。据统计 IDS 每天触发的报警中误报可达 99%[32]。这些信息无疑会影响

到报警关联算法的准确度和效率。因此，如何处理误报是一个重要问题。误报指由正常行为导致的报警(false positive)，有时也指那些代表失败攻击的报警，对于前者，已经有不少识别及过滤的方法。但对于如何处理失败攻击所触发的报警目前仍有争议。有些研究者主张直接删除，而另一些研究者认为攻击者通过失败的攻击也能获得有用信息(如攻击目标的可用服务或防御方式等)，因此应将它们也纳入关联过程[17]。我们认为失败攻击可以被结合进关联过程，但前提应是关联系统知道它们代表的是失败攻击，否则关联这类攻击很可能导致生成实际不存在的攻击场景。

目前识别及过滤正常行为导致的报警主要有以下几种方法：①基于“不断重现的报警序列很可能是由正常行为导致”这一假设的方法：例如文献[1]即用 frequent episode 挖掘报警数据，在识别出针对某个目标的频繁报警序列后，将其作为候选者提交给用户，由用户判定是否误报；文献[33]则从流的角度监控报警，它用经典时间序列方法建模报警流的规律性，在过滤掉其中的周期性、缓慢变化的 trend 及随机噪音成分后，认为余下的显著现象才是真实报警。②基于根源识别的方法：即通过对报警的抽象识别其触发根源，进而区分出正常行为导致的报警。例如文献[32]即提出了一种利用概念聚类(Conceptual Clustering)识别报警根源的方法。③基于分类的方法：文献[34]是这类方法的典型，它首先根据训练数据用机器学习技术创建出报警的分类器，然后再用其分类真实报警和误报。前两种方法目前仍需要人工干预。基于分类的方法能够实现完全自动化，但缺点在于很难得到理想的训练数据。

对于失败攻击所触发报警的识别可通过报警验证技术(alert verification)完成。现有的报警验证方法包括[6]：①比较攻击的前提与被攻击系统的配置，从而确定攻击能否成功；②建模攻击的预期输出，即攻击留在网络或主机上的可见且可查的踪迹(例如某些临时文件)，通过检查这些踪迹判断攻击是否成功。文献[10,35]即采用了第一种方法。文献[36]则将两种方法结合使用，提出了一种通用的报警验证框架。报警验证得到的结果可信度高，但需要关于被攻击系统的背景知识甚至存取权限，这在大规模网络上很难实现。

除上述误报识别方法之外，来自多个安全 sensor 的重复报警也能增强报警的可信度。另外，Peng Ning 等认为在构造出攻击场景之后，那些不能被关联的独立报警即可视为误报。但这种思想基于“成功攻击一般是多步攻击场景中的一个步骤，而误报通常都是孤立和随机的”这一假设，可是在实际情况中攻击者有时仅需发送一个数据包即可侵犯主机(如 Slammer Worm)，而且识别及过滤误报应当是获得好的关联结果的前提，而不应当通过关联过程本身来减少误报[6]。

7.2 漏报推理

现有的安全机制并不完善，尤其是 IDS，漏报某些攻击步骤的情况时有发生。因此，如何根据有缺失的报警数据得到正确的攻击场景，对于关联分析算法是一项重要的挑战。

目前流行的解决方法是根据某些信息(例如已知攻击场景)假设出虚拟攻击来代替缺失步骤。文献[37]是此类方法的典型，它首先用基于漏洞的攻击图生成网络中可能存在的攻击场景。在实际关联过程中，若发现报警关联路径上存在断点，即假设此处漏报了相关的攻击。类似的还有文献[38]。

这类假设方法存在许多局限，例如虚拟攻击只能来自已知攻击类型，甚至必须在已有场景中与当前报警直接相关。另外，因为攻击者可通过不同攻击手段达到相同目标，所以假设攻击的准确性很难保证。对于准确性问题，研究者已经开始尝试用验证技术来解决。已有的方法包括基于审计数据的假设攻击验证[24]和利用操作系统层对象依赖追踪技术的假设攻击验证[39]等。但其它局限尚无很好的解决方案。

7.3 报警与背景知识的结合

背景知识对于用户理解关联结果非常有用，而且报警关联若脱离系统安全策略和网络拓扑结构等背景知识，就很可能生成大量用户不感兴趣或无关紧要的结果。因此，研究者提出可用背景知识来辅助报警关联。现有方法主要包括报警影响分析(alert impact analysis)和为报警设置优先级(alert prioritization)。

报警影响分析[6]的目的是判断攻击对于网络正常操作的影响。这需要来自攻击发生地资产数据库(asset database)的信息。该数据库中存储了网络/系统中安装的服务、服务之间的依赖、它们的重要性、安全属性等细节。根据这些信息可以判断出哪些服务依赖于被攻击的目标，从而分析出攻击一旦成功会有何种后果，即影响系统的哪些服务或功能。

报警优先级设置是指按照某种原则为报警设定优先等级，以便在关联过程中关注重要报警、丢弃不重要或无关报警。优先级的设置原则通常是根据攻击所威胁到的资产的重要性以及用户对这类报警的兴趣度[4]。优先级设置的一般方法是[6]：首先分析系统的安全策略和安全需求，然后利用资产数据库的信息判断某一网络服务对于网络整体功能的重要性，最后根据该重要性及安全策略为针对这一服务的报警分配相应的优先级。

7.4 报警关联系统的安全性

安全报警关联系统本身也面临着诸多安全威胁。主要威胁有两类：①alert flood 攻击，即向安全 sensor 发送模拟入侵信息从而触发大量虚假报警，或冒充安全 sensor 直接向关联中心发送大量虚假报警，干扰其正常工作；②敏感信息泄漏，即从关联中心的报警数据库中获得关于报警来源机器的敏感信息，例如使用的网络服务、协议等。

对于 alert flood 攻击，现有解决方法是：①通过某种手段识别虚假入侵。例如 Snort 即是通过判断入侵数据包是否完成了 TCP 的 3 次握手来决定是否为其发起报警。这样由单个数据包组成的模拟入侵就很难触发虚假报警。②控制报警吞吐量。例如文献[40]即在 IDS 的输出组件与报警关联机制之间增加了“token bucket filter”，在控制报警流量的同时，尽量避免丢弃重要的报警。③建立安全 sensor 与关联中心之间的信任关系。这可以通过认证等机制实现。

对于敏感信息泄漏，现有方法是利用报警净化技术(alert sanitization)，即在保证关联所需信息的同时，尽可能地删除或掩盖敏感信息。这方面的方法已经有很多[6]，例如用常量代替敏感域，用序列化编号代替敏感域，用 Hash 函数加密敏感域等。除此之外，文献[41]提出了一种从组织结构上保证报警安全性的方法，它采用 P2P 随机报警路由机制，还设置了多个报警存储设施。安全 sensor 随机决定将报警送至哪个存储设施。这样，即使攻击者控制了某些报警存储设施，仍然无法判断报警的真实来源。

目前对于报警关联系统安全性的研究才刚刚起步，采用的方法大多是净化、加密、认证等传统安全防护手段。如何使这些手段更加适应报警关联系统的特征，以及如何为关联系统开发更能满足其特殊需求的防护措施，是研究者在未来需要关注的问题。

结束语 安全报警关联技术发展至今已有近10年，已提出了许多关联分析方法并取得了较好的实用效果，但是仍有许多重要问题尚未解决。例如现有的关联结果均未提供可信度值(confidence)，因此验证关联结果的正确性就成了必需步骤。此外，如何处理多攻击场景并发情况下的报警关联(此时源于不同主机的攻击可能由两个合作者发起，也可能属于不同攻击企图，仅用时间、目标等限制将无法区分它们)也是一直未解决的难题。另外，该领域尚缺乏公开的实验数据集和公认的评估标准。现有的实验大多沿用为评估入侵检测系统而设计的公共数据集(例如DARPA 2000)，很多攻击场景无法检验，而且在测试前必须对数据进行预处理，而不同预处理方式得到的结果差别很大，所以很难在不同关联系统之间进行比较。这已经成为了一个很大的制约安全报警关联技术发展的障碍。

未来安全报警关联领域值得关注的方向包括：异构安全机制报警的关联、自动化攻击意图识别、更加高效的实时关联算法、多攻击场景并发时的报警关联等。总体而言，这一领域的研究尚处在起步阶段，未来需要研究者完成的工作还有很多。

参 考 文 献

[1] Clifton C, Gengo G. Developing custom intrusion detection filters using data mining[C]// Proceedings of MILCOM 2000. Washington DC: IEEE Computer Society Press, 2000: 440-443

[2] Maggi F, Zanero S. On the use of different statistical tests for alert correlation[C]// Proc. of RAID 2007. Heidelberg: Springer Berlin, 2007: 167-177

[3] Goldman R P, Heimerdinger W, et al. Information modeling for intrusion report aggregation[C]// Proc. of DISCEX '01. Washington DC: IEEE Computer Society Press, 2001: 329-343

[4] Porras P A, Fong M W, Valdes A. A mission impact based approach to INFOSEC alarm correlation[C]// Proc. of RAID 2002. Heidelberg: Springer Berlin, 2002: 95-114

[5] Abad C, Taylor J, Sengul C, et al. Log correlation for intrusion detection a proof of concept[C]// Proc. of ACSAC 2003. Washington DC: IEEE Computer Society Press, 2003: 255- 264

[6] Christopher K, Fredrik V, Giovanni V. Intrusion detection and correlation: challenges and solutions[M]. Berlin: Springer, 2005

[7] Peng Ning, Yun Cui, Reeves D S. Constructing attack scenarios through correlation of intrusion alerts[C]// Proc. of ACM CCS 2002. New York: ACM Press, 2002: 245-254

[8] Debar H, Wespi A. Aggregation and correlation of intrusion-detection alerts[C]// Proc. of RAID 2001. Heidelberg: Springer Berlin, 2001: 85-103

[9] Autrel F, Cuppens F. Using an intrusion detection alert similarity operator to aggregate and fuse alerts[C]// Proc. of SAR 2005. 2005: 1-10

[10] Qin X, Lee W. Statistical causality analysis of INFOSEC alert data[C]// Proc. of RAID 2003. Heidelberg: Springer Berlin, 2003: 73-93

[11] Giacinto G, Perdisci R, Roli F. Alarm clustering for intrusion detection systems in computer networks[C]// Proc. of MLDM 2005. Heidelberg: Springer Berlin, 2005: 184-193

[12] Wang L M, Ma J F, Zhan Y Z. Enhancing the content of the intrusion alerts using logic correlation[C]// Proc. of AWCC 2004. Heidelberg: Springer Berlin, 2004: 137-142

[13] Xu D, Peng Ning. Alert correlation through triggering events and common resources[C]// Proc. of ACSAC'04. Washington DC: IEEE Computer Society Press, 2004: 360-369

[14] Valdes A, Skinner K. Probabilistic alert correlation[C]// Proc. of RAID 2001. Heidelberg: Springer Berlin, 2001: 54-68

[15] Staniford S, Hoagland J A, McAlerney J M. Practical automated detection of stealthy portscans[J]. Journal of Computer Security, 2002, 10: 105-136

[16] Templeton S J, Levitt K. A requires/provides model for computer attacks[C]// Proc. of NSPW 2000. New York: ACM Press, 2000: 31-38

[17] Zhou J, Heckman M, Reynolds B, et al. Modeling network intrusion detection alerts for correlation[J]. ACM Transactions on Information and System Security, 2007, 10(1): 1-13

[18] Huang N, Hung H, Kao C, et al. Construct efficient hyper-alert correlation for defense-in-depth network security system[C]// Proc. of ICOIN 2004. Heidelberg: Springer Berlin, 2004: 886-894

[19] Noel S, Robertson E, Jajodia S. Correlating intrusion events and building attack scenarios through attack graph distances[C]// Proc. of ACSAC 2004. Washington DC: IEEE Computer Society Press, 2004: 350-359

[20] Locatelli F E, Gaspary L P, Melchiors C, et al. Spotting intrusion scenarios from firewall logs through a case-based reasoning approach[C]// Proc. of DSOM 2004. Heidelberg: Springer Berlin, 2004: 196-207

[21] Julisch K. Data mining for intrusion detection: a critical review [C]// Barbara D, Jajodia S, eds. Applications of data mining in computer security. Berlin: Springer-Verlag, 2002: 33-62

[22] Treinen J J, Thurimella R. A framework for the application of association rule mining in large intrusion detection infrastructures[C]// Proc. of RAID 2006. Heidelberg: Springer Berlin, 2006: 1-18

[23] Qin X, Lee W. Discovering novel attack strategies from INFOSEC alerts[C]// Proc. of ESORICS 2004. Heidelberg: Springer Berlin, 2004: 439-456

[24] Peng Ning, Xu D, Healey C, et al. Building attack scenarios through integration of complementary alert correlation methods [C]// Proc. of NDSS'04. 2004: 97-111

[25] Lee S H, Lee H H, Noh B N. A rule-based intrusion alert correlation system for integrated security management[C]// Proc. of ICCS 2004. Heidelberg: Springer Berlin, 2004: 365-372

[26] Wang J, Lee I. Measuring false-positive by automated real-time correlated hacking behavior analysis[C]// Proc. of ISC 2001. Heidelberg: Springer Berlin, 2001: 512-535

[27] Peng Ning, Cui Y, Reeves D S, et al. Towards automating intrusion alert analysis[C]// Proc. of the Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection. George Mason University, USA, 2003: 1-19

(下转第29页)

[22] Getoor L. Multi-relational Data Mining using Probabilistic Relational Models: Research Summary[C]// Proceedings of the 1st Workshop in Multi-Relational Data Mining. 2004

[23] Lee M, Hsu W, Kothari V. Cleaning the Spurious Links in Data [J]. IEEE Intell. Syst, 2004

[24] Kalashnikov D V, Mehrotra S. Exploiting Relationships for Data Cleaning[R]. TR- RESCUE-03-02. UCI Tech. Rep, 2003

[25] Newcombe H, Kennedy J, Axford S, et al. Automatic Linkage of Vital Records[J]. Science, 1959(130): 954-959

[26] Fellegi I, Sunter A. A Theory for Record Linkage[J]. J. Amer. Stat. Assoc., 1969, 64(328): 1183-1210

[27] Winkler W E, Inkler W E. Advanced Methods for Record Linkage[C]// Proceedings of the U. S. Bureau of Census. 1994

[28] Hernandez M, Stolfo S. The Merge/Purge Problem for Large Databases[C]// Proceedings of the ACM SIGMOD Conference. San Jose, CA, 1995

[29] Winkler W. The State of Record Linkage and Current Research Problems[C]// Proceedings of the U. S. Bureau of Census, TR99. 1999

[30] Mccallum A K, Nigam K, Ungar L. Efficient Clustering of High-dimensional Data Sets with Application to Reference Matching [C]// Proceedings of the ACM SIGKDD Conference. Boston, MA, 2000

[31] 陈伟, 王昊, 朱文明. 一种提高相似重复记录检测精度的方法[J]. 计算机应用软件, 2006, 23(10): 29-30, 42

[32] 俞荣华, 田增平, 周傲英. 一种检测多语言文本相似重复记录的综合方法[J]. 计算机科学, 2002, 29(1): 118-119

[33] Cohen W, Kautz H, Mcallester D. Hardening Soft Information Sources[C]// Proceedings of the ACM SIGKDD Conference. Boston, MA, 2000

[34] Dong X, Halevy A Y, Madhavan J. Reference Reconciliation in Complex Information Spaces [C]// Proceedings of the ACM SIGMOD Conference. Baltimore, MD, 2005

[35] Mccallum A, Wellner B. Conditional Models of Identity Uncertainty with Application to Noun Coreference[C]// Proceedings of the NIPS. 2004

[36] Singla P, Domingos P. Multi - relational Record Linkage [C]// Proceedings of the MRDM Workshop. 2004

[37] Pasula H, Marthi B, Milch B, et al. Identity Uncertainty and Citation Matching[C]// Proceedings of the NIPS Conference. 2002

[38] Li X, Morie P, Roth D. Identification and Tracing of Ambiguous Names: Discriminative and Generative Approaches [C]// Proceedings of the AAAI. 2004

[39] Lin Jing, Sun Jun, Xu Wenbo. Quantum-behaved Particle Swarm Optimization with Adaptive Mutation Operator [C]// ICNC 2006, Part I, LNCS 4221. Heidelberg: Springer-Verlag Berlin, 2006: 959-976

[40] 曹建军, 张培林, 王艳霞, 等. 一种求解子集问题的基于图的蚂蚁系统[J]. 系统仿真学报, 2008, 20(22): 6146-6153, 6157

(上接第 14 页)

[28] Qin X, Lee W. Attack plan recognition and prediction using causal networks[C]// Proc. of ACSAC 2004. Washington DC: IEEE Computer Society Press, 2004: 370-379

[29] Liu P, Zang W Y, Yu M. Incentive-based modeling and inference of attacker intent, objectives, and strategies[J]. ACM Transactions on Information and System Security (TISSEC), 2005, 8 (1): 78-118

[30] Cabrera J B D, Lewis L, Qin X, et al. Proactive intrusion detection-a study on temporal data mining[C]// Barbara D, Jajodia S, eds. Applications of data mining in computer security. Berlin: Springer-Verlag, 2002: 195-227

[31] Vel O de, Anderson A, Corney M, et al. E-mail authorship attribution for computer forensics[C]// Barbara D, Jajodia S, eds. Applications of data mining in computer security. Berlin: Springer-Verlag, 2002: 229-250

[32] Julisch K, Dacier M. Mining intrusion detection alarms for actionable knowledge[C]// Proc. of KDD-2002. New York: ACM Press, 2002: 366-375

[33] Viinikka J, Debar H, Mé L, et al. Time series modeling for IDS alert management [C]// Proc. of AsiaCCS 2006. New York: ACM Press, 2006: 102-113

[34] Pietraszek T. Using adaptive alert classification to reduce false positives in intrusion detection[C]// Proc. of RAID 2004. Heidelberg: Springer Berlin, 2004: 102-124

[35] Porras P A, Fong M W, Valdes A. A Mission-Impact-based approach to INFOSEC alarm correlation [C]// Proc. of RAID 2002. Heidelberg: Springer Berlin, 2002: 95-113

[36] Xiao Min, Xiao Debao. Alert verification based on attack classification in collaborative intrusion detection[C]// Proc. of SNPD 2007. Washington DC: IEEE Computer Society Press, 2007: 739-744

[37] Wang L, Liu A, Jajoda S. An efficient and unified approach to correlating, hypothesizing, and predicting intrusion alerts[C]// Proc. of ESORICS 2005. Heidelberg: Springer Berlin, 2005: 247-266

[38] Cuppens F, Miège A. Alert correlation in a cooperative intrusion detection framework[C]// Proc. of the 2002 IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society Press, 2002: 202-215

[39] Zhai Y, Peng Ning, Xu J. Integrating IDS alert correlation and OS-level dependency tracking[C]// Proc. of ISI 2006. Heidelberg: Springer Berlin, 2006: 272-284

[40] Tedesco G, Aickelin U. Data reduction in intrusion alert correlation[J]. WSEAS Transactions on Computers, 2006, 5(1): 1-8

[41] Lincoln P, Porras P, Shmatikov V. Privacy-preserving sharing and correlation of security alerts[C]// Proc. of USENIX-Security '04. San Jose: USENIX, 2004: 17-32