



电信网络海量安全事件关联分析引擎技术研究

樊 宁,史国水,沈 军,金华敏

(中国电信股份有限公司广东研究院 广州 510630)

摘 要:关联分析引擎通过把孤立的安全事件集合关联为一个安全事件链,从大量误报告警与低级别告警中找出真正威胁告警,是安全运营中心分析安全态势、做出及时响应的关键技术模块。提出了一种结合状态机与推理机两类关联分析机制优点的关联分析引擎技术——基于序列状态推导的关联分析引擎,通过自动序列控制攻击场景规则的匹配,实现高效准确的海量安全事件的关联分析,能够较好地解决传统关联分析引擎在电信级网络应用中的问题。

关键词:安全运营中心;关联分析引擎;序列状态;电信级网络

doi: 10.3969/j.issn.1000-0801.2013.10.029

Correlation Analysis Approach About Numerous Security Information and Event in Telecommunication Network

Fan Ning, Shi Guoshui, Shen Jun, Jin Huamin

(Guangdong Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China)

Abstract: Correlation analysis engine which correlate isolated security event as a chain to find out the real threat from a large number of false alarms or low level ones, is a key module of security operations centre (SOC). The traditional correlation analysis mechanism is divided into two types: state machine and inference-engine. For poor precision and low efficiency, they don't adapt telecom network application. A new correlation analysis mechanism based on consecutive state by inference-engine was presented, which executed efficiently and accurately, to solve the problems of correlation analysis engine applied in telecom network.

Key words: security operations centre, correlation analysis engine, consecutive state, telecommunication network

1 引言

安全运营中心(security operations centre, SOC)是对网络及安全设备与系统进行综合分析,实现安全事件集中管理和监控的技术支撑平台。它通过监测网络中设备与系统所产生的安全事件信息,关联分析出网络当前安全威胁与潜在的安全风险,从而能够及时发出预警,避免网络承受重大损失。为达到及时响应的目标,SOC 更强调实时性^[1]。

近年来,SOC 在网络安全运营中得到了广泛应用。但在电信级网络,SOC 则面临着严峻的挑战,主要表现在以

下几个方面。

- 电信级网络涉及设备种类繁多、数量庞大,对 SOC 安全事件运行和响应效率要求更高。
- 网络拓扑复杂,网络时延等复杂网络环境下的常见问题可能对 SOC 运行造成影响。
- 电信级网络中的恶意攻击行为影响范围更广,一个中等规模的网络,每日产生的安全事件信息,已达百万计;电信级网络中的安全事件更是海量。在海量安全事件中高效挖掘出真正的安全隐患,已经成为 SOC 在电信级网络应用的瓶颈。

关联分析引擎是SOC分析安全态势、做出及时响应的核心技术模块。本文提出了一种新的关联分析引擎技术,能够较好地解决SOC在电信级网络应用中的问题。

2 关联分析技术

关联分析引擎是SOC的关键技术模块,也是安全事件管理最核心的内容。

SOC从网络中收集的大量安全事件信息中,许多并不具有真实的威胁,有些可能是威胁实施前期的迹象,有些可能只是实质威胁产生的连带告警。安全事件关联分析是从经过预处理的安全事件中抽取有用信息,通过关联处理相关性,把孤立的安全事件集合关联为一个安全事件链,从而在大量误报告警与低级别告警中找出真正威胁告警。关联分析引擎功能的实现目标:结合漏洞、资产及威胁信息,深度挖掘安全隐患,判断安全事件严重程度,重构整个攻击场景,降低误报率,帮助安全运维人员及时定位网络中潜在的安全隐患。

SOC关联分析引擎常用的关联机制可归结为状态机和推理机两种类型。其中,状态机是一种正向关联分析的方法,而推理机是一种深度挖掘的方法。

(1) 状态机

“状态机”式关联分析引擎^[2]是由网络安全事件及时驱动,满足预置条件的安全事件信息,可触发状态机的状态变迁。通过状态机状态记忆安全事件发生链,从而分析出安全事件的关联关系。“状态机”式关联分析引擎的工作原理如图1所示。

“状态机”式关联分析引擎具有很强的实时性,关联分

析效率较高。但由于状态机要求网络安全事件进入关联分析引擎的时序,必须与事件发生的真正时序一致,规则的因果关系才不会发生错乱;而电信级网络下,因为网络传输时延和处理时延的影响,安全事件的时序很可能会发生颠倒,这样关联分析引擎的状态机无法触发,SOC告警就会出现错报或漏报。因此“状态机”式关联分析引擎的分析准确度并不高。

(2) 推理机

“推理机”式关联分析引擎是通过匹配攻击场景模型进行关联分析,即根据攻击特征和发生概率事先构建一系列攻击场景模型^[3]。推理机接收到的安全事件,如果符合某一攻击场景模型部分特征,即假设其所属该攻击场景,然后通过更多安全事件中挖掘数据信息,以识别攻击判定的可信度,直到达到一定约束条件则认为特定攻击场景已发生并形成描述该攻击场景的告警。

“推理机”式关联分析引擎的工作原理如图2所示。

“推理机”式关联分析引擎因是在完整安全事件集合上进行分析,其漏报的可能性比较低。但由于需要在安全事件数据库中进行深度挖掘,海量数据集上推理出结果的效率会大幅下降。

3 基于序列状态推导的关联分析引擎

如上所述,电信级网络拓扑复杂,管理设备多,事件海量,传统的状态机和推理机关联分析机制很难兼顾关联分析的效率和精度。针对电信网络海量安全事件的应用环境,本文提出了一种结合状态机和推理机技术优点的改进技术方案——基于序列状态推导的关联分析引擎。

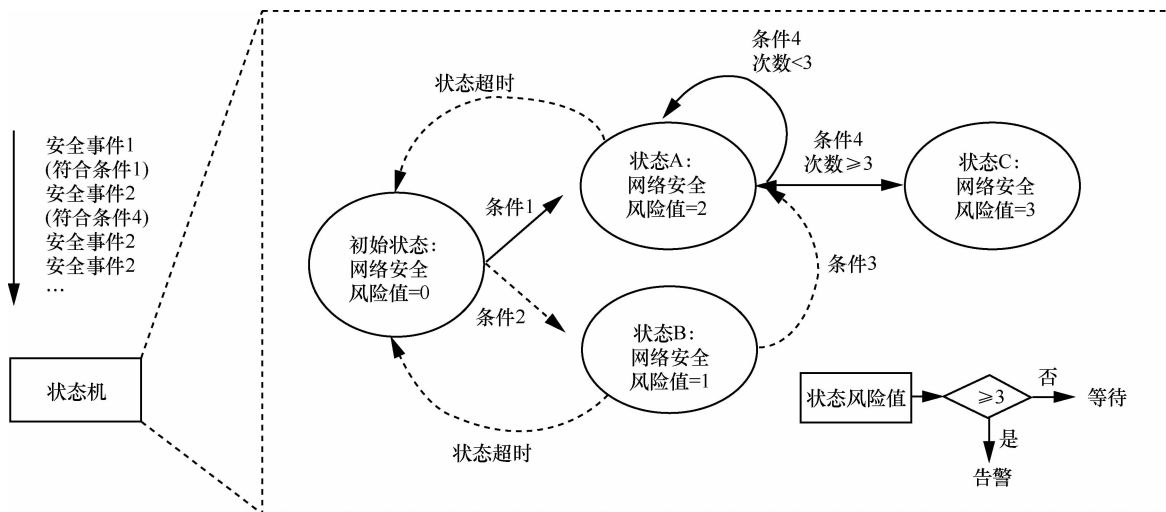


图1 “状态机”式关联分析引擎工作原理

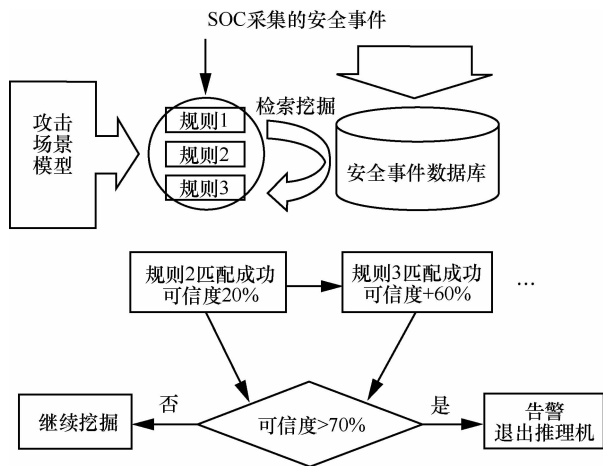


图2 “推理机”式关联分析引擎工作原理

3.1 引擎架构

基于序列状态推导的关联分析引擎由专家知识库、事件序列表、触发器、状态机等模块组成。其逻辑框架如图3所示。

安全事件信息中包含事件发生时间与事件接收时间。事件发生时间是发送安全日志的设备记录的日志产生时

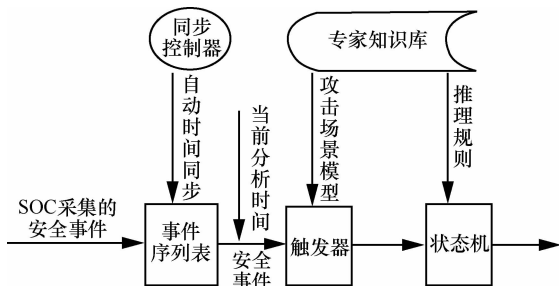


图3 基于序列状态推导的关联分析引擎逻辑框架

间；事件接收时间是SOC采集设备记录的安全事件到达采集设备的时间。事件序列表依据事件发生时间和事件接收时间对SOC采集的安全事件进行排序。同步控制器实时地自动微调事件序列表的同步时间。事件序列表以当前分析时间作为指针，按时序选出当前分析事件进入触发器进行判决。符合专家知识库中攻击场景模型的安全事件将引发状态机跳转，从而关联分析出安全事件链，找到真正的安全威胁。

基于序列状态推导的关联分析引擎的状态机与“状态机”式关联分析引擎相同，每一个状态的跳转都是按事件发生时间次序触发的。不同的是，“状态机”式关联分析引擎对进入引擎的安全事件时序没有检查，而基于序列状态推导的关联分析引擎通过事件序列表保障事件时序的正确性。

基于序列状态推导的关联分析引擎的另一个重要模块是专家知识库。专家知识库通过理解网络拓扑，挖掘已积累的安全攻击事件，构建起攻击场景模型系列。每一个攻击场景模型包含有网络结构、资产脆弱性、统计数据等信息，全面涵盖网络攻击的各种可能情况。

3.2 工作流程

基于序列状态推导的关联分析引擎利用已构建的攻击场景模型，依顺序对安全事件进行判决，符合攻击场景模型推理规则的安全事件将引起状态机触发跳转，其工作流程如图4所示。

(1)经预处理后的安全事件进入关联分析引擎，依据事件发生时间，按设备进行排序，形成通过设备进行区分

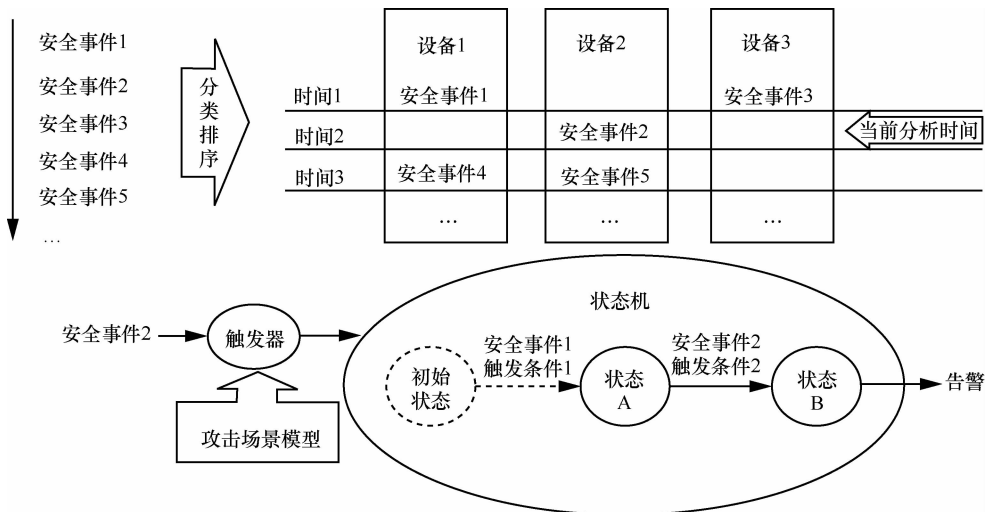


图4 基于序列状态推导的关联分析引擎工作流程

的事件序列表。

(2)以当前分析时间,同步事件序列表,在事件序列表之间次序跳转安全事件依时间顺序经触发器判决。

(3)当安全事件符合某一攻击场景模型时,触发器触发相应状态机至初始警备状态;当安全事件符合已触发状态机下一步跳转条件时,触发器触发相应状态机至下一步警备状态。

(4)直至状态机触发至最终态,关联分析引擎向外发出告警,状态机回复未触发状态。

(5)状态机尚未触发到最终态前,达到攻击场景模型的时限要求,状态机回复未触发状态。

(6)多个状态机可以同时被触发,同时处于警备状态。

(7)当新进入关联分析引擎的安全事件比事件序列表尾部的安全事件发生时间早,则按事件发生时间将安全事件插入合适的序列表位置。以新进入事件序列表的安全事件的发生时间作为当前分析时间。从新进入事件序列表的安全事件起,安全事件继续按时间顺序依次进入触发器进行判决。

3.3 自动时间同步控制器

从上述工作流程可见,基于序列状态推导的关联分析引擎的正常运作依赖于事件序列表中安全事件的正确排序。为保证安全事件按正确的发生时间排序,基于序列状态推导的关联分析引擎采用了自动时间同步的控制机制。

关联分析引擎工作之初,控制器将会依据各类设备

系统安全事件的接收时间,对事件序列表的时间排序做一个初步的同步。之后,在关联分析引擎工作时,自动时间同步控制器将记录每次状态机超时后回复至未触发状态,没有触发规则所涉及的设备,累计其失败匹配的次数。当失败次数达到一个统计阈值时,则对事件序列表进行微调。

3.4 效能分析

通过实验模拟 SOC 工作环境,对“状态机”式、“推理机”式和本文提出的关联分析引擎进行比较。实验环境如图 5 所示。

如图 5 所示,事件发生器、预处理模块、触发器保持不变,在更换关联分析引擎实现方法的情况下,对实验结果进行验证。实验证明,在实时性和精确性方面,“基于序列状态推导的关联分析引擎”有较大改进。从以下几方面分析关联分析引擎的效能。

(1) 海量事件分析效率

将噪声事件与随机模拟的 15 种安全事件链叠加作为前端输入,分别验证状态机、推理机和基于序列推导的关联分析引擎所支持的最大处理速率。结果见表 1(eps 表示每秒事件数;告警丢失量指 15 条安全事件链没有触发的告警条数)。

可见,“状态机”式关联分析引擎在 1 000 eps 时已经出现不稳定现象。而“推理机”式关联分析引擎所支持的最大处理速率是 2 000 eps,远远比不上基于序列推导的关联分析引擎 8 000 eps 的效率。

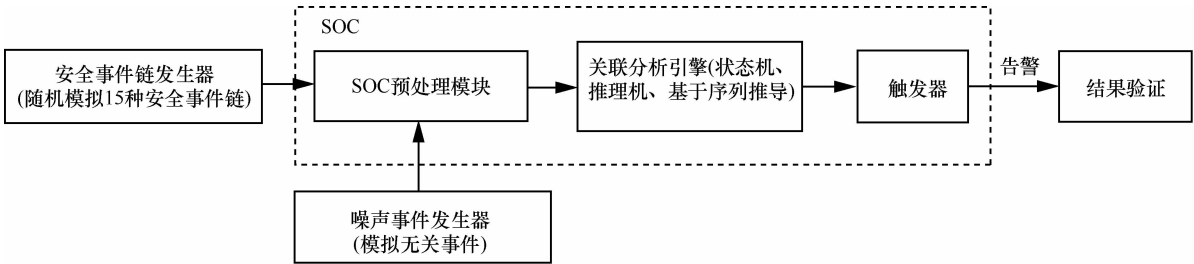


图 5 实验环境

表 1 分析结果

处理速率(eps)	状态机		推理机		基于序列推导	
	告警丢失量	分组丢失率	告警丢失量	分组丢失率	告警丢失量	分组丢失率
8 000	4 条	0	15 条	100%	0	0
4 000	2 条	0	15 条	27.81%	0	0
2 000	0	0	1 条	2.15%	0	0
1 000	1 条	0	0	0.07%	0	0
500	0	0	0	0	0	0



原因分析: SOC 预处理模块一般采用多线程对安全事件进行标准化、过滤、归并等处理。因各线程处理复杂度不一,后进入线程的安全事件可能会提前于先进入的事件完成,从而引起安全事件时序颠倒。对于“状态机”式关联分析引擎,这种情况会使得分析失灵,关键安全事件时序出错,可能会发生重要告警漏报,而在大量事件处理情况下,这种漏报现象更为突出。

“推理机”式关联分析引擎需要在 SOC 采集到的安全事件集合上挖掘出符合攻击场景模型的安全事件^[4]。即使可以采取机制,根据一些攻击场景模型条件缩小安全事件集合范围,也难以避免对于不同的攻击场景模型,反复检索、分析相同的安全事件。在单位时间内安全威胁多发时,挖掘效率会大受影响。

基于序列状态推导的关联分析引擎主体是采用“状态机”的工作模式,虽然在安全事件触发条件判定时,借鉴了攻击场景模型的思想,但对安全事件基本只做一遍分析,分析效率得到了保证。

(2) 安全事件发生时间记录失真

对安全事件链发生器进行调校,选择设备 A 的安全事件,设置生成后延时 5 s 再输出,以模拟安全设备时间不同步的情况。15 种安全事件链中有 9 种与设备 A 相关。将噪声事件与随机模拟的 15 种安全事件链叠加作为前端输入进行实验,结果显示:500 eps 情况下,“状态机”式关联分析引擎所有与设备 A 相关的告警全部漏报;而“推理机”式和基于序列状态推导的关联分析引擎则没有漏报。

原因分析:一般关联分析引擎对安全事件时间的判断,是依据安全事件携带信息中的“事件发生时间”或“事件接收时间”。实际网络中,只有部分设备系统通过 NTP 实现时间同步,一些设备的时间为手工配置,设备时间不容易达成一致,因此“事件发生时间”并不准确。而在大范围的网络环境中,事件接收时间可能会因为网络时延而出现误差引起混乱,这就为关联分析的因果关系判断带来困难。

基于序列状态推导的关联分析引擎方法引入事件时间序列表,通过将安全事件按设备区分,事件时间分别预先排序,再利用自动时间同步控制器,实时调整各设备事件时间序列表的基准位置,一方面保证了各设备彼此时间协调同步一致,另一方面减少了网络时延对状态机序列处理机制的影响。因此该方法在不降低关联分析效率的前提下,有效解决了时间失真的问题。

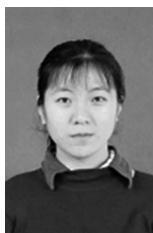
4 结束语

网络安全防护的目标是对安全攻击实现自动、准确、及时地响应,而这需要对网络威胁的正确理解和网络安全态势的准确把握。未来, SOC 将在网络安全态势评估、安全响应方面发挥越来越重要的作用^[5]。作为 SOC 的关键技术模块,关联分析引擎技术应当顺应网络安全发展的需要,在分析模型和分析机制上都不断创新突破。实践证明,单一关联分析技术无法应对复杂多变的网络安全态势监测。融合多种关联分析思想、结合优势,形成多层纵深关联将是关联分析引擎技术研究的一种可能思路。

参考文献

- 1 史简,郭山清,谢立.统一网络安全管理平台的研究与实现.计算机应用研究,2006(9):92~97
- 2 Harel D. Statecharts: a visual formalism for complex systems. Science of Computer Programming, 1987(8):231~274
- 3 Dain O M, Cunningham R K. Building scenarios from a heterogeneous alert stream. Proceeding of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, USA, 2001:231~235
- 4 陈春霞,黄皓.攻击模型的分析与研究.计算机应用研究,2005(7):115~118
- 5 姚键,叶保留,蔡圣闻等.安全管理研究综述.计算机科学,2004,31(8):1~4

[作者简介]



樊宁,女,中国电信股份有限公司广东研究院工程师,主要研究方向为网络信息安全事件分析和安全防护技术等。

史国水,男,中国电信股份有限公司广东研究院工程师,主要研究方向为 SOC 平台、移动互联网恶意程序监控等。

沈军,女,中国电信股份有限公司广东研究院高级工程师,主要研究方向为 IP 网络安全和网络应用安全技术等。

金华敏,男,中国电信股份有限公司广东研究院高级工程师,主要研究方向为 IP 网络安全和 IT 系统安全技术等。

(收稿日期:2013-08-25)