维普资讯 http://www.cqvip.com

因果告警相关方法在入侵检测系统中的应用与实现*)

王泽平 秦 拯
(湖南大学软件学院 长沙 410082)

摘 要 针对某公司入侵检测系统产品误警率高,将因果告警相关方法融入到原系统中,对告警信息进行相关分析。利用 DARPA 2000 入侵检测场景数据集 LLDOS1.0 对新系统进行实验验证,结果表明,通过新系统可有效降低误警率,并可用图形的形式显示告警信息之间的因果相关关系,形象揭示出攻击者的攻击过程与攻击策略。
关键词 入侵检测,因果关系,告警相关

Application and Implementation of Causal Alert Correlation Method in Intrusion Detection System

WANG Ze-ping QIN Zheng
(Software College of Hunan University, Changsha 410082, China)

Abstract Against a company intrusion detection system products superintendent high rate of false will cause alert correlation method into the original system, the alert correlation information is analyzed. Using 2000 DARPA intrusion detection scenario-specific datasets LLDOS1.0 for experimental verification of the new system, the results show that the new system can effectively reduce false alert rate and can be used to graphically display alert information in the form of a causal relationship, the image reveals an attacker to attack the course and attack strategy.
Keywords Intrusion detection, Causal relationship, Alert correlation

1 引言

经过二十多年的发展,入侵检测技术已日臻完善。概略地讲,入侵检测技术可以分为异常检测和误用检测。异常检测[1]是以一事物的正常行为为基础,任何偏离正常行为的事件都被看成入侵;误用检测[2]是基于已知的特征或系统弱点,任何匹配已知攻击模式或系统漏洞的行为都被认为是攻击。

但由于其技术本身的原因,入侵检测技术至今都无法克服其误警率高的缺点。为了弥补入侵检测技术的这种先天不足,近几年人们在入侵检测技术的基础上发展了告警相关技术。基于因果关系的告警相关方法[3]认为:攻击不是孤立的,它们是攻击序列的不同阶段,前面的攻击是为其后的攻击作准备。告警相关方法就是通过构造告警信息之间的相关关系,揭示出攻击者的攻击过程和攻击策略[4,5]。

本文针对入侵检测系统误警率高的缺点,在某公司已有入侵检测系统的基础上,将基于因果关系的告警相关方法的功能模块与原有入侵检测系统结合起来,形成一款具有告警相关分析功能的入侵检测系统。该系统首先利用入侵检测技术捕获告警信息(称之为原始告警信息),然后利用因果告警相关模块的功能分析这些原始告警信息之间的因果相关关系,剔除掉其中误告警信息,并以图形的形式显示有效告警信息之间的因果相关关系,揭示出攻击者的攻击过程和攻击策略[4,5]。

2 系统体系结构

2.1 体系结构概述

从整体的功能结构上看,本系统可以划分为传感器和控制台两大部分,如图 1 所示。传感器分布在被监控网段内,它主要完成被监控网段中网络报文的收集、解析、规则匹配,然后将符合规则要求的告警信息通过 COBAR 通信控制部件发送到控制台,同时根据规则要求处理对网络的响应。

控制台部分主要完成对告警信息的管理及分析,同时通过 COBAR 通信控制部件完成与传感器的数据交换,包括接收传感器的告警信息及向传感器发送控制信息(如匹配规则等)。控制台中的告警相关部件主要完成对告警信息的第二次分析,然后以图形的方式显示出攻击者的攻击过程。

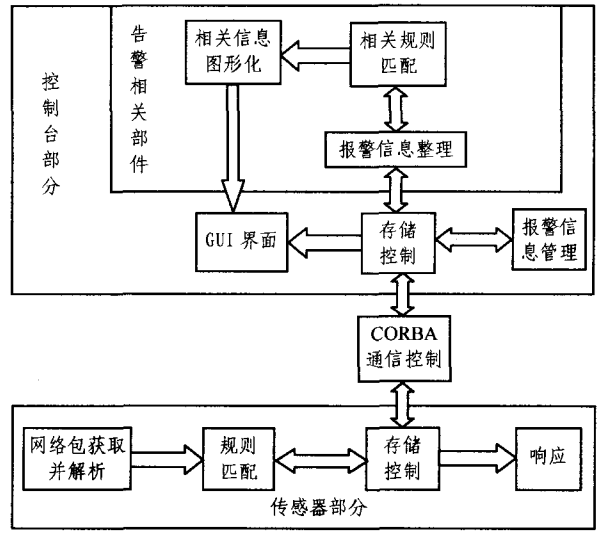

图 1 系统体系结构图

2.2 告警相关部件

告警相关部件是控制台的一个功能模块。它利用因果告警相关方法来对控制台数据库中所选择的告警信息进行分析,剔除掉其中的无效告警,并以图形的形式显示有效告警信息之间的因果相关关系,分析人员可以通过这种形象化的图形来分析攻击者的攻击过程及攻击策略。

*)国防科工委基础科研"十一五"规划项目(编号:20061143269),湖南省科技计划项目(No. 2006FJ4110),广东省科技项目(0711020400157,粤科基办字[2007]6 号),东莞市科技项目(2006D1046,2007108101021)。**王泽平** 硕士研究生,主要研究方向为信息安全、入侵检测技术;**秦 拯** 教授,主要研究方向为信息安全、软件工程。

维普资讯 http://www.cqvip.com

告警相关部件对告警信息的分析也是依据定义的告警相关规则进行的，为了保证规则定义和解析的通用性和可移植性，规则的定义结构采用了通用的 XML 格式。在规则的 XML 文件中，定义了三个数据部分，它们分别是谓词部分、隐含部分、超级告警部分[6]。

(1) 谓词部分

```
〈Predicates〉
〈Predicate
  Name="CiscoCatalyst3500XL"〉
  〈Arg
      id="1"
      Pos="1"
      Attr="varchar(15)"〉
  〈/Arg〉
〈/Predicate〉
〈Predicate
  Name="GainSMTPInfo"〉
  〈Arg
      id="28"
      Pos="1"
      Attr="varchar(15)"〉
  〈/Arg〉
  〈Arg
      id="29"
      Pos="2"
      Attr="varchar(15)"〉
  〈/Arg〉
〈/Predicate〉
〈Predicates〉
```

表示谓词 CiscoCatalyst3500XL 有一个长度为 15 个字节、编号为 1 的字符型参数。谓词 GainSMTPInfo 有两个参数，第一个参数的编号为 28，长度为 15 个字节，类型是字符型。第二个参数的编号为 29，长度为 15 个字节，类型是字符型。

(2) 隐含部分

```
〈Implication Phantom="Yes"〉
    〈ImplyingName〉
        GainOSInfo
    〈/ImplyingName〉
    〈ImpliedName〉
        OSUNIX
    〈/ImpliedName〉
    〈ArgMap〉
      〈ImplyingArg
        id="8"〉
      〈/ImplyingArg〉
      〈ImpliedArg
        id="26"〉
        〈/ImpliedArg〉
    〈/ArgMap〉
〈/Implication〉
```

表示通过获得的操作系统信息就能知晓操作系统的名称。

(3) 超级告警部分

```
〈HyperAlertType
    Name="Email_Almail_Overflow"〉
    〈Fact
        FactName="SrcIPAddress"
        FactType="varchar(15)"〉
    〈/Fact〉
    〈Fact
        FactName="SrcPort"
        FactType="int"〉
    〈/Fact〉
    〈Fact
        FactName="DestIPAddress"
        FactType="varchar(15)"〉
    〈/Fact〉
    〈Fact
        FactName="DestPort"
        FactType="int"〉
    〈/Fact〉
    〈Prerequisite〉
        〈Predicate
            Name="ExistService"〉
          〈Arg
           id="22"
           ArgName="DestIPAddress"〉
          〈/Arg〉
          〈Arg
              id="23"
              ArgName="DestPort"〉
          〈/Arg〉
        〈/Predicate〉
        〈Predicate
        Name=
        "VulnerableAlMailPOP3Server"〉
        〈Arg
            id="20"
            ArgName="DestIPAddress"〉
        〈/Arg〉
        〈/Predicate〉
    〈/Prerequisite〉
    〈Consequence〉
        〈Predicate
            Name="GainAccess"〉
            〈Arg
            id="4"
            ArgName="DestIPAddress"〉
            〈/Arg〉
        〈/Predicate〉
    〈/Consequence〉
〈/HyperAlertType〉
```

表示超级告警 Email_Almail_Overflow 的三元组[6]中的各部分的内容如下：

1. Fact 中有四个元素 SrcIPAddress 和 DestIPAddress 都是一个长度为 15 个字节的字符型数据，SrcPort 和 DestPort 都是一个整型的数据。

2. Prerequisite 有两个谓词，其中 ExistService 的两个参数的编号(与 Fact 段中一致)为 22，23。22 的值就是 Fact 域中的 DestIPAddress，23 的值就是 Fact 域中的 DestPort。

VulnerableAlMailPOP3Server 有一个编号为 20 的参数，值为 Fact 域中的 DestIPAddress。

3. Consequence 有一个谓词 GainAccess，有一个编号为 4 的参数，值为 Fact 域中的 DestIPAddress。

告警相关分析模块的运行流程如图 2 所示。在启动告警相关分析功能后，系统首先对告警相关规则进行解析，然后整理系统的告警信息，即将每一条系统的告警都看成是一个超级告警，根据解析后的规则找出每一超级告警的前提条件(Prerequisite)集合和结果(Consequence)集合，并保存到数据库中。

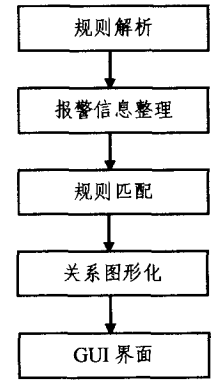

图 2 告警相关分析基本流

如果一个超级告警的结果集合正好包含在另一个超级告警的前提条件集合中，并且它们存在时间上的先后关系，我们就认为这两个超级告警的规则匹配成功。匹配成功后的超级告警将通过图形化的形式在 GUI 界面上显示出来。

3 实验结果分析

实验的目的是测试告警相关部件对入侵检测系统误警率的优化情况。由于告警相关图形反映的是网络入侵的攻击过程，因此我们利用 DARPA 2000[7]入侵检测场景数据集 LLDOS1.0 来测试我们设计的模块的运行情况。LLDOS1.0 包含了实施 DDoS 攻击的准备阶段的一系列攻击：探测，入侵，安装攻击服务程序的过程。

维普资讯 http://www.cqvip.com

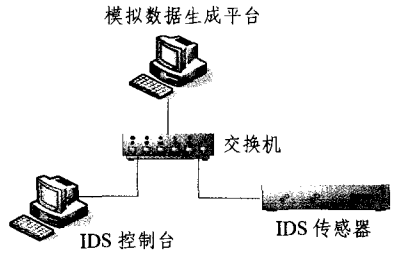

图 3 告警相关分析验证平台

实验网络平台如图 3 所示。模拟数据生成平台利用网络重播工具将 DARPA 2000 入侵检测场景数据集 LLDOS1.0 重新发送到 IDS 传感器所监控的网络上，IDS 传感器检测到网络攻击时将攻击信息发往 IDS 控制台。在完成重播一次数据集 LLDOS1.0 后，控制台就可以根据得到的数据集 LLDOS1.0 中的告警信息来检测告警相关模块的功能。

实验完成后，控制台共收集到传感器报告的告警信息 886 条，对这些告警信息进行告警相关分析后得到有效告警数 57 条。如果从告警成功的角度来计算误警率的话，成功的告警数为 36 条，误警率的比较情况如表 1 所示。从表 1 可以看出：系统从改进前到系统被改进后误警率从 98.94% 降低到了 36.84%，其改善效果是相当明显的。

表 1 误警率比较表

系统状态	总告警数	误告警数	误警率
原系统	886	850	98.94%
改进后系统	57	21	36.84%

其图形化后的部分形式如图 4 所示。从图 4 可以看出：只有 1,3 的攻击过程达到了攻击目的，而 2 中的缓冲区溢出攻击并未成功（至少没有发生后续更加危险的攻击）。根据这点我们可以进一步减少关心的告警信息数量。

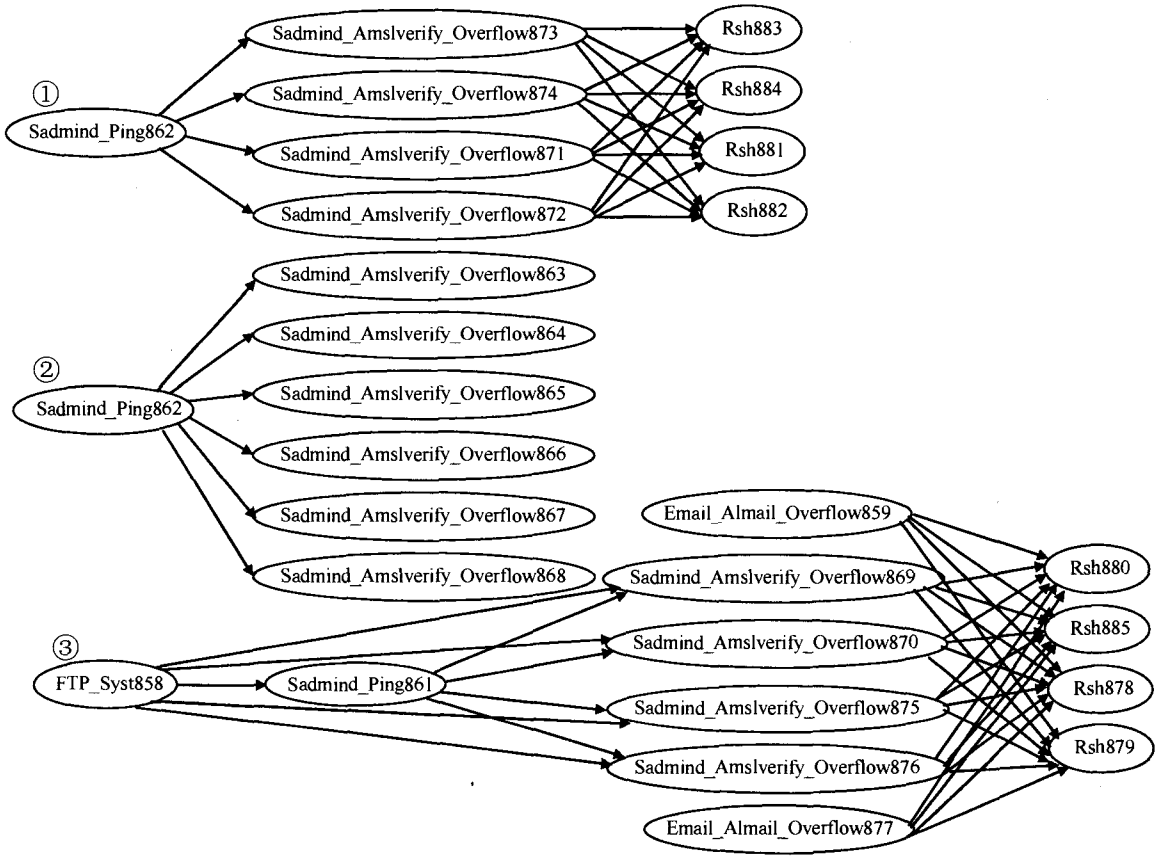

图 4 告警相关图形

结束语 通过将因果告警相关方法与入侵检测技术融合起来，在对原始告警信息进行告警相关分析后，能剔除掉原始告警信息中过多的冗余告警信息，有效地降低了入侵检测技术的高误警率。同时由于利用图形的形式来表示告警信息之间的因果相关关系，形象地揭示了攻击者的攻击过程和攻击策略，方便了网络管理。

参 考 文 献

[1] Javits H, Valdes A. The NIDES statistical component: Description and justification. Tech. rep. SRI International, Computer Science Lab- oratory, 1993

[2] Eckmann S, Vigna G, Kemmerer R. STATL: An Attack Language for State-based Intrusion Det- ection. Journal of Computer Security, 2002, 10(1/2): 71-104

[3] Ning Peng, Cui Yun, Reeves D S. Construct- ing Attack Scenarios through Correlation of Intrusion Alerts // Proceedings of the 9th ACM Conference on Computer&Communications Security. 2002, 11: 245-254

[4] Qin Zheng, Li Na, Zhang Da-fang. Improvement of Protocol Anomaly Detection Based on Markov Chain & Its Application // Proc the 3rd International Sym- posium on Parallel and Distributed Processing and A- pplications (ISPA 2005). 2005: 387-396

[5] 李亚琴，孙传林，雷杰. 入侵告警关联系统及关键技术的研究 [J]. 信息安全与通信保密，2006(8): 97- 99

[6] Ning P, Cui Y. Techniques and tools for analyzing intrusion alerts [J]. ACM Trans. on Information and System Security, 2004, 7 (2): 274-318

[7] MIT Lincoln Lab. 2000 DARPA intrusion detection scenario specific datasets [DB/OL]. http:// www. 11. mit. edu/IST/ideval/data/2000/2000_data_index. html, 2004-09-30