基于分层检测的协同攻击检测技术研究

经小川[1] 刘克强[2] 胡昌振[1]
(1.北京理工大学信息安全与对抗技术研究中心 北京 100081; 2.首都经济贸易大学信息学院 北京 100071)

〔摘要〕 协同攻击的复杂性使传统检测方法难以对其进行有效的检测。在对协同攻击行为的层次性和关联性的分析基础上,将协同攻击行为划分为基于时间的行为和基于空间的行为,结合适当的攻击表达方法,提出一种应用于网络协同攻击的检测方法,并详细介绍了该方法的特点和应用方式。
〔关键词〕 入侵检测系统 时序检测 功能检测 〔中图分类号〕 TN918
〔文献标识码〕 A 〔文章编号〕 1000-7857(2005)04-0004-04

A STUDY ON COORDINATED ATTACK DETECTION BASED ON DELAMINATION

JING Xiao-chuan LIU Ke-qiang HU Chang-zhen
(1. Information Security & Antagonism Research Center, Beijing Institute of Technology, Beijing 100081, China;
2. Information School, Capital Economy & Trade University, Beijing 100071, China)

Abstract: For the complexity of coordinated attacks, it is difficult to detect them efficiently by using the traditional methods such as misuse detection and anomaly detection. Based on the research work on the hiberarchy and reciprocity of attack behaviors, a solution for detecting coordinated attack with the conditional association and temporal method was suggested. A kind of attack representation that suitable to association analysis has been introduced.
Key Words: Intrusion Detection System(IDS), temporal detection, conditional detection **CLC Number:** TN918
Document Code: A **Article ID:** 1000-7857(2005)04-0004-04

1 引言

1.1 协同攻击

网络攻击按照其威胁的现实性可分为两类:结构化攻击和非结构化攻击。非结构化攻击是指一类在小范围内、攻击能力较弱、不能形成规模化有组织的攻击行为。这类攻击通常是采用单点攻击,攻击工具通常不会太复杂,它所造成破坏的范围、深度是有限的,攻击的实施者通常是单个有攻击能力的黑客或对公司不满的雇员等。结构化攻击则是在良好的计划组织条件下实施的攻击行为,它的特点是攻击点多、多技术、隐蔽性好、危害较大。协同攻击属于结构化攻击的一种,既具有结构化攻击的特点也有自身的单独特色。首先,协同攻击比普通结构性攻击威胁范围更大,使用的攻击技术更全面;其次,协同攻击不仅在攻击点上是分布的、协同的,甚至可以做到攻击软件上的协同,从而实施一定的攻击战术。

协同攻击是指一类由多个攻击者采取分布方式、在统一攻击策略指导下对同一任务目标发起攻击或探测的行为,其攻击的技术手段和攻击步骤由统一的攻击策略在各攻击者之间协调从而达到协同。

1.2 传统检测方法的失效性分析

传统的入侵检测方法(误用检测、异常检测)难以对协同攻击作出准确的判决,这是由于传统检测方法所建立的基础与网络协同攻击内在本质的不一致所造成的。异常检测则是利用数学方法对用户的日常行为方式形成一个模式,进而根据此模式与实时模式的差异值得出检测结果。此种方法对于协同攻击的检测不适用。

这是因为协同攻击行为本身就是一个涉及到多用户、多地址、多重行为表现的攻击行为,用户之间的不关联性、攻击行为表现形式的多样性造成了异常检测方法的无效。就目前来说,基于异常的入侵检测方法对这种攻击方式的检测基本上是无能为力的。

误用检测是对攻击行为的本身作出规范的描述,通过分析将攻击行为总结成若干特征而形成规则,然后和正在运行的各种行为进行比较,如果触发了某一规则,那么就认

收稿日期:2005-03-01
基金项目:国防科技基础研究项目
作者简介:经小川,男,1972~ ;北京市中关村南大街 5 号北京理工大学机电学院,博士研究生,研究方向为网络安全技术;E-mail: xiaochuan@jing.com.cn
胡昌振,1967~ ;北京理工大学机电学院,教授,研究方向为网络安全技术、数据融合;E-mail: chzhoo@public.bta.net.cn

为这种行为是一种攻击。这种检测方法与系统相对无关,通用性较强。但传统误用方法最致命的弱点在于把信息网络当作一个均匀平衡系统对待,忽略了信息网络的复杂性,忽略了用户行为的时空结构,把复杂的用户行为简单化了。但是,这种检测方法的优势是准确和高效。这种优势的基础在于对攻击行为进行深入而细致的分析,提练攻击行为作用在系统各阶段、各层面上的特征细节。可以这样说,攻击特征细节描述的规则越详细,其检测的效果就越准确。

本文认为,对于协同攻击检测的最关键之处在于分析组成协同攻击各子行为或事件之间的关联性,其具体体现在时序上的关联性和功能上的关联性两个方面。如果结合适当的检测算法能找到具有关联性的动作或事件,那么协同攻击就可以被检测到,甚至在检测进程中可以预测。

2 基于功能的检测

2.1 协同攻击子行为的功能关联

协同攻击是由一系列的攻击动作所组成,所有动作的根本目的都在于完成协同攻击所指定的目标。为了达到此目标,协同攻击将攻击任务分解为多个子任务并由不同的攻击行为完成。这些子任务通常是相关的,即一个子任务的完成是下一子任务开始的前提条件或者两个子任务的合成为另一子任务。对于协同攻击中的子攻击动作也是如此,前一攻击完成得到的信息或几个攻击得到信息的合成为下一攻击的初始条件。因此,称这些攻击动作之间是具有"前因后果"的,即动作之间的关联性。

将攻击动作定义为如下一个六元组:

Attack=<ID,Time,Source_IP,Dest_IP,Pre_Info,Post_Info>

其中:ID 为此次攻击的编号;Time 为攻击发生时间;Source_IP 为攻击源地址;Dest_IP 为攻击的目的地址;Pre_Info 为该次攻击前所需具备的信息;Post_Info 为通过该次攻击后所取得的信息。

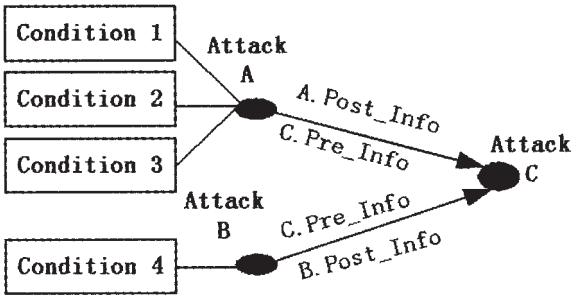

图 1 攻击动作关联

从图 1 中可以看出,攻击步骤 Attack C 在 Attack A 和 Attack B 动作结束之后进行,发起 Attack C 攻击之前所需用的信息为 Attack A 和 Attack B 攻击之后所获取的信息。在这种情况下,认为 Attack C 与 Attack A、Attack B 是关联的。

攻击行为之间的关联性包含强关联和弱关联两种。

(1)强关联。以图 1 为例,当攻击动作满足如下条件时:

Attack C. Dest_IP = Attack B. Dest_IP= Attack A. Dest_IP (1)

Attack C.Time> Attack A.Time≥Attack B.Time (2)

Attack C. Pre_Info= (Attack A. Post_Info)∧(Attack B. Post_Info) (3)

则称这 3 个攻击动作是强关联的。(1)式表示强关联攻击动作的目标是同一主机;(2) 式表明了强关联攻击动作的时序;(3)式表明了强关联攻击动作之间的信息传递。

强关联从攻击动作的时序性和信息传递的角度上说明了攻击动作之间的内在联系,即在协同攻击的条件下前一个或几个攻击的结果是下一个攻击的前提条件。一个满足了强关联条件的攻击序列,如果其攻击源不一致,那么该序列必然为协同攻击序列;如该序列攻击源是相同的则表示了一个单点攻击的完整过程。

(2)弱关联。当攻击动作序列不满足强关联的条件,而满足如下条件:

Attack C. Dest_IP= Attack A. Dest_IP= Attack B. Dest_IP

Attack C. Time−Attack A. Time=

Attack A. Time−Attack B.Time (4)

则称攻击动作是弱关联的。(4)式表明了弱关联动作链在攻击时间的时序间隔上有着严格的精确性,这同样是一次协同攻击的过程,只是攻击无结果,或是同一种攻击不断地循环为下一步的攻击取得了信息。通常的协同自动化攻击就满足了上述条件。

2.2 关联动作链的检测

协同攻击的检测在于是否能够在已报警的诸多攻击行为中找到攻击前提和攻击后果相关联的动作链。在寻找关联动作链时,使用普通 IDS 的报警作为输入数据源。当 IDS 报警显示有攻击行为时,记录当前的攻击行为和攻击时间,按照攻击描述六元组中各个参量进行填充。对于 Pre_Info 和 Post_Info 的填充则是根据攻击分类属性表查询获得。将常见的攻击经分类形成一张攻击属性表,表中对各类攻击的前提条件和该攻击成功后所可能得到的结果作了详细的描述。例如扫描类中针对主机端口的 PING 攻击,其前提为:

(Scan(Victim_port)∨GetInfo(Victim_port))

即攻击成功的前提是已获得主机的端口号或者是前步攻击已对端口进行过扫描。攻击完成后,其结果为:

(GetInfo (Victim_port,Active,Non−Active)∨GetTcpNumber(Victim))

即攻击成功后得到的信息为所攻击端口的活动状态、当前连接的 TCP 序列号等。

设定时间的截止阈值后,将经过六元编码的攻击动作按照时序的先后进行关联查找,即查找各攻击动作之间 Pre_Info 和 Post_Info 参数的合成关系。该查找过程实际上是一种寻优过程,即寻找关联动作链最长的序列。对于 M 个攻击动作,有如下种组合可能产生:

$$\sum_{i=2}^{m-1} C_m^i$$

显然,直接计算如此大的数据量是不太现实的。本文将寻优过程转化为如下的可控形式。设定一个效益函数,通过这个函数进行局部寻优,最终以局部的最优解合成全局的最优解。

对于满足关联条件的攻击来说,可将前后攻击写作如下形式:

$$X_{k+1}=AX_k+BU_k \quad (5)$$

其中:X_k 为初始攻击,U_k 为方向控制向量。(5)式表明搜索过程中,关联链中第 k 步攻击与第 k 个方向控制向量决定了攻击动作池中哪个动作为第 k+1 步攻击。

设定寻优过程的效益函数如下:

$$\mathrm{Len}(X_{k+1}, X_k)=\begin{cases}1 & X_{k+1}, X_k \text{关联}\\ 0 & X_{k+1}, X_k \text{非关联}\end{cases}$$

整个寻优过程就是要找到一个 N 阶段的方向控制策略：

$$(U_1, U_2, U_3, \cdots\cdots U_n) \in U \tag{6}$$

使如下总效益函数达到最大：

$$J^{*}=\underset{U_k}{\mathrm{Max}} \sum_{k=0}^{N-1} \mathrm{Len}(X_k, U_k) \tag{7}$$

图 2 表示了 7 个动作之间的关联过程。将攻击按照设定的时间片分层，首先判断 1 与下一层（以时序排列）2、3、4 的关联。若 1、2 有关联，则 $Len(1,2)=1$, $U_k=\{(1,2)\}$，然后将 1 节点 隐去，将 1、2 节点视为同一节点 2。当 2、3 点与 2、5 点同时关联时，保留同层之间的关联，将 2 隐去，两点视为同一点 3，*Len* 函数进行累加，此时 $Len(2, 3)=2$, $U_k=\{(1,2),(2,3)\}$。经过再次迭代即可找到这 7 个动作的关联链。

该种方法的特点在于，在整个查找关联的过程中，若 Len 函数在一个小区间[*K*, *N*]是最优的，则它满足在区间[*K*+1, *N*]仍是最优的。换言之，假如子过程是最优，那么由这些最优子过程所组成的全局过程也必定是最优的。

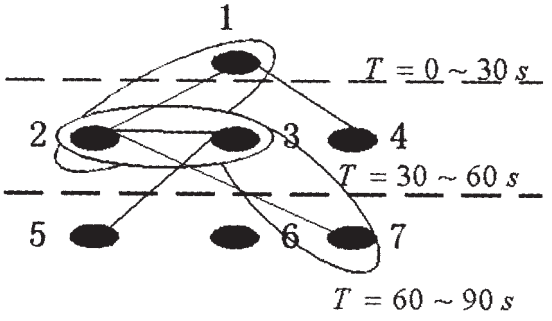

图 2 攻击关联过程示意图

3 基于时序的检测

3.1 协同攻击的时序模型

基于时序的检测是建立在对网络事件时序分析的基础上的。在这里网络事件所指的是由其它主机通过网络向目标主机发起的行为，包含两类：攻击行为和非攻击行为（一般的网络行为）。检测器的结构是建立在与普通 NIDS (Snorts)的协作基础上进行的，即由普通 IDS 先对网络事件进行过滤，分离出攻击事件和普通事件，然后通过对这两类事件的时序、条件关系的组合完成对协同攻击的检测。

时序检测中将网络事件表示为如下一个七元组：

E=(ID,Src_IP,Dst_IP,Dst_Port,Begin_Time,End_Time, Evt_Class)

其中：ID 为事件编号；Src_IP 为事件发起者源地址；Dst_IP、Dst_Port 为事件目的地址；Begin_Time 为事件的起始时间；End_Time 为事件的终结时间（在这里定义其等同于同一源 IP 下一事件的起始时间）；Evt_Class 为对该次事件的属性描述（若 Evt_Class 为 True，该次为一攻击事件（由普通 IDS 取得），否则为正常的网络事件）。

对于两个网络事件（或攻击事件）E_1 和 E_2，分析其起始时间和终止时间，存在时序关系见表 1。

3.2 协同攻击子行为的时序检测

通过将协同攻击所涉及的攻击动作和这些攻击动作之间的时序构建为检测规则，通过规则匹配方法，协同攻击是可以被检测到的。该规则涉及到两个方面的内容：某一时间段内的网络事件特征集和事件时序关系集。

表 1 网络事件时序区间关系

时序关系	时间条件	逆关系
equal	E_1.Begin_Time=E_2.Begin_Time E_1.End_time=E_2.End_Time	equal
starts	E_1.Begin_Time=E_2.Begin_Time E_1.End_Time<E_2.End_Time	inv-starts
meets	E_1.End_Time=E_2.Begin_Time	inv-meets
before	E_1.End_time<E_2.Begin_Time	after
during	E_1.Begin_Tim>E_2.Begin_Time E_1.End_Time<E_2.End_Time	inv-during
precedes	E_1.End_time<=E_2.Begin_time	succeeds

将协同攻击过程根据时序和事件属性的差异抽象为几个攻击阶段并提取各攻击阶段的特征，用阶段特征和阶段之间的时序关系作为检测规则（见图 3）。每一阶段可能包含 1 个或多个事件，每一事件有自身的特征同时具备共有的特性构成的阶段特征。将符合阶段特征的网络事件合并为阶段集合，然后比对所形成的攻击阶段是否符合时序关系，如符合则为协同攻击。

图 3 协同攻击阶段特征时序关系

阶段的特征有两个方面的含义：内部特征和外部特征。内部特征是指该阶段内部诸事件之间的时序关系和特征；外部特征是指阶段之间的时序关系和阶段之间的攻击功能条件构成。所谓攻击条件构成，是指形成该阶段应具备的必要信息条件（Pre_Info）和该阶段完成后所取得的新条件（Pre_Info），如进行端口攻击动作前应先进行扫描以获取端口信息。显然，后阶段的必要条件必然小于或等于前阶段完成后取得的新条件，即：

$(n+1)$.Pre_Info≤n.Post_Info

就 TCP 序列号劫持攻击来讲，可将其分为 4 个阶段。其中：n_1 阶段包含扫描类的事件，n_2 阶段包含使端口封闭的攻击事件。

如 n_1 阶段包含 A、B 两个事件，内部特征需满足：

(1) EA.Evt_Class=True 且 EB.Evt_Class=True；

(2) EA、EB 均为 SCAN 类攻击事件；

(3) EA.Dst_IP≠EB.Dst_IP，EA.Src_IP≠EB.Src_IP；

(4) EA·equal·EB。

外部特征需满足如下条件：

(1) n_1.Post_Info≤(EA.Post_Info)∨(EB.Post_Info)；

(2) E_A.Post_Info=GetInfo(Dst_IP_1(Port))∨GetInfo(IP_1, TCP_SN)（获取端口信息，获取序列号信息）；

(3) E_B.Post_Info=GetInfo(Dst_IP_2(Port))∨GetInfo(IP_2, TCP_SN)。

对于 n_2 阶段所包含的事件 C，其内部特征需满足：

(1) EC.Evt_Class=True;

网络系统生存性分析研究

王红艳　刘向东
(中国航天科工集团二院 706 所　　北京　100854)

〔摘要〕 采用随机点过程模拟网络攻击,根据系统对攻击可能导致的状态建立了网络系统状态转换概率矩阵,从而基于系统对攻击的反应建立了网络系统生存性的数学分析方法。
〔关键词〕 网络系统　生存性　转换概率　　〔中图分类号〕 TP309.2　TP393.08
〔文章标识码〕 A　　〔文章编号〕 1000-7857(2005)04-0007-03

A STUDY ON THE SURVIVABILITY OF WEB SYSTEMS

WANG Hong-yan　LIU Xiang-dong
(Institute 706, The Second Academy of China Aerospace Science and Industry Corp, Beijing 100854, China)

Abstract: The Stochastic Point Process was used to simulate attack processes that network systems might suffer from, and the transition probabilities matrix was constructed to simulate the impact of attacks on a certain system. By varying the state of system in the simulation, an analysis method to quantitate survivability of network systems was developed.
Key Words: web system, survivability, transition probability　　**CLC Numbers**: TP309.2　TP393.08
Document Code: A　　**Aticle ID:** 1000-7857(2005)04-0007-03

1 引言

随着信息技术的快速发展，信息网络系统的生存性已逐步成为关注的焦点，因为网络系统之中存在着各种各样需要解决的问题[1]。网络系统生存性是指信息网络系统面对攻击时的反应能力和遭受攻击后的恢复能力。在日益开放的网络环境中,不可能存在绝对完美的网络安全防御机制,我们所要做的是采取尽可能有效的网络安全防御措施在尽可能大的程度上抵制网络安全面临的威胁。工商企业或组织机构只能基于其需求、财力以及实际系统面临的潜在威胁,尽可能使系统生存能力达到一个最理想的期望值。评估一个系统的生存性对系统的安全决策具有重要的指导意义。通过测评分析网络系统当前的设计模式和防御机制对

收稿日期: 2005-03-01
作者简介: 王红艳,女,1977~ ;北京市 142 信箱 406 分箱 4 号中国航天科工集团二院 706 所,工程师, 主要研究方向为网络安全技术;
E-mail:prcwhy@sina.com

(2) EC 为 SYN Flood 类攻击事件。

外部特征需满足:

(1) 时序特征,即 n_2 阶段内事件与 n_1 阶段内的所有事件满足如下时序关系, n_2·succeeds·n_1;

(2) 条件特征,即

n_2.Pre_Info=n_1.Post_Info=GetInfo (Victim(IP,Port)),

n_2.Post_Info=Victim (Port, Active, Non_active)(在已获取端口信息的基础上进行端口攻击)。

同理,可继续归纳 n_3、n_4 阶段的内部和外部特征,以形成特征的规则描述。在检测时,通过分析一定时间段内的网络行为, 当网络事件或攻击事件符合上述阶段的内部特征时,将其加入该阶段。据此形成的各阶段若同时满足阶段的外部特征(时序特征、条件特征)时,即可认为是一次协同攻击。

从上述描述可以看出, 协同攻击是一个有步骤的行为集合,这个集合中的每一步骤之间存在着严格的时序关系。协同攻击检测的关键之处就在于分析协同攻击各阶段的攻击特征和时序关系, 从而形成特征集, 以此作为检测的判据。收集被检测网段在一定时间内的网络行为,先通过阶段特征将网络行为归并为阶段动作集, 然后匹配该阶段的时序关系,从而完成对协同攻击的检测。

4 小结

在协同攻击的检测中, 本文将其划分为功能层次上的检测和时序层次的检测,通过两种检测方式的协作(时序检测需要功能检测的协作)和结果的比对,可以对协同攻击作出有效的判别。

参考文献(References)

[1] 胡昌振. 网络入侵检测的误警问题探讨[J]. 信息安全与通信保密,2003(8):20~22
[2] 经小川,胡昌振,谭惠民. 基于关联序列分析的协同攻击检测技术研究[J]. 武汉理工大学学报,2004,26(6):78~82
[3] John Green. Analysis Techniques for Detecting Coordinated Attacks and Probes[C]. Usenix Networking'99
[4] 胡昌振. 信息安全的概念及方法论探讨 [J]. 科技导报,2004,22(3):18~21
[5] Peng Ning. Abstraction-based Intrusion Detection in Distributed Environments[M]. George Mason University, 2001

(责任编辑　肖庆山)