基于关系事件的网络复杂攻击检测技术研究

Study on Detection Technology of Complicated Network Attack Based on Related-Event

周建成/ZHOU Jian-cheng，宋曦轮/SONG Xi-lun

中国工程物理研究院化工材料研究所，四川绵阳 621900

Institute of Chemical Materials, China Academy of Engineering Physics, Mianyang 621900, Sichuan Province, China

[摘要] 应用传统的入侵检测方法无法实现对网络复杂攻击的检测，传统检测算法的重点在于观测独立事件或独立用户的行为特征，缺乏对事件之间相互作用关系的考量和分析，而复杂攻击可供检测的显性特征就在于事件间的关联特征。提出了一种基于复杂攻击子事件和子事件关系的检测方法，通过复杂攻击的检测范例，证明了该方法的有效性。

[关键词] 复杂攻击，离散事件，入侵检测　　**[中图分类号]** TP301
[文献标识码] A　　**[文章编号]** 1000-7857(2005)12-0044-03

Abstract: It is unrealistic to detect complicated network attacks based on traditional intrusion detection methods (TIDM) because of the TIDM algorithms emphasis on observing behaviors of independent event, which appears to be lack of the analysis of the interplay among events. The detection method based on relations among sub-events in complicated network attacks has been put forward in this paper. The example shows that method which are designed in this system can effectively detect the attacks.

Key Words: complicated network attacks,discrete events,intrusion detection　　**CLC Number**: TP301
Document Code: A　　**Article ID**: 1000-7857(2005)12-0044-03

1 引言

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，检测采用传统模式比对方式即可完成。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，特点是：威胁范围大，使用的攻击技术全面，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。按照 ISO/IEC15408 的定义，在大范围协同攻击的条件下，威胁甚至可能上升到 A 级。网络复杂攻击具有典型的结构化攻击特征，复杂攻击通常采用分布方式、在统一攻击策略指导下对同一任务目标发起攻击或探测，其攻击的技术手段和攻击步骤通常由统一的攻击策略在各攻击点之间协调从而形成协同效果。

2 传统检测算法在网络复杂攻击检测中的失效性分析

传统的入侵检测方法(误用检测、异常检测)难以对复杂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复杂攻击内在本质的不一致所造成的。异常检测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。此种方法对于复杂攻击的检测不适用，这是因为复杂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。复杂攻击是一个多阶段、多层次的复杂行为，用统计方法没有多大意义、涨落太大[1]。

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。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，这种检测方法作为目前应用最广的检测方法有其优势，那就是准确和高效。在对复杂攻击行为进行深入而细致的分析，以及提练攻击行为作用在系统各阶段、各层面上的特征细节的基础上结合误用检测方法，是当前解决问

收稿日期：2005-10-20
作者简介：周建成，男，四川绵阳 919 信箱 310 分箱中国工程物理研究院化工材料研究所，高级工程师，主要从事计算机网络、软件工程和信息安全的研究工作；E-mail：zjc@caep.ac.cn
宋曦轮(通讯作者)，男，四川绵阳 919 信箱 310 分箱中国工程物理研究院化工材料研究所，工程师，主要从事计算机网络、软件工程和信息安全的研究工作；E-mail：songxilun@163.com

题的一条可行途径。可以这样说,攻击特征细节描述的规则越详细,其检测就越准确。

3 基于关系的复杂攻击事件分解

网络复杂攻击过程是一个动态过程,它是多个入侵事件和普通网络事件的有机组成,这些事件间可能存在着各种各样的关系。一般入侵检测系统都仅对入侵事件进行静态分析,只关注系统所检测到的原始事件,而忽略了隐藏在这些原始事件背后的逻辑联系和攻击意图,因而无法从全局层面上进行攻击评价。从系统科学的角度上看,可以将攻防双方看作一个系统,其存在于不同的网络环境中,系统中的事件集合由离散事件组成。这是离散事件按照一定的运行规则相互作用而导致系统状态演化的一类动态系统。其运行规则可由时间、空间、功能 3 个维度的投影加以解析。

从时间-空间-功能上看,复杂攻击入侵过程是在特定时间、特定空间并具有特定功能的事件组合。如某一复杂攻击由事件$\{e_0,e_1,e_2,e_3,e_4\}$组成,其在<时间,空间,功能>三维坐标中的描述如图 1 所示。

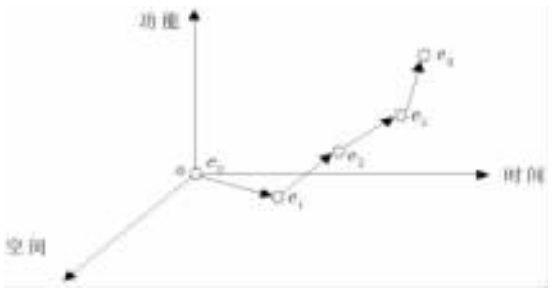

图 1　入侵行为在时间、空间、功能中的描述

其中,e_0 为起始事件,位于坐标原点。将任一离散事件可定义为如下八元组描述:E =<*ID*,*Time*,*Source_IP*,*Dest_IP*,*Begin_Time*,*End_Time*,*Pre_Info*,*Post_Info*>。

3.1 时间维特性描述

离散事件的特性之一,体现在事件间的时序排列或时序阶段排列上,其时间关系具有如下特征:

对于任意两个离散事件 E_1 和 E_2,分析其起始时间和终止时间,存在时序关系如下。

其时序检测特征可归并如下:持续——一些事件存在或发生的不大于或不小于一定的间隔时间,即 during、precedes 时序关系的组合;间隔——时间的发生有精确的间隔,即 $E_2.Time - E_1.Time=E_3.Time - E_2.Time$;序列——系列的事件按特定的顺序发生便可判断为入侵。

3.2 功能维特性描述

复杂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攻击所指定的目标。为了达到此目标,复杂攻击将攻击任务分解为多个子任务交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。对于复杂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的信息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,即离散事件功能间的关联性。可表示为如下形式:$E1.Post\_Info=E2.Pre\_Info$,或 $E1.Post\_Info \vee E2.Post\_Info=E3.Pre\_Info$,其中 *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。

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.	$E_1.Begin\_Time > E_2.Begin\_Time$ $E_1.End\_Time < E_2.End\_Time$	.inv-during.
.precedes.	$E_1.End\_time <= E_2.Begin\_time$	.succeeds.

3.3 空间维特性描述

入侵行为的空间复杂性,主要是指其行为可能出现在网络空间的各种层次上。对于网络空间的层次有不同的理解和分法,如可将网络空间分为网络层、应用层和系统层,也可以分为本局域网内和本局域网外。本文从入侵者和目标之间空间相对位置出发,着重描述两者之间空间对应关系,包括:一一对应,同一入侵者对同一目标进行的入侵行为;一对多,同一入侵者对多个目标发起的入侵行为;多对一,多个入侵者对同一目标进行的入侵行为;多对多,多个入侵者对多个目标进行的入侵行为。

比如,网络扫描攻击往往是由某一台主机发起的,通过对某一网段内的主机进行扫描,以确定进一步攻击目标,这种攻击行为中事件的空间关系为一对多。而一些复杂攻击则是由多台主机发起,通过相互间协作,以达到对某一确定主机进行入侵的目的,这种攻击行为中事件的空间关系则为多对一。

综上,可以看到复杂攻击是一个攻击主体利用时间或空间的操作对客体的入侵过程。这个攻击过程涉及到 5 个要素:时间、空间、主体、客体、操作(以功能形式体现)。其中时间、空间、主体这 3 个要素作为手段在攻击过程中是不断变化的,而操作作为目的是不变量,因此复杂攻击检测应该是以功能作为检测基准,通过分析时间、空间方面的变化组合对该检测基准的影响而作出判别。在检测过程中,时间特性意味着复杂攻击内离散事件在时序上的表现形式,空间特性意味着复杂攻击内攻击源和被攻击对象的地址转换关系,功能特性意味着复杂攻击诸子事件在功能上的相互关联。因而,复杂攻击的检测应从时序、功能序和空间位置 3 方面的规则分别进行规则比对,然后通过结果融合以确定攻击判据。

4 应用离散事件关联的复杂攻击检测

在仿真的数据准备过程中,将基于 Land 的 TCP 序列号截取复合攻击与其它普通攻击、普通网络事件按发生时间的顺序组成事件集,测试事件关联方法能否在此事件集内将复合攻击分离并检测出来。基于 Land 的 TCP 序列号截取复合攻击基本示意如图 2 所示。

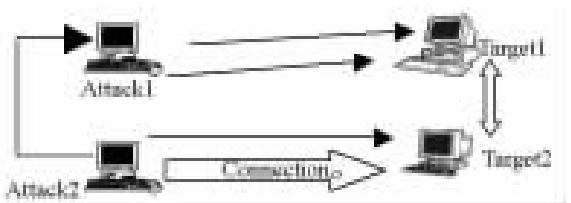

图 2　基于 Land 的复合 TCP 序列号截取攻击

图 2 中 Target1 与 Target2 处于连接状态,通过复合攻击的方式,使攻击主机冒充 Target1 与 Target2 进行连接;Attack1 通过 Scan 扫描 Target1 的端口,获取活动端口信息;Attack2 通过 Scan 扫描 Target2 的端口,获取活动端口信息;Attack2 通过伪连接发送请求至 Target2 的端口(Ping-V),根据当前 TCP 序列号计算下一连接序列号;Attack1 通过 Land 攻击封闭 Target1 的活动端口;

Attack2 通过计算的 TCP 序列号连接 Target2，建立 TCP 连接。其中，Ping-V 为一种变形的 Ping 攻击，其特殊之处在于通过 Ping 返回的 SYN+ACK 号，预测出目标机下一连接的 SYN+ACK 号。

应用离散事件时序特性和功能特性对该复合攻击进行描述如下（见图 3）。其中，时序特性以时间阶段特性进行描述[4]，空间维特性包含在时序和功能序的 IP 描述当中。

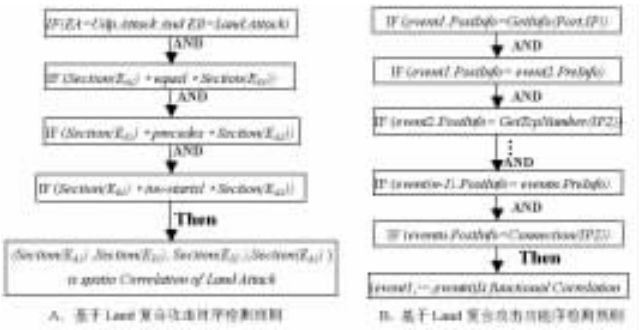

图 3　时序与功能序检测规则

测试数据集由 Land TCP 序列号截取攻击、普通网络事件（Tcp_Connection、Ftp、Login）、攻击事件 DNS-Query、Smurf 组成。（取自 Snort 和 WinpCap 的阶段审计记录），得到如下的事件集。

测试所用检测器由通用 IDS（Snort）、审计事件器（WinpCap）和基于图 2 规则建立的复合事件匹配器所组成。Snort 和 WinpCap 分别负责提取网络内离散攻击事件和普通网络事件，复合事件匹配器负责对这些离散事件进行时间规则匹配，以验证是否为复合攻击事件。

复合事件匹配器内时序规则比对结果：

表 2　攻击测试事件集

攻击/事件	ID	Time	源 IP	目标 IP
UDP_Scan	12 709	10:11:01	192.168.0.11	192.168.0.21
UDP_Scan	12 710	10:11:07	192.168.0.10	192.168.0.22
Ping-V	13 328	10:11:11	192.168.0.11	192.168.0.22
FTP-CWD	13 551	10:11:45	192.168.0.10	192.168.0.22
Land	13 599	10:11:47	192.168.0.10	192.168.0.21
Dns-Query	15 711	10:11:52	192.168.0.11	192.168.0.21
TcpConnection	16 126	10:12:00	192.168.0.11	192.168.0.22
Smurf	16 474	10:12:06	192.168.0.10	192.168.0.22
NetUse	17 031	10:12:11	192.168.0.11	192.168.0.21

{*Sec1*(12 709)·*equal*·*Sec*(12 710)}AND{*Sec*(12 710)·*precedes*·*Sec*(13 599)}AND{*Sec*(13 599)·*inv-startsl*· *Sec*7(16 126)}；

{*Sec*(12 709),*Sec*(12 710),*Sec*(13 599),*Sec*(16 126)}*is spatio arrangement*{*Land+TCP_Serial*}。

复合事件匹配器内功能规则比对结果：

*UDP_Scan*_12709，*Ping-V*，*Tcp_Connection is functional arrangement*；

*UDP_Scan*_12710，*Abnormal_Scan*，*Flood is functional arrangement*；

*UDP_Scan*_12709，*FTP_CWD*，*Smurf is functional arrangement*。

时序规则与功能规则的融合结果：

(*Sec* (12709),*Sec* (12710),*Sec* (13599),*Sec* (16 126))AND (*Sec* (*UDP_Scan*12709). *Dst_State=busy*)AND (*Sec* (*UDP_Scan* 12710). *Service_Class=connection*)。

序列 12 709、12 710、13 599、16 126 在时序检测和功能检测均成立，且目的主机状态满足，该序列构成基于 Land 的 TCP 序列号截取复合攻击。

5 结论

通常来说，网络上的复杂攻击表现形式很繁杂，但究其本质是由若干个简单攻击行为和普通网络行为所组成。因此，对于复杂攻击的检测应遵循以下途径：① 复杂攻击→分解→简单攻击+简单网络行为；② 简单攻击+简单网络行为→分解→原子攻击行为+原子网络行为；③ 原子攻击行为+原子网络行为→检测→原子检测结果；④ 原子检测结果 1+…+原子检测结果 n→ 融合 → 复杂攻击检测结果。

其中，复杂攻击采用何种方式方法分解为可检测的原子事件、原子事件之间的关联分析、原子事件检测结果的融合方法都是今后应重点研究的方向。这种基于事件分解的深入研究，将有助于我们把握攻击事件的本质，推动对复杂攻击的检测。

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. 本体论在网络入侵检测技术中的应用[J]. 四川大学学报(工程科学版)，2005，37(3): 105-109.
[3] MARK R B, KESDOGAN D. Transaction-based anomaly detection Proceedings of the Workshop on Intrusion Detection and Network Monitoring[C]. USENIX Networking Press,1999.
[4] 经小川，胡昌振，谭惠民. 基于时序分析的网络协同攻击检测技术研究[J]. 计算机应用，2004, 24(11): 25-28.
[5] ECKMANN S T, VIGNA G, KEMMERER R A. Statl: an attack language for state-based intrusion detection: proceedings of the ACM Working on Intrusion Detection [C]. IEEE Computer Society Press, 2000.

（责任编辑　王　芷）

·图片科技新闻·

吉林石化公司爆炸冒出的浓烟

携带污染物的松花江水流

吉林石化公司爆炸事故给松花江流域造成严重污染

11 月 13 日下午 1 时 45 分，位于吉林省吉林市龙潭区的中国石油吉林石化公司双苯厂发生着火爆炸事故。爆炸共造成 5 人死亡、1 人下落不明、2 人重伤、21 人轻伤，并使约 100 t 的硝基苯等高毒性化学物流入松花江，给江水及其流域的生态环境造成严重污染。为防止松花江下游沿岸居民发生饮水中毒事件，爆炸事故发生后，吉林省即时封堵了污染排放口，并通知直接从松花江取水的单位和居民停止生活取水。黑龙江省哈尔滨市政府也决定，自当月 22 日中午起，停止供应自来水 4 天。11 月 26 日监测的水质数据表明，受污染的松花江水流至哈尔滨段四方台水源地时，江水中的硝基苯浓度已超过国家标准的 30.1 倍。松花江干流在经过哈尔滨市 700 km 水域后，将汇入位于中俄边界的黑龙江，污染水流还可能威胁与我国接壤的俄罗斯东部地区哈巴罗夫斯克。该地区为此已于 11 月 25 日宣布进入紧急状态。随着经济的蓬勃发展，我国正面临严峻的环境挑战，松花江污染事件再次敲响了我国环保的警钟。

（本刊记者　苏　青）