大规模网络安全态势评估系统

赵鹏宇,刘 丰,张宏莉,王 爽
ZHAO Peng-yu,LIU Feng,ZHANG Hong-li,WANG Shuang

哈尔滨工业大学 国家计算机信息内容安全重点实验室,哈尔滨 150001
China National Computer Information Content Security Key Laboratory,Harbin Institute of Technology,Harbin 150001,China
E-mail:zhaopengyu@pact518.hit.edu.cn

ZHAO Peng-yu,LIU Feng,ZHANG Hong-li,et al.Security situation evaluation system for large scale network.Computer Engineering and Applications,2008,44(33):122-124.

Abstract: When processing large-scale network security events,a network security situation evaluation system can be useful and help user to deal with these security events.This paper proposes an approach that computes network security disaster index and designs a security situation evaluation system for large scale network.Using replaying network security events,this system can evaluate network security situation,compute disaster index of whole network and give a policy of processing these security events. The results of experiment illustrate that this approach is effective for evaluating large scale network security situation.
Key words: security situation evaluation;disaster index;parallel/distributed network simulation;security events

摘 要:在大规模网络安全事件应急响应过程中,一个网络安全态势评估系统可以起到很好的辅助决策作用。提出了一种计算网络安全危害指数的方法,并在这种方法基础上设计实现了一个大规模网络安全态势评估系统。该系统通过对网络安全事件的模拟重放,对网络安全状况进行评估,给出网络整体的安全危害指数,并提出针对安全事件的响应控制策略。系统运行结果表明,这种安全态势评估的方法针对大规模网络安全行为是有效的。
关键词:安全态势评估;危害指数;并行网络模拟;安全事件
DOI:10.3778/j.issn.1002-8331.2008.33.038 **文章编号:**1002-8331(2008)33-0122-03 **文献标识码:**A **中图分类号:**TP393

1 引言

随着网络应用的普遍推广,各种安全事件层出不穷,对网络造成不同程度的危害。但具体的危害程度是多大,目前的应用和研究尚难以回答。常见的网络安全设施如防火墙、入侵检测系统等通常以日志的形式报警,仅能说明哪些网络主机查到哪些主机遭受哪种入侵,难以描述整个网络的入侵状况或受灾程度。

当前国内外的一些网络安全态势评估的方法或是孤立地分析每个报警、评估其威胁程度而不能提供针对网络的整体态势报告,或是提出基于模糊数学的一些理论研究而没有实现具体的原型系统。鉴于这种情况,论文的工作将基于网络主机的报警信息及相关的网络拓扑数据,提出网络安全危害指数的计算方法,并对网络整体的安全态势进行评估,以便于用户掌握网络受攻击的程度、事件分布状况,并辅助用户制定应急响应策略。

2 网络安全危害指数及其计算方法

网络安全事件对网络造成的危害主要体现在对网络节点和链路造成的危害。具体的说,对网络节点的危害是指哪种性质的事件发生在多少数量、处于何种重要程度的节点上;对链路的危害是指多大的入侵流量发生在多少数量、处于何种位置(是否骨干)的链路上。网络节点的类型包括路由器节点、服务器节点和普通用户的主机节点三类,对节点的危害程度与节点类型、受灾节点的数量和节点的重要性有关;对链路的影响与该链路上承载的入侵流量、链路的重要性和受影响的链路数量有关。

由此,在评估网络安全态势前,需要首先收集网络拓扑连接关系图、安全事件日志、主机定位信息和入侵路径等信息。根据对网络拓扑连接关系图的分析,可获知节点的类型是路由器或是主机节点。根据 whois 信息可知主机节点为服务器或普通用户。

在网络连接构建的过程中, 自然地形成一种层次关系,可通过对网络拓扑图中节点度进行聚类分析获得。该层次关系体现了链路或路由节点的重要程度。度越大则骨干位置越突出(或核心交换作用),度越小则其所处位置越边缘。链路所承载的入侵流量可通过统计安全事件发生期间经过该链路的数据包得到。

因此,综合节点和链路的损害度、重要性和数量,可得出整

基金项目:国家 242 基金资助(No.2005C33)。
作者简介:赵鹏宇(1983-),男,硕士生,主要研究领域为网络与信息内容安全;刘丰(1981-),男,硕士学位,主要研究领域为网络与信息内容安全;张宏莉(1973-),女,教授,博士生导师,主要研究领域为网络信息安全。
收稿日期:2007-12-17 **修回日期:**2008-03-06

个网络的受灾程度。综上，本文提出的网络安全态势评估方法如图 1 所示。

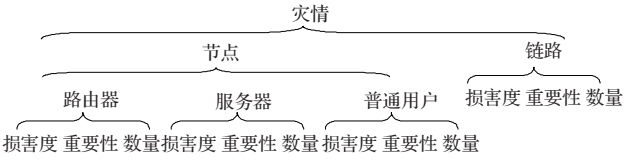

图 1　安全态势评估方法

根据上述方法给出危害指数的量化计算公式，R 即危害指数，如下所示：

$$R=f(\boldsymbol{\theta},\boldsymbol{C}_i,\boldsymbol{D}_i)=\sum\boldsymbol{\theta}\cdot(\boldsymbol{C}_i\cdot m^{\boldsymbol{D}_i}) \quad (1)$$

其中，$\boldsymbol{\theta}$ 为网络节点和链路的损害度的权重向量，$\boldsymbol{C}_i$ 是相应的节点或链路的数量，$\boldsymbol{D}_i$ 是相应的节点或链路的重要等级，m 在这里是一个修正值。

(1)节点或链路的损害度的计算

节点的损害程度与事件的性质相关。具体的说，不同性质的安全事件对节点造成的危害不同，这依赖于系统的定义。例如 DDOS 攻击和蠕虫事件对节点的损害度较大，而端口扫描事件对节点的损害度较小。由此，可根据安全事件性质将安全事件分类，不同类别的事件对节点定义不同的损害程度。

链路的损害程度与链路上承载的入侵流量相关，这可由链路的冲击强度描述，其计算方法如下：

链路的冲击强度=链路的吞吐量(由入侵产生)/事件时间段/链路带宽

根据上述公式所得的链路冲击强度即描述了链路的损害程度。入侵产生的流量越大，对链路的冲击强度越大，则链路的损害度越大；反之，则链路的损害程度就小。链路由入侵产生的流量可以通过对网络安全事件的模拟重放统计得到。

(2)受灾节点或链路的数量计算

受灾节点：安全事件经过的网络节点被称作受灾节点，它包括受灾的路由器、服务器和普通用户主机。

受灾链路：安全事件流经的链路被称作受灾链路。

通过对网络安全事件的重放模拟，可统计计算出受灾节点和受灾链路的数量。

(3)节点或链路重要等级的计算

由于网络中处于骨干位置的节点和链路的重要程度要高于处于边缘位置的，因此，不同层次的节点和链路具有不同的重要等级。采用如下的方法为节点和链路计算重要等级。

将整个网络中的节点划分为 5 个等级。首先，将主机节点定义为第 1 级。将直接与主机相连的路由器定义为第 2 级，与第 2 级节点相连而不与第 1 级相连的节点定义为第 3 级，以此类推。大于或等于第 5 级的网络节点均看作第 5 级。其中，对于主机中的服务器节点适当地提高其等级，以体现它的重要程度。

对于链路划分为 4 个等级。连接 1 级和 2 级节点的链路等级定义为第 1 级，连接 2 级和 3 级节点的链路等级定义为第 2 级，以次类推。连接同等级节点的链路的等级与节点相同。

这部分数据可通过对网络拓扑连接关系图的分析得到。

将上述数量和重要等级按公式(1)进行计算，归一化后与损害度 $\boldsymbol{\theta}$ 分量相乘，便得到了最终的大规模网络安全事件的危害指数 R。

3　网络安全态势评估系统

该系统的设计目标是利用分布式网络模拟器 PDNS，以真实网络拓扑数据、主机特征数据、传播路径信息，模拟安全事件在网络上的传输，通过计算传播速度、流量、通信压力等因素得出安全事件对网络造成的威胁并计算整个网络的安全危害指数，进而提出应急响应策略，并能够对响应策略进行模拟验证。

其实现的功能包括如下几个方面：

(1)在实际测得的网络拓扑数据、安全事件记录、主机特征数据的基础上，进行大规模网络及安全行为模拟，重现事件的发展过程；

(2)计算各传播路径上的负载状况，计算安全事件对网络基础链路造成的通信压力，估计其损耗程度；

(3)分析网络安全事件分布范围、传播速度、带宽占用等因素对网络节点和链路造成的影响，计算安全事件的危急指数；

(4)基于网络安全事件的传播路径分析、网络分布分析等，生成合理的应急响应策略；

(5)对生成的应急响应策略进行模拟，验证其处理安全事件的有效性。

根据上述功能需求，系统可划分成若干模块：数据预处理模块、拓扑划分模块、并行模拟脚本生成模块、模拟结果分析模块、危害指数计算模块和生成控制策略模块。整个系统的结构如图 2 所示。

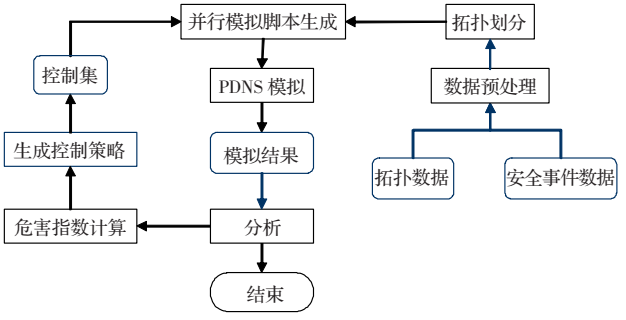

图 2　大规模网络安全事件态势评估系统结构图

图中的矩形框图表示程序模块，圆角矩形表示输入或输出数据。系统的输入数据为网络拓扑数据和安全事件数据。这两部分数据分别由外部的拓扑探测系统和报警信息数据库提供。

系统的工作流程如下：

首先，由数据预处理模块对输入数据进行处理，该部分包括对网络拓扑中链路延迟和带宽的估算、转换数据格式、生成拓扑划分器的输入数据。

其次，根据并行模拟的粒度对网络拓扑图进行拓扑划分。拓扑划分采用广泛使用的图划分工具 METIS。

第三，根据拓扑划分的结果，结合安全事件信息，生成并行模拟脚本，并将模拟脚本分送到各个参与模拟的节点机上，通过 PDNS 平台启动模拟过程。

第四，模拟结果分析模块分析模拟数据，计算网络相关的性能参数。

第五，危害指数计算模块对安全事件进行态势评估，给出宏观网络的危害指数，并根据事件特征生成响应控制策略，提出控制节点集合。

第六，为评价所提出的控制策略，在提出的控制策略基础上第二次运行模拟，根据模拟结果重新进行安全事件的态势评

估,以验证控制策略的有效性。

下面分小节详述系统中的关键模块。

3.1 PDNS 模拟平台

网络模拟是研究网络安全行为的一个有效手段。但研究以 Internet 为背景的大规模网络安全事件时，对模拟机的配置提出了极高的要求。因此,常用的单机开源网络模拟器 NS2 在处理大规模网络时存在一定的困难。PDNS(Parallel/Distributed NS)是一个基于 NS2 实现的较通用的并行网络模拟器。它可以将整个模拟任务分布在多台通过 TCP/IP 网络相连的节点机上,使用多台模拟机并行运行来共同完成一个模拟任务。在运行 PDNS 的过程中,每一个模拟节点只知道一部分拓扑,运行与它相关的安全事件,所有模拟节点共同协作模拟大规模网络上的安全事件,通过分布式来达到较好的模拟性能。

系统利用 PDNS 作为模拟平台,在真实的全国网络拓扑上分布式模拟大规模安全事件。模拟平台通过对输入进行模拟,重现安全事件的发展过程或验证所提出的响应控制策略的有效性。

3.2 数据预处理和拓扑划分模块

数据预处理模块是整个系统运行的起点。它的功能包括根据拓扑数据进行链路带宽和延迟的估算、对安全事件文件的格式转换、转换拓扑划分可接受的输入文件格式等。

在拓扑数据预处理结束后,拓扑文件得到了估算的带宽和链路延迟的值,同时通过预处理,得到了拓扑划分器可接收的输入文件格式。而拓扑划分模块的主要功能有二:一是根据数据预处理模块的输出,对网络拓扑进行划分,以进行后来的并行式网络模拟；二是根据拓扑划分的结果生成拓扑数据文件,该文件为后续生成模拟脚本模块中提供需要的全部网络拓扑数据。

3.3 模拟脚本的生成

并行模拟脚本生成模块的主要功能是根据输入的网络拓扑数据和安全事件信息,生成模拟脚本。与 NS2 不同,PDNS 的模拟脚本需要交由多个参与模拟的机器共同运行,每个参与的模拟机只知道网络拓扑图的一部分,同时负责模拟与该部分拓扑相关的安全事件。因此,当一条安全事件的源目节点位于不同的模拟机上时,不同的模拟机则需要协作共同完成该事件的模拟。为了支持这种跨机之间的通讯,PDNS 加入了跨机的路由节点、为需要远程访问的节点设置 IP、创建远程链路等机制。因此,生成 PDNS 模拟脚本的过程要远比 NS2 复杂。并行模拟脚本生成的流程如图 3 所示。

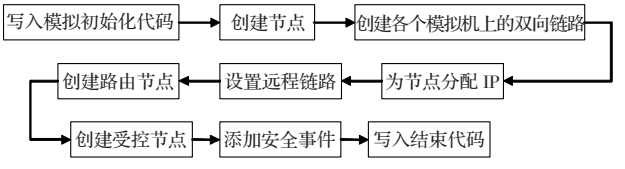

图 3 并行模拟脚本生成的流程

3.4 其他模块

数据分析模块负责对模拟结果进行统计计算,得出受灾节点和链路的数量、链路承载的入侵流量、事件传播路径等数据。这些数据将被危害指数计算和控制策略模块使用。

危害指数计算模块根据第二节提出的危害指数计算方法,对网络安全事件的危害指数进行量化的计算。为方便评价,将网络安全的危害指数划分为 5 个等级,区间为[0,0.1]、[0.1,0.2]、[0.2,0.3]、[0.3,0.5]、[0.5,1],分别对应等级 1 到 5,表示对网络的危害程度逐级增大。

控制策略生成模块根据的 5 个指标计算每个节点的受灾程度，并根据节点受灾程度将其划分为不同级别的控制节点,提出控制节点集合。5 个指标分别为:节点度中心性、所属网络类型、所控路由器集合、经由节点的事件数和群集系数。5 个指标中的经由节点的事件数为分析模块从模拟结果中获得,其他指标由拓扑数据中计算得到。

4 实验结果

硬件环境：系统分布在 3 台同构的模拟节点机上运行,节点机的 CPU 采用 AMD Athlon™ 64 Processor 3000+,主频 1.8 GHz,每台节点机配置内存 3.0 G。

软件环境：操作系统:Red Hat Enterprise Linux AS release 3(Taroon);内核版本:Linux version 2.4.21-4.EL;PDNS:2.27;METIS:4.0;G++:g++（G++）3.2.3。

拓扑采用全国网络拓扑:66 072 个路由节点,96 073 条链路,969 969 个主机。对于不同的安全事件规模,系统的运行效率、控制前和控制后的危害指数如表 1 所示:

表 1 实验结果

事件数	内存开销/MB	时间开销/min	危害指数（控制前）	危害指数（控制后）
100 000	1 800	122	0.277 340	0.189 814
200 000	2 000	180	0.283 523	0.196 684
300 000	2 100	239	0.283 896	0.206 165

通过实验结果可以看出,随着安全事件数量的增加,网络危害程度有上升的趋势。在应用了系统生成的应急响应策略后再次对网络安全状况进行态势评估,可以看到网络危害程度有较明显的下降。根据 3.4 节定义的危害程度的 5 个等级,控制后安全危害由等级 3 下降到等级 2,说明了系统生成的应急控制策略具有一定的积极作用,同时证明提出的计算网络安全危害指数的方法是有效的。

5 结论

针对大规模网络安全态势评估,提出了一种计算网络安全危害指数的方法。该方法基于主机的报警日志信息和网络拓扑数据,综合网络节点和链路的危害程度,计算网络整体的安全态势。在此方法基础上,设计并实现了一个大规模网络安全态势评估系统。该系统通过在真实的网络拓扑中模拟大规模安全事件的行为，分析安全事件对网络节点和链路造成的危害,通过对事件的安全态势评估给出网络危害指数,并辅助用户指定应急响应策略以及验证其有效性。

系统的运行结果表明，该系统可通过分布式网络模拟对 66 072 个路由节点的全国网络拓扑和 10 万条以上的安全事件进行安全态势评估。通过对不同规模的事件的安全评估,可以看出评估的结果较准确的反映了网络的安全状况。因此,该系统对于大规模网络安全事件的态势评估是有效的。

参考文献:

[1] 王晓锋,方滨兴,云晓春,等.并行网络模拟中的一种拓扑划分方法[J].通信学报,2006,27(2):16-21.

(下转 127 页)