一种测量和评估网络安全性的方法*

胡汉平+, 陈 翔, 张宝良, 郭文轩

(华中科技大学 图像识别与人工智能研究所,湖北 武汉 430074)

An Approach to Measure and Evaluate the Network Security

HU Han-Ping+, CHEN Xiang, ZHANG Bao-Liang, GUO Wen-Xuan

(Institute for Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan 430074, China)

+ Corresponding author: Phn: +86-27-62588328, Fax:+86-27-87547745, E-mail: hphu@mail.hust.edu.cn, http://www.hust.edu.cn

Received 2003-07-16; Accepted 2005-01-06

Hu HP, Chen X, Zhang BL, Guo WX. An approach to measure and evaluate the network security. *Journal of Software*, 2005,16(11):1939−1945. DOI: 10.1360/jos161939

Abstract: Based on the active defense model of the network data transmission, a method of security measurement of the network data transmission is proposed. Deceptive packets are used in the active defense model to trap attacks. In addition, statistical quantification is used to measure and evaluate the security of the network data transmission according to network status parameters. This method not only helps make the policy of network data transmission accurately and efficiently, but also guarantees the security of the network data transmission.

Key words: active defense; security measurement; quantification; network data transmission

摘 要: 基于网络数据传输过程中的主动防御模型,提出了一种对网络数据传输过程中的安全性进行测量、量化和评估的方法.它利用主动防御模型中的诱骗数据报文,在对攻击进行诱骗的同时,根据网络状态参数对网络数据传输的安全性进行测量和评估.该方法为网络数据传输策略的制定和网络数据的安全传输提供了有效的标准.

关键词: 主动防御;安全测量;量化;网络数据传输

中图法分类号: TP393 文献标识码: A

数据在网络传输过程中容易被攻击者故意破坏或扰乱,导致接收者无法正常接收数据.针对这样的问题,我们提出了网络数据传输过程中的主动防御模型(如图1所示).该模型主要由端子系统和动态安全域子系统组成.在端子系统中综合运用了传输服务器的“主”、“僚”机切换技术、数据加密技术、网络测量技术以及安全调度技术等,为数据传输和数据服务提供了安全保证.动态安全域子系统,重点针对数据传输过程中的攻击,综合运用了安全路由控制和网络测量等技术,建立有效的安全覆盖,并根据网络安全状态,管理和维护安全覆盖的有效性和可靠性,在对攻击进行诱骗的同时,为数据传输提供动态的安全路径.

* Supported by the National Natural Science Foundation of China under Grant No.90104029 (国家自然科学基金)

作者简介: 胡汉平(1960−),男,湖北武汉人,博士,教授,博士生导师,主要研究领域为信息安全,智能信息系统;陈翔(1979−),男,硕士,主要研究领域为网络安全;张宝良(1969−),男,博士,讲师,主要研究领域为网络安全;郭文轩(1982−),男,硕士生,主要研究领域为网络安全.

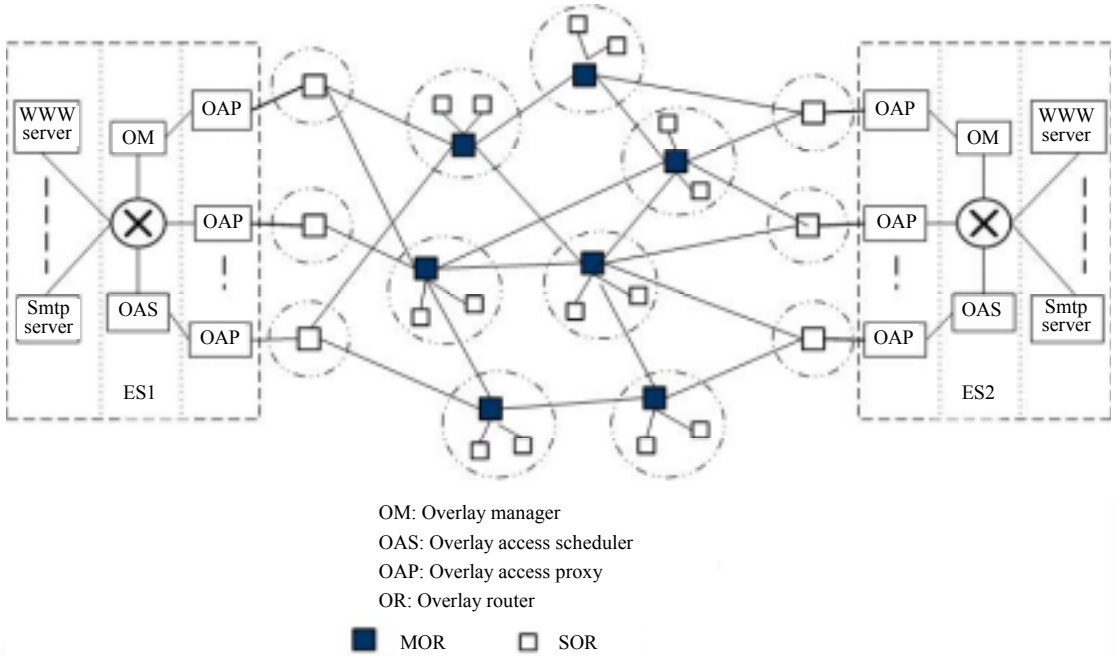

Fig.1 The model of active defense of the network data transmission

图 1 网络数据传输过程中的主动防御系统模型

综上所述,对数据传输过程中的安全状态进行测量、量化和评估,是网络数据传输中主动防御模型的基础.目前国内外对于网络状态的测量、量化和评估,主要集中在对网络基本性能以及网络服务质量状态参数的测量上.互联网工程任务组(IETF)中的 IP 性能测量工作组(IPPM WG),主要致力于 IP 网络性能测量的规范化工作[1],从理论上来定义网络测量的相关问题.工作组 TE WG 针对网络服务质量,进一步提出了 Flow Measurement[2]的测量方法.但他们对于网络数据传输中的安全测量问题都只是简略地提及,并未给出相应的策略和方法.Knorr 和 Róhrig 对于电子商务应用安全性的评估进行了探讨[3],他们通过安全性矩阵将总体安全性的评估分散到几个方面的方法值得借鉴;Brocklehurst 等人提出了一种对软件系统可用性进行评估的方法[4]:用系统发生故障的概率或事务成功完成的比率作为度量标准;肖道举等人针对网络环境中的潜在漏洞,建立了基于插件的网络安全评估模型[5],重点考察网络环境的安全漏洞状态,通过用户服务漏洞的风险程度以及对应权值来定量地分析网络端系统的安全性,但是并没有说明漏洞在系统中所占权值的真正含义,而本文则明确地给出了破坏权值的含义.Madan 等人针对入侵容错系统的安全性,提出了一种测量和量化模型[6],计算在各种攻击情况下安全失效的概率.但是,对网络数据传输过程中的安全性如何进行测量、量化和评估,也没有提出有效的解决方法.

本文试图就这个问题,在主动防御模型[7]的基础上,利用该模型中的诱骗报文,在对攻击进行诱骗的同时,通过本文所提出的反映网络数据传输过程安全性的统计量化方法,依据服务质量参数(如吞吐率、带宽、资源利用率等);数据安全性(如完整性、机密性等)和传输节点的安全性(如节点的健康状态、一段时间内遭受攻击的次数等)等指标对网络数据传输过程中的安全性进行综合评估.为网络数据传输策略的制定和网络数据的安全传输提供了有效的保障.

1 测量方法

在本文所给出的测量方法中利用了主动防御模型[7]中的诱骗报文.该报文的格式如图 2 所示.

Option (1)	TTL (1)	Sequence number (2)
Packet length (2)		Data pointer (2)
Check value (2)		Reserved (2)
Data		

Fig.2 The format of the trap packet header

图 2 诱骗报文头格式

图 2 中括号内的数字表示各字段的长度.报文头中的“选项”字段,用于说明测量报文的类型.“TTL”字段,用于测量路由器之间的间隔.“序列号”字段,用于说明测量报文的测量顺序.“报文长度”字段,说明诱骗报文长度.“数据指针”字段,用于说明下一个可用的测量数据空间偏移地址,以“选项”字段起始地址为基准.“校验值”字段,用于计算报文头的校验值.“保留”字段,用于功能扩充.“数据”字段,用于连接具体的测量数据,长度根据“报文长度”字段的说明预先确定.在本文模型中,对于数据传输中的安全性测量是在两个不同的层面进行的,即同一个动态安全域中各路由器之间的安全性测量和数据传输中发送端和目的端之间路径的安全性测量.前者进行细粒度的测量和分析,后者则需要将各中途节点的测量结果带回测量的发起端.两者在数据字段的格式上是有所区别的(如图 3 所示).

Algorithm (1)	Random number (2)
Hash value (12)	

(a) The data format for the intra-domain measurement

(a) 域内测量数据字段的格式

Primary router's address (4)	
Measurement interval (2)	Measurement result 1(2)
Measurement result 2(2)	Measurement result n(2)

(b) The data format for the end-to-end measurement

(b) 端到端测量数据字段的格式

Fig.3 The data segment format of the trap packet

图 3 诱骗报文中的数据字段的格式

以数据完整性测量为例,动态安全域内发起测量的路由器(OR),按照选定的分布规律(如指数分布、泊松分布、几何分布等[1]),在预定时间间隔 t 内发送测量报文.接收到测量报文的相邻路由器将路径上的测量结果处理后放置于本地的 MIB 中,以供查询使用.在主安全路由器(PSR)中,与其相邻的路由器的路径测量结果存储在 MIB 中,再根据测量结果,选定备用安全路由器(SOR),在必要的时候进行权限提升.

对于端系统用户,向传输控制服务器(OM)提交测量任务.传输控制服务器的测量模块将任务按照测量规则进行分解,并加入测量队列.在预定的时刻,按照测量策略(包括测量时间长度、测量报文发送分布规律、测量安全属性指定等)执行测量任务.完成测量之后,传输控制服务器把测量结果存入本地测量结果数据库中,用于用户查询和数据离线分析.最终结果以报表或图形方式提交给用户.

2 测评方法

假设一条传输路径经过 N 个动态安全子域,每个动态安全子域中具有一个主安全路由器 $PSR_i(1 \le i \le N)$.选取数据在网络传输过程中可能存在的 k 种攻击(如 DoS 攻击、机密性破坏、完整性破坏等)

$A_j(1 \le j \le k) = \begin{cases} 0, & \text{攻击未发生} \\ 1, & \text{攻击发生} \end{cases}$ 为安全性评价指标.

在时间间隔 t 内, PSR_i 进行 m 次安全测量,分别记录下本节点各种攻击组合出现的次数 n'_{ij}, 可以得到测量统计矩阵如下:

$A_1A_2...A_k$	PSR_1	PSR_2	…	PSR_N
00…0	n'_{11}	n'_{21}	…	n'_{N1}
00…1	n'_{12}	n'_{22}	…	n'_{N2}
…	…	…	…	…
11…1	n'_{12^k}	n'_{22^k}	…	n'_{N2^k}

由于该矩阵状态较多,为了减少空间消耗,进行样本空间变换,记录没有发生攻击的次数 S_0 和受到安全攻击 A_j 的次数 n_{ij} ($0 \le n_{ij} \le m$),可以得到测量矩阵如下:

	S_0	A_1	A_2	…	A_k
PSR_1	n_{10}	n_{11}	n_{12}	…	n_{1k}
PSR_2	n_{20}	n_{21}	n_{22}	…	n_{2k}
…	…	…	…	…	…
PSR_N	n_{N0}	n_{N1}	n_{N2}	…	n_{Nk}

计算在节点 PSR_i 上进行的 m 次测量中,攻击 A_j 出现的概率:

$$p_i(A_j) = \frac{n_{ij}}{\sum_{i,0 \le j \le k} n_{ij}} \quad (1 \le j \le k, 1 \le i \le N) \tag{1}$$

根据安全需求的不同,对每种攻击 A_j ($1 \le j \le k$)定义破坏权值.其权值越高,威胁性越大:

$$0 \le w_{ij} \le 1 \quad (1 \le j \le k, 1 \le i \le N) \tag{2}$$

定义攻击 A_j ($1 \le j \le k$)对该传输路径各节点的威胁评价因子:

$$D_i(A_j) = w_j \times p_i(A_j) \quad (1 \le j \le k, 1 \le i \le N) \tag{3}$$

定义单点威胁评价因子:

$$D_i(A) = \sum_{1 \le j \le k} w_j \times p_i(A_j) \quad (1 \le i \le N) \tag{4}$$

定义整个路径上,攻击 A_j ($1 \le j \le k$)的威胁评价因子为

$$D(A_j) = \sum_{1 \le i \le N} D_i(A_j) \tag{5}$$

定义路径威胁评价因子为

$$D(path) = \max_{1 \le i \le N} \{D_i(A)\} \tag{6}$$

在给出了各种量化的定义之后,下面本文将对在上述量化方法中如何确定参数和抽样等问题进行讨论.

2.1 确定破坏权值w_{ij}($1 \le j \le k, 1 \le i \le N$)的方法

在选定破坏权值的时候要遵循两个基本原则:破坏权值要能准确地反映测量发起者对于各种安全威胁因素的认知程度;破坏权值要能清晰地反映对测量发起者而言,在各种对安全性产生威胁的因素之间所存在的差别.因此,可以采用下述方法来确定破坏权值:

1) 确定可测量的攻击集合 $A = \{attack_1, attack_2, ..., attack_n\}$,并将用户划分为不同的服务类型 $S = \{S_1, S_2, ..., S_m\}$;
2) 根据已有的经验数据,确定对不同的服务类型 $S_i (1 \le i \le m)$ 在单位时间 t 内, $\forall attack_j \in A (1 \le j \le n)$ 的攻击强度增长率为 ΔA_j 时,其威胁评价的增长率 ΔD_{ji} 和被攻击系统恢复到正常状态所花费代价的增长率

ΔC_{ji};

3) 对每种服务类型 $S_i(1 \le i \le m)$,从可测量攻击集合 A 中选择对应的攻击测量子集合 $A_i, A_i \subseteq A$;

4) 对于 $\forall attack_j \in A_i$,计算 $\rho_j = \dfrac{\Delta D_{ji} + \Delta C_{ji}}{\Delta A_j}$,得到一组比值 $\rho_1 : \rho_2 : ... : \rho_k$;

5) 将上述比值映射到区间[0,1]之间,即可作为破坏权值 $w_{ij}(1 \le j \le k, 1 \le i \le N)$.

在第 2)步计算 ΔA_j, ΔD_{ji} 和 ΔC_{ji} 的时候,可能三者具有不同的量纲,例如 ΔA_j 通过单位时间内攻击增加的次数来进行度量, ΔD_{ji} 通过被攻击点的资源利用率的增加来度量,而 ΔC_{ji} 则通过恢复时间的延长来度量.在这种情况下,需要按照一定的比率对 ΔD_{ji} 和 ΔC_{ji} 的量纲进行统一,例如,对 ΔD_{ji} 和 ΔC_{ji} 分别利用处理器增加的处理时间和增加的恢复时间作为度量标准.

由于上述方法将用户进行了分类,因此可针对不同用户的服务特点选取不同的测量对象,突出用户对主要安全威胁的不同认知程度.另外,选取攻击破坏程度和恢复代价的变化率与攻击强度变化率的比值作为评估标准,相对于单纯的攻击强度评估标准,可以更好地反映不同安全威胁因素之间的差别.

2.2 抽样方法

在文献[2]中,针对网络 IP 性能度量参数框架中测量样本的收集提出了一种可行的方法.在该方法的基础上,根据本测量法的特点,本文给出了一种在两个层次上提取测量样本的方法.

在本文中,对数据传输过程中安全性的测量是在两个不同的层面进行的,其中动态安全域内各路由器之间的安全性测量是测量任务能够顺利完成的基础.在进行该层面的安全性测量时,测量分为多组进行.路由器之间进行安全性测量的时间间隔采用了与 IGMP 协议相类似的方式,每相邻两组测量开始的时间间隔由安全路由器在指定的间隔区间内随机选择.每一组测量内的样本采集则采用泊松采样方法获得.

对于网络安全性测量以及收集测量样本的一个关键是要具有无偏性,即收集到的样本不会因为本身的偏差而不能准确地反映度量参数的变化和一致性.为此,本文采用了选取最大时间间隔 Δt 和采样次数 N 的泊松采样方法,即将在区间[0, Δt]内服从均匀分布的 N 个随机数作为每一组测量中相邻两次采样之间的时间间隔.其采样的步骤如下:

1) 根据最大的采样时间间隔 Δt 和采样次数 N,确定最小测量时间间隔 $\lambda = \Delta t / N$;

2) 产生在[0,1]之间服从均匀分布的随机数 $u_i, 1 \le i \le N$;

3) 计算抽样间隔 $e_i = \dfrac{-\log(u_i)}{\lambda}, 1 \le i \le N$;

4) 计算抽样开始时刻序列 $t_i = \sum_{1 \le j \le i} e_j, 1 \le i \le N$;

5) 按照得到的时刻序列,在开始测量后的 t_i 时刻进行第 i 次测量,直到本组测量完成.

显然,完成一组测量所需要的时间 $T = \dfrac{1}{2} \times \Delta t \times (N+1)$. 因此,一般通过控制测量的最小时间间隔使得时间 T 在可接受的范围内.此外,在由选定的 Δt 确定 N 时,需要保证 $t_p \le \lambda$ (t_p 为节点处理一个测量数据报文所需要的最少处理时间),这样就不会因为受到处理时间的限制而影响测量的实效性.

3 系统安全量化实例分析

在覆盖网络系统 SOS(secure overlay services)[8]里,利用静态攻击条件下成功传输的概率 $\Pr[U_{S,T} = 1]$ 作为传输安全性评估的方法之一.本节将利用该方法的思想和本文所提出的方法对同一组数据进行对比评估.

假定对于两个传输端之间,由发端、传输动态安全域中主安全节点和目的端构成的两条传输路径 $Path_1$ 和 $Path_2$,选取 3 种可测量攻击:完整性攻击(attack of int)、DoS 攻击(attack of DoS)和端口扫描攻击(attack of PortScan).在同一时间段内,采用本文中提出的方法进行测量和量化,得到如下的两个统计矩阵:

传输路径 $Path_1$				
	S_0	A_1 (完整性破坏)	A_2 (DoS 攻击)	A_3 (端口扫描)
S	18	1	1	0
T	16	4	0	0
R	14	0	6	0

传输路径 $Path_2$				
	S_0	A_1 (完整性破坏)	A_2 (DoS 攻击)	A_3 (端口扫描)
S	17	1	3	0
T	15	1	2	5
R	12	6	0	2

按照本文中的方法确定攻击 A_1, A_2, A_3 在各点上具有相同的权值 $w_i = \{0.5, 0.9, 0.3\}$.经过计算,得到的结果如图 4 和图 5 所示.

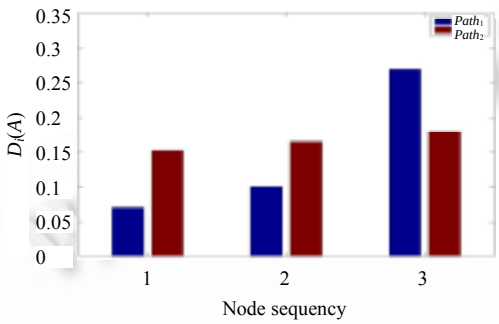

Fig.4 The threaten factor of point

图 4 单点威胁评价因子结果图

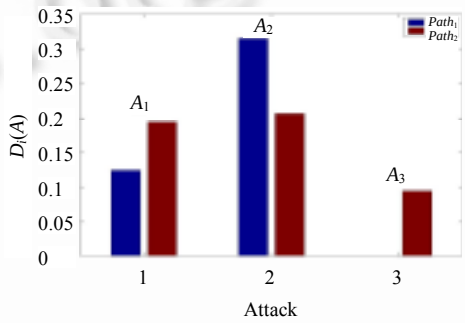

Fig.5 The threaten factor of A_j to the path

图 5 攻击 A_j 对路径的威胁评价因子图

从图 4 中可以很直观地看出,路径 $Path_1$ 中安全路由器 R 的单点破坏因子值较高,分析其原因,是因为该点在测量期间受到较为严重的 DOS 攻击,而且对应的破坏权值说明 DOS 攻击造成的破坏性较大.在图 5 中也可以明确地看到,在选定的 3 种可测量攻击中,DOS 攻击对于传输路径的破坏性最大,这与图 4 中所得到的结果是相吻合的.同时,由于在测量期间,路径 $Path_1$ 沿途的节点并没有发生端口扫描攻击,所以,在图 5 中 $Path_1$ 的 A_3 威胁评价因子为 0.

按照“水桶原理”,网络数据传输过程中威胁最大的节点往往是防范的重点.由公式(6)计算路径总体威胁评价因子,得到 $D(path_1) = 0.27$, $D(path_2) = 0.18$.故可以得出路径 $Path_1$ 的安全性低于 $Path_2$ 的安全性.结合上述图表分析,本方法的评价结果符合测量的真实情况.

但是,若根据 SOS 系统中的静态攻击评估方法,采用生存概率模型对上述实例进行安全性量化,计算得到生存概率为 $\Pr(path_1) = 0.504, \Pr(path_2) = 0.312$, 即路径 $Path_1$ 的安全性高于 $Path_2$ 的安全性.这个结果与实例的定性分析结果相悖.其原因在于,该模型是针对整个 SOS 系统的生存能力进行大粒度的量化,而本文提出的方法,基于传输路径中细粒度的网络测量数据,并在此基础上进行了建模分析.另外,相对于 SOS 中单纯的生存概率模型,本文提出的方法中引入破坏权值的概念,能够与不同的应用服务质量和安全需求相对应,粒度更细,能更有效地结合本系统中的应用需求.

4 结论及未来的工作

本文提出的方法,结合统计概率和权值限定,能够对传输过程中的安全性进行真实而有效的量化,有利于对传输路径、节点安全性以及网络攻击对数据传输的威胁进行评估,为整个系统的决策和管理提供有力的依据.

本方法提出了一种可行的安全性量化思路,将来的工作将主要集中在该量化方法的扩展、深化方面.而且

网络环境是一个动态变化的环境,随时都有可能出现新的攻击形式和威胁,如何及时反映这种变化,并进行有效的响应,人工智能以及模糊控制技术可能是一个值得探讨的方向.

致谢 在此,我们向对本文的工作给予支持和建议的同行,尤其是华中科技大学图像识别与人工智能研究所的王祖喜和吴小刚老师表示感谢.

References:

[1] Paxson V, Almes G, Mahdavi J, Mathis M. Framework for IP performance metrics. RFC2330, 1998.

[2] Brownlee N. Traffic flow measurement: Meter MIB. RFC2720, 1999.

[3] Knorr K, Röhrig S. Security of electronic business applications—Structure and quantification. In: Bauknecht K, Madria KS, Pernul G, eds. Proc. of the 1st Int'l Conf. on Electronic Commerce and Web Technologies (EC-Web 2000). Berlin/Heidelberg: Springer-Verlag, 2000. 25−37.

[4] Brocklehurst S, Littlewod B, Olovsson T, Jonsson E. On measurement of operational security. IEEE AES Systems Magazine, 1994, 9(10):7−16.

[5] Xiao DJ, Yang SJ, Zhou KF, Chen XS. An evaluation model of network security. Journal of Huazhong University of Science and Technology (Nature Science Edition), 2002,30(4):37−39 (in Chinese with English abstract).

[6] Madan B, Goševa-Popstojanova K, Vaidyanathan K, Trivedi KS. Modeling and quantification of security attributes of software systems. In: Proc. of the Int'l Conf. on Dependable Systems and Networks (DSN 2002). Washington: IEEE Computer Society, 2002. 505−514.

[7] Zhang BL, Hu HP, Wu XG, Kong T. A network-based VPN architecture using virtual routing. Wuhan University Journal of Natural Sciences, 2005,10(1):161−164.

[8] Keromytis AD, Misra V, Rubenstein D. SOS: Secure overlay services. In: Proc. of the ACM SIGCOMM 2002. Pittsburgh, 2002. 61−72. http://nms.lcs.mit.edu/~kandula/killbots/killbots_files/sos.pdf

附中文参考文献:

[5] 肖道举,杨素娟,周开锋,陈晓苏.网络安全评估模型研究.华中科技大学学报(自然科学版),2002,30(4):37−39.