

基于灰色理论的攻击者攻击能力评估

赵博夫¹, 殷肖川¹, 吴传芝²

(1. 空军工程大学电讯工程学院, 西安 710077; 2. 南空装备部, 南京 210000)

摘 要: 分析网络攻击对目标网络的破坏效果以及攻击者的攻击能力。基于灰色理论, 提出一种评估攻击者攻击能力的方法, 给出评估的指标体系, 对评估准则进行计算。在实际网络中进行攻击实验, 结果表明, 该评估方法能有效对网络攻击过程中攻击者的攻击能力进行定量评估。

关键词: 攻击效果; 攻击能力; 信息获取; 灰色理论

Attack Ability Evaluation of Attackers Based on Grey Theory

ZHAO Bo-fu¹, YIN Xiao-chuan¹, WU Chuan-zhi²

(1. Telecommunication Engineering Institute, Air Force Engineering University, Xi'an 710077, China;

2. Air Armament Department of the South, Nanjing 210000, China)

【Abstract】 This paper analyzes the attack effect of target network and the ability of attackers, basing on Grey theory, it evaluates the ability of attackers in the process of network attacks. It gives the evaluation index system, and calculates the evaluation criterions. Experimental results in the actual network show that the method can quantitatively evaluates the ability of attacker in the process of network attacks.

【Key words】 attack effect; attack ability; information access; grey theory

DOI: 10.3969/j.issn.1000-3428.2011.14.037

1 概述

随着计算机网络技术的飞速发展, 网络攻击成为破坏敌方网络、获取重要信息的一种手段^[1]。为有效评测网络攻击, 制定更加高效的攻击策略, 需要对网络攻击效果进行定性及定量的评估。

目前, 网络攻击效果评估技术主要研究受攻击前后网络安全性的变化, 以此反映网络的安全状况, 对网络攻击过程中攻击者能力的积累及网络潜在的安全风险研究不足。文献[2]研究了网络攻击破坏程度的评估问题。文献[3]借鉴信息论中“熵”的概念, 提出了描述网络安全性的网络熵, 并利用熵差对攻击效果进行描述。文献[4]定义了网络攻击的原子功能, 即网络攻击效果集合中原子的、独立的、具有明确含义的攻击效果, 并根据“属性-原子功能-评估指标-采集指标”构建评估指标体系。文献[5]将网络面临的威胁作为网络攻击效果的评估指标, 利用模糊综合评判法进行综合评估。文献[6]针对网络攻击前后网络安全性变化, 利用粗糙集理论构造评估模型, 并提出了计算方法。

攻击者攻击能力的积累、权限的提升是网络攻击效果中不可缺少的组成部分。随着网络攻击的进行, 攻击者不断获取目标网络的信息, 破坏网络安全的各项指标, 获取对方系统的有用信息, 取得对目标系统的控制权限甚至破坏对方系统, 致使对方计算机网络和系统崩溃、失效或错误工作。

针对上述问题, 本文从网络攻击的破坏效果、攻击者的攻击能力 2 个方面, 对网络攻击效果进行分析。在此基础上, 研究攻击者的攻击能力在网络攻击过程中的变化, 并利用灰色理论进行了评估。

2 网络攻击效果

计算机网络攻击是攻击者窃取、修改、阻塞、降低或破坏存储在计算机网络中的信息, 或计算机系统与计算机网络

本身的一切动作的集合^[7]。网络攻击效果包含 2 个方面:

- (1) 目标计算机网络安全性的破坏;
- (2) 攻击者破坏目标计算机网络、窃取相关信息能力。

2.1 目标网络的破坏效果

在网络攻击过程中, 攻击者往往会对目标主机原有配置信息进行修改, 甚至是对目标主机进行破坏。这种破坏效果可能是攻击者刻意安排的, 也可能是攻击者不希望发生的。但攻击者的这些操作使目标主机的状态与被攻击之前发生变化, 这些变化体现了网络攻击对目标网络中计算机造成的破坏。

2.2 攻击者的攻击能力

网络攻击的过程既是目标网络遭受破坏的过程, 又是攻击者的权限不断提升的过程。随着网络攻击的实施, 攻击者对目标网络掌握和控制程度不断加深。其中, 攻击者的攻击能力包含 2 个方面: 信息获取, 信息打击。

2.2.1 信息获取

从网络过程的分析中可以看出, 攻击者对目标网络的信息一直处于不断获取的状态。信息获取指攻击者通过各种攻击手段所掌握的目标网络的相关信息。在网络攻击的过程中, 任何一种攻击方法的成功实施都需要具备一定的条件, 攻击者掌握的信息越全面, 所采取的攻击方法的成功率就越大。因此, 攻击者所获取的信息是攻击者攻击能力的重要组成部分。通常, 攻击者获取的信息主要包括: 目标主机的 IP 地址, 主机名, 开放的端口, 开放的服务, 各种账户信息, 存在的漏洞等。

2.2.2 信息打击

信息打击指攻击者能够主动对目标网络实施的攻击操作

作者简介: 赵博夫(1986—), 男, 硕士研究生, 主研方向: 信息对抗, 网络安全; 殷肖川, 教授; 吴传芝, 工程师、硕士

收稿日期: 2011-01-13 **E-mail:** fengyun860000@139.com

值。依据网络攻击的特点及一般规律,不妨假设 $a=1.5$, $b=3.5$, $c=5.5$, $d=7.5$ 。

(2)灰色评价权矩阵的计算

对于评估指标 i , d_i 表示所有评语集下该评估指标的灰色评估总系数, r_{ij} 表示第 j 个评语集下该评估指标的灰色评价权。则:

$$d_i = \sum_{j=1}^4 d_{ij} \quad (7)$$

$$r_{ij} = \frac{d_{ij}}{d_i} \quad (8)$$

其中, r_{ij} 是灰色评估权矩阵的基本组成元素。对 r_{ij} 进行组合得到灰色评价权矩阵 R 。

$$R = \begin{pmatrix} r_{11} & r_{12} & r_{13} & r_{14} \\ r_{21} & r_{22} & r_{23} & r_{24} \\ M & M & M & M \\ r_{m1} & r_{m2} & r_{m3} & r_{m4} \end{pmatrix} \quad (9)$$

(3)评价结果计算及分析

设该评估准则的权重向量为 w , $w=(w_1, w_2, \dots, w_m)$, 其评价结果记为 B :

$$B=w \cdot R=(b_1, b_2, b_3, b_4) \quad (10)$$

其中, 评估结果 B 表示每个评语集等级所占的比重。为了定量分析准则层的评估指标, 需要对评语集的每个等级取一个分数, 本文依据网络攻击效果评估的一般规律, 假设每个评语集对应的分数 $\{100, 80, 60, 40\}$ 。由此对该评估准则 i 进行定量打分, 记为 S_i :

$$S_i=100 \times b_1 + 80 \times b_2 + 60 \times b_3 + 40 \times b_4 \quad (11)$$

3.2.3 评估目标的综合评判

设目标层与准则层之间的权重向量 $c=(c_1, c_2, \dots, c_k)$, 则目标元素的结果 A :

$$A=c \cdot S \quad (12)$$

4 实验与分析

4.1 实验环境及实施过程

本次实验的目的是检验上述评估方法在攻击者攻击能力评估过程中的应用, 并对实际网络攻击过程中攻击者的攻击能力进行定量打分。

实验在百兆网络环境下进行。实验过程中用到的设备包括: 路由器一台、交换机一台、PC 机若干、攻击模拟器一台(负责对目标网络实施攻击)。实验网络的拓扑结构见图 3。

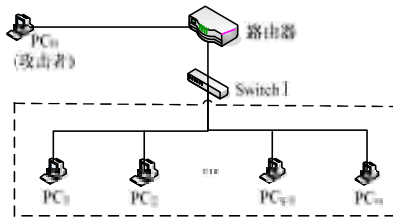


图 3 实验网络的拓扑结构

在攻击开始前, 依据专家打分的方法, 计算出信息获取所占的权重 0.3, 信息打击所占的权重 0.7, 信息获取对应评估指标的权重为 $(0.349, 0.039, 0.116, 0.078, 0.064, 0.035, 0.010, 0.186, 0.124)$, 信息打击对应评估指标的权重为 $(0.362, 0.099, 0.066, 0.121, 0.110, 0.035, 0.054, 0.030, 0.020, 0.015, 0.030, 0.058)$ 。

具体实验过程如下:

(1)攻击方对目标网络进行端口扫描, 发现目标网络中存在 5 台计算机。且计算机 PC_1 和 PC_3 的 445 号端口开放。

(2)对计算机 PC_1 和 PC_3 进行漏洞扫描, 发现计算机 PC_1 中存在 MS08067 漏洞。

(3)利用 MS08067 漏洞工具对计算机 PC_1 实施缓冲区溢出攻击, 实验结束。

可以看出, 网络攻击具有时序性, 攻击者的攻击能力随着网络攻击的进行不断发生变化。在网络攻击开始前, 攻击方对目标网络的信息一无所知。随着攻击方对目标网络进行端口扫描和漏洞扫描, 攻击方发现目标网络存在 5 台计算机, 且有 2 台计算机的 445 端口开放, 其中一台计算机存在 MS08067 漏洞。在此基础上, 攻击方利用 MS08067 漏洞工具对计算机 PC_1 实施攻击, 获取了一定的权限。信息获取的评估指标测量值如表 1 所示。

表 1 信息获取的评估指标测量值

评估指标	测量值	备注
IP 地址	5	192.168.1.3~192.168.1.7
主机名	0	—
端口(开放)	2	PC_1 、 PC_3 的 445 号端口开放
服务(开放)	0	—
系统账户/口令信息	0	—
应用程序账户/口令信息	0	—
数据库账户/口令信息	0	—
操作系统漏洞	1	PC_1 存在 MS08067 漏洞
应用程序漏洞	0	—

信息打击的评估指标测量值如表 2 所示。其中, 测量值“1”表示在缓冲区溢出攻击成功后, 攻击者可对目标网络中 1 台计算机 PC_1 进行该操作, 测量值“0”表示攻击者不能对目标网络中的任何主机进行该项操作。

表 2 信息打击的评估指标测量值

评估指标	测量值
添加文件	1
篡改文件	1
删除文件	1
篡改注册表	0
篡改系统账户/口令信息	1
篡改应用程序账户/口令信息	0
篡改数据库账户/口令信息	0
记录键盘信息	0
篡改系统配置参数	1
篡改网络配置参数	1
篡改系统服务	0
远程操作应用程序	1

4.2 实验结果分析

4.2.1 信息获取的评估

对于网络攻击实验的测试结果, 根据信息获取的评估指标测量值和式(3)~式(8), 得出灰色评价矩阵:

$$R = \begin{pmatrix} 0 & 0.75 & 0.25 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0.25 & 0.75 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

将上述结果代入式(10), 计算综合评价向量:

$$B=(0, 0.262, 0.116, 0.273)$$

上述结果表明, 攻击者信息获取能力的评估结果并不属于优、良、中、差当中的任何一个等级, 它属于良、中、差等级之间的一个灰色区间。

根据式(11), 计算信息获取的分数 $S=38.84$ 。

分数 S 是对攻击者在网络攻击过程中所获取的信息进行的定量评分, 它反映了网络攻击过程中攻击者不断地借助各种攻击手段获取目标网络信息。

4.2.2 信息打击的评估

综合分析网络攻击实验的实验结果, 根据信息打击的评估指标测量值和式(3)~式(8), 得出灰色评价矩阵:

$$R = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (13)$$

将上述结果代入式(10), 得到综合评价向量:

$$B=(0, 0, 0, 0.73)$$

实验结果表明, 攻击者信息打击能力的评估结果属于一个和差等级比较接近的灰色区间, 且该区间与其他等级不相交。

根据式(11), 得出信息获取的分数 $S=29.2$ 。分数 S 是对攻击者的信息打击能力的定量评分, 它反映了攻击者在网络攻击过程中积累的权限及对目标网络操作的能力。

4.2.3 攻击者攻击能力的综合评估

根据式(12), 得出攻击者攻击能力的综合分数 $A=35.948$ 。由此可见, 攻击者的攻击能力由 2 个部分组成, 即攻击者在

网络攻击过程中获取的目标网络的相关信息, 攻击者对目标网络进行非法操作的能力。

5 结束语

本文研究了攻击者的攻击能力在网络攻击过程中的积累过程, 并利用灰色理论对攻击者的攻击能力进行定量评估。但本文的评估方法主要基于网络攻击的客观效果, 对攻击者的攻击意图考虑不足, 下一步将据此对该评估方法进行改进。

参考文献

- [1] 徐建军, 单 懿, 仇广煜, 等. 网络攻防训练模拟系统的研究与实现[J]. 计算机工程, 2010, 36(7): 129-131.
- [2] Lala C, Panda B. Evaluating Damage from Cyber Attacks: A Model and Analysis[J]. IEEE Trans. on Systems, Man and Cybernetics, Part A: Systems and Humans, 2001, 31(4): 300-310.
- [3] 张义荣, 鲜 明, 王国玉. 一种基于网络熵的计算机网络攻击效果定量评估方法[J]. 通信学报, 2004, 25(11): 158-165.
- [4] 胡 影, 郑康锋, 杨义先. 一种基于原子功能的网络攻击效果评估指标体系[J]. 计算机工程与科学, 2008, 30(10): 1-4.
- [5] 李雄伟, 于 明, 杨义先, 等. Fuzzy-AHP 法在网络攻击效果评估中的应用[J]. 北京邮电大学学报, 2006, 29(1): 124-127.
- [6] 王会梅, 王永杰, 张义荣, 等. 粗糙集理论在网络攻击效果评估中的应用研究[J]. 计算机应用研究, 2007, 24(6): 118-120.
- [7] 鲜 明. 网络攻击效果评估导论[M]. 长沙: 国防科技大学出版社, 2007.
- [8] 邓聚龙. 灰色系统理论教程[M]. 武汉: 华中科技大学出版社, 1990.
- [9] 王会梅, 王永杰, 鲜 明. 基于移动 Agent 的网络攻击效果评估数据采集[J]. 计算机工程, 2007, 33(14): 160-162.

编辑 顾姣健

(上接第 113 页)

定理 2 基于椭圆曲线上离散对数问题的困难性, 方案能够抵抗类型 攻击者 A_2 的攻击。

如果攻击者能够进行适应性选择消息和选择身份攻击, 那么存在算法 ϕ 能够伪造有效的代理盲签名。即挑战者 D 通过与攻击者 A_2 的交互协议, 利用 A_2 的伪造能力能够解决离散对数问题的难题。由于已知系统公钥 P_{pub} , 要想通过 $P_{pub} = sP$ 来求解 s 将面临离散对数困难性的难题, 而离散对数问题是难解的, 因此方案是安全的。

敌手和代理签名者进行交互, 假若敌手在签名过程中得到了信息 (U', h, V') 。由 $V' = hS_p + P_2$ 要想得到代理签名密钥 S_p , 必须知道 P_2 , 而 P_2 是代理签名者随机选取的, 由 $U' = e(P_2, P_{pub})$ 求 P_2 将面临求解双线性对分叉问题的难题。因此, 敌手不会从盲签名的交互过程中得到任何秘密信息。

5 结束语

无证书代理盲签名在不可跟踪的电子现金、匿名的电子投票、密码协议、电子货币等电子商务领域有着广泛的应用空间。本文结合无证书公钥密码体制和代理盲签名的特点, 提出一种无证书的代理盲签名方案。该方案既具有代理签名和盲签名的性质, 又消除了对证书的依赖, 解决密钥托管等

问题。基于椭圆曲线上离散对数问题的困难性, 方案具有存在性不可伪造, 安全性更高。

参考文献

- [1] Mambo M, Usuda K, Okamoto E. Proxy Signature: Delegation of the Power to Sign Messages[EB/OL]. (1996-09-15). <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.14.8266>.
- [2] Chaum D. Blind Signatures for Untraceable Payments[C]//Proc. of Advances in Cryptology Crypto'82. New York, USA: Plenum Press, 1983.
- [3] Jan J K. A Security Personal Learning Tools Using a Proxy Blind Signature Scheme[C]//Proc. of International Conference on Chinese Language Computing. [S. l.]: IEEE Press, 2000.
- [4] 李方伟, 邱成刚. 一种基于 ElGamal 签名体制的代理盲签名[J]. 计算机应用与软件, 2009, 26(3): 134-135, 157.
- [5] 李 霞, 杨长海. 基于椭圆曲线的门限多代理盲多签名方案[J]. 计算机工程, 2009, 35(13): 169-171.
- [6] Riyami S, Paterson K. Certificateless Public Key Cryptography[EB/OL]. (2003-10-21). <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.81>.

编辑 陈 文

