

基于动态博弈的粗糙网络安全分析模型

张 晶, 李 艳

(西安建筑科技大学管理学院, 西安 710055)

摘 要: 基于攻击图的主动网络安全测评是网络安全的战略研究方向,但目前多数网络攻击模型都是从攻击一方的角度进行分析,忽略了整个攻防过程中连接关系及知识体系的粗糙性。为此,结合攻击粗糙图和动态博弈理论提出粗糙网络安全分析模型 RNSAM。以粗糙部件访问关联图为基础,刻画某时刻网络拓扑结构状态下网络部件主体之间的粗糙访问关系,通过对攻击策略集和防御策略集在知识域空间上的粗糙刻画来反映攻防过程中的动态决策机制,同时给出攻击策略选取算法,指出在当前网络连接状态和攻防双方知识水平下的最优防御策略。实例分析结果表明,RNSAM 能够完整模拟网络攻击过程,使网络管理员以最小的代价采取相关防御措施。

关键词: 网络风险分析;网络攻击模型;攻击图;粗糙博弈分析;粗糙网络;粗糙图

中文引用格式:张 晶,李 艳.基于动态博弈的粗糙网络安全分析模型[J].计算机工程,2015,41(4):129-134.

英文引用格式:Zhang Jing, Li Yan. Rough Network Security Analysis Model Based on Dynamic Game[J]. Computer Engineering, 2015, 41(4): 129-134.

Rough Network Security Analysis Model Based on Dynamic Game

ZHANG Jing, LI Yan

(School of Management, Xi'an University of Architecture & Technology, Xi'an 710055, China)

[Abstract] Now the network security evaluation method based on attack graph becomes the main research point, but most of the network attack models are analyzed from the standpoint of the attack side, and ignore the whole process of the connection relationship between offensive and defensive and the roughness of the knowledge system. This paper uses the rough access components association graph to describe the rough access relationship among the network components at some time and some special network topology state, through the rough characterization of the attack and defense policy set in the knowledge domain space to reflect the dynamic decision-making mechanism in the process of offensive and defensive. It gives the optimal attack policy-selection algorithm simultaneously, points out the most possible defensive policy in the current state of the network connection and the knowledge level of both sides of offensive and defensive. Examples show that the results of the analysis can help the defense side of the network administrator take related defensive measures better.

[Key words] network risk analysis; network attack model; attack graph; rough game analysis; rough network; rough graph

DOI: 10.3969/j.issn.1000-3428.2015.04.024

1 概述

信息化概念的全球化扩展和普及,使得“信息”成为了具有经济价值的资源,同时随着互联网等计算机处理技术的飞速发展,使得信息资源的全球化

利用成为了可能,但网络入侵行为的简单化和智能化使得信息所有方和信息使用方的所有权关系发生了改变,而且这一转变似乎具有不可逆转的趋势,由此产生的信息安全问题成为了当前的关注焦点。在网络安全技术的发展初期,以静态被动防御措施为

基金项目:陕西省教育厅科研计划基金资助项目(2013JK0185);陕西省重点学科专项基金资助项目(E08001);陕西省高校哲学社会科学重点研究基地建设专项基金资助项目(DA08046);陕西省高校哲学社会科学特色学科建设专项基金资助项目(E08003, E08005);西安建筑科技大学人才科技基金资助项目(RC1324)。

作者简介:张 晶(1981-),女,讲师、博士,主研方向:信息安全,管理科学与工程,决策分析;李 艳,博士、CCF 会员。

收稿日期:2014-05-04 **修回日期:**2014-05-29 **E-mail:** sy_liyan137@126.com

主,随着入侵技术的普及和发展,这种防御手段缺乏主动能力的缺陷越来越突出。建立主动的防御安全体系^[1],通过态势感知、风险评估、安全检测等手段来实施主动防御成为了目前网络安全技术的战略目标。

文献[2]对国内外当前的主动网络安全测评技术进行了详细的分析和总结,而攻击图模型^[3-4]、特权图模型^[5-6]、高级随机模型^[7-8]等技术试图全面模仿攻击方的攻击行为,通过模型检测的方式进行定性分析,进而对当前网络存在的可能漏洞和风险进行防御,这种攻击模型的刻画方式试图从攻击一方的有限行为分析来提供安全状态结果,存在着很大的局限性。文献[9-10]对安全成本评估及攻防投资回报等提供了很好的研究思路,文献[11-12]也从不同的角度对网络安全量化分析做出了卓有成效的探讨。

文献[13-14]从网络连接关系和实体之间的交互过程出发,将粒度细化到了部件主体级,同时结合粗糙图的基本理念,提出了一种粗糙网络攻击分析模型,使得攻击分析结果和安全建议更加合理。但是上述网络攻击模型大部分都是从攻击者一个单方面的角度出发,对固定拓扑结构和一方攻击问题进行模拟,而网络入侵过程一定是攻击方、正常用户、防御方(安全管理员)等的多方行为,这种“策略相互依存”的理念^[15]是网络安全决策模型分析的理论基础。文献[16]使用不完全信息重复博弈方法对攻击和防御双方的行为进行了建模,文献[17]使用随机博弈的方法得出了攻防各方的最优策略及纳什均衡,文献[18]将完全信息静态博弈应用到DDoS的分析与设计上取得了一定的效果,文献[19]提出了基于博弈论的入侵推理模型,为网络安全的博弈分析做出了进一步的探讨。

在实际网络环境中,由于知识类型、参与程度等方面的限制,无论是攻防双方是正常的使用用户,对当前网络的认知都存在着一一定程度的粗糙性,因此,本文在前述研究成果的基础上,结合攻击粗糙图和动态博弈理论提出一种新的粗糙网络安全分析模型(RNSAM),该模型以部件粗糙访问关联图为基础,刻画了某一时刻网络拓扑结构状态下网络部件主体之间的粗糙访问关系。通过对攻击者的攻击策略集,防御者的防御策略集在知识域类型空间上的粗糙刻画来反映攻防过程中的决策机制。同时给出攻击策略选取算法,指出在当前网络连接状态和攻防双方的知识水平下的最优防御策略。

2 RNSAM 模型

在整个网络攻防的周期过程内,攻击者可以采取多种攻击方式,调整攻击参数,同时防御者也可以

设置或者调整防御策略,因此可以将整个过程看作是一个多阶段不完全信息博弈过程^[20]。同时攻防双方对某一个服务器的攻击和防御都是在服务器上的某一应用程序或服务级别上的,因此,本文仍然采用“安全依赖关系”的概念,在部件级别上来刻画网络连接关系和攻防双方知识水平的粗糙性,并在此基础上进行分析,下面给出相关定义。

定义1 部件主体为一个二元组 $C = (n, s)$,表示一个部件 C 在网络节点 n 上提供的一个服务 s ,攻击者的攻击过程就是通过部件主体之间的连接来完成的。

定义2 部件主体间的权限关系为一个三元组 $C_p = (C_{xi}, C_{yj}, P)$,表示在节点 x 上的部件主体 i 在节点 y 的部件主体 j 上拥有 P 的权限。

定义3 部件主体之间的链路连接关系为一个三元组 $C_l = (C_{xi}, C_{yj}, L)$,表示在节点 x 上的部件主体 i 在节点 y 的部件主体 j 上拥有连接关系集 L ,这里的 L 特指部件之间的普通网络连接关系集合,如:网络连接关系和服务发布方式等。

定义4 部件主体之间的访问关系在有向图中表示为一个带有连接弧的有向边^[14] $e_k^a(C_{xi}:C_{yj}) = (C_{xi}, C_{yj}, C_p, C_l)$,其中, $k \in [1, +\infty]$ 为相同2个部件之间不同连接的索引标识; α 为方向属性,若弧带正方向,即 $\alpha = +$ 则 $e_k^+(C_{xi}:C_{yj})$ 表示节点 x 上的部件主体 i 在节点 y 的部件主体 j 上具有 C_p 的访问权限,同时具有 C_l 的连接关系,此时称 C_{xi} 为 $e_k^+(C_{xi}:C_{yj})$ 的头, C_{yj} 为 $e_k^+(C_{xi}:C_{yj})$ 的尾;若弧带负方向,即 $\alpha = -$ 则含义相反。

通过上述4个定义,可以将物理链路表达的网络拓扑关系转换成基于部件主体的逻辑连接关系。如图1所示,其可以简单描述为网络节点 A 上的部件主体 m 对网络节点 B 的部件主体 i, j 分别具有某种访问关系。

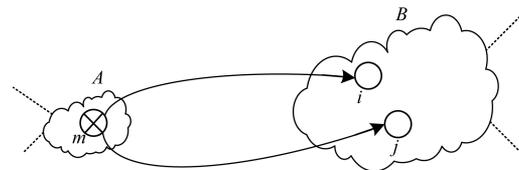


图1 部件网络连接关系

定义5 部件粗糙连接图为一个四元组 $CRCG = (N, C, E, \mathfrak{R})$ 。其中, $N = (n_1, n_2, \dots, n_m)$ 代表网络中独立的网络节点集合; C 是当前节点所拥有的部件主体的集合; $E = \cup e_k^a(C_{xi}:C_{yj})$ 代表部件主体之间的权限和所有的连接关系的集合; $\mathfrak{R} = (r_1, r_2, \dots, r_{|\mathfrak{R}|})$ 是由权限或者其他连接关系所构成的不同的属性集合,且 \mathfrak{R} 中包含 $(C_{xi}:C_{yj})$, 即属性集 R 是和有向边上部件主体相关联的。

这样对于 E 上的不同连接关系属性集 $R \subseteq \mathfrak{R}$, E 中的边可以分为不同的等价类,根据粗糙图的基本定义,可以用以下 2 个精确图来定义部件粗糙连接图 $CRCG$ 。

$$\overline{CRCG} = \{e_k^a(C_{xi}:C_{yj}) \in E \mid [e_k^a(C_{xi}:C_{yj})]_R \subseteq X\}$$

$$\underline{CRCG} = \{e_k^a(C_{xi}:C_{yj}) \in E \mid [e_k^a(C_{xi}:C_{yj})]_R \cap X \neq \emptyset\}$$

这里通过定义 5 来描述部件主体间连接关系的粗糙性。

如图 2 所示,位于网络节点 A 上的部件主体 m 对位于网络节点 B 上的部件主体 DB 和 FTP 具有访问权限,假设和 DB 之间的连接方式有 3 种 ($IDriver$ 方式, $JDBC$ 的 $thin$ 方式和 $JDBC$ 的 $OCI8$ 方式),则部件 m 和部件 DB 之间的连接论域图如图 2(a) 所示(每条虚线代表一种连接方式),即 $\overline{CRCG} = \{IDriver, JDBC-thin, JDBC-OCI8\}$,由于防火墙等限制在进行关联时只支持 $JDBC$ 的方式,即 $\underline{CRCG} = \{JDBC-thin, JDBC-OCI8\}$ 其部件连接粗糙图如图 2(b) 所示。可以看到相比于对部件 FTP 连接关系的描述(图 2 中的实线表示)这样的粗糙刻画更加准确。

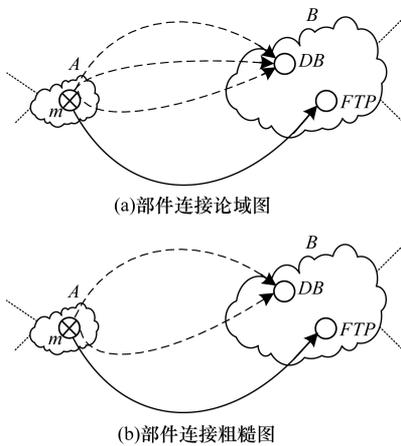


图 2 部件粗糙连接图

定义 6 攻击策略集为一个三元组 $\theta_A = \{E, \mathfrak{R}, \phi_A\}$,其中, E, \mathfrak{R} 的含义和定义 5 中的含义相同; ϕ_A 表示 E 中的部件 C_{xi} 对部件 C_{yj} 在属性集 \mathfrak{R} 的条件下所能采取的攻击方法。攻击策略集 θ_A 是一个粗糙集,可以使用以下 2 个精确图进行刻画:

$$\theta_A = \{\phi_A \in \phi \mid [\phi_A]_\phi \subseteq X\}$$

$$\underline{\theta}_A = \{\phi_A \in \phi \mid [\phi_A]_\phi \cap X \neq \emptyset\}$$

定义 7 防御策略集为一个三元组 $\theta_D = \{E, \mathfrak{R}, \varphi_D\}$,其中, E, \mathfrak{R} 的含义和定义 5 中的含义相同; φ_D 表示对于 E 中的部件 C_{xi} 对部件 C_{yj} 在属性集 \mathfrak{R} 的条件下的攻击所能采取的防御方法。防御策略集 θ_D

也是一个粗糙集,可以使用以下 2 个精确图来进行刻画:

$$\theta_D = \{\varphi_D \in \varphi \mid [\varphi_D]_\varphi \subseteq X\}$$

$$\underline{\theta}_D = \{\varphi_D \in \varphi \mid [\varphi_D]_\varphi \cap X \neq \emptyset\}$$

网络攻防的量化分析是国内网络安全研究的热点^[11-13],也是进行攻防博弈分析的基础,攻击策略和防御策略的细化分类将会在后续的工作中重点讨论,本文主要参考文献[21]中对攻击策略和防御策略的分类及相关收益量化的计算方法,结合本文的前述定义对攻击收益和防御代价定义如下:

定义 8 攻击收益为 $Cost_A = (\theta_A, A_{Cost})$,其中, θ_A 是定义 6 中所描述的攻击粗糙集; A_{Cost} 代表 E 中的某一部件对另一部件应用某种方法攻击所获取的收益。因为进行攻击时攻击者的收益往往要比系统的损失小的多,所以本文也将系统的损失作为攻击者收益^[21],即 $A_{Cost} = AL \times criticality \times (Cost_1 \times p_1 + Cost_c \times p_c + Cost_A \times p_A)$,其中, AL 是攻击致命度代表某类攻击所能具有的危害程度(用 0 ~ 10 之间的数值来表示); $criticality$ 是攻击目标的资源损失; $Cost_1$ 表示资源属性中的完整性代价; p_1 表示资源对于完整性代价的偏重; $Cost_c$ 表示资源属性中的机密性代价; p_c 表示资源对于机密性代价的偏重; $Cost_A$ 表示资源属性中的可用性代价, p_A 表示资源对于可用性代价的偏重;并且 p_1, p_c, p_A 之间满足 $p_1 + p_c + p_A = 1$ 的关系。

定义 9 防御代价为 $Cost_D = (\theta_D, D_{Cost})$,其中, θ_D 为定义 7 中所描述的防御粗糙集; D_{Cost} 代表为了防止 E 中的某一部件对另一部件的攻击采取相应的防御策略时所付出的代价,即 $D_{Cost} = C_O + C_N + C_R$,其中, C_O 代表操作代价,用以表示防御者的防御操作消耗的时间和计算资源的数量; C_N 代表负面代价,用以表示防御策略导致系统无法正常工作或服务下降等带来的损失; C_R 代表残余损失,用以表示防御系统执行防御策略后,攻击对系统带来残余的未被消除的损失。

基于上述对部件粗糙连接图、粗糙攻击集、粗糙防御集及相关量化分析的定义,可以构建出粗糙攻防博弈连接图来对网络连接关系和攻防双方的知识体系进行粗糙集刻画及进一步的量化分析。粗糙攻防博弈论域图如图 3(a) 所示,在对连接关系进行粗糙处理的基础上增加了攻击集和防御集的描述, $\{a_1; 10\}$ 是攻击收益量化的结果,表示针对某种连接方式采用 a_1 攻击方法所获得的收益,图 3(b) 表示的是攻防博弈粗糙图及相关的量化结果;图 3(c) 表示网络部件连接图。

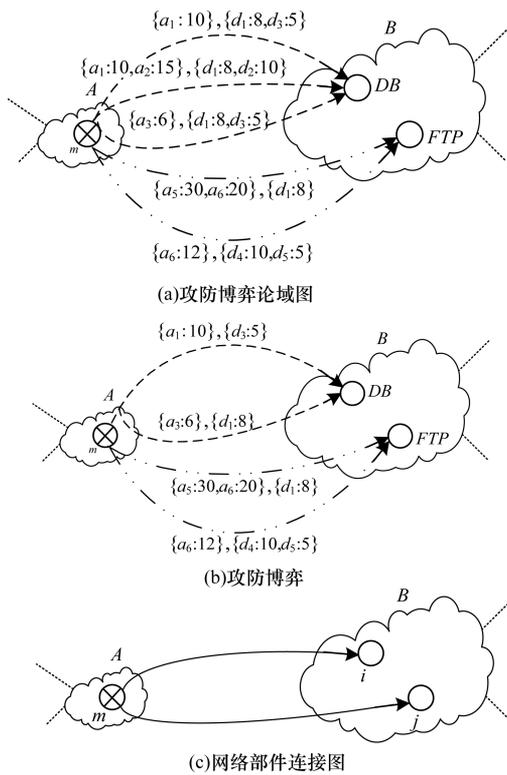


图3 粗糙攻防博弈图

定义 10 RNSAM 模型为一个四元组 $RNSAM = \{CRCG, U, \theta, Cost\}$, 其中, $CRCG$ 是部件粗糙连接图使用权限访问和依赖关系来描述部件节点之间的粗糙连接程度; $U = \{U_A, U_D\}$ 表示网络攻防过程中的参与方的集合, 根据基本假设^[15], 本文假设只有攻击者和作为系统管理员的防御者 2 个参与方; $\theta = \{\theta_A, \theta_D\}$ 表示攻击粗糙策略集和防御粗糙策略集; $Cost = \{Cost_A, Cost_D\}$ 表示 2 个部件节点之间的攻防量化关系结果, 实际运算过程中可用量化的收益效用矩阵来表示^[21]。

3 模型应用与分析

3.1 基于 RNSAM 模型的攻击策略选取算法

实际的攻防过程中可能会出现攻击收益和系统损失不相等的情况, 即会出现非零和博弈的状况, 网络攻防的过程中攻击方与防御方之间的关系是非合作的和对抗性的, 而且总是通过策略的实施保证自己的收益最大化, 但由于攻防双方的不确定性, 在某些情况下可能不存在纳什均衡, 由此导致了混合策略的产生, 表示网络攻防的双方在处理对方的未知策略时可以根据先验知识来对对方的策略分布进行估计, 也即采用混合防御策略。为了对多步攻击及防御者的综合行为进行刻画, 本文依托于混合策略纳什均衡^[22]的概念给出基于 RNSAM 模型的攻击策略选取算法。

算法 基于 RNSAM 模型的攻击策略选取算法

输入 RNSAM 模型图

输出 可能攻击路径、攻击策略及最优防御策略

Step1 通过网络漏洞, 网络配置等自动化工具生成 RNSAM 模型, $RNSAM = \{CRCG, U, \theta, Cost\}$ 。

Step2 构建攻击策略集 $\theta_A = \{E, \mathfrak{R}, \phi_A\}$ 以及防御策略集 $\theta_D = \{E, \mathfrak{R}, \phi_D\}$ 。

Step3 运用基于粗糙图的攻击图生成算法及网络风险最大流算法生成可能攻击路径^[14]。

Step4 判断是否满足零和博弈条件, 若“是”则转向 Step5, “否”则转向 Step7。

Step5 根据定义 9 计算所有防御策略的防御收益 $\lambda_{Dij} = \sum Cost_D$ 。

Step6 对于每一个攻击策略计算攻击收益 $\lambda_{Aij} = Cost_A - \sum Cost_D$, 并生成效用矩阵。

Step7 对于非零和博弈, 根据定义 8 计算攻击收益之和, 生成攻击收益 $\lambda_{Aij} = \sum Cost_A + AC$, 其中, AC 代表攻击成本用负值表示。

Step8 计算防御收益 $\lambda_{Dij} = \sum Cost_A - Cost_D$, 并生成效用矩阵。

Step9 如果效用矩阵 λ 存在鞍点, 则应用纯策略算法^[22]求解, 否则使用混合策略求解算法^[22]求解。

Step10 在攻击路径的基础上, 分析得出攻击策略和防御策略。

Step11 返回攻击路径 θ_{path} 、攻击策略 $\{\theta_A\}$ 及最优防御策略 $\{\theta_D\}$ 。

3.2 实例验证与结果分析

为了对本节中所提出的模型相关定义描述的准确性, 以及算法的正确性进行验证, 说明进行网络攻防博弈分析在网络安全分析方面的优势, 本文以一个实际的例子进行说明。

本文所采取的实验网络拓扑结构如图 4 所示, 攻击者 Eve 位于互联网的一个节点上, 在攻击者 Eve 和局域网之间存在着防火墙以及 IDS 等防护设备; 局域网通过交换机相连, 由一台 PC 机和 3 台服务器组成, 其中 DB Server 为 Oracle 数据库服务器, 操作系统为 Linux 系统, FileServer 操作系统为 Windows 操作系统, EmailServer 操作系统为 Windows 操作系统。

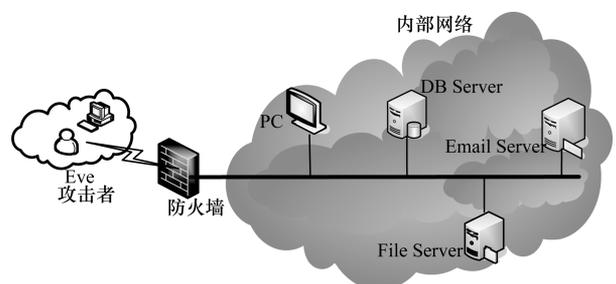


图4 实验网络拓扑结构

其中由于网络管理员水平的限制等原因, DB Sever 存在着 TNS Listener 以及本机缓冲区溢出的漏洞, FileSever 存在着 Ftp. rhost 漏洞, EmailServer 存在着 SMTP 溢出以及 Apache 本地溢出漏洞。假设攻击者的攻击目标是位于 FileServer 上的 File 文件,通过自动化生成工具可以生成如图 5 所示的实验网络攻防博弈论域图,对每一个漏洞有很多的攻击方法(其中实线代表正常的访问连接关系,点线或者虚线代表攻击关系),但是由于攻击者的能力所限,只能使用一些典型攻击方法来进行攻击,则攻击集 $\theta_A = \{a_1, a_2, a_3, a_4, a_5, a_6\}$,其中, a_1 代表以普通用户的身份进行登陆; a_2 代表以管理员的身份进行登录; a_3 代表通过溢出攻击来对 DB 服务器的攻击; a_4 代表针对 Ftp. rhost 漏洞的专用工具攻击; a_5 代表 ApacheChunk 攻击; a_6 代表垃圾邮件攻击。防御集

$\theta_D = \{d_1, d_2, d_3, d_4, d_5\}$ 其中 d_1 代表登录账号修改; d_2 代表针对漏洞进行补丁升级; d_3 代表关闭服务; d_4 代表关闭 FTP 进程; d_5 代表 Email 端口关闭。这样结合表 1 的量化结果,即可得到如图 6 所示的网络攻防博弈粗糙图。

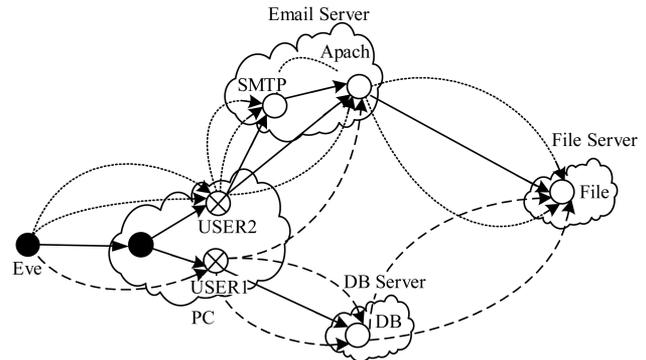


图 5 攻防博弈论域图

表 1 攻防方式及量化结果

BID	漏洞描述	典型攻击方式	AL	典型防御方法	Cost _O	Cost _N	位置
5033	TNS Listener	溢出攻击	8	补丁、关闭服务	10	0	DB
8668	本地溢出	本地溢出攻击	5	补丁、关闭服务	10	2	DB
328	Ftp. rhost	Ftp. rhosts	10	关闭 Ftp 服务	10	10	File
4033	SMTP 溢出	垃圾邮件攻击	1	取消 Mail	10	2	Email
3886	Apache 本地溢出	Apache Chunk	10	补丁、关闭服务	10	0	Email

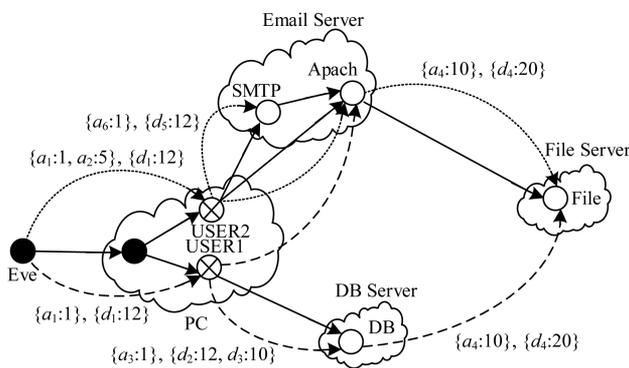


图 6 攻防博弈粗糙图

实验网络的攻防博弈粗糙图可以用图 7 的弧目录形式来表示。通过对攻防博弈下近似粗糙图的分析可以得到 Eve 的攻击路径有 3 条。第 1 条攻击路径序列为 $(a_1$ 或 $a_2, a_5, a_4)$, 即 Eve 通过管理员用户或者正常用户登录后, 假冒 USER2 使用 Apache Chunk 进行攻击进而控制 Apache, 再通过 Ftp. rhost 漏洞的专用工具取得 File 的访问权限; 第 2 条攻击路径序列为 (a_1, a_5, a_4) , 即 Eve 通过正常用户登录后, 假冒 USER1 使用 Apache Chunk 进行攻击进而控制 Apache, 再通过 Ftp. rhost 漏洞的专用工具取得 File 的访问权限; 第 3 条攻击路径序列为 (a_1, a_3, a_4) 即 Eve 通过正常用户登录后, 假冒 USER1 使用溢出攻击来对 DB 服务器的攻击, 进而通过 Ftp. rhost 漏

洞的专用工具取得 File 的访问权限。

	Eve	USER1	USER2	Apache	DB	File
Eve		$\{a_1\}, \{d_1\}$	$\{a_1, a_2\}, \{d_1\}$			
USER1				$\{a_5\}, \{d_2, d_3\}$	$\{a_3\}, \{d_2, d_3\}$	
USER2				$\{a_5\}, \{d_2, d_3\}$		
Apache						$\{a_4\}, \{d_4\}$
DB						$\{a_4\}, \{d_4\}$
File						

图 7 实验网络攻防博弈粗糙图的弧目录表示形式

在攻防策略和攻击路径确定后, 需要根据攻防代价及基于 RNSAM 模型的攻击策略选取算法来实现最优防御策略选择的过程。为了简化分析, 本文采用零和非合作攻防博弈模型来进行分析, 从而仅需计算防御代价即可。根据表 1 的量化数值结果及攻击和防御代价的计算公式可得到如下所示的攻防博弈收益矩阵, 其中, A_1, A_2, A_3 代表 3 条攻击路径; D_1, D_2, D_3, D_4 代表阵地每一条攻击路径所能采取的防御策略组合。

	D_1	D_2	D_3	D_4
A_1	210	90	270	150
A_2	120	180	240	210
A_3	180	45	240	240

文献[22]已经证明了实验中的有限博弈一定会有一个均衡点, 应用 3.1 节定义的算法可以得到一

个 Nash 均衡: $p_a = \{2/11, 9/11, 0\}$, $p_d = \{0, 32/85, 13/85, 40/85\}$, 即对于攻击者 Eve 来其会以 2/11 的概率选择第 1 条攻击路径, 以 9/11 的概率来选择第 2 条攻击路径; 防御者会以 32/85 的概率选择针对 Apache 进行补丁升级措施, 以 13/85 的概率关闭 Apache 服务进程, 以 40/85 的概率来暂时关闭 FTP。所以作为管理员的防御者可以选择 D_2 、 D_4 或者两者的组合来保证位于 FileServer 上 File 的安全性。

4 结束语

随着入侵技术的普及和简单化, 静态被动防御的缺陷已经越来越明显, 基于攻击图的主动防御策略越来越受到重视, 但是以往的模型大都是从攻击者或者防御者的角度进行分析, 而且对网络的详细连接关系和攻防双方的知识域水平等都没有考虑, 因此, 本文结合攻击粗糙图和动态博弈理论, 提出了粗糙网络动态博弈安全分析模型 (RNSAM), 将权限关系拓展为某一时刻网络拓扑结构状态下网络部件主体之间的粗糙访问关系, 攻击策略选取算法可以描述攻防过程中的动态决策机制, 并得出最优防御策略, 通过实例分析阐明了模型的应用过程, 验证了算法的效率和准确性, 说明了本文模型在过程刻画完整性及制定最优防御策略方面的优势。

进一步研究工作包括: 扩展模型包含时间因素, 增加攻击步时的概念(不局限于某一时刻), 探讨整个攻击演化过程中攻防双方相互制约关系对攻击的影响, 同时进一步验证本文算法的合理性和有效性。

参考文献

- [1] 方滨兴. 解读信息安全创新突破点 [EB/OL]. [2014-04-15]. <http://www.cert.org.cn/2007051823317.html>.
- [2] 林 闯, 汪 洋, 李泉林. 网络安全的随机模型方法与评价技术 [J]. 计算机学报, 2005, 28(12): 1943-1956.
- [3] Schneier B. Secrets and Lies: Digital Security in a Networked World [M]. New York, USA: John Wiley & Sons, 2000.
- [4] Dacier M. Towards Quantitative Evaluation of Computer Security [D]. Toulouse, France: Institute National Polytechnique de Toulouse, 1994.
- [5] Ortalo R, Deswarte Y, Kaaniche M. Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security [J]. IEEE Transactions on Software Engineering, 1999, 25(5): 633-650.
- [6] Porras P A, Kemmerer R. A Penetration State Transition Analysis: A Rule-based Intrusion Detection Approach [C] // Proceedings of the 8th Annual Computer Security Applications Conference, November 30-December 4, 1992, San Antonio, USA. Washington D. C., USA: IEEE Press, 1992: 220-229.
- [7] Stevens F, Courtney T, Singh S, et al. Model-based Validation of an Intrusion-tolerant Information System [C] // Proceedings of the 23rd Symposium on Reliable Distributed Systems. Washington D. C., USA: IEEE Press, 2004: 184-194.
- [8] Madan B, Go eva-Popstojanova K, Vaidyanathan K, et al. A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems [J]. Performance Evaluation, 2004, 56(1-4): 167-186.
- [9] Mercuri R T. Security Watch: Analyzing Security Costs [J]. Communications of the ACM, 2003, 46(6): 15-18.
- [10] Bistarelli S, Fioravanti F, Peretti P. Defense Trees for Economic Evaluation of Security Investments [C] // Proceedings of the 1st International Conference on Availability, Reliability and Security. Los Alamitos, USA: IEEE Computer Society, 2006: 416-423.
- [11] 冯萍慧, 连一峰, 戴英侠, 等. 面向网络系统的脆弱性利用成本估算模型 [J]. 计算机学报, 2006, 29(8): 1375-1382.
- [12] 董 红, 邱菀华, 吕俊杰. 基于成本分析的入侵检测响应模型 [J]. 北京航空航天大学学报, 2008, 34(1): 39-42.
- [13] 李 艳. 基于 T-G 保护系统的网络攻击与评价模型研究 [D]. 西安: 西安建筑科技大学, 2010.
- [14] 黄光球, 李 艳. 基于粗糙图的网络风险评估模型 [J]. 计算机应用, 2010, 30(1): 190-195.
- [15] Fudenberg D, Tirole J. Game Theory [M]. Cambridge, USA: MIT Press, 1991.
- [16] Burke D. Towards a Game Theory Model of Information Warfare, AFIT/GSS/LAL/99D-1 [R]. Airforce Institute of Technology, 1999.
- [17] Lye K W, Wing J. Game Strategies in Network Security, CMU-CS-02-136 [R]. Pittsburgh, USA: School of Computer Science, Carnegie Mellon University, 2002.
- [18] Xu J, Lee W. Sustaining Availability of Web Services Under Distributed Denial of Service Attacks [J]. IEEE Transactions on Computers, 2003, 52(4): 195-208.
- [19] Liu Peng, Zang Wanyu. Incentive-based Modeling and Inference of Attacker Intent, Objectives, and Strategies [C] // Proceedings of the 10th ACM Computer and Communications Security Conference. New York, USA: ACM Press, 2003: 179-189.
- [20] 张少俊, 李建华, 陈秀真, 等. 基于动态博弈理论的分布式拒绝服务攻击防御方法 [J]. 上海交通大学学报, 2008, 42(2): 198-201.
- [21] 姜 伟, 方滨兴, 田志宏, 等. 基于攻防博弈模型的网络安全测评和最优主动防御 [J]. 计算机学报, 2009, 32(4): 817-827.
- [22] Robert G. A Primer in Game Theory [M]. New York, USA: Pearson Higher Education, 1992.

编辑 金胡考