

信息安全攻防博弈研究

孟祥宏

(呼伦贝尔学院 计算机科学与技术学院, 内蒙古 海拉尔 021008)

摘 要:信息安全中攻防对抗的本质可以抽象为攻防双方的策略依存性,防御者所采取的防御策略是否有效,不应该只取决于其自身的行为,还应取决于攻击者和防御系统的策略。通过对信息安全攻防不对称性、不完全信息、合理性、重复博弈等特点的分析,以及博弈模型要素和一般模型的分析,构建了信息安全的攻防模型,并对其博弈过程进行了详尽地研究与分析。最后,建议应从攻防博弈的视角来研究信息安全问题,为信息安全问题的解决提供一种新的思路。

关键词:信息安全;博弈;攻击;防御

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2010)04-0159-04

Study on Offence and Defense of Information Security Based on Game Theory

MENG Xiang-hong

(School of Computer Science and Technology, Hulunbeier College, Hailaer 021008, China)

Abstract: Information countermeasures can abstract strategy dependency in essence. Defender's strategy is available or not, not only rest with his behavior, but also rest with attacker's behavior. Through analyzing the characters of information countermeasures, such as information asymmetry, imperfect information, rationality and game repetition etc, and analyzing the game model and its elements, uses game theory to construct offence-defense model, and then studies the process of attacker and defender in detail. At last, suggests to study information security problems from game theory views, and provides a new idea to solve these problems.

Key words: information security; game theory; attack; defense

0 引言

信息安全问题的发生原因,一类是人的过失性,这与人总会有疏漏犯错误有关;另一类是人因某种意图,有计划地采取各种行动,破坏一些信息和信息系统的运行程序,以达到某种破坏目的,这种事件称为信息攻击。受到攻击的一方当然不会束手待毙,总会采取各种可能反抗这一行为(包括预防、应急措施),力图使对方攻击难以凑效(或弱化至最小),以减小己方的损失,以至惩处(或反攻)对方等,这种双方对立行动事件称为信息攻防对抗^[1]。信息安全中攻防对抗的本质可以抽象为攻防双方的策略依存性,防御者所采取的防御策略是否有效,不应该只取决于其自身的行为,还应取决于攻击者和防御系统的策略。所以可以利用博弈论来研究攻防矛盾及其最优防御决策等信息安全攻防对

抗难题^[2]。Samuel N Hamilton 指出,博弈论将在网络攻防对抗领域发挥重要作用,是未来信息安全很有前途的研究方向^[3]。

文中运用博弈论对信息安全攻防的博弈模型以及攻防过程进行了研究与分析。

1 相关研究

博弈论是在具有相互对抗和反应特征的社会经济环境中最有效的决策理论和经济分析工具,是研究各个理性决策主体在其行为发生直接相互作用时的决策,以及这种决策的均衡问题的一种方法论。它主要是研究人们在利益相互影响的格局中如何使自己收益最大化的策略选择问题。

国内外的学者利用博弈论对网络信息安全问题作了很多相关的研究。早在1997年,文献[4]中就提出应使用动态博弈来对网络中的正常节点和恶意节点进行理性分析的想法。文献[5]将攻防双方看作非零和动态博弈中的两个局中人,并计算了双方的最优响应策略。国内运用博弈论对攻防问题研究的文献数量不

收稿日期:2009-07-22;修回日期:2009-11-03

基金项目:内蒙古自治区2008年科研计划项目(NJSy08168)

作者简介:孟祥宏(1971-),男,内蒙古赤峰人,博士,副教授,研究方向为电子政务、网络安全。

多,主要出现在近三年。如,文献[6]利用演化博弈论研究信息安全的攻防问题,建立了信息安全攻防的博弈模型,并分析了攻防双方的复制动态及进化稳定策略;文献[2]中把网络攻防双方建模为二人非合作博弈模型,并给出了攻防博弈模型的形式化描述,用此模型来研究网络攻防双方的矛盾冲突和最优决策;文献[7]将信息安全看作企业与入侵者之间的一个博弈,企业使用信息安全技术的目标是最小化入侵者带来的损失,企业的信息安全投资收益依赖于入侵的程度,而入侵者入侵的收益依赖于被发现的可能性,入侵者被发现的可能性依赖于信息安全技术。文献[8]将不完全信息动态博弈引入到网络攻防的分析过程,讨论了均衡策略的存在性,完善了网络攻防对抗模型。

这些研究都将信息安全问题视作攻击方与防御方的动态博弈,分别从攻防双方的策略以及互动来研究信息安全问题。

2 信息安全攻防特点

真正的安全不是单方面的,也不是静态的,而是基于社会大背景下的一种信息对抗方式,是一个动态的过程。

(1) 攻防不对称性。

攻防不对称性主要体现在攻防技术、攻防成本、攻防主体、攻防信息的不对称性上。如攻防技术的不对称方面体现在如下两个方面:①每个防御措施必定针对一个漏洞或者攻击技术,但并非每个漏洞或者攻击形式都存在相应的有效防御,同一漏洞可能存在多种攻击方式,增加了对攻击行为的预测难度,相对于攻击知识,防御措施总是有一定滞后。②虽然是从攻防对抗中获取知识,但由于攻守地位的不同,防御者需要掌握所有的攻击技术和漏洞信息才能达到与攻击者相平衡。

(2) 不完全信息。

在信息安全中,信息是指一切与攻防有关的知识,包括信息网络系统脆弱性知识、攻防参与者的攻防能力知识、过去的攻防行动和结果以及外界环境的作用等。受身份和自身角色的影响,攻防双方对于博弈信息的了解是不对称的。防御方能够准确、具体和全面地了解网络状态和网络拓扑结构,相反,攻击者虽然在攻防对抗知识上有自身的优势,但在目标系统信息获取上往往还只是一个盲目搜索和攻击试探的过程;而防御者虽然熟悉自己的安防系统,但却无法预测攻击在何时、何地以何种方式进行,只能全面考虑所有可能的攻击,针对存在的弱点处处设防、时时警惕。

(3) 合理性。

在博弈中,如果参与者积极寻找使自己博弈优势最大的办法,那么在某种意义上说博弈是合理的。在网络安全模型中假设攻防双方具有相近的知识也是合理的。攻击者选择最有效的方法进攻,而防御者也总是希望以最好的方法防御,攻击者和防御者在博弈期间都希望自己的行为达到最大的成效,因而他们是合理的参与者。

(4) 重复博弈。

在信息安全攻防中,攻防双方是不断地重复博弈的。攻击促进了防御的发展,防御技术的发展也刺激了攻击者不断寻找新的攻击方法。防御者成功的原因在于:总结到的攻击方法在攻击者所拥有的攻击方法中所占比例大,并且防御方法比攻击方法更复杂。攻击者成功的原因在于:在老的攻击方法失效之前发明新攻击方法,同时其复杂性必须能够保证新攻击方法层出不穷。

3 信息安全攻防博弈模型

3.1 博弈模型要素

一个完整的博弈模型通常包括参与者、战略、信息、行动、效用(支付)五个基本要素^[9]:

(1)参与者(Player):参与人,或称局中人,是参与博弈的直接当事人,是博弈的决策主体和策略制定者,其通过选择行动(战略)以最大化自己的支付水平。在信息安全攻防对抗中,如同一切博弈理性人,防御方在作为一个理性人进行决策时,其考虑的是己方的安全利益最大化,而攻击方决策时,考虑的是使得攻击效益最大化,这与博弈论中的参与人定义正好相符。

(2)战略(Strategies):战略是参与者在给定信息集的情况下的行为规则,它规定参与者在何种情况下采取何种行动。对于攻防双方的战略表示,具体说就是攻击与防御策略的选择规则。在攻防博弈模型中,攻防双方的策略和最优策略求解可表示为多种形式,而且动态博弈过程中需在对大量博弈策略的组合进行选择 and 判断后,即进行策略空间的合理检索,才能求解得出博弈方的均衡策略解。

(3)信息(information):对于环境、其他参与人的特征和行动的知识。信息集(information set)是博弈论中描述参与人信息特征的一个基本概念,可以被理解为参与人在特定时刻有关变量值的知识,一个参与人无法准确知道的变量的全体属于一个信息集。

共同知识(common knowledge)是与信息有关的重要概念。“共同知识指的是所有参与人知道,并且所有参与人知道所有参与人知道…”的那部分知识。除共同知识外,参与人还不同程度地享有私人信息,这也同

时构成了博弈双方的不确定信息。

(4)行动和行动序列(Sequence):行动是参与人在博弈的某个时空点的决策变量。行动可能是离散的或者连续的,但它一定是有序的。即参与者采取行动都存在顺序(Sequence)。在动态博弈中,同样的参与人,同样的行动集合,行动的顺序不同,每个参与人的最优选择就不同,博弈的结果就不同。特别是在动态博弈过程中,不同参与人行动有先后关系,其决策是不同时间点上的变量。由于双方在采取行动前的信息量不同,因此其最终结果与静态博弈结果不相同。信息安全攻防过程中,攻防双方的纳什均衡有时不止一个,而只有一种情况在实际中会发生。

(5)效用函数(Utility):效用函数是指在特定的战略组合下参与人得到的确定效用水平,或者是指参与人得到的期望效用水平。任何参与人的目标都是选择战略,使得其期望效用函数最大化。

博弈论最重要的一个特征就是强调个体理性,即在给定约束条件下,追求个体效用函数的最大化。而同时任何个体效用水平不仅取决于自己的战略选择,而且取决于所有其他参与人的战略选择。

3.2 攻防博弈的一般模型

博弈论模型是对各种现实生活状况抽象概括,可为探讨博弈论在信息安全攻防中应用的可行性提供理论基础。由于网络拓扑异构、应用平台异构、防御者和攻击者的类型差异等诸多原因给网络信息带来了极大的不确定性、模糊性和不完整性,而且攻防双方对于网络环境和对方行为等信息的获取方法存在客观差异,它们的博弈过程属于不完全信息动态博弈,其相应得到的均衡为精炼贝叶斯均衡^[10]。根据博弈理论,精炼贝叶斯均衡是在不完全信息的情况下,重复多次静态博弈得到的结果,结合贝叶斯均衡、子博弈精炼均衡和贝叶斯推断方法可计算得到问题的解。

根据上述博弈模型的五要素,构建了开放式的网络攻防博弈的一般模型,如图1所示。

3.3 信息安全攻防博弈模型

信息安全攻防博弈模型就是描绘攻防双方通过控制相关的攻防技术与管理而展开博弈的过程,博弈的是信息系统的脆弱性。

攻击方与防御方的策略相互影响、互动是攻防对抗模型的基本假定。作为攻击方,通过提高攻击能力运用各种攻击技术,发现、利用对方网络系统的脆弱

性,增加防御方网络系统的安全风险,增大攻击成功的可能性,但同时也受防御方和环境影响而存在不确定性;作为防御方,通过提高防御水平运用各种防御技术发现、弥补己方网络系统的脆弱性以降低安全风险并减小受攻击的可能性,但同时也受攻击方和环境影响而存在不确定性^[11]。

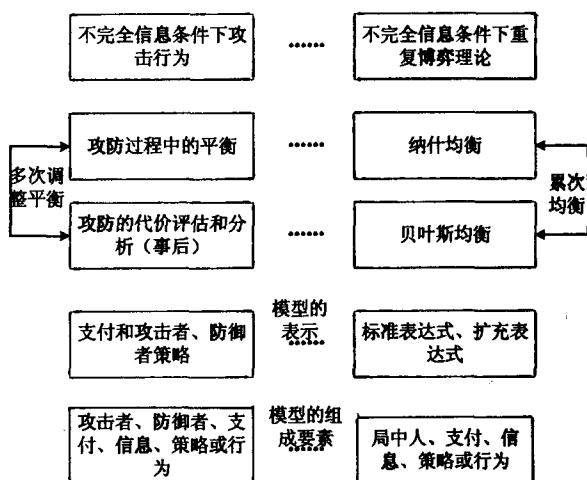


图1 攻防博弈的一般模型

根据攻防双方的上述博弈过程,构建信息安全攻防对抗模型,如图2所示。博弈过程不仅是对抗双方选择策略进行博弈的过程,也是不断获取并修正信息,甚至改变(调整)效用的过程,因此可以说是一个带有对抗性质的实时动态决策过程。

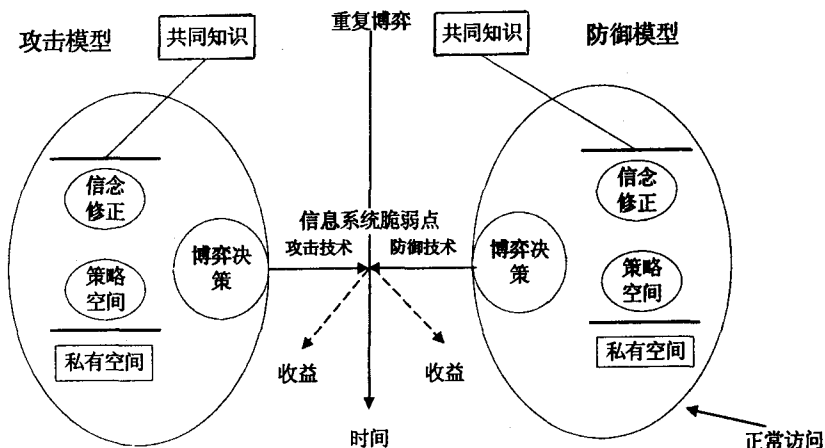


图2 信息安全攻防博弈模型

4 博弈过程分析

攻防的过程就是攻击者与防御者的博弈过程,攻击者和防御者是一种非合作博弈,其根本原则就是使成本(损失)最小化或赢得(利益)最大化,并由此确定己方的行为策略。具体而言,对攻击者来说,无论防御者采取何种防护策略,攻击者总希望采用一种合适的混合策略达到攻击的目的;而同时,防御者也总是希望

找到一种合适的混合策略来防御攻击者。

根据上述博弈模型要素分析,将信息安全概括为攻防双方的动态博弈过程。假设黑客攻击行为 A^1 ,防御方行为 A^2 ,这个随机博弈模型可用如下五元组进行描述:

$$G = (S, A^1, A^2, Q, R^1, R^2, \beta)$$

其中 $S = (\xi_1, \xi_2, \dots, \xi_i, \dots, \xi_N)$ 是网络时空变化的状态集,博弈不断地由一个状态转换到下一个状态; $A^k = \{a_1^k, \dots, a_m^k\} k = 1, 2, M^k = |A^k|$ 表示攻防双方的策略集,每次状态转移中采取的策略都是其策略集的某个子集,既可以是纯策略也可可是多策略组合。 $R^k: S \times A^1 \times A^2 \times S \rightarrow \mathcal{R}$ 分别是攻防双方在每次状态转变过程中采取一定策略的效用水平; $Q: S_i \times A_k \times B_k \times S_{i+1} \in [0, 1]$ 为状态转移方程,其由网络状态、攻防双方采取的策略确定; β 是折现率, $(0 < \beta < 1)$ 用于计算未来的收支情况对于参与人当前行为的影响程度,较高的折现率意味着参与人更重视未来收支。

攻防博弈过程描述如下:假设在时刻 t , 博弈处于状态 $S_t \in S$, 攻击方和防御方分别从自己的策略集中选取策略 a_t^1 和 a_t^2 , 这样攻击方和防御方分别获得收益 $R_t^1 = R^1(s_t, a_t^1, a_t^2)$, $R_t^2 = R^2(s_t, a_t^1, a_t^2)$, 然后博弈进入下一状态 S_{t+1} 。根据不完全信息动态博弈理论,在网络动态对抗的环境下,双方当期收益不仅取决于当前状态和这种状态下攻防双方策略以及系统行为,还取决于决策人对于对方类型所做的概率分布判断。假设此时攻击者对防御者类型的概率判断为 $(\mu, 1 - \mu)$, 根据不完全信息博弈理论,其期望收益为 $R_t^1 = R^1(s_t, a_t^1, \mu)$, 同理防御方的期望收益也受到其主观判断的影响。

攻防的动态博弈过程如图 3 所示。对信息系统的访问包括外部用户和内部用户,外部用户分为合法用户和非法用户,内部用户分为按权限访问的正常用户和越权用户。攻击者指外部非法用户和内部越权用户。攻击方有(攻击,不攻击)策略选择,而防御方则有(防御,不防御)策略选择。该博弈的安全均衡稳定是在一种动态过程中达到的,也就是说,防御是一个:被攻击-发现攻击-安全平衡-新的攻击-发现攻击-再平衡,螺旋式上升的过程。

攻防博弈中,攻防双方一个回合接着一个回合的博弈,各自获得各自的成效。双方都不知道攻防什么时候结束。在每一回合中,攻防双方必须基于自己的策略做出决定,以使自己在有效的时间内得到最好的成效。每一回合结束后,对于防御方来讲,要充分总结经验、亡羊补牢,加强预防措施,或变被动为主动,主动

追击攻击者;对于攻击方来讲,要对攻击行为产生的后果进行评估,判断是否达到了攻击目的,是否隐藏了自己的踪迹,是否需要进入下一轮的攻击……

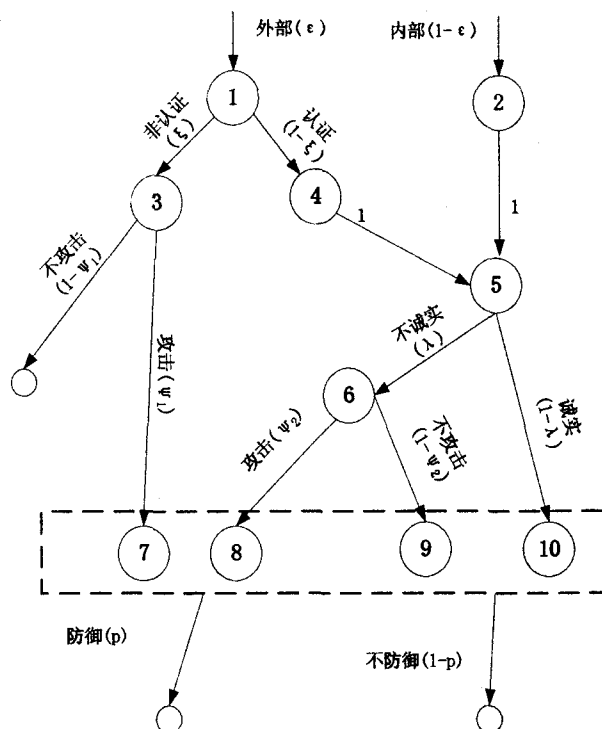


图 3 信息安全攻防的动态博弈过程

5 结束语

从博弈论的观点来看,信息安全实际上是信息保护者(防御方)与入侵者(攻击方)之间的博弈。文中从博弈论的新视角研究信息安全问题,建立了信息安全攻防博弈模型,分析了攻防的博弈过程,为解决现实中的信息安全问题提供了一种新的思路。过去总从防的角度考虑安全问题,如果从攻防博弈的角度考虑,将会带来意想不到的收获。

参考文献:

- [1] 王 跃,罗森林. 信息系统与安全对抗理论[M]. 北京:北京理工大学出版社,2006:79-80.
- [2] 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(4):817-826.
- [3] Hamilton S N, Miller W L, Ott A, et al. The Role of Game Theory in Information Warfare[C]//Proceedings of 4th Information Survivability Workshop. Vancouver, Canada. Washington, DC, USA: IEEE Computer Society Press, 2002: 45-46.
- [4] Syverson P E. A different look at secure distributed Computation[C]//In: Proceedings of the 1997 IEEE Computer Security

```

}
```

只要在三个 return 前加上这段代码:

```

struct list_head * elem1 = (struct list_head *)elem //elem 为当前节点
if(elem1->prev != head){
//前移一个位置
elem1->prev->next = elem1->next;
elem1->next->prev = elem1->prev;
elem1->next = elem1->prev;
elem1->prev = elem1->next->prev;
elem1->prev->next = elem1;
elem1->next->prev = elem1;
//重新设置优先级,保持与原程序的一致性,使得修改不会引起原程序的变化
struct nf_hook_ops * elemprev = (struct nf_hook_ops *)elem1->prev;
struct nf_hook_ops * elemnext = (struct nf_hook_ops *)elem1->next;
(elemprev->priority%2 == 1 && elemnext->priority%2 == 1)? elem->priority = (elemprev->priority/2 + elemnext->priority/2 + 1):(elemprev->priority/2 + elemnext->priority/2);
}
```

3.2 算法测试

本实验的测试环境是在实验室自行搭建的局域网上,在自然使用的条件下测试的。防火墙主机采用的操作系统是 centos5.2, 因为内核模块编程的需要,所以在其上下载了版本是 2.6.18 的内核源代码自己编译安装了一个系统,试验就是在 linux-2.6.18 内核上进行的。CPU 是 Intel Celeron 1.60G,内存 0.99G,自适应 10/100M 网卡双网卡。在 filter 模块的钩子点 NF_IP_FORWARD 设置了 200 条规则,并在上面加载了 20 个实现单一功能的 hook 函数模块。还编写了一个统计模块 statist.ko,用来统计每个 hook 函数返回非 NF_ACCEPT 的次数和每条规则匹配的次數。通过一段时间的自然使用,对比了 hook 函数返回非 NF-

ACCEPT 的次數和 hook 函数在 hook 函数链表中的位置,发现返回非 NF_ACCEPT 的次數越多,相应 hook 函数的位置越靠前。同样规则的匹配次數越多,位置越靠前。与预期一样,证明算法是有效的。

4 结束语

Netfilter 被认为是一个非常强大的内核防火墙系统。但是由于其规则匹配和 hook 函数调用都采用线性的方式,当规则集很大,挂载的钩子函数较多时,其性能会有明显的降低。我们的算法通过让防火墙根据环境自适应的动态调整规则和 hook 函数的次序,减少了规则匹配的次數和 hook 函数“无效”调用的次數,从而提高了防火墙的效率。当然,提高 Netfilter 效率的还有其他的方法,比如防火墙的体系结构,防火墙的负载均衡等。

参考文献:

- [1] 倪继利. linux 安全体系分析与编程[M]. 北京:电子工业出版社,2007.
- [2] 朱立才,杨寿保,宋舜宏. Netfilter/iptables 防火墙性能优化方案与实现[J]. 计算机工程与应用,2006,42(15):117-120.
- [3] Baba T, Matsuda S. Tracing Network Attacks to Their Sources[J]. IEEE Internet Computing, 2002,62(2):107-109.
- [4] 毛德操,胡希明. Linux 内核源代码情景分析[M]. 杭州:浙江大学出版社,2006.
- [5] 博嘉科技. linux 防火墙技术探秘[M]. 北京:国防工业出版社,2002.
- [6] 王丽辉,李涛,张晓平,等. 一种联动防火墙的网络入侵检测系统[J]. 计算机应用研究,2006,23(3):95-97.
- [7] Bllovin S M. Security problems in the TCP IP protocol suite[J]. Computer Communications Review, 1998,92(2):81-83.
- [8] Steven M B, William R C. Network Firewalls[J]. IEEE Communications, 1994,9(9):67-69.

(上接第 162 页)

ty Foundations Workshop. Washington, DC, USA: IEEE Computer Society,1997:109-115.

- [5] Lye Kong-wei, Jeannette M W. Game strategies in network security[J]. International Journal of Information Security, 2005,4(1-2):71-86.
- [6] 孙薇,孔祥维,何德全,等. 基于演化博弈论的信息安全攻防问题研究[J]. 情报科学,2008(9):1408-1412.
- [7] 朱建明, Raghunathan S. 基于博弈论的信息安全技术评价模型[J]. 计算机学报,2009(4):828-834.

- [8] 贾春福,钟安鸣,张炜,等. 网络安全不完全信息动态博弈模型[J]. 计算机研究与发展,2006,43(22):530-533.
- [9] 谢识予. 经济博弈论[M]. 第2版. 上海:复旦大学出版社,2002:20-41.
- [10] 曹晖,王青青,马义忠. 基于动态贝叶斯博弈的攻击预测模型[J]. 计算机应用,2007(6):1545-1547.
- [11] 何宁,卢昱,王磊. 网络控制论在网络攻防中的应用[J]. 武汉大学学报:理学版,2006(5):639-643.