

一种基于 FSA 的网络安全评估模型

邓 磊¹, 高德远¹, 周 雯², 陈付龙²

(1 西北工业大学 计算机学院, 陕西 西安 710072; 2 安徽师范大学 计算机科学与技术系, 安徽 芜湖 241002)

摘 要: 文中建立了一种基于有限状态机(Finite State Automata, FSA)的网络安全评估模型. 根据网络安全模型所涉及的各种安全信息及其相关属性, 用状态来表示攻防双方的安全形势; 用状态迁移表征攻防双方各种行为所带来的安全形势变化; 用状态转移图的形式直观地描绘出安全状态迁移过程. 通过模拟攻击者入侵网络的过程和系统实现安全防御的过程, 验证了该模型的有效性.

关键词: 网络安全对抗; 有限状态机; 状态迁移; 状态转移图

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2013)09-0046-04

A Network Security Evaluation Model Based on FSA

DEND Lei¹, GAO De-yuan¹, ZHOU Wen², CHEN Fu-long²

(1 School of Computer, Northwestern Polytechnical University, Xi'an 710054, China;

2 Department of Computer Science and Technology, Anhui Normal University, Wuhu 241002, China)

Abstract: A network security evaluation model based on Finite State Automata (FSA) is proposed. According to all kinds of security information and its related properties in the model, the states are used to indicate the security situation of both attack side and defense side; the state transitions are used to indicate the dynamic security situation of the action for both attack side and defense side; the transition diagram is used to describe the transition processes of security status. Experimental results show that the model is more suitable for Network security modeling with simulating the intrusion processes of attackers and the security defense process.

Key words: network security confrontation; FSA; state transition; state transition diagram

1 引言

随着网络的开放性、互联性、动态性和复杂性不断增加, 网络入侵事件也急剧增多. 因此, 评估网络安全风险成为网络安全研究的一个重要方面^[1]. 近年来比较流行的网络安全模型有: 攻击树模型和攻击网模型, Petri 网、UML 等技术均被应用在评估网络安全中^[2].

有限状态自动机^[3] (Finite State Automata, FSA) 是具有离散输入和输出系统的数学模型之一, 常用来建立拥有有限个状态的系统模型.

本文通过分析动态变化的网络空间中安全问题

的攻防对抗本质, 以形式化的方法表征网络安全对抗中各种安全事件的关系及其对网络安全状态的影响, 反映网络安全对抗中安全状态的变迁过程及其变化规律, 提出了基于 FSA 的网络安全评估模型.

2 FSA 网络安全评估模型

计算机网络空间中的攻击和防御是一个动态变化的对抗过程, 双方通过实施各种行为推动安全平衡状态的不断变化. 在任意确定时刻, 均存在某种确定的状态与系统相对应, 且系统运行状态只有有限种, 最终均将处于一种终止状态. 因此, 用有限自动机描述和构造网络安全模型, 能够模拟网络系统的

收稿日期: 2012-11-20; **修回日期:** 2012-12-22

基金项目: 安徽省自然科学基金(1308085QF118); 教育部人文社会科学基金资助项目(11YJ880119); 安徽师范大学创新基金项目(2011cxjj01); 安徽师范大学博士科研启动基金项目(132-151201)

运行状态及其动态迁移,尤其是由各种安全事件导致的安全状态转移。

2.1 安全评估模型的形式化描述

定义1 基于FSA的网络安全模型

将网络安全模型描述为一个确定的有限状态自动机^[4]:

$$M=(S,E,\lambda,\delta,S_0,S_F) \quad (1)$$

其中:

(1) $S=\{s_0,s_1,\dots,s_n\}$ 为状态的有限集合,描述研究对象所处的状态;

(2) $E=\{e_0,e_1,\dots,e_m\}$ 为原子事件的非空有限集合。 E 中的事件会导致系统发生状态转移;

(3) $\lambda=\{n,a,r\}$ 为事件标识集合,用来标记发生事件的类型: $\lambda=n$,表示正常访问事件; $\lambda=a$,表示恶意攻击事件; $\lambda=r$,表示攻击响应或恢复事件;

(4) $\delta:S\times E\rightarrow S$ 为 M 的安全状态转移函数。根据事件类型的不同,确定安全状态转移的方向;

(5) $S_0\subseteq S$ 为系统的初始状态集。在每个特定的运行周期,系统都是从某个确定的状态开始运行的,这个状态就是目标网络或攻击者的起始状态;

(6) $S_F\subseteq S$ 为终止状态/接受状态的集合,根据所研究对象定义不同的内容。

当模拟和分析攻击者的入侵过程时, $S_F\subseteq OS$,表示攻击目标实现的成功状态集;当研究目标网络的安全属性变化时, $S_F\subseteq DS$,表示安全防护的目标状态集。

2.2 安全状态分析

状态集 S 定义了目标网络或者攻击者在网络运行过程中的实时状态,通过所研究对象的属性来描述和体现。可将状态集分成两种情况:系统状态集 DS 和入侵状态集 OS 。

(1) 系统状态 DS

系统安全状态由网络实体的属性集合来确定。在时刻 τ 将实体主机的状态表示为: $s^\tau(h)=\{h_{id}, h_{type}, h_{address}, h_{OS}, h_{assets}, h_{servs}, h_{vuls}\}$ 。

(2) 入侵状态 OS

入侵状态表征攻击者成功执行攻击行为后的状态。攻击者入侵网络的过程,就是攻击方和防御方的状态迁移过程,在这个过程中,不仅系统的安全状态在改变,而且入侵状态也在不断发生变化。入侵状态集合定义为 OS 。

3 基于FSA的网络安全模型实例与分析

本实例为实验室的局域网,地址范围为 192.168.

65.1~192.168.65.150。局域网通过路由器与外网连接,内部网有一台 WWW Server(Z)。正常情况下,局域网内各主机之间可以互相访问,但外部主机需经过防火墙和 IDS 的过滤才能进入内网,如图 1 所示。

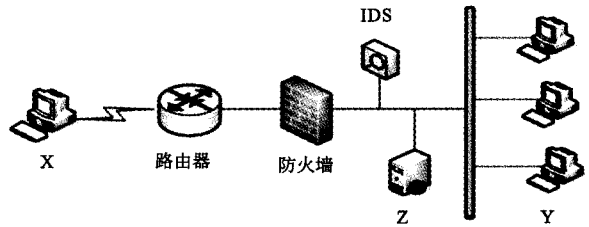


图1 实验网络的拓扑结构图

现有一个外部攻击者,企图通过控制 Z 达到摧毁网络的目的。从一台已被攻破的主机 X ,通过反复扫描和探测,获取了目标主机 Z 的信任关系列表,并试图与其中的一台被信任主机 Y 利用非法手段使 Y 丧失正常工作能力,目的是冒充 Y 的 IP 地址入侵 Z 。方法是,冒充 Y 发送伪造的 TCP 请求包,与 Z 建立三次握手连接,获得 Z 的访问权限,并向 Z 植入后门程序,达到完全控制 Z 的目的。

3.1 目标网络配置和攻击信息

(1) 本实例的主机集合为:

$$HOST=\{X,Y,Z,\dots\}.$$

(2) 本例中所涉及主机的属性描述见表 1。

(3) 主机之间的连接关系

①网络访问关系:

$$CONT=\{(X,Y,\{http,r\log in,RPC\}), (X,Z,\{http\}), (Y,Z,\{http,IIS\}), L\}.$$

②信任关系: $TRST=\{(Z,Y), L\}$ 。

(4) 安全属性要求及攻击目标

访问控制策略集合:

$$ACS=\{(Y,Z,user), (X,Z,none), (X,Y,access), \dots\}$$

入侵者的初始权限集合:

$$PX=\{privil(X,Y)=access, privil(X,Z)=none\}$$

入侵目标:

$$Gattack=G1\cap G2=EF(privil(Y,Z)=none) \cap EF(privil(X,Z)=root)$$

入侵目标中隐含了攻击目标机的两个步骤:第一步是破坏信任主机 Y 的可用性需求,使之无法接受和处理正常的访问请求;第二步是破坏目标主机 Z 的机密性和完整性需求,获取对于目标主机 Z 的非法访问权限。

表 1 实验网络的主机初始状态的属性列表

Host_id	Host_type	Host_address	Host_OS	host_serve	Host_vuls
X	PC	未知	Windows XP	未知	无
Y	Workstation	192.168.65.116	Windows XP	http, RPC, FTP, Rlogin	CVE-2005-0688 CAN-2003-0352 CVE-1999-0651
Z	Web Server	192.168.65.10	Windows 2003 server	IIS, http, Rlogin, RPC	CVE-1999-0651 CAN-2003-0352

3.2 实验网络的安全模型

实例网络的有限自动机安全模型为: $M=(S, E, \lambda, \delta, S_0, S_F)$.

(1) 事件集: $E=E_A \cup E_N \cup E_R$.

① 异常事件集合: $E_A = \{ae_1, ae_2, ae_3, ae_4, ae_5, \dots\}$.

Probe(探测类攻击):

$ae_1 = (finger, X, (Y, Z))$

$ae_2 = (showmount, X, (Y, Z))$

$ae_3 = (rpcinfo, X, (Y, Z))$

DoS(拒绝服务类攻击):

$ae_4 = (LAND, X, Y)$

$ae_5 = (SYN-Flooding, X, Y)$

$ae_6 = (DDos, X, Y)$

FakeConnection 攻击:

$ae_7 = (FakeConnection(fakeY), XZ)$

RemoteCommand 攻击:

$ae_8 = (RemoteCommand(fakeY), XZ)$

② 正常事件集合: $E_N = \{ne_1, ne_2, ne_3, \dots\}$.

③ 响应事件集合: $E_R = \{re_1, re_2, re_3, re_4, \dots\}$,

如表 2 所示.

(2) 状态集: $S = \{\{s_0, s_m\}, \{s_{aj}\}, \{s_{fl}\}, I, J, L = 1, 2, \dots\}$, 其中初始状态集 $S_0 = \{s_0\}$, 终止状态集 $S_F = \{s_{ak}, s_{fl}, s_0, \dots\}$.

3.3 实验网络安全状态分析

实例中的攻击者试图对内部网实施 IP Spoofing 攻击, 其过程包括^[5]: ①通过探测目标网络, 确定可以被欺骗的目标主机和一个目标主机信任的主机及其信任模式; ②通过 DoS 攻击破坏被信任主机的可用性, 使之丧失正常工作能力; ③通过猜测目标主机的 TCP 序列号, 伪装成被信任主机, 远程连接目标主机; ④利用获得的非法连接和访问权限, 在目标主机上放置后门, 达到完全控制目标主机的最终目的. 实例网络的安全对抗示意图如图 2 所示.

由图 2 可见, 攻防双方的行为形成一个动态变化的对抗过程. 不仅网络实体在日常访问和交互过程中, 时刻都有被侵犯和泄露的危险, 同时, 攻击者

表 2 异常事件的主要响应策略列表

E_A	E_R	主要内容
ae_1	re_1	(a) 修补主机 Y、Z 上关于 Rlogin 的漏洞; (b) 废除基于地址认证建立的主机信任关系; 删除所有. rhosts 文件, 并清空/etc/hosts.equiv 文件, 然后禁用 r 一类的远程调用命令.
ae_2	re_2	(a) 设置防火墙及包过滤规则, 配置边界路由器, 安装过滤器, 检查并禁止来自外网、但源 IP 地址为内网 IP 地址的数据包; (b) 丢弃不符合过滤规则的非法数据包; (c) 修补漏洞 CVE-2005-0688.
ae_3	re_3	(a) 重置被攻击主机上的所有半请求状态连接, 并设置半请求连接的最大数目; (b) 设置防火墙过滤规则, 过滤并丢弃 TCP Syn-Flooding 报文; (c) 修补漏洞 CVE-2002-0283.
ae_4	re_4	(a) 防止 TCP 序列号被猜测成功, 如: 增加初始序列号的增长速率, 增加攻击者对序列号的搜索难度; 使用随机化产生的初始序列号. (b) 用网络监听工具监测并分析数据包的源和目的 IP 地址. (c) 修补 Z 上的相应漏洞, 关闭被入侵的端口.
ae_5	re_5	防止攻击者利用建立好的连接和获得的 root 权限向目标机发送数据和远程执行代码. 如: (a) 为漏洞 CAN-2003-0352 安装补丁程序, 封堵 135 端口; (b) 关闭已经被入侵的端口(如 512, 513, 514 等), 禁用 r 命令
ae_6	re_6	安装漏洞补丁程序
ae_7	re_7	人工方法进行强制修复, 如增加内存、重新配置系统参数、重启等, 使系统回到初始状态
ae_8	re_8	
ae_9	re_9	

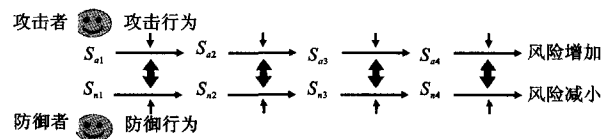


图 2 实例网络的安全对抗示意图

在入侵过程的每个环节上也时刻存在被防范和阻断的威胁. 在这个过程中, 哪一方获取的信息更多更早, 哪一方实施的行为在先, 哪一方就获得更大的优势和获胜主动权.

3.4 模型比较与分析

将本文的网络安全建模方法与近年来比较流行的攻击树模型和攻击网模型进行比较, 如图 3、图 4 和图 5 所示.

可见图 3 和图 4 都侧重于描述多阶段攻击中的

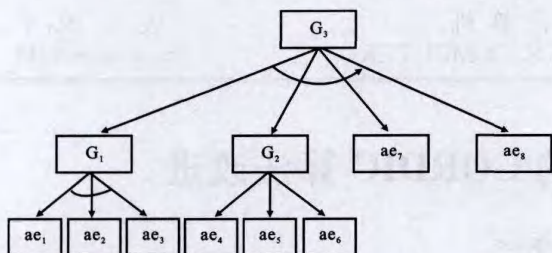


图3 实例网络中入侵行为的攻击树模型

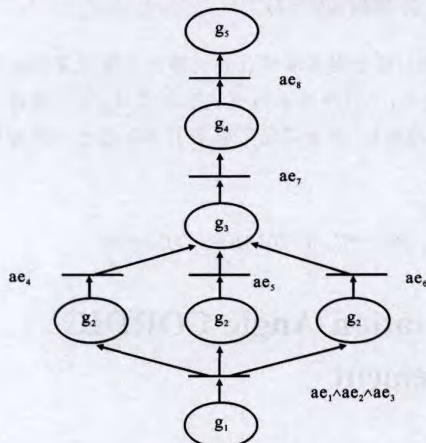


图4 实例网络中入侵行为的攻击网模型

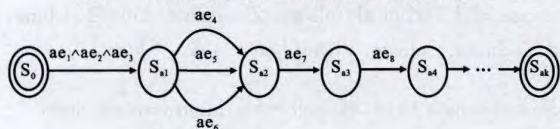


图5 实例网络中入侵行为的安全状态转移图

攻击行为及其逻辑关系,而没有将攻击过程和实现方法与具体的目标网络配置相关联,因此也就不能反映攻击行为对特定目标系统造成的影响和危害,不能直接用于网络安全评估。图5的模型不仅描述了攻击过程和过程实现中使用的攻击方法,而且强调了每一阶段的攻击行为给特定目标网络及其实体带来的安全改变,充分体现了攻击行为的过程特征和威胁特性。

4 结束语

基于FSA的网络安全评估模型主要为解决网络安全对抗中双方各种行为建模问题而提出的,它结合了FSA技术的优点,安全描述能力更强,适用于网络安全风险的分析和评估,也可以帮助管理员实现安全决策、攻击响应和入侵预测等。

参考文献:

- [1] 孙强,陈伟,王东红,等.信息安全管理:全球最佳实务与实施指南[M].北京:清华大学出版社,2004.

- [2] Ray I, Poolsapassit N. Using attack trees to identify malicious attacks from authorized insiders[C]// Proceeding of the 10th European Symposium on Research in Computer Security. Milan, Italy: Springer-Verlag, 2005:231-246.
- [3] Castro L N de, Timmis J. Artificial immune systems: a novel paradigm to pattern recognition[C]//Artificial Neural Networks in Pattern Recognition. Springer Verlag, University of Paisley, UK; 2002(2):67-84.
- [4] Wei Li. A genetic algorithm approach to network intrusion detection [EB/OL]. (2003-11-5). [2013-5-1]. <http://www.giac.org/paper/gsec/3703/genetic-algorithm-approach-network-intrusion-detection/105794>.
- [5] Robert Meyer, Michel Cukier. Assessing the attack threat due to IRC channels[C]//Proceedings of the 2006 International Conference on Dependable Systems and NetworkS. Philadelphia, PA, USA: IEEE Computer Society, 2006:467-472.

作者简介:



邓磊男, (1976-), 博士研究生。研究方向为网络安全。

高德远男, (1946-), 教授, 博士生导师。研究方向为计算机体系结构、微处理器设计和VLSI系统设计。



周雯女, (1989-), 硕士研究生。研究方向为嵌入式计算与普适计算、信息安全。



陈付龙男, (1977-), 博士, 副教授。研究方向为嵌入式计算与普适计算、信息物理融合系统。