第7卷第1期　　空 军 工 程 大 学 学 报(自然科学版)　　Vol. 7 No. 1
2006年2月　　JOURNAL OF AIR FORCE ENGINEERING UNIVERSITY(NATURAL SCIENCE EDITION)　　Feb. 2006

基于有限状态机的多阶段网络攻击方法研究

王英梅[1]，　程湘云[1]，　刘增良[2]
(1. 北京科技大学 信息工程学院，北京　100083;2. 国防大学，北京　100011)

摘　要:提出了针对多阶段攻击分析的多阶段有限状态机模型,用于分析复杂的攻击行为。通过M-FSM模型能够对攻击的步骤和路径进行综合分析,从而发现网络中存在的安全漏洞和不当的安全配置。在对多阶段攻击进行综合分析的基础上,系统管理员可以以最小的投入对系统进行加固。

关键词:攻击模型;多阶段攻击;有限状态机;风险评估
中图分类号: TP393.08　　**文献标识码**:A　　**文章编号**:1009-3516(2006)01-0031-04

目前大多数网络安防方法是被动的,都是在安全事件发生后才处理,像防火墙和入侵监测系统这样的边界设备都需要在完全了解网络攻击特点的基础上继续完善,以满足新的网络服务的需求。但是,现阶段分析网络威胁和预测网络面临风险的能力非常有限。识别新的安全漏洞和新的入侵并把这些信息融入到对威胁评估的过程中还需要很长时间。在很多情况下,威胁评估由于缺少对网络安全事件驱动因素的了解变得很有限。为了了解大规模攻击所造成的影响以及如何有效制定不同的安全响应策略,建立网络攻击模型是非常重要的。通常情况下对于计算机攻击是单独建模的,比如在入侵监测系统中,通过警报来报告每个攻击[1]。但是,真正的入侵事件经常是由一系列相互独立的攻击步骤组合而成,并且每一步都是被我们所知的典型攻击方式。随着对企业和政府系统的协作式、多阶段的攻击事件越来越多,了解复杂的攻击类型、攻击模式,建立完善的攻击模型变得更加紧迫。本文提出一种多阶段有限状态机模型来分析网络攻击。这一模型将单个模型化的攻击结合到一起,能够发现攻击者对特定攻击目标的路径。通过这一模型,使网络安全管理员在分析攻击路径的基础上,制定优化策略对网络环境进行加固。

1　网络攻击模型的研究

目前在攻击建模方面的研究大部分集中在攻击类型的划分和漏洞的分类上[2,3],这些分类研究在实践上非常有用并且为更深一步的研究奠定基础,不足的是这些分类不能系统的表示协作攻击和分布式攻击的集成特性。一些攻击模型是利用分布式资源(系统)收集的信息来建立的,他们集中研究从分布式网络扫描器获得数据的某一种攻击模型。JIGSAW[4]描述了根据攻击能力来描述攻击组成的一种工具。在攻击模型的建立过程中,大多数基于图的形式。从简单的树状模型到更正式一些的 petri 网模型,图的描述能够抓住一个成功攻击的每个环节。以图的方式来描述攻击模型区别于其他攻击模型的地方是攻击者所采取的视点不同。由于攻击者的目标和方法在几乎所有安全条件下扮演着非常重要的角色,攻击模型越接近于这一问题,对于在新的系统中发现漏洞、在软件开发期避免漏洞的产生,以及对于已知漏洞评估和网络安全风险评估都有很大的作用。文献[5]描述了用故障树方法对攻击建模的例子。每个树有一个顶节点,代表攻击的最终目标的实现。子节点表示为达到其父节点的攻击目的而必须发生的攻击行为。但是使用攻击树方法不能描述一个攻击需要的先决条件,另外攻击行为和结果状态在一个节点上记录容易导致模糊节点标记。

收稿日期:2005-06-13
基金项目:国家自然科学基金资助项目(60572162)
作者简介:王英梅(1974-),女,河北唐山人,博士生,主要从事网络安全研究.

2 用多阶段有限状态机模型(M - FSM)分析网络攻击

本文在分析网络攻击特点的基础上,认为网络系统遭到攻击的前后为不同的状态,利用有限状态机的原理对多阶段的网络攻击进行建模,形成网络攻击多阶段有限状态机模型(Multi - stage Finite State Machine Model ,M - FSM)。使用有限状态机能够描述一个攻击发生后系统的变化。一个错误/故意的操作造成的系统状态的改变将会给下一次攻击制造机会。M - FSM 的目的是探寻每一步的操作,更准确地说是分析为达到整个攻击目的,在整个操作中每一步的行为。换句话说,分析这个模型为的是发现针对关键网络资源的攻击路径。从这些攻击路径能够根据最初的网络系统配置产生一个配置表达式用于分析网络安全的需要。根据这个表达式,可以对如何加固网络防止攻击做出决策。为了这个目的,模型建立采取 3 个步骤:①将每个阶段的行为表示成一个原子有限状态机(atom FSM, aFSM),它表示一个机器上攻击的输出,这样可将一个达到某一目标的若干操作描述成一系列原子有限状态机(aFSM);②将一系列操作联系起来描述攻击行为;(3)简化 M - FSM 产生表达式。

M - FSM 模型结构如图 1 所示。原子有限状态机 aFSM 包括一个转换和两个状态。转换描述针对一个计算机或系统的一个攻击行为。两个状态为:①初始状态(precondition):系统存在一个攻击可以利用的漏洞,②结果状态(postcondition):被攻击后的状态,比如,此时系统可能有不必要的端口被非法打开。因为每个单独的行为都可以用初始状态、结果状态表示出来,因此很容易建立相应的原子有限状态机(aFSM)。然后将 aFSM 结合,描述成 M - FSM 对误操作和可能的攻击行为建模。在建立 M - FSM 后,根据攻击和条件的依存关系(通过初始状态和结果状态)的直接描述能够计算出攻击路径。

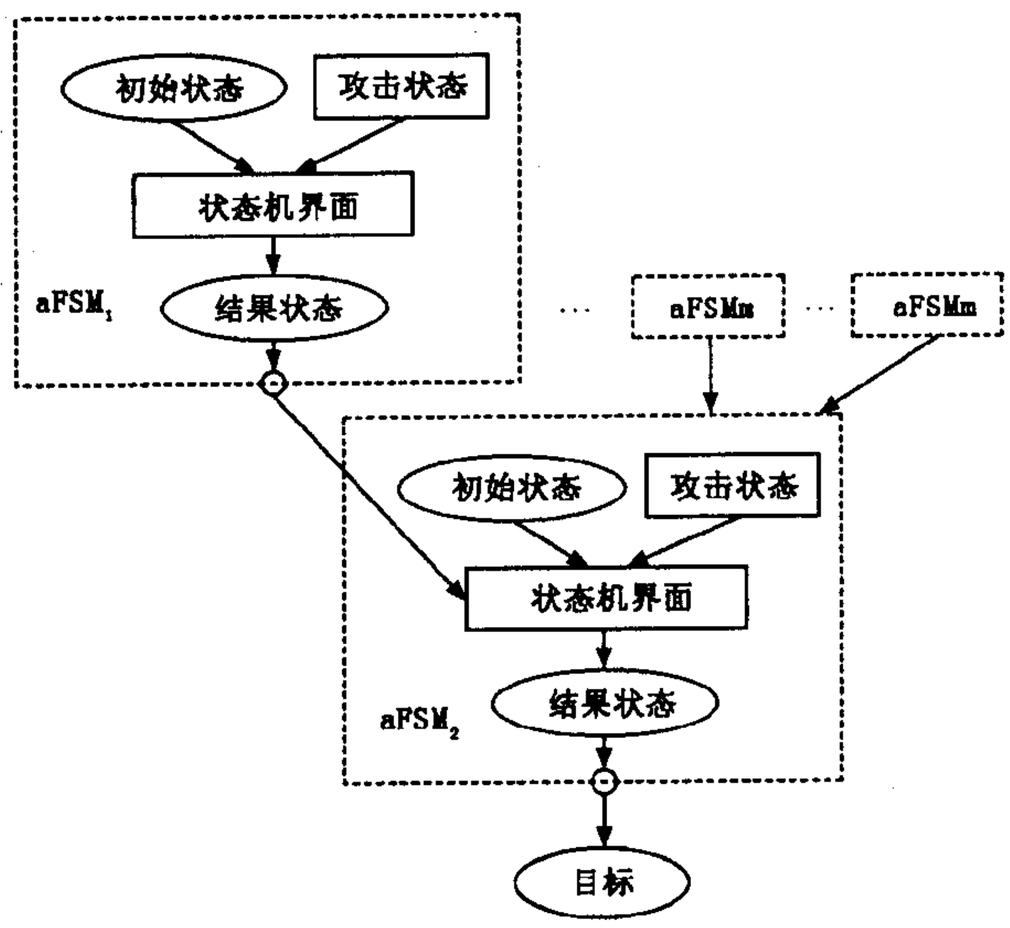

图 1 M - FSM 模型

网络攻击模型能够通过一系列步骤建立起来:首先,发现最初的攻击条件 Einit,从初始攻击状态建立一个有限状态图 Ginit。如果可能,能够建立所有的攻击集合 Eexec,这些攻击是被攻击者成功执行的。这个集合将帮助自动建立攻击模型图。于是,从攻击初始条件 Einit,找到攻击行为 Eexec,该攻击行为的初始条件或其中一个攻击条件与 Einit 的结果状态匹配。通过寻找 Eexec,可以持续地为有限状态图 Ginit 增加原子状态。最终,图 Ginit 描述从初始状态 Einit 向前发展的情况,也就是图中的攻击结果是由 Einit 可达到的。同时,能够将使攻击实现的初始状态在图中表示。在多阶段有限状态机模型建立之后,明确了元素间(初始状态、攻击、结果状态)的关系。由于元素间的相互依赖关系,将该图称为依靠图。接下来,对前向可达的依靠图进行简化,相同的状态机的界面被合并。依靠图是由必需的、足够的攻击集构成的完备集,也就是,由所有被执行的攻击行为和为达到攻击目的的所有攻击构成,任何对攻击行为的增加和删减都会影响结果。因此依靠图描述最小化的攻击路径的集合,最小化的攻击集合就是如果在这个图中去掉任何一个攻击都会影响整个攻击结果。最后,在此基础上就可以仅考虑安全的配置问题。换句话说,初始状态和一系列原子状态机构成了简化的依靠图。于是,这里可以看作一个安全配置的表达式产生了。这个分析过程产生了所有可能的加固安防措施(初始状态分布的集合表示出了已采取的安全手段),并且对网络服务的影响最小。安全分析人员可以比较不同的措施选择一个最好的组合。

3 应用案例

本部分通过一个例子描述如何使用 M - FSM 发现网络中达到一个特定目标的攻击路径。通过分析 M - FSM 结果来决定加固网络安防的最佳方式。试验环境是由一个网络服务器(安装 Windows NT4.0,IIS)、一个邮件服务器(安装 Linux 系统,使用 ssh,wu - ftp 协议)构成,两个服务器通过集线器相连。防火墙通过

策略将他们与外网分离。在本实验中,攻击目标是获得一个邮件服务器的根目录(root)的访问权限。但是,为了获得它,攻击者必须越过防火墙,该防火墙保护邮件服务器和支持公共网络访问的计算机。公共网络服务器安装了 Microsoft 的 IIS,发送邮件服务器是 Linux 操作系统使用 SSH 和 Wu - ftpd。防火墙执行策略包括:进入网络的连接仅允许进入网络服务器,网络服务器运行 IIS,进入的邮件允许进入发邮件服务器,进入的 FTP 流量被阻断。这个例子显示了一个存在漏洞的服务在直接访问被阻断的情况下是如何被利用的。通过分析,最初的攻击位置是发生在攻击机,被定义为初始状态。通过列出所有可能的从给定计算机到其他目的计算机的连接,网络连接被表示在计算机级。防火墙减少了每台计算机连接列表的大小。这里仅测试是否能够在邮件服务器上获得使用超级用户权限执行访问。

图 2 描述了这个例子的结果 M - FSM 模型。尽管设计出防火墙策略来保护邮件服务器,但外部攻击者仍能够获得超级用户的权限执行对邮件服务器的访问。攻击模型表示了最初利用网络服务器上的 IIS 漏洞最终导致邮件服务器被攻击的情况。IIS 远程数据服务漏洞使攻击者能够在网络服务器上执行程序。由于 IIS 远程数据服务漏洞提供的通道,网络服务器上的远程拷贝程序被执行,可以从攻击机上下载一个 rootkit。于是 Rootkit 中的 port - forwarding 程序被执行,安装一个通过网络服务器从攻击机到发送邮件服务器的 ftp 服务的通道。最终,wu - ftpd 的攻击代码被执行通过前向的连接而不是通过发邮件服务器获得了那里根目录的访问权限。通过 M - FSM 模型,能够迅速的根据初始条件计算出攻击目标条件的表达式。建立攻击模型的目的是寻找到最佳的方式来发现网络中的漏洞并且对其进行防护。接下来推导公式从中发现对网络加固的方法。我们最集中关心的事情是什么使得攻击发生(什么使连接产生),对 M - FSM 根据初始条件进行简化,网络服务器在存在条件 C1、C2、C3 的情况下才能使攻击进一步进行,因此状态 C1、C2、C3 是不可缺少的状态,可以对 aFSM1、aFSM2 进行合并。简化图如图 3 所示。根据简化图,可以发现在同时满足条件 C1、C2、C3、C4 或同时满足 C1、C2、C3、C5 的情况下可以使攻击实现。因此表达式可表示为:Goal = C1C2C3(C4 + C5)。

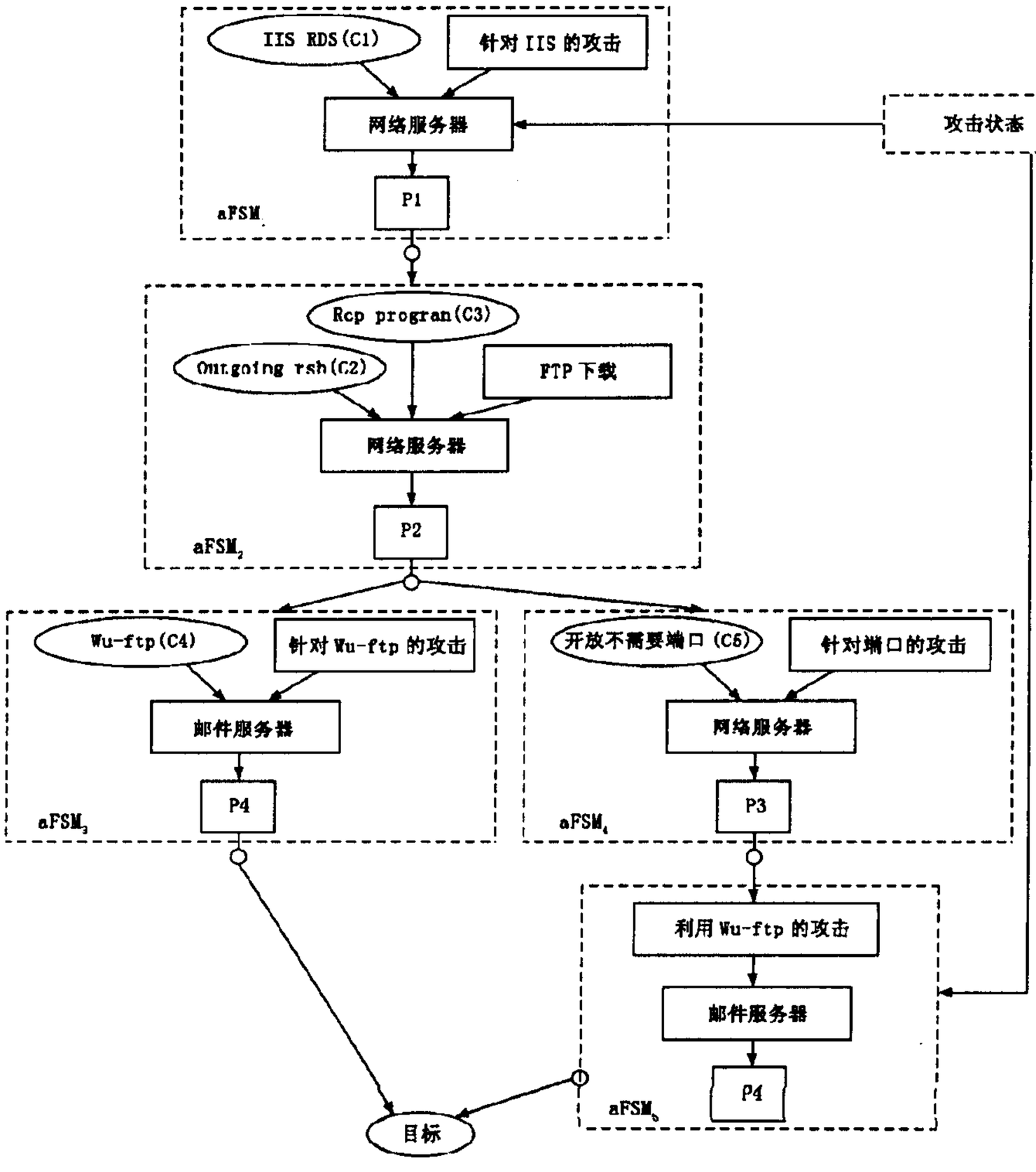

图 2　攻击模型

注:P1:以超级用户权限在受害机器上执行程序的能力;P2:将受害机器上的程序拷入攻击机;P3:攻击者通过中间人的传输层与受害机器连接;P4:在受害机上执行超级用户访问。

通过图 3 和表达式的描述,发现初始条件的两个配置确实提供了网络的安全保护,同时存在其他的安全配置方法:①打补丁或将网络服务器上的 IIS RDS 网络服务禁止(C1);②从网络服务器上禁止输出 RSH (C2);③从网络服务器上移除 RCP 程序(C3);④打补丁或从网络服务器上禁止到邮件服务器得 wu - ftpd (C4),并且关闭网络服务器上所有没有使用的端口(C5)。

如果分开考虑,这 4 个选项每个都开支不大,在没有影响到攻击目标工作的情况下这些加固措施都不能忽略。网络管理员可以基于单个加固措施选择整体费用最小安全管理方法。

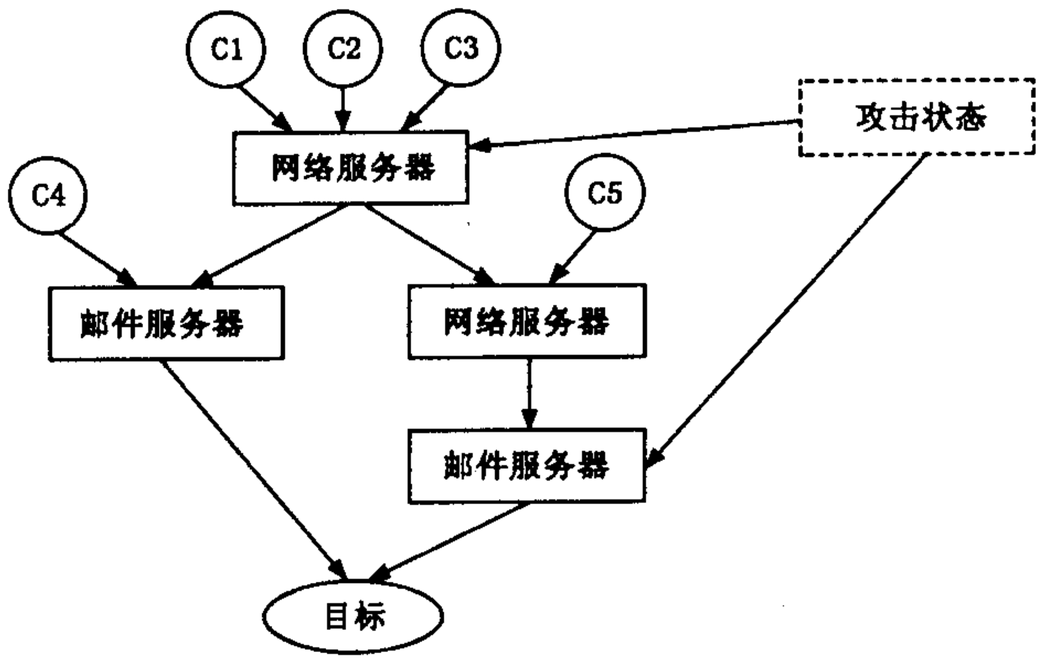

图 3 模型简化图

4 结论

本文提出了一种基于多阶段有限状态机模型的网络攻击分析方法。基于 M - FSM 模型,能够分析网络组成部分的安全依存关系,识别网络系统中存在的漏洞。该模型使网络管理员能够合理的选择网络配置,提供尽可能的安全防范措施,并且使网络加固的费用最小。

参考文献:

[1] 门 健. 网络告警管理系统的设计与测试[J]. 空军工程大学学报(自然科学版),2004,5(4):63 - 66.

[2] Taimur Aslam, Ivan Krsul, Spafford Eugene H. Use of A Taxonomy of Security Faults[A]. Proceeding of the Nineteenth NIST - NCSC National Information Systems Security Conference[C]. Baltimore:1996. 551 - 560.

[3] John Douglas Howard. An Analysis of Security Incidents on the Internet 1989 - 1995[R]. Pittsburgh: Carnegie Mellon University, 1997.

[4] Steven J Templeton, Karl Levitt. A Requires/Provides Model for Computer Attacks[A]. Proceeding of the New Security Paradigms Workshop 2000[C]. New York:2000,31 - 38.

[5] 向 尕,曹元大. 基于攻击分类的攻击树生成算法研究[J]. 北京理工大学学报,2002,23(3):23 - 25.

(编辑:田新华)

The Research for Multi - stage Network Attacks Based on FSM

WANG Ying - mei[1], CHENG Xiang - yun[1], LIU Zeng - liang[2]

(1. College of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China; 2. National Defense Academy, Beijing 100011, China)

Abstract: An M - FSM model is proposed for the multi - stage vulnerable operations. The goal of this M - FSM is to reason how the implemented step - by - step operation, or more precisely each step activity within the whole operation, contributes an attack goal. This model can be used in discovering attack paths to critical network resources. From these attack paths the system administrator can then derive an expression for network safety in terms of the initial configuration and take measures to reinforce the network.

Key words: attack model; multi - stage attack; finite state machine; risk assessment