面向 Web 服务安全的 SCIT 改进模型的研究

申普兵,薛保泽,吴 波,陈树文
(国防科技大学 信息通信学院,陕西 西安 710106)

摘 要:网络空间日趋复杂,原有的网络安全防护手段大多属于被动防御,难以应对当前复杂的网络安全环境,随着 Web 服务的迅速发展,Web 服务系统成为网络攻击的重灾区。针对当前网络的安全防护构建部署固定静态的现状,移动目标防御旨在构建动态不可预知的系统,使防护对象机动化,增加攻击者代价和开销来抵御攻击。借鉴移动目标防御 SCIT (self cleansing intrusion tolerance)模型的思想,为网络 Web 服务系统引入终端运行环境随机化切换,增加终端控制器、终端清洗审计以及终端资源池等模块,增加抵御终端攻击的能力,进一步扩展系统的随机面维度,增加系统随机性。从入侵成功的概率统计来看,攻击面的增加和设计配置的多元,使攻击者入侵成功概率较原有模型平均下降 46.44%,有效增强了系统的安全性。

关键词:网络安全;移动目标防御;Web 服务;SCIT 模型;入侵攻击;攻击面
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2019)09-0092-05
doi:10.3969/j.issn.1673-629X.2019.09.018

Research on Web Services Security Based on SCIT Improved Model

SHEN Pu-bing, XUE Bao-ze, WU Bo, CHEN Shu-wen
(School of Information and Communication, National University of Defense Technology, Xi'an 710106, China)

Abstract: The network space is becoming more and more complex. The original network security means are mostly passive defenses, which is difficult to cope with the current complex network security environment. With the rapid development of Web services, Web service system has become the focus of network attacks. In view of the current situation of fixed and static construction and deployment of network security protection, mobile target defense aims to build a dynamic and unpredictable system, motorizing the protected objects, and increasing the cost and overhead of attackers to resist attacks. Based on the idea of the self cleansing intrusion tolerance (SCIT) model, the improved Web service system is added the client controller, client cleaning audit and client resource pool, randomizing switching in the client operating environment, which increases the ability to resist client attacks and further expand the random dimension of the system. From the perspective of probability statistics, the increase of the attack surface and diversity of the design configuration make the attacker's probability of successful invasions lower than the original model by 46.44%, effectively enhancing the security of the system.

Key words: network security; moving target defense; Web service; SCIT model; intrusion attack; attack surface

0 引 言

当前网络安全事件频发,网络信息安全问题日益突出。现有的网络安全防护手段虽然能够在一定程度上增强网络的安全性,但它依然存在防护手段单一,防护响应被动和部署固定等问题。特别是 Web 服务虽然凭借标准化高、扩展性强以及升级维护简单等优点得以迅速发展,但是系统本身部署静态又具有很强的开放性,极易受到外部的窥探入侵。基于原有 SCIT 安全防护模型虽然能够有效增强服务器抵抗入侵的能力,但对于终端的攻击无能为力,改进模型引入终端运行环境随机化切换可以很好地解决这一问题。

1 移动目标防御技术

针对当前网络配置静态,部署相似以及漏洞持续,导致网络系统处于"漏洞找不尽、补丁打不完、攻击防不住"的被动态势[1-3],美国白宫提出"改变游戏规则"全新的移动目标防御设想。不同于以往的安防构建,该设想并不追求完美无暇的防御体系来对抗攻击,而

收稿日期:2018-11-08 **修回日期**:2019-03-11 **网络出版时间**:2019-04-24
基金项目:国家自然科学基金(61605247)
作者简介:申普兵(1964-),男,教授,研究方向为计算机网络安全;薛保泽(1989-),男,硕士研究生,研究方向为移动目标防御。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20190424.1051.060.html

是通过系统构建部署及策略的多样化,减少脆弱性暴露时间,增加攻击者的难度和代价,进而提高系统的弹性[4]。为此学者们进行了积极的探索。例如,文献[5]提出了基于地址和端口的随机化技术(APOD),利用基于地址和端口的跳变隧道伪装目标主机;文献[6]提出基于 SDN 技术实现 IP 地址的变化,使用虚拟 IP 地址进行通信,实现信息的隐藏;文献[7]在文献[6]基础上将 IP 变化分为高频和低频两种部署嵌套,进而降低变化带来的开销;文献[8]提出 MT6D 技术,利用 IPv6 较大的地址空间,不断改变 IPv6 地址实现主机的隐身;文献[9]提出一种移动目标防御方法,通过私有协议随机化和路径选择随机化策略,提高攻击者实施窃听的难度;文献[10]提出利用自动化编译器产生功能相同但代码不同的程序,为程序生成不同副本,大大增加入侵者成本;文献[11]提出了 SCIT(self cleansing intrusion tolerance)服务器切换模型,通过服务器不断清洗和切换阻断来自外部的攻击。文中在文献[11]提出的 SCIT 服务器模型的基础上进行改良,增加终端控制器、终端清洗审计以及终端资源池等模块,扩展系统的随机面维度,主动防御性能明显增强。

2　网络攻击模型

一次典型的入侵攻击行为一般包括基础信息获取,漏洞扫描,漏洞利用,入侵控制和擦除痕迹等五个步骤,每个入侵步骤都依赖于系统属性和拓扑结构的静态部署。一旦系统属性发生变化,当前入侵行为即被中断,入侵失败。黑客入侵时间与造成的损失满足图 1 的“S”曲线[12-13]。

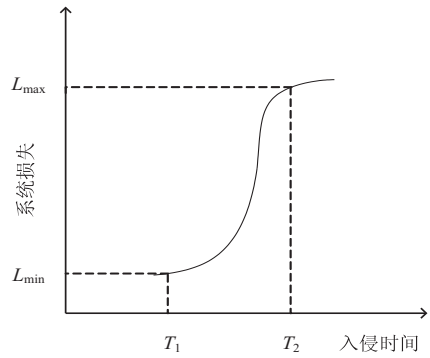

图 1　“S”曲线

由图 1 可知,当攻击者入侵时间 $T < T_1$ 时,损失较小,表明此时黑客正在获取基础信息和漏洞扫描,此时损失处于 L_{min};当攻击时间 $T_1 < T < T_2$,损失随时间呈指数大幅度增长,此时攻击者正在利用权限的提升,控制系统窃取信息;当 $T > T_2$ 时,损失随时间已变化不大,损失趋向高损失门限 L_{max},此时黑客正在进行擦除痕迹等收尾工作。

分析图 2 可知,动态切换系统运行环境可以有效抵御入侵。在 t_0 时刻,系统随机切换运行环境 E_0,并生成防御方案 p_0,则(E_0, p_0)构成网络系统内部环境。两次切换运行环境时间间隔为 t_{t0},对于一次成功的攻击来说,攻击所需时间($t_{i1}+t_{i2}+t_{i3}+t_{i4}+t_{i5}$)$<t_{t0}$,反之当攻击所需时间($t_{i1}+t_{i2}+t_{i3}+t_{i4}+t_{i5}$)$>t_{t0}$,甚至探测时间($t_{i1}+t_{i2}+t_{i3}$)$>t_{t0}$,则入侵失败。假设每次入侵攻击所需时间是固定不变的,当 $t_{t0} < T_1$ 时,即网络系统切换时间小于入侵探测时间,则能够有效抵御攻击者的恶意入侵,而且切换运行环境速度决定系统对抗入侵的能力。

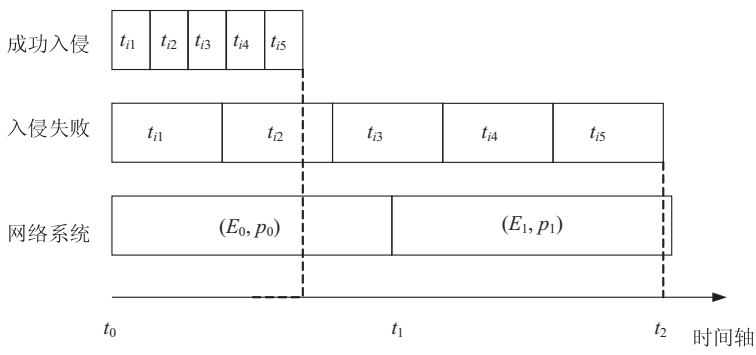

图 2　攻击生存周期示意

3　基于 SCIT 改进模型 Web 服务安全防护设计

3.1　功能模块实现

与传统 Web 服务器系统不同,基于 SCIT 模型的服务器由以下六个模块组成:中央控制器、请求分发器、信息共享模块、数据清洗模块、审计模块、服务器资源池。改进模型在基本模型的基础上为客户端增加终端控制器、终端清洗审计以及终端资源池等模块。功能模块如图 3 所示。

(1)请求分发器。接受来自客户端的 Web 访问请求,根据中央控制器指令将访问请求数据转发给指定服务器,并将服务器处理后的数据转发给用户。

(2)信息共享模块。用于服务器资源池中各个服务器的数据共享。

(3)数据清洗模块。对完成工作的服务器进行清

洗,清洗是清空服务器所有内存和文件数据的过程,根据系统备份的镜像文件,恢复至初始状态,此时等待审计。

(4)审计模块。对清洗完成的服务器进行审核,检验系统是否恢复至纯净安全状态,审计通过,释放服务器资源,否则对服务器重新清洗,并对存在的攻击行为进行取证分析。

(5)服务器资源池。构成服务器的物理主机和虚拟主机所有软硬件资源。一个 Web 服务系统核心软件栈主要由虚拟化平台、操作系统、数据库、服务器软件以及 Web 应用程序构成,由于软件的多样性和兼容性,系统可以随机选择软件构成多样化的服务器来抵抗攻击。服务器资源池的功能如下:

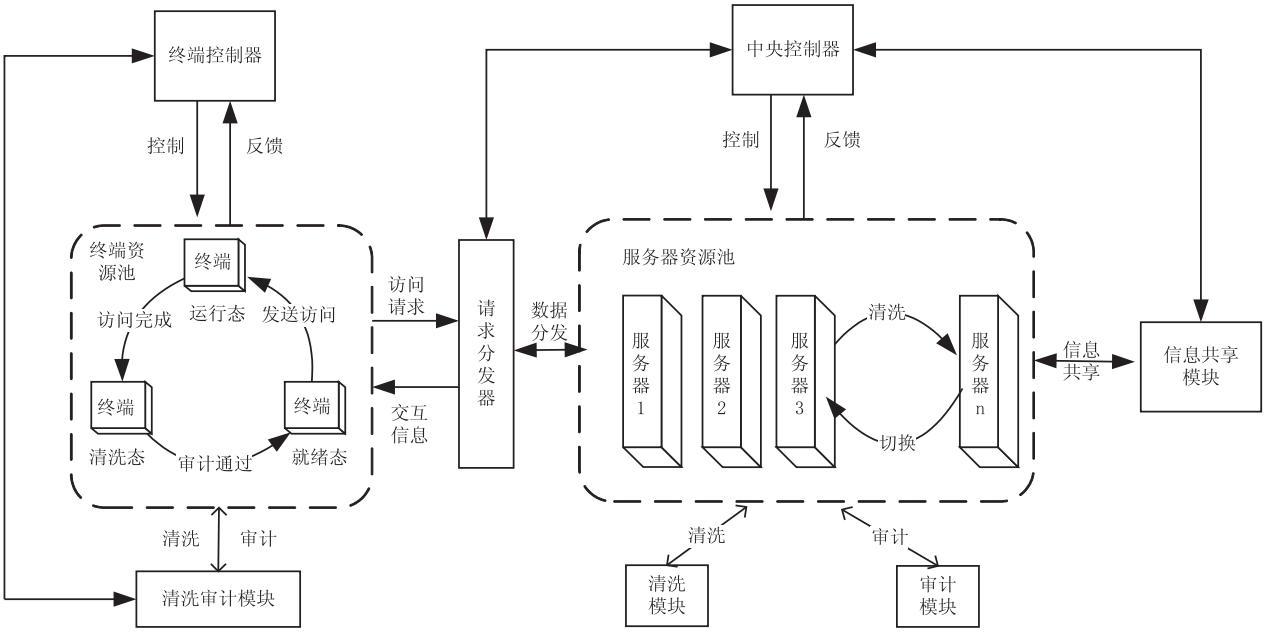

图 3 功能模块

①根据中央控制器指令,依据调度算法随机选取各类资源,为当前访问请求建立新生服务器。调度算法应遵循随机原则,使攻击者无法判断出下一时刻服务器软件构成。

假设开设一个 Web 服务器需要一个服务器资源池,有功能相同但结构或版本不同的软件,将 Web 应用程序用 P 表示,其中共有 p 种不同的编程语言实现 Web 编程;服务器软件用 S 表示,共有 s 种不同类型服务器软件;数据库软件用 D 表示,共有 d 种不同类型的数据库;操作系统用 O 表示,共有 o 种不同的操作系统;虚拟化平台用 V 表示,共有 v 种不同的虚拟平台,则服务器共有 $p * s * d * o * v$ 种类型,任意时刻建立的服务器如图 4 所示。

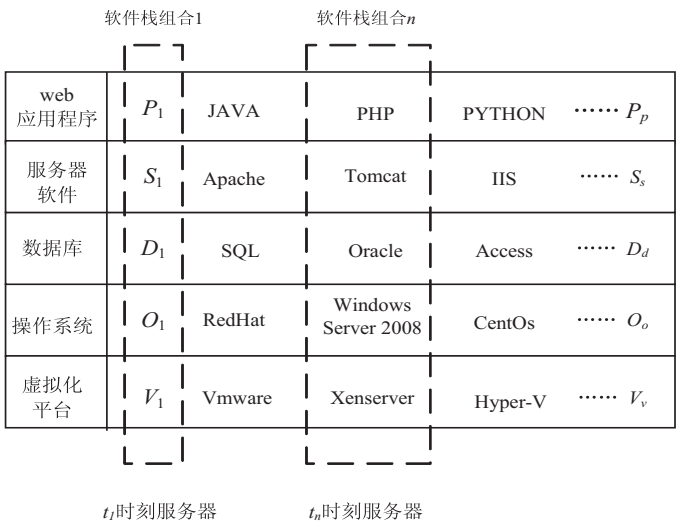

图 4 服务器软件栈

②建立运行态、清洗态和就绪态三种服务器状态转换模型,在保证 Web 服务质量的条件下实现服务器

状态的无缝切换。

运行态:服务器正在处理来自客户端的访问请求,提供信息服务,此时服务器处于在线状态;

清洗态:对运行完的服务器进行清洗和审计,此时服务器处于离线状态;

就绪态:服务器经过清洗审计,等待调度访问的状态。

(6)中央控制器。中央控制器是整个系统的大脑,用于协调控制各个模块的正常运行。

(7)终端控制器。负责协调控制各个功能模块和终端,是整个终端系统的控制核心。主要功能:利用调度算法在资源池内为特定终端选择资源,构建多样化运行环境;利用特定算法设定终端的具体状态,例如运行态、清洗态和就绪态;命令清洗审计模块对终端进行清洗审计。

(8)终端清洗审计模块。对完成访问的终端进行清洗,清洗终端内存和数据,并根据镜像文件恢复至初始状态,清洗完成后审计,审计通过,开始新的访问,未通过继续转入清洗。

(9)终端资源池。参照服务器资源池,为终端开设资源池,构建新生软件栈。软件栈主要由虚拟化平台、操作系统和浏览器构成,通过不同的排列组合来实现终端系统的多样化。为终端建立运行态、清洗态和就绪态三种状态模型,实现终端状态的无缝切换。

3.2　系统工作流程

(1)终端向终端控制器提出 Web 访问申请,控制器利用调度算法在资源池中随机选择特定资源,生成新的软件栈,构建特定运行环境。此时终端从就绪态切换至运行态,而后向请求分发器发送 http 请求;

(2)请求分发器接到访问请求后,向中央控制器报告;

(3)中央控制器根据调度算法随机生成新的软件栈,组建新生服务器,服务器为就绪状态,构成就绪服务器组;

(4)根据中央控制器指令,请求分发器将终端访问请求发放到就绪服务器组的某一选定服务器,此时服务器从就绪态切换为运行态;

①运行服务器与信息共享模块建立联系,实时共享数据;

②运行服务器将运行状态反馈给中央控制器,为下一步制定策略提供依据;

③运行服务器通过请求分发器与终端进行通信交互。

(5)Web 服务结束,服务器进入清洗状态,审计后释放资源至资源池中,等待下一轮的访问;终端也进入清洗状态,审计通过后释放资源,跳转至步骤 1,如此循环往复,实现系统的整体防护。

4　基于改进模型安全防护效能分析

通过不断地切换服务器和终端的运行环境,使系统呈现多样化状态以迷惑攻击者,增加入侵的难度和代价,但是防御的性能取决于变化的速度和不可预知性,已有文献[14]从数学的角度对系统软件的多样性组合问题进行定量分析,下面着重分析改进模型抵抗入侵的效能。

假设服务器的软件栈由三层(分别为 L、M、H)组成,分别对应虚拟化平台、操作系统、服务器软件,其中 L 层共有 T_1 种类型,M 层共有 T_2 种类型,H 层共有 T_3 种类型。为方便计算,终端只增加一个维度的多样性,即 E 层,E 层对应浏览器层,E 层共有 T_4 种类型,则 Web 系统共有 $T_1 * T_2 * T_3 * T_4$ 种类型。资源池中的软件选择组合是随机的,每次任意类型软件被入侵的概率是均匀分布的,即 L 层 L_a 被入侵的概率为 $1/T_1$;M 层 M_b 被入侵的概率为 $1/T_2$;H 层 H_c 被入侵的概率为 $1/T_3$;E 层 E_d 被入侵的概率为 $1/T_4$。其中 $L_a \in \{L_1, L_2, \cdots, L_{T_1}\}$,$M_b \in \{M_1, M_2, \cdots, M_{T_2}\}$,$H_c \in \{H_1, H_2, \cdots, H_{T_3}\}$,$E_d \in \{E_1, E_2, \cdots, E_{T_4}\}$。

每次成功的入侵必须入侵 X 层才能成功,则入侵成功的概率可由以下公式所得。

当 $X=1$ 时:

$$\begin{aligned}P_1 = {} & P\{L=L_a \cup M=M_b \cup H=H_c \cup E=E_d \mid X=1\} = P\{L=L_a\} + P\{M=M_b\} + P\{H=H_c\} + \\ & P\{E=E_d\} - P\{L=L_a, M=M_b\} - P\{L=L_a, H=H_c\} - P\{L=L_a, E=E_d\} - P\{M=M_b, H=H_c\} - \\ & P\{M=M_b, E=E_d\} - P\{H=H_c, E=E_d\} + P\{L=L_a, M=M_b, H=H_c\} + P\{L=L_a, H=H_c, E=E_d\} + \\ & P\{M=M_b, H=H_c, E=E_d\} + P\{L=L_a, M=M_b, E=E_d\} - P\{L=L_a, M=M_b, H=H_c, E=E_d\} = \\ & \sum_{i=1}^{4} \frac{1}{T_i} - \sum_{1 \leqslant i < j \leqslant 4} \frac{1}{T_i T_j} + \sum_{1 \leqslant i < j < k \leqslant 4} \frac{1}{T_i T_j T_k} - \frac{1}{T_1 T_2 T_3 T_4}\end{aligned}$$

当 $X=2$ 时:

$$\begin{aligned}P_2 = {} & P\{L=L_a \cup M=M_b \cup H=H_c \cup E=E_d \mid X=2\} = P\{L=L_a, M=M_b\} + P\{L=L_a, H=H_c\} + \\ & P\{L=L_a, E=E_d\} + P\{M=M_b, H=H_c\} + P\{M=M_b, E=E_d\} + P\{H=H_c, E=E_d\} - \\ & 2P\{L=L_a, M=M_b, H=H_c\} - 2P\{L=L_a, H=H_c, E=E_d\} - 2P\{M=M_b, H=H_c, E=E_d\} -\end{aligned}$$

$$2P\{L=L_a,M=M_b,E=E_d\}+3P\{L=L_a,M=M_b,H=H_c,E=E_d\}=\sum_{1\leqslant i<j\leqslant 4}\frac{1}{T_iT_j}-\sum_{1\leqslant i<j<k\leqslant 4}\frac{2}{T_iT_jT_k}+\frac{3}{T_1T_2T_3T_4}$$

当 $X=3$ 时：

$$P_3=P\{L=L_a\cup M=M_b\cup H=H_c\cup E=E_d\mid X=3\}=P\{L=L_a,M=M_b,H=H_c\}+P\{L=L_a,H=H_c,E=E_d\}+P\{M=M_b,H=H_c,E=E_d\}+P\{L=L_a,M=M_b,E=E_d\}-3P\{L=L_a,M=M_b,H=H_c,E=E_d\}=\sum_{1\leqslant i<j<k\leqslant 4}\frac{1}{T_iT_jT_k}-\frac{3}{T_1T_2T_3T_4}$$

当 $X=4$ 时：

$$P_4=P\{L=L_a\cup M=M_b\cup H=H_c\cup E=E_d\mid X=4\}=P\{L=L_a,M=M_b,H=H_c,E=E_d\}=P\{L=L_a\}P\{M=M_b\}P\{H=H_c\}P\{E=E_d\}=\frac{1}{T_1T_2T_3T_4}$$

由以上概率公式可得，当 T_1、T_2、T_3、T_4 分别取 1 时，则入侵概率为(1.000，1.000，1.000，1.000)，即此时系统处于静态配置状态，被入侵几率最大。当 T_1、T_2、T_3、T_4 分别取 3 时，当前系统共有 81 种不同的组合类型，则入侵成功概率为(0.802 5，0.407 4，0.111 1，0.012 3)，入侵成功率分别下降了 19.75%、59.26%、88.89%、98.77%，与文献[11]相比，在同等条件下，入侵概率平均下降 46.44%。

5 结束语

文中旨在为网络内 Web 服务提供一种动态防御机制，在 SCIT 基本模型基础上，为系统增加终端运行环境随机化切换，进一步增加系统的随机性，使攻击者入侵成功概率明显下降，有效增强系统抵抗入侵的能力。系统切换的速度决定了系统抵抗入侵的能力，但是速度越快必然导致稳定性下降，增加额外开销。引入弹性调度算法动态调整系统的变化速率平衡变化率和稳定性之间的矛盾关系将是下一步研究的重点和方向。

参考文献：

[1] 邬江兴. 网络空间拟态防御研究[J]. 信息安全学报，2016，1(4)：1-10.

[2] 杨正校，刘 静. 工业控制系统信息安全防范研究[J]. 软件，2014，35(8)：55-58.

[3] 李 刚. 计算机网络安全隐患与应急响应技术[J]. 软件，2012，33(5)：131-133.

[4] 张晓玉，李振邦. 移动目标防御技术综述[J]. 通信技术，2013，46(6)：111-113.

[5] ATIGHETCHI M，PAL P，WEBBER F，et al. Adaptive use of network-centric mechanisms in cyber-defense[C]//Sixth IEEE international symposium on object-oriented real-time distributed computing. Hokkaido，Japan：IEEE，2003：183-192.

[6] JAFARIAN J H，AL-SHAER E，DUAN Qi. Openflow random host mutation：transparent moving target defense using software defined networking[C]//Proceedings of the first workshop on hot topics in software defined networks. Helsinki，Finland：ACM，2012：127-132.

[7] AL-SHAER E，DUAN Qi，JAFARIAN J H. Random host mutation for moving target defense[C]//International conference on security and privacy in communication systems.[s. l.]：[s. n.]，2012：310-327.

[8] HARDMAN O，GROAT S，MARCHANY R，et al. Optimizing a network layer moving target defense for specific system architectures[C]//Proceedings of the ninth ACM/IEEE symposium on architectures for networking and communications systems. San Jose，California，USA：IEEE，2013：117-118.

[9] 马多贺，李 琼，林东岱，等. 基于 POF 的网络窃听攻击移动目标防御方法[J]. 通信学报，2018，39(2)：73-87.

[10] JACKSON T，SALAMAT B，WAGNER G，et al. On the effectiveness of multivariant program execution for vulnerability detection and prevention[C]//Proceedings of the 6th international workshop on security and measurements and metrics.[s. l.]：[s. n.]，2010：1-8.

[11] HUANG Y，GHOSH A K. Introducing diversity and uncertainty to create moving attack surfaces for Web services[M]//Moving target defense：creating asymmetric uncertainty for cyber threats. Berlin：Springer，2011：131-151.

[12] 蔡桂林，王宝生，王天佐，等. 移动目标防御技术研究进展[J]. 计算机研究与发展，2016，53(5)：968-987.

[13] HONG J B，DONG S K. Performance analysis of scalable attack representation models[C]//IFIP international information security conference.[s. l.]：Springer，2013：330-343.

[14] 齐晓霞，黄 俊，蒋 凡. 基于 SCIT 的移动目标防御系统分析研究[J]. 计算机工程与应用，2014，50(20)：96-99.