基于自动机理论的网络攻防模型与安全性能分析

郭 威, 邹江兴, 张 帆, 沈剑良

国家数字交换系统工程技术研究中心 郑州 中国 450002

摘要 针对当前自动机模型对系统状态表达不完整, 单一视角建模无法满足网络攻防行为刻画需求的问题, 本文提出一种视角可变的变焦有限自动机(Zooming Finite Automata, ZFA)结构。ZFA 使用完整的参量集合取值对状态进行标示, 设置观测系数增强模型对于多角度分析系统行为过程的能力。结合 ZFA 结构给出了网络攻防模型和安全性能分析方法, 分析揭示了传统安全手段的天然劣势以及移动目标防御技术的局限性。最后, 讨论了网络空间拟态防御(Cyberspace Mimic Defense, CMD)技术中核心部件——异构执行体的实现结构, 从理论上证明了构建“多参数”不确定性可获得超线性增益。

关键词 网络空间安全; 自动机; 变焦; 攻防模型; 安全性能; 网络空间拟态防御; 多参数不确定性

中图法分类号 TP309.1 DOI 号 10.19363/j.cnki.cn10-1380/tn.2016.04.003

A Cyberspace Attack and Defense Model with Security Performance Analysis Based on Automata Theory

GUO Wei, WU Jiangxing, ZHANG Fan, SHEN Jianliang

National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China

Abstract The incompletion of current automata model for system state expression and the singleness of angle on modeling cannot meet the requirement for characterization of cyberspace attack and defense. To address the problem, this paper proposes an angle-variable Zooming Finite Automaton (ZFA) structure. In ZFA, a complete set of parameters is used to identify the status of the state, and the observation coefficient it set up to enhance the ability of system analysis in a multi angle. The cyberspace attack and defense model and the security performance analysis method are given by means of the ZFA structure. The analysis reveals the natural disadvantage of the traditional security methods and the limitations of the moving target defense technology. Finally, the core components of the Cyberspace Mimic Defense (CMD) theory -- executive isomer architecture is discussed, and theoretically proved that the super linear growth of uncertainty can be obtained by construction at “Multi parameter”.

Key words cyberspace security; automata; zooming; attack and defense model; security performance; cyberspace mimic defense; multi parameter

1 引言

近年来, 主动防御已成为网络空间安全领域最炙手可热的研究热点。2011 年, 美国 NSTC(National Science and Technology Council)推出了移动目标防御[1](Moving Target Defense, MTD)技术, 试图构建防御者“可控”的目标环境, 扭转当前“易攻难守”的安全态势。随后, 国内研究团队也提出了网络空间拟态防御(Cyberspace Mimic Defense, CMD)的概念[2], 通过在异构冗余体制中导入动态性、随机性和“去协同化”机制提升其抗攻击性能, 从而增加攻击者利用漏洞和后门的难度。

然而, 即便安全技术的研究发展十分迅速, 信息安全领域中一个公认的事实仍没有变: 对攻防行为一直缺乏抽象的研究模型, 这使得研究者们难以跳出具体环境的限制对现有安全技术进行分析评估。例如, 在 MTD 的多个应用场景中, 研究者们提出的突破思想[3-5]十分相似, 文献[6]将这些问题归纳为 MTD 的覆盖性, 不可预测性和时效性挑战, 但由于缺乏抽象描述模型和系统性分析, 目前只能借助

通讯作者: 张帆, 博士, 副研究员, Email: 13838267352@qq.com。

本课题得到国家自然科学基金面上项目网络空间拟态安全异构冗余机制研究(61572520)资助、国家自然科学基金创新研究群体项目(No.61521003)和国家重点研发计划项目(Nos. 2016YFB0800100, 2016YFB0800101)支持。

收稿日期: 2016-09-10; 修改日期: 2016-09-30; 定稿日期: 2016-10-17

加密、安全存储等存在争议的手段进行改进[7], 并没有从本质上解释和解决 MTD 自身的技术局限。此外在研究实践中, 虽然我们已经验证了异构, 冗余, 动态, 随机等概念对于提高系统安全性的正向作用, 但却难以描述其生效过程, 度量其安全增益, 从而无法对各种安全机制进行有效的取舍和评判。上述案例说明, 对攻防模型研究的滞后性极大的束缚了信息安全领域的发展。

造成建模困难的主要原因是: 在考虑安全问题时, 攻防的条件、过程、目标等因素具有复杂性, 难以进行高度抽象。在面对未知威胁时, 各种因素更是具有不确定性, 使得模型的构建相当困难。相比之下, 研究者们更愿意将精力集中在系统的漏洞挖掘与利用等工作上[7]。其研究场景相对固定, 能够确立具体的威胁种类和防御环境, 既降低了研究难度, 同时也更容易加以应用。但其问题在于, 一旦攻防条件与假设不一致, 即便稍有偏差, 研究成果的有效性也难以保证。

本文根据攻防模型与安全性能评估的研究现状, 结合系统运行特性, 在有限自动机(Finite Automata, FA)基础上提出一种可变焦有限自动机(Zooming Finite Automata, ZFA)描述模型。利用 ZFA 对网络攻防过程进行了建模, 以安全性能和客观因素的角度对现有安全技术进行了分析, 揭示了传统安全手段的天然劣势及 MTD 技术的局限性。最后根据 CMD 中构建动态异构冗余机制(Dynamic Heterogeneous Redundancy, DHR)的基本思想, 结合 ZFA 结构给出了一种“多参数”不确定的异构实现与性能分析。

2 研究现状与问题分析

文献[8]中对攻击图谱模型进行了全面的综述, 介绍和分析了其近 25 年的研究情况。这种攻防模型的最大特点是抽象性强且层次清晰, 它将根节点作为攻击目标, 子节点为子目标, 叶子节点为最基本目标, 将整个攻击过程抽象成树结构。在模型应用中, 可以结合子孙节点到祖先节点的难度量化为边的权值, 从而对整个攻击的难度进行刻画。文献[9]结合了贝叶斯理论设计了贝叶斯攻击图谱, 通过数据集训练后能够得到某攻击目标的非条件概率, 能够很好地服务于有针对性的安全部署。尽管攻击图谱得到了广泛的研究和应用, 但其劣势也相当明显, 就是无法刻画未知的攻击目标和子目标路径, 因此对未知威胁不具备刻画和分析能力。

另一种较为普及的攻防模型是攻击面(Attack Surface, AS)理论。文献[10]为了给出软件安全评判指标, 提出了 AS 理论和基于 I/O 自动控制模型的系统描述方法。一个给定系统的 AS 度量是资源在规则、通道和数据三个维度上的总贡献, 度量的大小表明攻击者可能对系统破坏的程度, 以及攻击者造成这种破坏的所需投入的努力。作为 AS 度量系统的建模工具, I/O 自动机的使用出于两方面考虑。首先在外部运行环境下, 一个具有入口点与出口点的防御系统, 可等效为一个具有输入操作和输出操作的 I/O 自动机环境; 另外 I/O 自动机的构成属性决定了, 其模型在给定的环境中推断出系统 AS 的可行性。

AS 理论的优势在于能将所有系统行为等价表示为 I/O 操作, 所以必然能涵盖全部已知未知威胁, 使攻防模型能更好的服务于攻防技术发展。但其问题在于, AS 认为攻击总是可达的, 评估时只关注于系统的可被攻击性, 忽略了系统的防御性, 而这一点恰恰在开放服务系统中显得尤为重要。当设计者难以去缩小系统的攻击面时, 如何扩大防御面, 使得目标攻击面尽可能的对于攻击者不可达, 可能是更为有效的手段。

前人的研究成果给本文带来了的启示是(1)逻辑上对攻击过程进行分段能够有效的对整个攻击过程进行量化评估; (2)自动机模型能够对整个系统进行完整描述, 从而更好地建立攻防模型。那么, 本文将以自动机理论为基础, 针对安全问题建模和分析时的需求, 提出以下两点改进动机对传统模型进行拓展: (1)系统的全局状态变化对于攻击和防御的识别分析至关重要, 需要尽量完整的表达; (2)系统运行过程中, 往往是多个逻辑层面组合交叠着运行, 在一个孤立的“视角”下通常难以辨识正常行为与攻击行为, 应当予以拓展。

3 ZFA 结构与功能设计

首先, 讨论了面向安全问题基于自动机理论的系统建模方法, 给出了变量的符号描述。然后, 提出一种观测视角可变的 ZFA 结构, 并且证明了 ZFA 用于系统建模的正确性和唯一性。最后, 给出了系统关键概念的 ZFA 描述。

3.1 建模分析与参数符号化

自动机理论的现有应用, 都会根据具体场景将模型建立在一定固定的逻辑层面上。正则表达式[11]刻画了字符匹配逻辑; 软件状态机(Finite State machine, FSM)[12]刻画了软件运转逻辑; I/O 自动机[13]刻画了系统环境的交互逻辑。

一个系统的自动机模型, 是由多个逻辑面并列交叠而成。例如在深度包检测系统中, 预处理层面刻画了数据包的拆分重组过程; 包检测层面刻画了字

符匹配过程; 信息统计层面刻画了业务数量计数过程; 检测系统的硬件设计逻辑、宏观运转过程等等都能用自动机进行描述, 而所有这些的混合体才构成了一个完整的系统自动机。为便于形象的表达, 逻辑层面可称为“观测视角”, 记为 ω。

对系统进行建模时, 其静态属性由特征参量来标识, 记为 *Var*, 全部参量构成了参量集合 *V*。参量取值将决定系统状态, 由 *q* 表示, 函数ρ用于从具体取值中提取参量, $\rho(q)= V$; 其动态属性指 *q* 经过一定的触发条件φ产生迁移的规则, 即系统的迁移逻辑, 记为 δ。系统与外界环境的交互抽象为输入 *i* 和输出 *o*, *i* 是触发条件的组成部分, *o* 是系统的参量子集, 即满足$\rho(i)\subseteq\rho(\varphi)$, $\rho(o)\subseteq V$。那么从模型上, 设定观测视角就等同于确定一个集合, 以集合中的参量对系统静态和动态属性进行刻画分析, 故 $\omega\subseteq V$ 且选定过程与系统属性间不相关。

本文用到的符号如下表所示。

表 1 本文使用的参数符号与描述

符号表示	符号描述
$a, b, c, i, j, k, l, m, n, x, y, t, p, \gamma$	通用变量
$V=\{ Var_1, Var_2, \ldots, Var_n\}$	参量集合
$q=\{Var_1=val_1, Var_2= val_2, \ldots, Var_n= val_n\}$	一个系统状态
$Q=\{q_0, q_1, \ldots, q_m\}$	系统的状态集合
$i=\{Var_1=val_1, Var_2= val_2, \ldots, Var_i= val_i\}$	一个环境输入
$o=\{Var_1=val_1, Var_2= val_2, \ldots, Var_j= val_j\}$	一个系统输出
$\varphi=\{Var_1=val_1, Var_2= val_2, \ldots, Var_k= val_k\}$	一个触发条件
$\Sigma=\{\varphi_1, \varphi_2, \ldots, \varphi_m\}$	触发条件集合
$\delta_{xy}: \delta(q_x, \varphi) \to q_y$	状态转移函数
ρ	提取参数函数
$S=\{V, \delta\}$	目标系统
M	一个自动机
$\omega=\{ Var_1, Var_2, \ldots, Var_l\}$	观测系数
F	接受状态集合
A	攻击序列
$\{S_1, S_2, \ldots, S_m\}$	异构构建集合
$\{E_1, E_2, \ldots, E_n\}$	异构执行体集合
$\{R_1, R_2, \ldots, R_n\}$	输出结果集合

计算机系统是极其复杂的, 我们并不试图将 ω 设置到整个参量集合, 即物理意义上将一个完整的系统从物理层、硬件逻辑层、系统软件层等直至高级应用层全过程使用自动机描述出来, 至少对于目前的技术水平还难以实现。本文拓展参量集合和设置 ω 的目的在于(1)细粒度划分系统状态, 提高对引发安全问题的异常因素的辨识能力; (2)增强自动机的表达能力, 刻画出系统运行的完整过程, 抽象出安全问题中跨逻辑层的复杂情况; (3)建立不同逻辑层面间, 单一层面与整个系统间的联系, 有助于研究系统参量间的耦合性。

3.2 ZFA 结构设计

可变焦有限自动机(ZFA), 根据所设定的观测视角, 生成该视角下的状态和跳转过程。一个确定性 ZFA 的构成如下:

- 一个观测系数 ω, 满足 $\omega\subseteq V$;

在系数 ω 下, 生成 DFA 五元组:

- 一个有穷的状态集合 Q^{ω};
- 由触发条件φ^{ω}组成的集合 Σ^{ω}, 且$\rho(\varphi^{\omega})\subseteq V$;
- 转移函数 δ^{ω}, 以一个状态和一个触发条件为变量, 返回一个状态;
- 一个初始状态 ${q_0}^{\omega}$, 且 ${q_0}^{\omega}\in Q^{\omega}$;
- 一个接受状态集合 F^{ω}, 且 $F^{\omega}\subseteq Q^{\omega}$;

当 ZFA 非形式化表示为状态转移图时, 在注明 ω 的情况下, 系数角标可省略, 如下图所示。

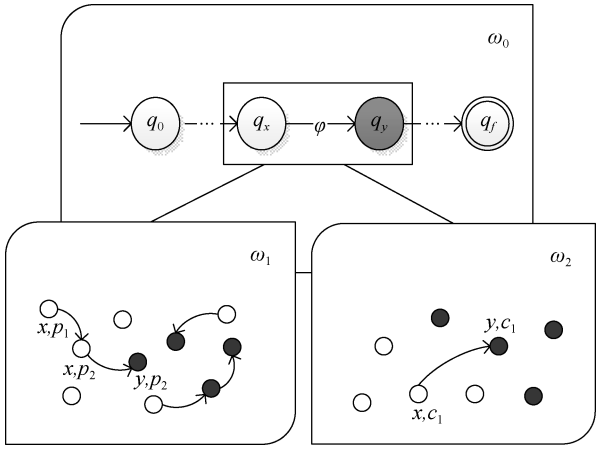


图 1 以不同系数进一步观测 ω_0 下的某一跳转

图 1 给出了一个 ZFA 应用示例。ω_0 通常会选取一个完整的逻辑层面, 如 TCP 连接生命周期, 扫雷游戏运转过程等等, 可认为是**“显性”观测视角**; 为了进一步观测逻辑层面的实现过程, 可增加观测的参数, 拉近到**“隐性”视角**。假设 ω_1 与 ω_2 分别取参数内存位置 *p* 和运行处理器 *c*, 那么图 1 所示的物理意义为: 对于 ω_0 层上 q_x 至 q_y 的跳转, 存在 5 种内存实现方式$<p_1\to p_2, p_2\to p_2, \cdots>$, 且只有 c_1 处理器能够实现处理。

3.3 证明与分析

为了保证基于 ZFA 系统建模的正确性, 给出以下证明。首先, 由信息系统的基本设计原则可得:

定理 1 已知 *t* 时刻系统 *S* 的状态 q_t 和外界输入 *i*, 则下一运行状态 q_{t+1} 唯一可确定

证明. (反证法)假设 q_{t+1} 不确定或确定但不唯一, 则分情况讨论:

i. 若 q_{t+1} 不确定, 与系统设计的确定性前提相矛盾

ii. 若 q_{t+1} 不唯一, 与系统设计的可控性前提相矛盾

综上分析, 定理 1 可得证。

定理 2 对任意离散数字有限系统 S, 存在一个 FA 能够对其进行完整描述

证明. 由 S 的离散性和数字性, 可知系统的参量个数和状态个数都是可列的, 则以自动机中的 q 进行描述。又因为系统的有限性, 有限次递归定理 1, 则 FA 可以完整描述 S 得证。

相比于传统的自动机模型, ZFA 能够有效还原系统的全局状态, 并配合 ω 进行观测。在不同的观测视角下, ZFA 并没有改变系统基本状态和跳转逻辑, 而是将其从不同层面灵活的呈现出来, 以便于表达和分析攻防模型中不同层次间的关系。

上述定理表明了 ZFA 结构用于系统全过程描述的正确性和唯一性。

假设 1 在运行过程中系统 S 不变, 即状态参量集 V 和转移函数 δ 保持不变

上述假设保证了 ZFA 的时不变性, 即不考虑引起 S 变化的输入 i。实际上这类输入是普遍存在的, 在加载和换出程序的过程中, 都会引起 V 和 δ 的变化。假设的原因在于, 在攻防建模和分析中, 变化过程通常可以忽略不计。例如, 在分析安置后门过程时, 相比于具体安装过程, 防御者可能更关注于攻击者后门安装前的准备过程, 以及安装后的系统运转过程。

尽管从理论上保证了系统的 ZFA 描述具有正确性, 唯一性和不变性, 但由于计算机的逻辑复杂度极高且无记忆, 所以完整描述的可行性很差。如何解决这个问题, 需要展开进一步研究。

3.4 系统关键概念的 ZFA 描述

(1) 视角的可伸缩性

定义 1 视角的放大与缩小

已知两个观测系数 ω_1 和 ω_2, 则存在集合 ω' 满足 $\omega'=\omega_1\cup\omega_2$, ω' 称为以 ω_2 放大 ω_1 后的观测视角, 或以 ω_1 放大 ω_2 后的观测视角。

已知两个观测系数 ω_1 和 ω_2, 则存在集合 ω' 满足 $\omega'=\omega_1-\omega_2$, ω' 为以 ω_2 缩小 ω_1 后的观测视角。

在 3.2 中提到了显性视角与隐性视角的概念, 它们是相对而言的, 根据观测习惯进行区分界定。一般地, 将一个有完整意义的逻辑层面设定为显性视角, 将加入关注参量后的放大视角设定为隐性视角。

(2) 功能等价与功能等价系统

在 ZFA 结构上, 功能可描述为某 ω 下达到特定状态 q_y^{ω} 的一段状态跳转序列 $q.^{\omega}\rightarrow\cdots\rightarrow q_y^{\omega}$, 记为$(q., q_y)^{\omega}$, 和该序列上的附加跳转限制条件(必须由某状态起始, 经历某状态, 由某输入触发等等)。功能等价跳转存在的必要条件由下列命题满足。

命题 1 (定理 1 的逆否命题)当下一运行状态 q_{t+1} 唯一确定时, 则 t 时刻系统 S 的状态 q_t 和外界输入 i 可能不唯一

命题 1′ 已知 t 时刻系统 S 的运行状态 q_t, 则存在一个或不止一个的(q_{t-1}, φ)满足 $\delta(q_{t-1}, \varphi)\rightarrow q_t$

命题 1′说明了一个可达状态的前序状态可能存在多个, 递归应用命题 1′可知达到某一状态 q_y^{ω} 的跳转序列 $\delta_{\square y}{}^{\omega}$ 可能存在多个, 这就为功能等价的存在性提供了必要条件。

定义 2 当跳转序列 δ_1^{ω} 和 δ_2^{ω} 有相同的跳转限制条件时, 则称它们功能等价

由定义 2 可以给出功能等价系统的定义。

定义 3 系统的功能等价集合

对于 S_1 功能集合 Φ 中任一功能, S_2 中存在跳转序列 δ 达到特定的目标状态且满足其限制条件, 则 Φ 为二者的等价集合, 或称 S_1 和 S_2 关于 Φ 等价。

4 基于 ZFA 的攻击过程建模

首先, 对攻击过程进行了分析和 ZFA 建模, 然后对网络中典型的攻击手段进行了分类分析。

4.1 攻击过程的基本模型与度量方法

攻击过程(Attack Process, AP)可分为离线和在线两个阶段, 离线阶段的主要任务是剖析目标系统, 研究出攻击方法和探测手段, 并根据攻击方法做好相应的准备; 在线阶段就是实施攻击的过程, 需要根据实际探测情况展开相应的攻击行动。

从模型上来说, 攻击过程与正常过程的地位是等价的, 都是系统自动机的一部分。在 3.3 中, 证明了系统运转过程可用 ZFA 等价表示, 进一步的, 离线阶段可认为是系统 ZFA 的描述过程; 在线阶段则刻画为由特定的输入所触发的一连串状态即攻击序列, 其终点就是攻击者的目标状态。本文中主要以攻击序列作为核心对象进行讨论。

定义 4 攻击序列

对于 S 上的目标状态 q_f^{ω}, 攻击者从 $q_0{}^{\omega}$ 出发, 由输入触发的跳转序列, 记为 A。

图 2 是系统 S 在内存位置 ω 视角下的状态跳转图, p_1 是一个用户态程序, p_2 是一个 Shellcode 程序, δ_4

是溢出引发的跳转。$\delta_0 \sim \delta_3$ 都是 p_1 中的正常跳转，经过 δ_4 跳至攻击者设定的 Shellcode 位置。$\delta_0 \sim \delta_4$ 就构成了一个攻击序列 A, q_f 是溢出攻击的目标状态(暂没有考虑后续的提权过程，只讨论溢出过程)。

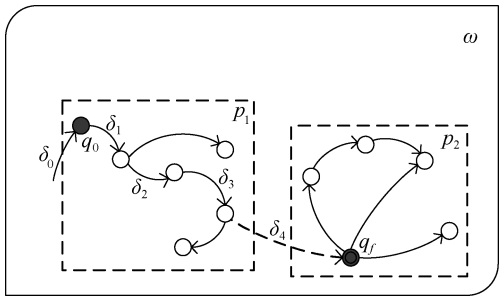


图 2　基于 ZFA 的溢出攻击示意图

定义 5　步骤难度

攻击触发某一次状态跳转所需要付出的代价，付出代价的决定因素根据具体应用环境而定。

定义 6　攻击难度

整个攻击序列的步骤难度之和，取决于步骤总数与步骤难度。

本文并不针对攻击难度进行详细讨论，只定性给出了其含义，实际应用中将根据不同场景设定刻画难度的量化变量。

4.2　典型攻击模式的 ZFA 描述与分析

A. 侧信道攻击

侧信道攻击[14]是侵犯私密性(Confidentiality)的代表性方法，它以非常规的方式获取目标系统的私密信息，尤以加密密钥为主。与传统的信息收集方式不同，在侧信道攻击过程中，攻击者并不需要构建攻击序列，与目标系统间也没有显性交互。

下图表示了以 CPU 辐射能量[15]为侧信道参量的经典窃密方法，在 ZFA 中分别以两种不同的隐性视角观测加密过程的状态特征，ω_1 设定为密钥值，ω_2 设定为侧信道特征 γ。

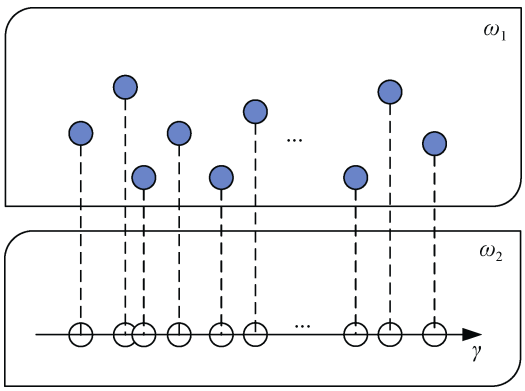


图 3　能量侧信道攻击的 ZFA 表示

如图 3 所示，攻击者可以根据获取的能量参数 γ 的值，得到对应的密钥值。这种攻击方式实现基础和思想在于，系统状态的私密信息与 γ 特征能够呈现较明显的映射关系，并且 γ 具备传递特性，可以被攻击者获取。那么对于攻击者而言，私密信息的“传递”犹如形成了一条信息“通道”，只要对应 γ 取值还原出相应的信息值，便实现了隐私信息的获取。

实施侧信道攻击的工作量主要集中在离线阶段，CPU 能量的分析算法优劣将直接决定攻击成功率。在线阶段的主要工作量是尽力获取目标系统的 CPU 型号，以便有针对性的使用还原算法。

B. 越权型攻击

现有系统都会用户设定读权限、写权限和执行权限。通常来说，对除了管理员外的访问者只会分配读权限，而越权型攻击就是一种使攻击者非法拥有写权限甚至执行权限，从而威胁系统的攻击模式。

权限，物理意义可理解为系统赋予使用者的操作集合。以 ZFA 结构刻画，是使用者能够到达的状态 q 与触发条件中的输入 i，即能够实现的 $\delta(q, \varphi)$的集合。那么，所谓的越权其实就是对可操作集合的非法化扩大。这里的非法化并不是针对系统运转过程，而是对于设计者和使用者，这种扩大是存在威胁的。综上所述，越权攻击的主要手段来自于对系统漏洞和后门的利用。

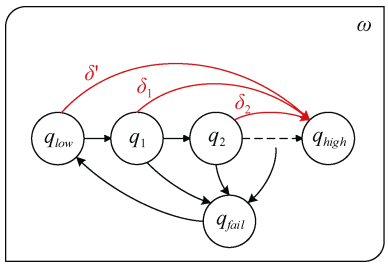


图 4　SQL 注入攻击的 ZFA 示意图

图 4 中，q_{low} 与 q_{high} 分别为低权与高权状态，q_1, q_2, …为数据库认证过程，q_{fail} 为认证失败状态。由于系统缺乏输入合法性检查，攻击者将查询语句漏洞转化为 δ_1、δ_2 等跳转，使其跳过了认证过程直接达到 q_{high}，使得越权得以实现。倘若系统被安插了后门程序，则可以通过δ'直接进入达到 q_{high}。

相对于其他攻击模式，越权攻击的过程比较复杂，其离线和在线的工作量都很大。对于一个庞大的系统，能够找到一个可利用的漏洞就需要消耗大量的时间和人力，另外还要设计 Shellcode 和提权代码等等。实施攻击过程中，通常包含大量的信息收集工作，然后通过精确的攻击序列触发漏洞和提权过程。

一般来说, 越是底层的提权攻击实施起来也就越为复杂。

当然, 这种方式所带来的效益也是最大的, 一旦掌握了系统最高权限, 将会造成极大危害。攻击者还可以通过安插后门来大大简化攻击过程, 降低再攻击的工作量。其防范的难点在于(1)大规模系统中漏洞后门的泛在化与未知性为越权攻击提供了温床; (2)除了某些关键性跳转外, 攻击序列与正常序列在各 ω 上基本一致。

C. 资源耗尽型攻击

每个系统的负载能力都是有限的, 所以严格来讲, 资源耗尽并不算是系统的异常状态。而攻击者正是利用了这一必然缺陷, 有预谋的大规模占用系统计算、内存、外设等资源, 使正常请求无法被响应, 从而达到威胁系统可用性(Availability)的目的。

以 SYN 洪泛为例, 内存中半连接队列使用情况作为观测系数 ω, 则目标系统 ZFA 表示如下。

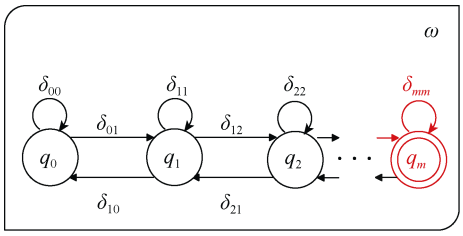


图 5 半连接队列使用情况的 ZFA 表示

如图所示, m 表示系统半连接队列的最大长度, $q_0, q_1, \ldots, q_m$ 为根据队列长度划分的系统状态。洪泛攻击时, 向右的跳转 δ 构成了攻击序列, 其目标态为 q_m。此后新的 SYN 将触发 δ_{mm}, 连接请求被丢弃, 无法得到响应。

设置 ω 使“视角”聚焦于如处理器、内存、外设等资源上, 对其他资源耗尽型攻击方式构建 ZFA, 得到类似的状态跳转情况, 其一般表示如下。

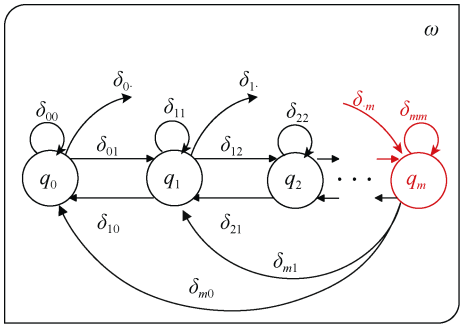


图 6 资源耗尽型攻击的一般 ZFA 表示

图 6 所示, 超过资源界限的请求将触发跳转 $\delta^{\omega}_{\square m}$ 且无法被响应。资源耗尽攻击之所以难以防范, 原因在于(1)攻击基于开放服务接口, 攻击序列与正常序列在其他隐性视角 ω 上的基本一致, 难以区分; (2) 攻击序列简单易构; (3)可分布式实现。综上, 这种攻击模式的工作量主要集中在离线阶段, 需要构建起一定规模的傀儡机器, 确保在短时间内发送超出目标系统负载的恶意请求。目前, DDoS 已经成为网络中各大服务提供商面临的最棘手问题[16]。

小结:

对于目标系统和防御者来说, 当前最大的威胁是越权型攻击模式。资源耗尽型攻击虽然难以防范破坏性大, 但这种攻击能被迅速感知, 便于迅速发起应对措施; 侧信道攻击, 能够掌握秘钥等私密信息, 有时也是服务于越权攻击的有力手段; 而越权攻击, 尤其是基于未知漏洞和后门的攻击方法, 属于未知威胁, 难以防范且危害巨大。

本节利用 ZFA 对攻击过程进行了建模, 分类攻击方法并从不同观测维度上探索其共性特点。其意义在于(1)提出了一种攻击过程的建模方法, 有助于进一步抽象和研究攻防技术; (2)将目前防御单个攻击的“点处理”方式转化为对处理某种攻击模式的“面处理”方式。

5 基于 ZFA 的防御模型与安全性能分析

本节利用 ZFA 对几种典型防御方法进行建模和安全性能分析, 讨论了传统防御方法对于现有网络攻击的天然劣势, 以及 MTD 的技术局限。此前, 先给出一个理想的攻击假设和安全性能说明。

假设 2 对于攻击过程的离线阶段, 攻击者已掌握目标系统所有漏洞和利用方法

安全性能: 本文将防御技术对攻击序列构造的难度增益作为安全性能的评价指标。在假设 2 下, 步骤难度排除了攻击者研究漏洞使用和信息收集方法的代价, 攻击前的准备代价等等, 以攻击序列的长度作为攻击难度的衡量标准, 其中主要考虑在面对下一跳多个选择时所付出的选路代价。

5.1 传统防御方法

根据第 4 节中攻击过程的 ZFA 描述, 摧毁攻击序列最简单直观的方式无非两种: 阻塞与重塑, 以此可以将传统安全手段分为两类。

(1) 通过嵌入阻塞功能使攻击过程不可达。

A. 身份认证

图 7 中给出了身份认证的模型示意, 使用 ω 截取认证逻辑视角下的关键步骤。认证状态由 q_l 表示, 其中仅有一个正确输入 i 能够激活跳转 δ_{ture}, 使运行过程继续进行, 否则将在认证逻辑上终止。

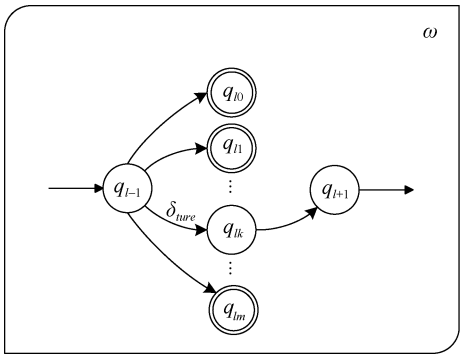


图 7　身份认证的 ZFA 结构示意

实际应用中, 无论是静态、动态密码、还是数字证书、指纹虹膜等都可以归结为此模型。从 ZFA 上分析, 身份认证的安全增益来自于δ_{ture} 的熵值, 因此对于攻击序列构造来讲, 难度增益取决于 m 的大小和δ_{ture} 的更新间隔。其中, 过认证序列段长度的理论上限为O(m), 且在下一个更新时刻前, 这个值会随着攻击经验积累而逐渐减小。但是, 如果存在漏洞或后门利用后绕过 $q_{l-1}\rightarrow q_{l+1}$ 的方法, 那么通过序列长度将为绕行长度O(1)。

这种手段能够以一个独立的模块嵌入到某一逻辑层次上, 具有很强的普适性, 这也是造成现如今认证泛滥的根本原因。

B. 访问控制

访问控制与身份认证方法类似, 在实际中广泛应用于网络设备系统中, 以包过滤技术, 应用网关技术, 代理服务技术为代表。以图 8 模型示意为例, 将ω设定为防火墙功能逻辑的相应系数, 那么, 从状态q_{l0}至q_{lm}仅有某些i能够被接受继而触发δ_{appr}跳转, 其他状态将拒止于此。对于规则有效的攻击序列, 其序列长度是+∞; 如果规则无效, 那么其序列长度为O(1)。

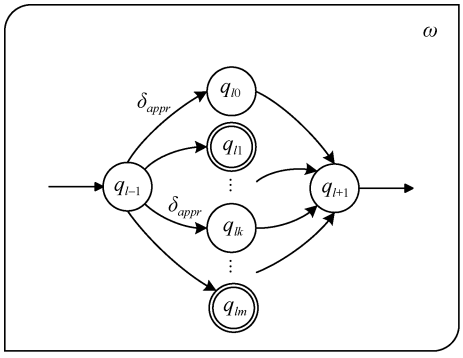


图 8　防火墙的 ZFA 结构示意

访问控制试图阻截攻击者利用不安全的服务接口对内部网络进行攻击, 并且能够实现数据流的监控、过滤、记录和报告等附加功能, 以便于安全管控。虽然它对于规则有效的攻击能够起到绝对的阻断, 但现有攻击方法大都在其规则 ω 层面与正常行为完全一致, 因此访问控制的使用被严重受限。

C. 匹配检测

模式匹配的基础结构和思想由访问控制演变而来, 其主要进步是结合了知识库(病毒库、木马库、安全策略库等)和信息收集分类分析方法, 主动探测和发现疑似对象的异常行为和特征。

如图 9 所示, 在 ZFA 结构上, 匹配检测技术将阻截功能进行了模块化, 其核心设计是一个正则匹配引擎(RE)。与访问控制相比, 其安全性能的提升主要体现在 RE 模块的规则数量与高速匹配上。如果进一步拉近视角, 将 ω 设定在 RE 模块内, 其匹配引擎本质上等价于 FA。在实际应用中, 规则集的膨胀所导致的自动机状态空间爆炸问题是匹配技术应用受限的关键[17]。

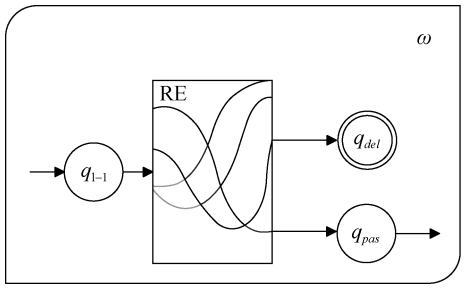


图 9　匹配检测技术的 ZFA 结构示意

D. 隔离技术

阻塞思想的极致运用是隔离技术。以过去的普遍认知, 物理网络隔离的 S 不会受到外界攻击的威胁, 攻击序列无法构造。但侧信道攻击的出现彻底打破了隔离技术的美好幻想。现实中, 难以实现绝对意义上的隔离, 因此只要攻击者能够有可利用的“信道”, 就能够实现精密构造的攻击过程。

(2) 通过重塑系统逻辑使原有漏洞跳转不可用

相比于第一类的阻塞方式, 重塑方法能够更加彻底的解决问题。由于重塑使得系统状态转移图发生变化, 利用相关漏洞的跳转δ将不可用, 关联的输入集合 Σ 都变为无效。

值得权衡的是, 如果想大面积重塑系统逻辑, 势必耗费巨大, 其可实现性很低且不能确保新的系统逻辑不存在漏洞; 而小范围打补丁的方式, 则完全依赖于对漏洞的搜寻查找, 难以做到全覆盖。

如图所示, 系统的补丁程序将原有攻击序列中的跳转进行清除, 或转化为合法跳转。从安全性能上分析, 对于原有漏洞不可用的攻击序列, 其序列长

度将变为+∞; 未涉及的漏洞攻击, 该段序列长度为O(1)。这种方式的局限在于可利用漏洞数量未知性, 从以往的经验上完全修补是无法做到的。且由于利益关系, 现实中补丁发布往往滞后于其开始利用, 在这段真空期内, 无有效手段进行防护。

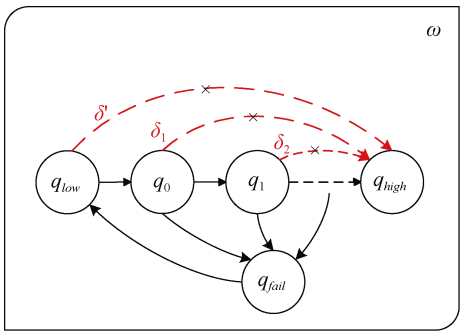


图 10 利用补丁程序移除敏感的跳转路径

小结分析:

现如今, 传统防御方法已经发展的相当成熟了。但是相对于网络攻击而言存在着天然劣势。在对攻击过程进行建模分析时, 提到了攻击的两个阶段。对于现有系统和传统防御手段, 最大的局限性其实在于**静态、确定、相似的**结构。也就是说, 虽然可以对系统进行加固, 对规则进行完善, 但由于目标环境仍是静态、确定和相似的, 所以难以抵挡攻击者在离线阶段的研究分析, 新的未知威胁和“绕路”手段将会不断产生, 危害整个网络环境。

5.2 MTD 技术

MTD 是近年来兴起的一种主动防御技术, 其基本思想是通过改变脆弱的系统特征参量 *Var*, 在防御者已知的隐含前提下, 使 *Var* 对攻击者呈现变化, 增加攻击成功的代价。如果攻击者以分析该系统 *Var* 为前提, 那么期望于在攻击者掌握这些特性和构造攻击的时间内, 系统能够做出改变, 扰乱攻击序列的构建。

其代表性应用有地址空间随机化(ALSR), 指令集随机化(ISR), 软件多样化(Software Diversity), 动态 IP 和端口等等。

如图 11 所示, 当我们对不同的应用场景设置其动态参量集合 V_m 为观察系数 ω 时, 却发现了一个很特别的现象。首先, 在相应的观测系数 ω 下, 各种应用场景的 ZFA 结构结构基本一致, 只是 m 的取值有所差别; 再有, MTD 的 ZFA 结构与传统防御方法中的身份认证 ZFA 结构也极其相似。

基于这样一个认知, 结构的相似逻辑过程其性能特性上必然也存在相似性。这样对比来看, 文献[6]

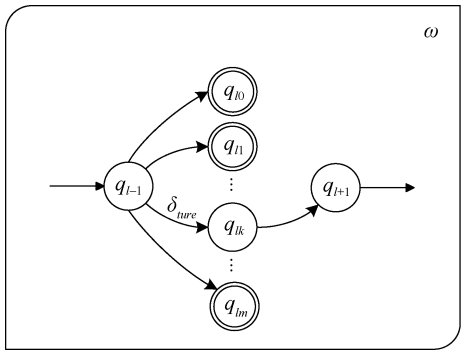


图 11 MTD 技术的 ZFA 结构

中所归纳的覆盖性, 时效性和不可预测性能够在此得到更深入而形象的解释。

不过, MTD 技术的出发点当然要比身份认证高明的多, 它并不是一种嵌入式的安全功能, 而是深入至攻击者频繁利用的系统参量 *Var*。这样一来, 无论是已知或未知威胁, 凡是需要准确的 *Var* 信息才能形成有效攻击的行动将全部受到阻碍, 系统的安全增益大大提升。对于受阻的攻击序列来讲, 需要付出的代价为O(m), 不受阻的攻击序列长度为O(1)。

综上分析, 以 ZFA 结构角度看, MTD 相当于高级别的身份认证技术, 其局限性在也十分明显。(1)防御机制限于某个 ω 层面, 与 ω 不相关的攻击过程无法得到防御; (2)安全性能决定于可动态变化的最大值 m, 存在暴力破解甚至巧妙绕过的可能; (3)动态变化的时间 t 也是安全性能的重要因素, 同样也是制约着系统性能的问题。

6 用拟态防御构建“多参数”的不确定

6.1 CMD 及其 DHR 体系结构

网络空间拟态防御(CMD)是一种基于功能集 Φ 上的异构等价执行体的主动防御技术。其核心思想是使目标系统具备动态异构冗余(Dynamic Heterogeneous Redundancy, DHR)的良性体制, 通过改进系统架构获得安全增益。

如图 12 所示, 由输入代理、异构构件集合、动态选择模块、执行体集合和一致性表决模块组成其基本结构。动态选择模块将根据相应算法, 从功能等价的异构构件集合$\{S_1, S_2, \ldots, S_m\}$中选出 n 个异构构件作为执行体集合$\{E_1, E_2, \ldots, E_n\}$。系统运行时, 输入代理将输入复制转发给当前执行体集合中各元素 E_*, 对应的执行结果集合$\{R_1, R_2, \ldots, R_n\}$由一致性判决模块处理后得出系统的输出。

DHR 是拟态防御系统的一种体系结构, 其核心思想是: 引入结构表征的不确定性, 使异构冗余执

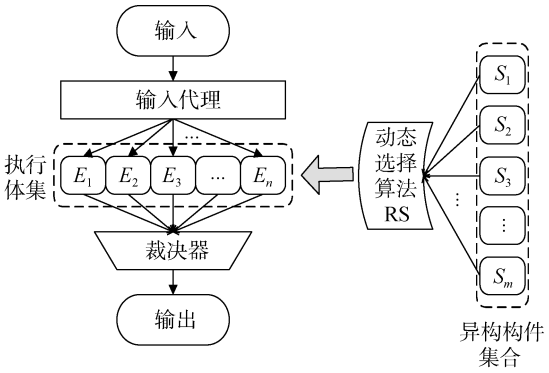


图 12　DHR 基本结构图

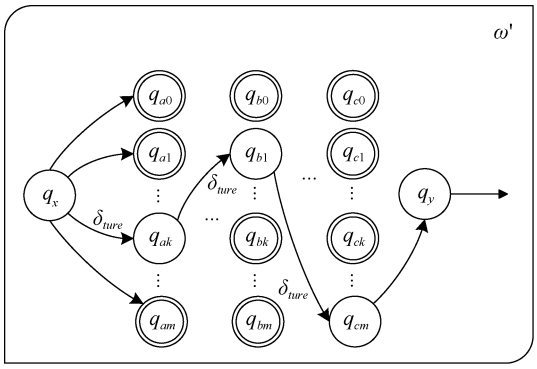


图 13　多参数 MTD 技术的 ZFA 结构

行体具有动态化、随机化的内在属性, 并在空间上严格隔离异构执行体之间除了共同的输入通道和输入请求序列外, 不存在其他的可利用的协同途径或机制, 通过构建动态异构冗余构造系统来弥补现有“有毒带菌”信息系统的安全缺陷。

目前, CMD 技术已经成功实现于 Web 服务器系统与路由器系统中, 并通过了国家权威单位的相关测试评估[18]。联合测试团队在确认提交的受测系统本征功能和性能满足国家或行业标准且全过程可保持的前提下, 通过拟态及非拟态模式对比方式验证 CMD 防御的有效性, 通过渗透测试验证 CMD 对各种渗透攻击的防御能力, 通过“白盒”及“配合植入”后门或病毒木马等开放式测试手段, 检验了 CMD 构造在“去协同化”条件下的协同攻击难度。Web 服务器拟态防御原理验证系统, 共完成 7 类 70 项 161 例测试验证, 内容包括功能测试、HTTP1.1 协议一致性测试、安全性测试、接入测试、性能测试、兼容一致性测试和互联网渗透等测试验证。路由器拟态防御原理验证系统, 共完成 6 类 43 项 43 例测试验证, 内容包括安全性测试、OSPF 协议功能测试、性能测试和互联网渗透等测试验证。

6.2　等价异构体的 ZFA 结构

CMD 的测试成功给予了研究者们极大的动力, 本文试图从 ZFA 结构上描述其核心部件——等价异构体的实现过程并分析其安全性能。

从安全原理上来说, CMD 是 MTD 的一种“多维度”拓展。经过 5.2 小节对 MTD 的 ZFA 的模型分析能够自然的想到, 如果对攻击过程所涉及的参量集合 V_a 进行完整覆盖, 那么将会给攻击者创造巨大的困难。

如图所示, 多参数上的 MTD 技术应用将会使不确定性达到超线性增长。最理想的情况是, 当 c 个参量正交时, 系统的不确定性呈多项式 $O(m^c)$增长; 最差的情况是, 当 c 个参量相关系数为 1 时, 系统的不确定性呈线性增长 $O(m)$。

然而, 实际情况是(1)随机化的理想前提条件是已知了大多数攻击过程, 这一点并不满足; (2)随机化的参量需要对攻击过程有影响, 且影响程度应该尽可能大, 而目前已知的影响关系甚少; (3)随机化集合中的各系统参量应保证相关性尽量小, 而目前对其相关性关系认知不足。

除此之外, 系统在对参数集合进行随机化时需兼顾服务性能。通常攻击行为使用的系统服务就是正常服务接口, 因此如果想为攻击者创造更大的麻烦, 势必也会使系统的可用性大打折扣。更严重的是, 为了保证 MTD 机制的安全性, 系统还需要考虑参量集合的动态性变化, 这将进一步加剧系统可用性的降低。

在 3.4 中, 命题 1′为功能等价的存在性提供了必要条件。这里做出如下假设。

假设 3　存在功能集合 Φ, 有不止一个系统 S 关于 Φ 等价

在假设 3 的前提下, 存在跳转序列 δ 达到特定的目标状态且满足其限制条件, 这里设定限制条件是由相同的输入 i 出发。

实际应用中, 假设 3 通常是可满足的, 那么下列 ZFA 实现结构的存在性从理论上得到了验证。

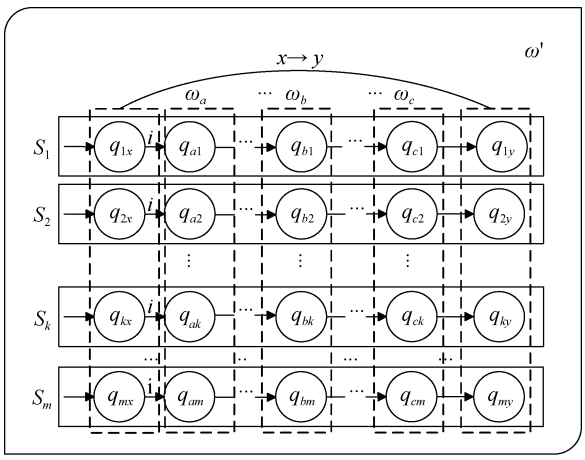


图 14　基于多参数不确定构建的一种实现结构

图 14 中, $a1 \neq a2 \neq \ldots \neq ak \neq \ldots \neq am$, $b1 \neq b2 \neq \ldots \neq bk \neq \ldots \neq bm$, $c1 \neq c2 \neq \ldots \neq ck \neq \ldots \neq cm$。从 ω' 上看 m 个系统实现了从 x 输入 i 最终到 y 的相同跳转。但是以攻击过程相关的观测角度 *abc*…下其运行过程可能处于不同的状态。如果再满足条件“x 出发除 i 以外的输入将导致最终达不到统一到 y 的跳转”, 那么此 ZFA 结构就满足了图 13 模型中的功能, 将其中满足上述要求的系统, 统称为异构等价体。异构等价体为构建“多参数”的不确定性提供了一种实现方案, C 个异构等价体的不确定性最高可呈多项式 $O(m^c)$增长, 带来了巨大的防御增益。

当然, 想要满足参量间的完全正交条件是几乎不可能的, 所以 CMD 引入了动态性和冗余性使得异构模型的实现要求得到了降低, 这在 DHR 的抗攻击文献中已经得到了证明, 本文不再进行讨论。

7 结论与下一步工作

针对当前自动机理论用于安全领域建模存在的问题提出改进动机: (1)系统的全局状态变化对于攻击和防御的识别分析至关重要, 需要尽量完整的表达; (2)系统运行过程中, 往往是多个逻辑层面组合交叠着运行, 在一个孤立的“视角”下通常难以辨识正常行为与攻击行为, 应当予以拓展。根据上述 2 点动机, 本文提出一种可变视角的 ZFA 结构, 使用整个系统的参量的取值标示不同状态, 通过设置观测系数, 从而实现灵活多角度的对系统进行描述和分析。从而达到了以下 3 点效益: (1)细粒度划分系统状态, 提高对引发安全问题的异常因素的辨识能力; (2)增强自动机的表达能力, 刻画出系统运行的完整过程, 抽象出安全问题中跨逻辑层的复杂情况; (3)建立不同逻辑层面间, 单一层面与整个系统间的联系, 有助于研究系统参量间的耦合性。

结合 ZFA 对攻防过程进行了建模, 从 3 种典型的攻击模式上分析了现有网络安全威胁的特点。随后, 讨论了传统安全手段的天然劣势及 MTD 技术的局限性。最后, 结合 CMD 思想与其 DHR 模型, 从理论上用 ZFA 构建一种“多参数”不确定性的实现结构, 单从攻击序列的在线长度上考虑, CMD 中的异构执行体所带来的防御增益最高能达到多项式增长 $O(m^n)$, 极大提高了目标系统的防御增益。

本文提出的 ZFA 和攻防模型, 存在以下问题值得继续研究: (1) ZFA 对于复杂系统运行全过程的建模可行性很低; (2) ZFA 结构无法刻画系统动态变化过程; (3)对攻防模型中的攻击难度和防御增益没有给出完整量化方法。

对于 ZFA 结构来说, 下一步工作有(1)探索 ZFA 建模实现的可行方法; (2)研究系统状态机动态变化的描述方法; (3)继续挖掘模型对于安全问题研究中的定性定量结论。

根据 ZFA 对于现有安全技术分析, 对于构建不确定的主动防御技术, 下一步工作有(1)研究系统行为与参量的影响关系; (2)研究系统不同参量间的相关性关系; (3) CMD 技术的具体实现研究和测试。

参考文献

[1] Baker Stewart, “Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program,” Foreign Affairs, pp. 8-10, Dec. 2011.

[2] Wu Jiangxing, “Meaning and Vision of Mimic Computing and Mimic Security Defense,” Telecommunications Science, vol.30, no. 7, pp. 1−7 (in Chinese), 2014.
(邬江兴, “拟态计算与拟态安全防御的原意和愿景”, 电信科学, 2014, 30(7): 1-7.)

[3] Strackx R, Younan Y, Philippaerts P, et al, “Breaking the memory secrecy assumption,” in Proc. Eurosec 2009, pp. 1-8, March, 2009.

[4] Snow K Z, Monrose F, Davi L, et al, “Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization,” in Proc. IEEE Symposium on Security and Privacy, pp. 574-588, 2013.

[5] Dmitry Evtyushkin, Dmitry Ponomarev, Nael Abu-Ghazaleh, “Jump Over ASLR: Attacking Branch Predictors to Bypass ASLR,” in Proc. 49th IEEE/ACM International Symposium on Microarchitecture (MICRO), 2016.

[6] Hobson T, Okhravi H, Bigelow D, et al, “On the Challenges of Effective Movement,” in Proc. ACM Workshop on Moving Target Defense, pp. 41-50, 2014.

[7] Hoque N, Bhuyan M H, Baishya R C, et al, “Network attacks: Taxonomy, tools and systems,” Journal of Network & Computer Applications, vol.40, no. 1, pp. 307-324, 2014.

[8] Kordy B, Pièvre-Cambacédès L, Schweitzer P, “DAG-based attack and defense modeling: Don’t miss the forest for the attack trees,” Computer Science Review, s 13–14, pp. 1-38. 2013.

[9] Poolsappasit N, Dewri R, Ray I, “Dynamic Security Risk Management Using Bayesian Attack Graphs,” IEEE Transactions on Dependable and Secure Computing vol.9, no. 1, pp. 61-74, Jan-Feb, 2012

[10] Manadhata P K, Wing J M, “An Attack Surface Metric,” IEEE Transactions on Software Engineering, vol.37, no. 3, pp. 371-386, 2011.

[11] M Sipser, “Introduction to the theory of computation,” China Machine Press, 2006.

[12] Chow T S, “Testing Software Design Modeled by Finite-State Machines,” in Conformance testing methodologies and architectures for OSI protocols, IEEE Computer Society Press, pp. 178-187, 1995.

[13] N. Lynch and M. Tuttle, “An introduction to input/output automata,” CWI-Quarterly, vol.2, no. 3, pp. 219–246, Sep 1989.

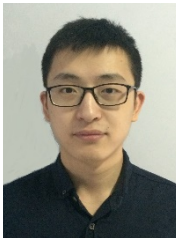
[14] Yarom, Yuval, and K. Falkner, “FLUSH+RELOAD: a high resolution, low noise, L3 cache side-channel attack,” in Proc. USENIX Security Symposium, pp. 719-732, 2014.

[15] Kocher P, Jaffe J, Jun B. “Differential Power Analysis,” Advances in Cryptology CRYPTO’ 99, Springer Berlin Heidelberg, 1999.

[16] Mirkovic J, Reiher P, “A taxonomy of DDoS attack and DDoS defense mechanisms,” Acm Sigcomm Computer Communication Review, vol.34, no. 2, pp. 39-53, 2010.

[17] Zhang SZ, Luo H, and Fang BX, “Regular expressions matching for network security,” Journal of Software, vol.22, no. 8, pp. 1838−1854 (in Chinese), 2011.
(张树壮, 罗浩, 方滨兴, “面向网络安全的正则表达式匹配技术”, 软件学报, 2011, 22(8):1838-1854.)

[18] 上海市科学技术委员会给国家科技部高新技术发展及产业化司的专题报告, “拟态防御原理验证系统测试评估工作情况汇总”, 2016.8.



郭威　于 2015 年在信息工程大学计算机科学与技术专业获得硕士学位。现在国家数字交换系统工程技术研究中心信息与通信工程专业攻读博士学位。研究领域为主动防御、网络体系结构。Email: guowjss@126.com

邬江兴　中国工程院院士, 国家数字交换系统工程技术研究中心教授、博士生导师, 研究领域为主动防御、交换技术与宽带信息网络、高效能计算。

张帆　于 2013 年在信息工程大学通信与信息系统专业获得博士学位。现任国家数字交换系统工程技术研究中心副研究员, 硕士生导师。研究领域为主动防御、芯片设计技术、高性能计算。Email: 13838267352@qq.com

沈剑良　于 2014 年在国防科学技术大学电子科学与技术专业获得博士学位。现任国家数字交换系统工程技术研究中心助理研究员, 在站博士后。研究领域为网络体系结构、主动防御、可重构计算等。Email: shenjianliang@outlook.com