【信息科学与控制工程】　　doi：10.11809/scbgxb2017.04.028

面向 APT 攻击的网络安全防护体系能力分析

倪振华，刘靖旭，王泽军，刘　鹏

（解放军信息工程大学，郑州 450001）

摘要：分析了预防高级可持续攻击（Advanced Persistent Threat，APT）技术和攻击流程，并在 PPDR 网络安全防护模型的基础上，构建了面向 APT 攻击的网络安全防护体系；利用系统动力学方法，建立体系能力模型，并进行仿真分析，为进一步提高网络安全防护能力提供决策建议。

关键词：APT 攻击；系统动力学；仿真分析

本文引用格式：倪振华，刘靖旭，王泽军，等. 面向 APT 攻击的网络安全防护体系能力分析[J]. 兵器装备工程学报，2017(4)：127－131.

Citation format：NI Zhen-hua，LIU Jing-xu，WANG Ze-jun，et al. Ability Analysis of Network Security Protection System for APT Attack[J]. Journal of Ordnance Equipment Engineering，2017(4)：127－131.

中图分类号：TP451　　**文献标识码**：A　　**文章编号**：2096－2304(2017)04－0127－05

Ability Analysis of Network Security Protection System for APT Attack

NI Zhen-hua，LIU Jing-xu，WANG Ze-jun，LIU Peng

（The PLA Information Engineering University，Zhengzhou 450001，China）

Abstract：The technology of Advanced Persistent Threat（APT）attack and the process of attack were analyzed. Based on PPDR network security protection model，the network security protection system for APT attack was constructed. Based on the system dynamics method，the system capability model was established for the APT attack process，and the simulation analysis was carried out to provide the decision-making for further improving the network security protection capability.

Key words：APT attack；system dynamics；simulation analysis

随着计算机技术和互联网的不断发展，网络信息系统所面临的安全问题日趋严重。APT（Advanced Persistent Threat）即高级可持续攻击，是近几年出现的新型综合性网络攻击手段，具有针对性、持续性、多态性、隐蔽性等特点[1]。目前，许多学者提出了不同的防御 APT 攻击的信息安全框架，为网络信息系统的构建提供了重要的参考依据，而检验防护体系是否合理有效，分析和优化网络安全防护体系能力显得尤其重要[2-6]。

系统动力学（System Dynamics，SD）是美国麻省理工学院的 Jay W. Forrestet 教授提出的研究系统动态行为的一种计算机仿真技术，根据系统论、控制论、信息论以及系统理论等，运用定性与定量相结合的方法对网络安全防护体系能力展开分析，能够查找网络体系构架的薄弱环节，做好针对性的补救措施。

1　面向 APT 攻击的网络安全防御流程

APT 攻击是传统网络入侵、渗透手段的集成和综合运用，其攻击过程可概括为 6 个阶段：侦查准备阶段、代码传入阶段、初次入侵阶段、保持访问阶段、扩展行动阶段和攻击收

收稿日期：2016－11－02；**修回日期**：2016－12－22

基金项目：全军军事类研究生资助课题（2015JY129）

作者简介：倪振华（1986—），男，硕士研究生，主要从事军事管理评估与决策研究。

益阶段[8]。与传统攻击相比,APT 攻击具有更强的组织性,其攻击目标更加明确、攻击手段更加复杂,造成的危害也更大。

1.1 APT 攻击防御核心技术

1)沙箱技术。如果攻击者利用零日漏洞实施攻击,传统的特征匹配检测技术将无法应对,使用沙箱技术识别未知攻击与异常行为是一个很有效的方法。

2)信誉技术。安全信誉是对网络资源和服务相关实体安全可信性的评估和看法,建立包括 WEB URL 信誉库、文件 MD5 码库、僵尸网络地址库、威胁情报库等,可以为新型病毒、木马等 APT 攻击的检测提供强有力的技术辅助支撑,实现网络安全设备对不良信誉资源的阻断或过滤。

3)异常流量分析技术。通过对流量建模,识别异常行为。由于无法提取未知攻击的特征,只能先对正常的网络行为建模。当发现网络连接的行为模式明显偏离正常模型时,就可能存在网络攻击。

4)密码技术。针对 APT 攻击的过程中控制权限的非法获取和重要信息资产的窃取,相应地使用密码技术,能够更好地保护系统的安全。

5)大数据技术。通过对网络数据分析,将可疑的网络扫描信息、Web 会话、Email 记录、防火墙日志等信息进行智能化关联分析,将传统的基于时间点的检测转变为基于历史时间窗的检测。

1.2 网络安全防御流程

针对 APT 攻击的 6 个阶段,需要在每个攻击阶段运用相应的技术策略进行防御。面对 APT 攻击的侦查准备阶段,需要更多地应用管理技术来预防。通过加强管理手段、法规制度等,加强对人员以及组织的安全管理。面对 APT 攻击的后 5 个阶段,则更多地应用技术手段来应对,结合 APT 攻击防御核心技术的同时,应用传统的安全防护技术,如 IDS/IPS 入侵检测、安全网关、监控审计等。

同时,利用大数据技术,对相关安全事件进行纵向与横向关联分析,建立如图 1 所示的网络安全防御流程。

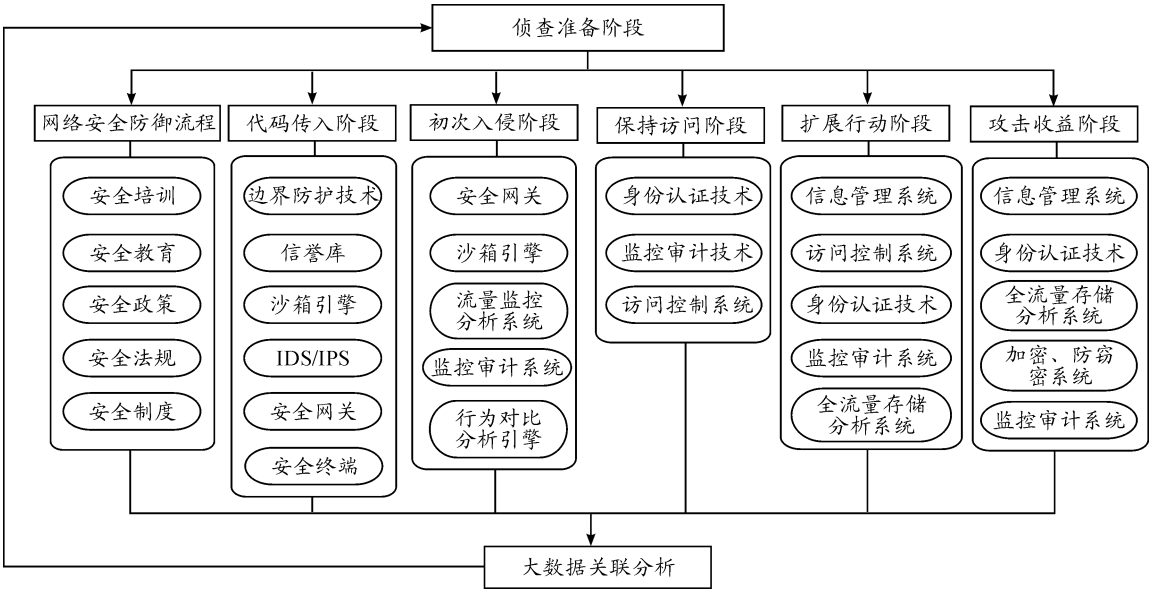

图 1 面向 APT 攻击的网络安全防御流程

2 面向 APT 攻击的网络安全防护体系框架构建

2.1 PPDR 网络安全防护模型

PPDR 模型,如图 2 所示,是美国国际互联网安全系统公司(ISS)在 90 年代末提出来的,由动态的管理角度给出目标系统防御基本原则,现今此模型已成为国际认可的、实际可操作、信息指导系统安全建设与安全运营模型构架[9]。PPDR 模型遵循整体安全策略控制跟指导,全面结合了防御工具(像防火墙、系统操作的身份认证、加密等手段),同时利用检测工具(像漏洞评估、入侵检测等系统)了解、评估系统安全状态,把系统恢复到“安全性最高”、“风险最低”状态。防御、检测跟响应组成一个完整、动态安全循环,PPDR 模型是一个动态模型,其中引进了时间的概念,而且对如何实现系统安全,如何评估安全的状态,给出了可操作性的描述。

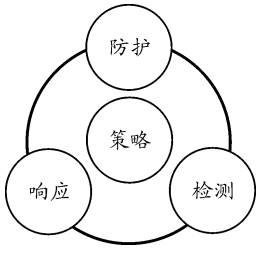

图 2 PPDR 模型

PPDR 模型给网络安全管理提供了方法,所有的安全问

题都可以在统一的策略指导下，采取防护、检测、响应等不断循环的动态过程。然而，PPDR 安全模型唯一的动态因素是建立在检测上，而解决手段仅仅是防护。如果要使这种安全模型取得成功必然要依赖系统正确的设置和完善的防御手段，并且在很大程度上针对固定的威胁和环境弱点，但它忽略了网络安全的动态性特征。

2.2 网络安全防护体系框架

面向 APT 攻击的网络安全防护体系是一项系统工程，不是对各个系统的简单罗列，而是对构成网络安全防护体系各个分系统功能的具体明确，通过对各个分系统的分解，明确各个保障源组成部分的功能及其相互关系。根据 PPDR 网络安全防护模型及 APT 攻击的防御流程，设计网络安全防护体系框架如图 3 所示。

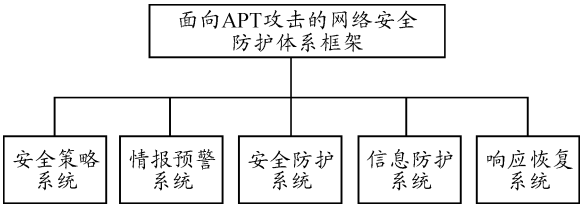

图 3 面向 APT 攻击的网络安全防护体系框架

1）安全策略系统。安全策略系统是为了保证网络安全防护体系能够高效运行，对体系内的资源进行统一管理分配，使整个体系达到效能最大化的主要组织系统。安全策略系统由人员管理子系统、控制决策子系统、技术保障子系统和法规制度子系统组成，是整个体系的中枢神经和指挥中心，如图 4 所示。

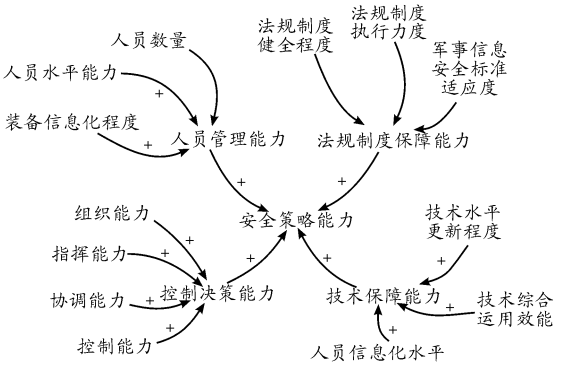

图 4 安全策略系统能力

2）情报预警系统。情报预警系统是网络安全防护体系的“眼睛”，是综合运用各种监测设备和信息获取手段，对可能发生的情况进行分析处理，从而达到提前预防、减少损失的目的。情报预警系统由情报获取子系统、情报处理子系统和情报共享子系统组成，在网络安全防护过程中，对 APT 攻击的检测除了内网本身收集到的数据以外，第三方机构提供的 APT 攻击信息对于检测 APT 攻击也至关重要，可以突破单点防护的传统观念，有效提高系统防御 APT 攻击的能力，如图 5 所示。

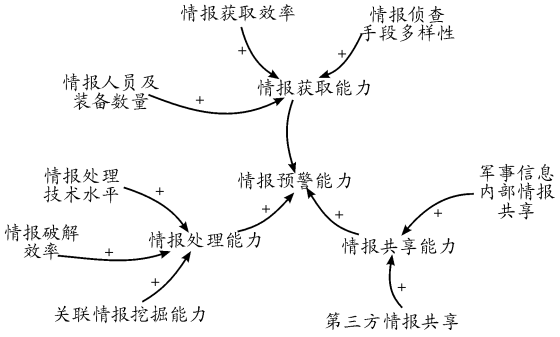

图 5 情报预警系统能力

3）安全防护系统。安全防护系统是网络安全防护体系的基础，合理运用各种资源，根据不同情况对资源投入量进行调整，使防御效果最大化。安全防护系统由防火墙子系统、数据加密子系统、访问控制子系统和网络欺骗子系统等组成，安全防护系统的运行直接影响着整个防护过程，如图 6 所示。

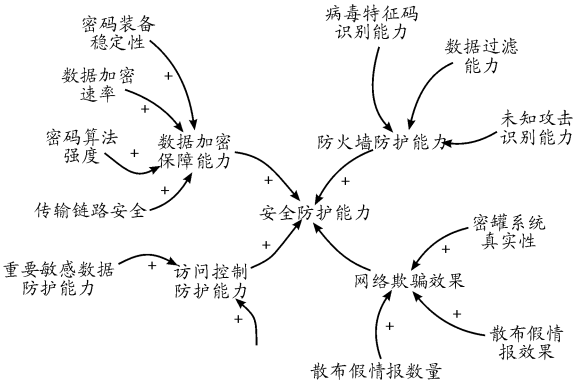

图 6 安全防护系统能力

4）信息防护系统。信息防护系统是网络安全防护体系的重要支撑，通过各种技术手段的使用，对体系内数据进行加密、隐藏甚至欺骗，从而达到防护的目的。信息防护系统由身份认证子系统、监控审计子系统、入侵检测子系统和病毒防护子系统组成，确保信息的完整性、保密性和可用性，如图 7 所示。

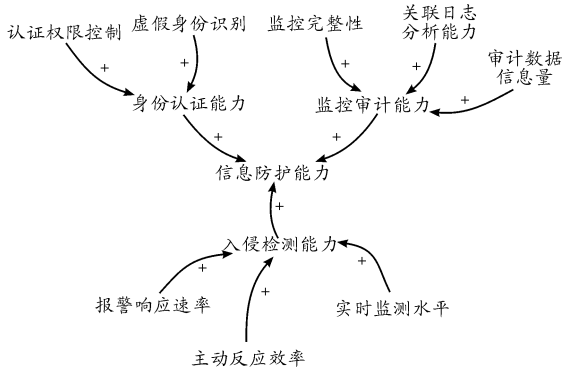

图 7 信息防护系统能力

5）响应恢复系统。响应恢复系统是对体系内各信息系

统的运行进行安全评估,在出现安全威胁时自动处理。响应恢复系统由系统重构子系统、应急响应子系统、数据恢复子和攻击溯源子系统等组成,确保在各种情况下体系的正常运转,如图 8 所示。

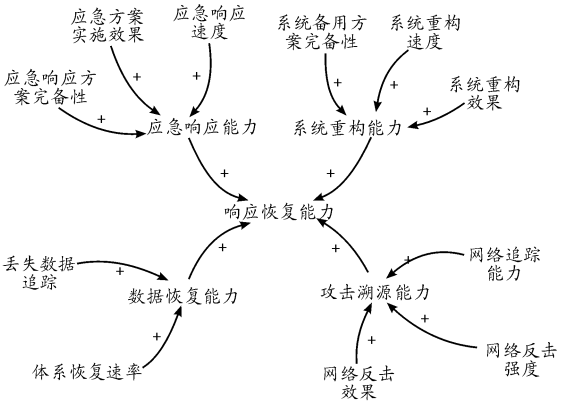

图 8 响应恢复系统能力

3 面向 APT 攻击的系统动力学模型

网络安全防护体系能力发挥的最终目的是有效阻止 APT 攻击以及消除体系内部的木马后门,恢复系统受感染损坏的资源。通过分析体系能力,对网络安全防护体系能力构成要素发挥功能的程度和重要性进行衡量,找出关键要素、核心环节和防御弱点,为更好地发挥防护能力提出改进措施。

3.1 APT 攻击过程描述

根据 APT 攻击的 6 个阶段和攻击特性,选取网络安全防护体系中的一部分,假设共有节点 N,攻击过程简化如图 9 所示[10-11]。

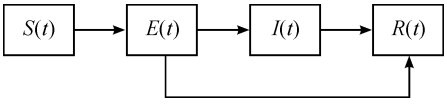

图 9 APT 攻击过程

针对某种未知 APT 攻击来说,$S(t)$表示当前网络中易感染节点的数目,$E(t)$表示 APT 攻击已经取得后门权限节点的数目,$I(t)$表示已经被感染节点的数目,$R(t)$表示通过有效的防护手段变成免疫节点的数目。

$$\frac{\mathrm{d}S(t)}{\mathrm{d}x} = -\gamma S(t)E(t);\ S(0) = S_0 \tag{1}$$

$$\frac{\mathrm{d}E(t)}{\mathrm{d}t} = \gamma S(t)E(t) - \omega\varepsilon I(t) - \mu R(t);\ E(0) = E_0 \tag{2}$$

$$\frac{\mathrm{d}I(t)}{\mathrm{d}t} - \omega\varepsilon I(t) - \lambda R(t);\ I(0) = E_0 \tag{3}$$

$$\frac{\mathrm{d}R(t)}{\mathrm{d}t} = \mu R(t) + \lambda R(t);\ R(0) = E_0 \tag{4}$$

$$S(t) + E(t) + I(t) + R(t) = N \tag{5}$$

其中 γ 定义为 $S(t)$转变为 $E(t)$的速率,ε 定义为 $E(t)$转变为 $I(t)$的速率,μ 定义为 $E(t)$转变为 $R(t)$的速率,λ 定义为 $I(t)$转变为 $R(t)$的速率,ω 为延时函数。式(1)说明了易感染节点个体数量的变化率随着易感染个体和取得后门个体的数量上升而下降,这同样也受限于式(2),因为易感染节点个体的数量以与已经取得后门权限节点个体数量相反的方向增加或减少。式(2)说明了取得后门权限节点个体数量的变化率根据易感染节点个体和取得后门权限个体的数量之比增加或减少,其中还需要减去感染节点和免疫节点个体的数量。式(3)、(4)表达了一个简单的线性关系。式(5)说明整个网络节点个数保持恒定,与每个状态的数量无关。

3.2 面向 APT 攻击的系统动力学流图

本文在分析前述构建的网络安全防护体系框架的基础上,选取影响网络安全防护体系能力的重要因素,把体系中 $E(t)$、$I(t)$和 $R(t)$作为水平变量,建立面向 APT 攻击的系统动力学流程如图 10 所示。

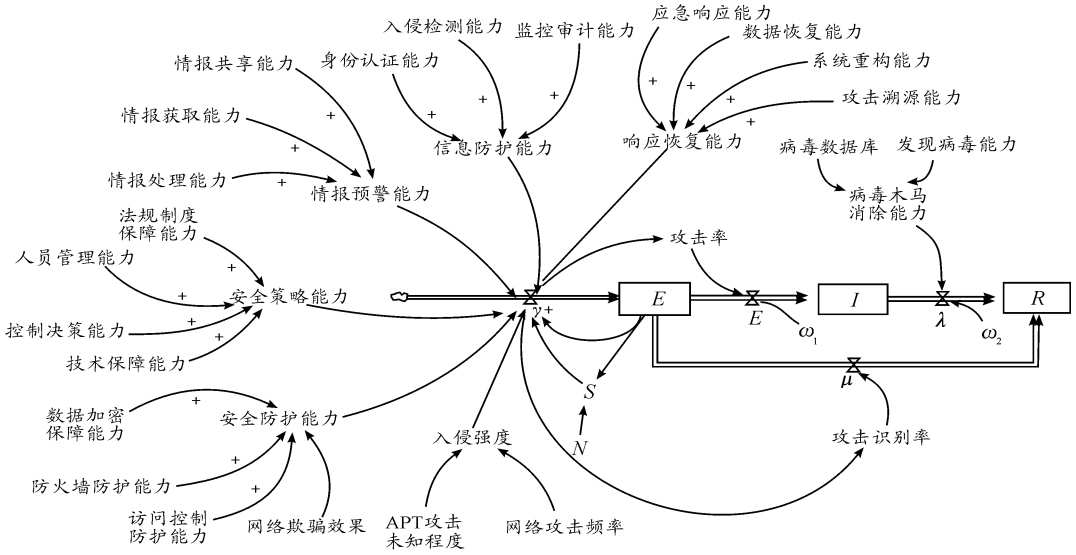

图 10 面向 APT 攻击的系统动力学流图

其中主要参数方程:

$\gamma = E * S *$ 入侵强度/信息防护能力/情报准确性/管理控制能力/节点重要性;

$E = \mathrm{INTEG}(\gamma - \varepsilon - \mu, 10)$;

$\varepsilon = \mathrm{DELAY\ FIXED}$(攻击率,$\omega_1$,0);

$I = \mathrm{INTEG}(\varepsilon - \lambda, 0)$;

$\lambda = \mathrm{DELAY\ FIXED}$(病毒木马清除能力,$\omega_2$,0);

$\omega_1 = \omega_2$;

$R = \mathrm{INTEG}(\lambda + \mu, 0)$;

μ = 攻击识别率。

4 模型仿真分析

为了分析各变量在网络安全防护体系中的作用和地位,针对面向 APT 攻击的系统动力学流图,对各变量赋初值,并通过调整关键变量的取值,看 $E(t)$、$I(t)$ 和 $R(t)$ 的变化曲线,剖析结果。

假设网络安全防护体系运行过程中,设置 INITIAL TIME = 0,FINAL TIME = 50,TIME STEP = 0,Units for time 单位为天,初始节点 $N = 100$, $E(t)$ 的初始值为 10,运行 Vensim 软件模拟,可得各个变量的仿真结果,分析相关变量对仿真结果造成的影响。

图 11 所示为各变量取初值时,网络安全防护体系内节点的变化曲线。在网络防护过程中,γ 随着时间的变化,增加会慢慢变缓,同时 $E(t)$ 受其影响,开始增加较快,之后也会随着时间增加慢慢变缓。观察所构建模型的仿真结果,可以发现网络安全防护体系系统动力学模型和实际防护过程效果基本一致,随着时间增长,节点中存在漏洞的个数会越来越少,体系内被植入后门的节点都是先增加后减少,最后在体系整体作用下,植入后门的节点趋于零;$I(t)$ 在延时函数的作用下,过了病毒的潜伏期或者由于攻击者直接控制,受感染的节点会逐渐增加。$R(t)$ 受攻击识别率和病毒木马清除能力的影响,也会慢慢增加,但受限于 μ 和 λ 的影响。

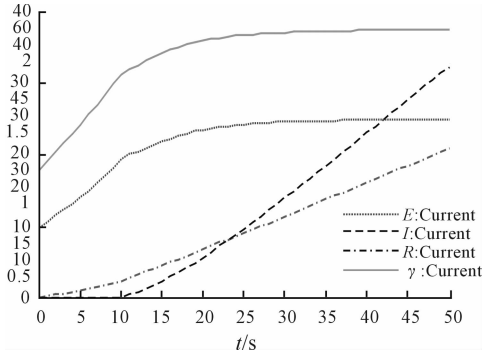

图 11 γ、$E(t)$、$I(t)$ 和 $R(t)$ 的变化趋势

图 12 所示为调整安全策略能力、情报预警能力、安全防护能力、信息防护能力和响应恢复能力后,使 γ 值变小后 $E(t)$、$I(t)$ 和 $R(t)$ 变化趋势。通过增强安全策略能力,提升情报预警能力或者加强安全防护能力,使得 γ 变小,说明以上措施能够有效减少 $S(t)$ 被植入后门的速率,使 $E(t)$ 增加的速率变慢。

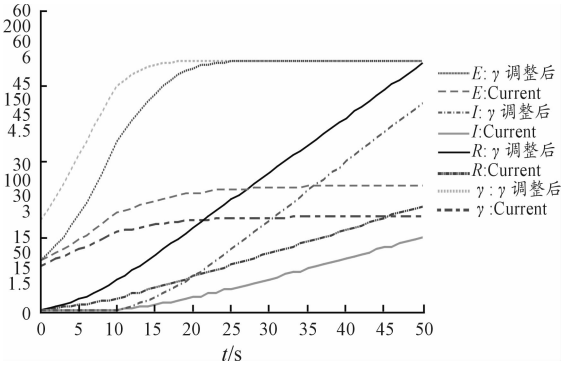

图 12 γ 值变小后的变化趋势

分析模型的仿真结果,可以得出以下结论:

1) 面向 APT 攻击的网络安全防护体系依赖于各个系统能力的合成。从仿真结果可知,在面向 APT 攻击初始,系统处于被动状态,体系内被植入后门以及受感染的节点处于增加的状态,随着时间的增加,各系统发挥各自作用,使系统逐渐恢复,被植入后门的节点和被感染节点数目减少,转变成免疫节点。

2) 体系内各系统能力的增加能够提升体系整体防御能力。各系统能力增加,都能使得体系防御能力增加,但也不是无止尽地增加,同时还需要各系统的配合。如单纯增加信息防护能力,会使系统内网络变得更复杂,同时人员增多使得管理控制能力下降,对于体系维护造成困难,维护成本也相应提高。

3) 体系内模拟数值与真实网络环境有一定差距。网络安全防护体系内各系统能力量化受主观影响较大,且攻击者发动攻击的延迟无法与真实情况相符,只能取出平均值,这在网络安全防护中是至关重要的,数据的窃取破坏往往持续时间较短。

5 结束语

本文运用系统动力学的方法对面向 APT 攻击的网络安全防护体系能力进行了分析,通过研究,对建设和提高体系防护能力有一定的积极意义,但如何合理配置体系资源,以及各种力量手段的应用,还需要进一步的研究。

参考文献:

[1] 陈剑峰,王强,伍森. 网络 APT 攻击及防范策略[J]. 信息安全与通信保密,2012(7):24 - 27.

[2] 李凤海,李爽,张佰龙. 高等级安全网络抗 APT 攻击方案研究[J]. 信息网络安全,2014(8):109 - 114.

(下转第 152 页)

通过计算,上述10组数据计算机评分与专家评分差值 x 的数学期望 $E(x)=2.15$;均方差 $\sqrt{D(x)}=3.293$。比较得出二者之间的差距并不显著,本研究所建立的油门杆定量评判模型较为合理。

3 结论

针对飞行操作存在明显的个体差异,本研究借助LabVIEW记录油门杆模拟操作的数据,建立了油门杆操作评判模型,并引入粗糙集理论定量分析油门杆操作水平,最终将数据反馈给操作人员。操作人员接受反馈结果,针对自身操作不当之处,及时做出相应调整。结果表明,基于粗糙集理论的评判模型能有效对油门杆操作进行评判,为今后进行飞行动作的定量评判提供了一种思路。

参考文献:

[1] 李珍,王海涛,赫云飞. 面向人机工效的座舱显控设备布局问题研究[J]. 飞机设计,2016,36(1):1-7.

[2] 武强,李晓重,陈根生,等. 座舱发动机油门杆的操纵对发动机工作影响的分析[C]//中国科学年会. 贵阳:[出版社不详],2013.

[3] YEE Leung,FISCHER M M,WU Weizhi Wu,et al. A rough set approach for the discovery of classification rules in interval-valued information systems[J]. International Journal of Approximate Reasoning,2008,5(2):233-246.

[4] 鲍新中,刘澄. 一种基于粗糙集的权重确定方法[J]. 管理学报,2009,6(6):729-732.

[5] 高尚. 基于Rough集和支持向量机的作战飞机效能评估[J]. 计算机工程,2006,32(14):184-186.

[6] YE Qing,WU Xiaoping,ZHANG Changhong. An Intrusion Detection System based on evidence theory and Rough Set Theory[J]. Journal of Electronics,2009,26(6):777-781.

[7] 郭庆,吴磊. 多粒度背景下直觉模糊信息系统的粗糙集及其决策[J]. 系统工程与电子科技,2016,38(2):347-351.

[8] 黄嘉智. 基于LabVIEW的高速数据采集及管理系统设计[D]. 北京:北京理工大学,2016.

[9] 袁浩. 基于量子蚁群算法的粗糙集属性约简方法[J]. 计算机工程与科学,2010,32(5):82-84.

[10] 赵振宇,韩维. 飞机着舰轨迹稳定性及飞行员操纵策略研究[J]. 兵工自动化,2015(11):26-29.

(责任编辑 杨继森)

(上接第131页)

[3] 杜跃进,翟立东,李跃. 一种应对APT攻击的安全架构:异常发现[J]. 计算机研究与发展,2014(7):1633-1645.

[4] 许婷. 一种有效防范APT攻击的网络安全架构[J]. 信息安全与通信保密,2013(6):65-67.

[5] 高赟,周薇,韩翼中. 一种基于文法压缩的日志异常检测算法[J]. 计算机学报,2014(1):73-86.

[6] 周涛. 大数据与APT攻击检测[J]. 信息安全与通信保密,2012(7):29.

[7] 钟永光,贾晓菁,李旭. 系统动力学[M]. 北京:科学出版社,2009.

[8] 付钰,李洪成,吴晓平,等. 基于大数据分析的APT攻击检测研究综述[J]. 通信学报,2015(11)23-26.

[9] 王永光. 基于petri网的网络安全防御体系评估模型的研究[D]. 长沙:湖南大学,2014.

[10] 胡向东,刘竹林. 网络化测控系统的信息安全方法研究[J]. 重庆理工大学学报(自然科学),2016(5):81-87.

[11] TED G. Lewis/NETWORK SCIENCE Theory and Applications[M]. 北京:机械工业出版社,2011.

(责任编辑 杨继森)