Journal of Computer Applications
计算机应用,2018,38(S2):157-163,169
ISSN 1001-9081
CODEN JYIIDU
2018-12-25
http://www.joca.cn

文章编号:1001-9081(2018)S2-0157-07

基于拓扑漏洞分析的网络安全态势感知模型

李腾飞*,李 强,余 祥,巫岱玥
(国防科技大学 网络工程系,合肥 230037)
(* 通信作者电子邮箱 ltfstudy@sina.cn)

摘 要: 针对网络安全态势感知研究存在缺乏有效的网络安全态势数据采集和要素提取方法,网络安全态势的理解和分析计算难以进行的现状,建立基于拓扑漏洞分析的网络安全态势感知模型。首先,采用扩展有限状态机描述网络中当前状态和可能发生的状态,确定网络的所有状态;其次,计算威胁存在概率、威胁状态概率、状态转移概率和威胁损失等态势组成值,综合得到网络安全态势;最后,通过数值对比,明确网络的安全状态。实验结果表明:建立的网络安全态势感知模型与实际网络安全态势相比,均方差为1.2%;与层次分析模型和神经网络模型相比,均方差降低1.5%~2.1%。

关键词: 网络安全;拓扑漏洞分析;安全态势感知;态势获取;态势理解
中图分类号: TP393 **文献标志码:** A

Network security situational awareness model based on topological vulnerability analysis

LI Tengfei*, LI Qiang, YU Xiang, WU Daiyue
(*Department of Network Engineering, National University of Defense Technology, Hefei Anhui* 230037, *China*)

Abstract: In view of network security situational awareness research, there is a lack of effective data collection and element extraction methods, and it is difficult to understand, analyze and calculate network security situation. Therefore, a network security situational awareness model based on topology vulnerability analysis was established. Firstly, the extended finite state machine was used to describe the current state and possible states of the networks, thus determining all the states of the network. Secondly, the probability of threat, the probability of threat status, the state transition probability and the threat loss were calculated, and then the network security situation was obtained synthetically. Finally, the security state of the network was determined by numerical comparison. The experimental results show that, the mean square error of the network security situational awareness model is 1.2%, compared with the actual network security situation; compared with the analytic hierarchy process and the neural network model, the mean square error decreased by 1.5% to 2.1%.

Key words: network security; topological vulnerability analysis; security situation awareness; situation acquisition; situation comprehension

0 引言

网络安全态势感知(Network Security Situation Awareness, NSSA)的概念早在1999年就提出了,它是指在大规模网络环境中,对能够引起网络态势发生变化的要素进行提取、理解、评估、显示以及对未来发展趋势的预测[1]。拓扑漏洞分析(Topological Vulnerability Analysis,TVA)[2]是指通过获取网络系统中的漏洞信息、拓扑信息、攻击信息等,分析网络可能遭受的安全威胁以及预测攻击者利用漏洞可能发动的攻击,构建拓扑漏洞图,展示网络中可能存在的薄弱环节,评估网络安全状态的技术。

网络安全态势感知是网络空间安全领域研究的热点和重点。文献[3]基于报警信息和性能指标,提出一种自下而上、先局部后整体的层次化网络安全态势感知模型,建立确定的数学表达式,对服务、主机和网络三个层次分别进行评估,实现网络安全态势感知定量描述;但该模型的数学公式在构建时依赖于专家知识,主观随意性较强,缺少科学依据。文献[4]在分层的基础上,加入威胁、管理员和用户三方,建立Markov博弈模型,判断当前网络安全态势,给出最佳加固方案;但缺少对数据近似处理,应对网络复杂的能力较弱。文献[5]采用拓扑漏洞分析方法中面向网络系统的分析方法,通过探测获取网络设备及连接安全信息,获取网络中的漏洞、网络流量、拓扑等信息,确定网络系统的当前状态及可能存在的薄弱环节,实现网络安全态势感知。文献[6]提出一种基于神经网络的网络安全态势感知模型,采用自适应遗传算法对网络参数进行优化并实现网络安全态势感知;但在数据采集、要素提取时,未提供有效的计算方法,而采用人工执行,效率较低。文献[7]采用基于规则的拓扑漏洞分析方法,通过规则对采集的要素数据进行分析处理,减少计算量,提高态势感知的效率。文献[8]采用DS(Dempsetr/Shafer)证据理论建立态势指标和评估准则,通过专家知识融合推理实现网络安全态势感知,降低了网络安全态势要素不确定性对态势的影响;但融合推理规则众多,使得推理代价高、效率低。文献[9]将层次的网络和感知调控相结合,形成闭环反馈控制结构,建立

收稿日期:2018-01-15;修回日期:2018-04-04。
基金项目:电子工程学院技术基础条件建设项目(72160603);电子工程学院科研基金资助项目(KY16Z002)。
作者简介:李腾飞(1993—),男,安徽和县人,硕士研究生,主要研究方向:网络与信息安全; 李强(1962—),男,安徽合肥人,教授,硕士,主要研究方向:软件工程、信息安全; 余祥(1986—),男,江西景德镇人,讲师,硕士,主要研究方向:软件工程、信息安全; 巫岱玥(1994—),男,四川乐山人,硕士研究生,主要研究方向:软件分析、信息安全。

网络安全态势融合感控模型，实现网络安全态势变化趋势；但融合的结果以数值形式展示，不便于理解网络安全态势。文献[10-11]针对数值表示方法过于专业化，采用拓扑漏洞分析技术中图的表示方法描述网络安全态势。

在网络安全形势日益恶化的今天，如何快速有效地获取网络系统的安全状况、提高网络安全应对水平、增大网络安全的预警时间，成为网络空间安全领域研究的重要问题。网络安全态势感知研究存在的问题是缺乏有效的网络安全态势数据采集和要素提取方法，使得网络安全态势的理解和分析计算难以进行。针对这一研究现状，提出一种基于拓扑漏洞分析的网络安全态势感知模型，从网络安全态势信息获取入手，通过网络安全态势要素的获取、理解和分析处理，采用形式化的方式描述获取要素及其关联关系，计算网络系统安全态势值，实现网络安全态势感知。模型的结果易于理解，优化了传统的纯数值表示，与实际结果更相符。

1 拓扑漏洞分析

拓扑漏洞分析为网络安全态势感知的“态势识别”“态势理解”和“态势展示”提供了技术支持，是通过对网络系统中漏洞间依赖关系和网络攻击路径的分析，获知网络系统安全态势的一种方法。，也是实现网络安全防御的一项技术。拓扑漏洞分析由三个部分组成：信息获取、信息理解和信息展示，其内容构成如图1所示。

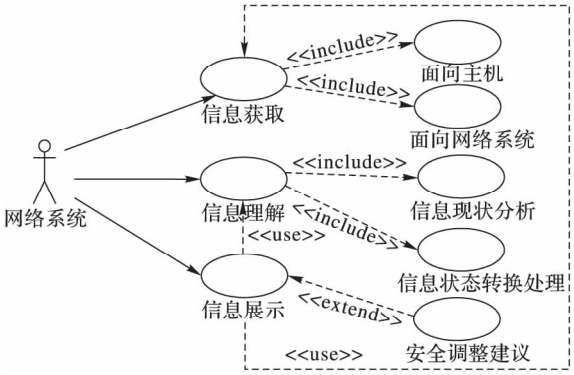

图1 拓扑漏洞分析内容构成

1)信息获取。是采用扫描或者探测的手段获取网络系统中拓扑漏洞分析所需信息的方法。根据获取信息对象的不同，拓扑漏洞的信息获取方法可分为面向主机的拓扑漏洞分析方法和面向网络系统的拓扑漏洞分析方法[6,12]。

2)信息理解。是对获取的网络信息采用拓扑漏洞分析的方法进行处理，包括信息现状分析和信息状态转换处理。

3)信息展示。是对信息理解分析结果的图形化展示和对网络系统安全状况调整的建议。

网络安全态势感知[6,13]是对所收集的网络安全态势信息融合分析、计算理解，判断网络安全态势状况并对网络安全态势进行预测。网络安全态势感知包括安全状态的获取、识别、确认和评估，不论是网络安全态势的获取和识别还是网络安全态势的确认和评估，都需要相应的理论和方法。拓扑漏洞分析技术的“信息获取”“信息理解”和“信息展示”为解决网络安全态势感知的获取、识别、确认和评估提供了技术支持。因此，利用拓扑漏洞分析技术的“面向主机”和“面向网络系统”的信息获取方法，获取网络安全态势信息，通过对获取的网络安全态势信息提炼和分析，能够得到网络安全态势感知态势理解所需的参数，为态势理解提供支持；利用拓扑漏洞分析技术中的态势信息分析计算、安全状态描述、网络系统安全评估、网络系统安全威胁预测的方法，对网络安全态势感知中的网络安全状况进行理解、评估和预测。

2 网络安全态势感知模型

要获取网络安全态势，就需要对网络系统的安全状态信息数据进行分析、处理，因此需要建立网络安全态势感知模型。网络安全态势感知模型用于感知网络安全态势，应解决两个问题：态势要素的分析处理和安全态势值的计算。对获取的要素分析处理时需要描述要素之间的状态转换关系，掌握要素信息及其关联关系；网络安全态势值的计算是在状态分析处理的基础上，针对当前及可能发生的状态，计算网络安全态势值，明确网络安全态势，因此所建立的网络安全态势感知模型是一个基于拓扑漏洞分析的网络安全态势感知模型(Network Security Situation Awareness Model，NSSAM)，如图2所示。

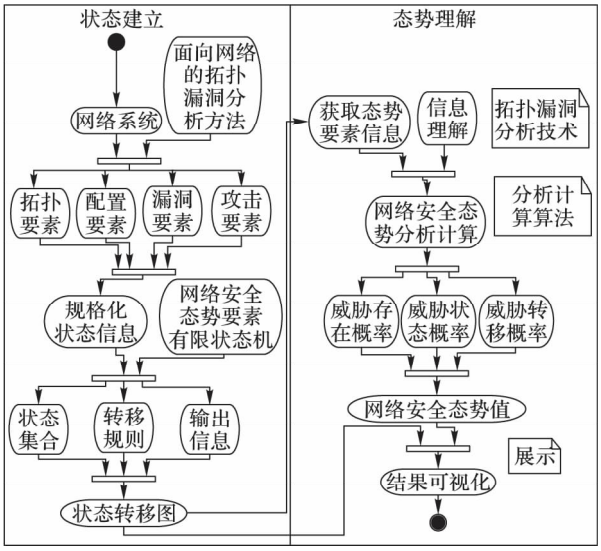

图2 基于拓扑漏洞分析的网络安全态势感知模型

从图2可以看到，基于拓扑漏洞分析的网络安全态势感知模型是通过两个步骤实现：1)状态建立。对网络系统采用面向网络的拓扑漏洞分析方法得到拓扑要素、配置要素、漏洞要素和攻击要素，规格化形成状态，作为输入，采用拓扑漏洞分析技术中信息状态转换处理方法，利用有限状态机的形式化表示方法建立状态语义、输出语义及状态转换规则。2)态势理解。以状态建立结果为输入，采用拓扑漏洞分析技术中信息理解方法，建立公式计算网络中威胁存在概率、状态转移概率和威胁损失等数据，得到网络安全态势值。

2.1 状态建立

状态建立是建立有限状态机描述网络安全态势，即建立网络安全态势有限状态机。网络安全态势包括网络中当前状态和可能发生的状态。

2.1.1 网络安全态势有限状态机

网络安全态势来源于规格化的态势信息，即当前网络安全状态包括拓扑结构、配置，可能发生状态是指漏洞攻击状态。由于网络受到自身原因或者外界干扰会导致网络安全态势发生改变，所以网络中状态会发生转移，因此使用有限状态自动机[14-15]对形成的状态进行分析描述。

定义1 网络安全态势有限状态机(Network Security Situation Patulous Finite State Machine，NSSPFSM)是扩展的有

限状态机,用六元组表示:

$$NSSPFSM = (S, I, s_0, F, T, \delta) \quad (1)$$

$S = \{s_0, s_1, \cdots, s_n\}$,状态的集合,表示在任意时刻,有限状态机只能处于一个确定的状态。对拓扑结构、配置和漏洞攻击描述时,将存在不同的状态,具体状态语义如表 1 所示。

I:输入集合,网络系统中拓扑、配置、漏洞攻击等安全状态。

s_0:初始状态,即当前由拓扑、配置、漏洞攻击等组成的网络安全状态。

F:结束状态,表示所有可作为状态分析终点的状态。

T:输出集合,表示态势发生改变可能导致的变化或者空输出(无变化)。拓扑结构、配置和漏洞攻击因状态转移将产生不同的输出,具体输出语义如表 2 所示。

$\delta = S \times I \rightarrow S$ 是转移函数,由当前状态和输入决定,通过状态转移规则产生相应的状态转移。拓扑结构、配置和漏洞攻击由于当前状态和输入不同,状态转移规则也不同,具体规则在 2.1.2 ~ 2.1.4 节中描述。

表 1　状态语义

序号	有限状态机	语义	记号	说明
1	全部	初始状态	St_Initial	表示状态机的开始
2		结束状态	St_End	表示状态转化结束,是伪状态
3	拓扑结构	结构变化状态	St_Structure	表示拓扑结构发生变化,中间状态
4	有限状态	节点信息状态	St_Node	表示节点的信息发生变化
5	机 TEFSM	节点联系状态	St_Link	表示节点联系的信息发生变化
6		配置变化状态	Dt_Deploy	表示配置发生变化,中间状态
7	配置状态	端口状态	Dt_Port	表示端口的状态发生变化
8	有限状态	服务状态	Dt_Service	表示开放服务状态发生变化
9	机 DEFSM	操作系统状态	Dt_OS	表示设备操作系统状态发生变化
10		软件版本状态	Dt_Edition	表示软件版本状态发生变化
11		漏洞变化状态	Lt_Change	表示漏洞发生变化,中间状态
12		主机状态	Lt_Host	表示漏洞所在主机发生变化
13	漏洞攻击	漏洞利用后果状态	Lt_After	表示利用后果发生变化
14	有限状态	攻击变化状态	At_Change	表示攻击发生变化,中间状态
15	机 LEFSM	攻击源状态	At_Host	表示攻击发起主机发生变化
16		漏洞利用状态	At_Use	表示利用漏洞的变化
17		攻击前提状态	At_Pre	表示攻击前置条件的变化

表 2　输出语义

序号	有限状态机	语义	记号
1	拓扑结构有限状态机 TEFSM	拓扑结构变化产生 IP 地址变化	OutP_IP
2		拓扑结构变化产生节点数目变化	OutP_Node
3		拓扑结构变化产生节点联系变化	OutP_Link
4		拓扑结构变化产生拓扑结构变化	OutP_Structure
5		拓扑结构变化不产生具体信息变化	OutP_Invalid
6	配置状态有限状态机 DEFSM	配置状态变化产生端口数目变化	OutP_PortD
7		配置状态变化产生服务开放变化	OutP_ServiceD
8		配置状态变化产生操作系统变化	OutP_OSD
9		配置状态变化产生软件版本号变化	OutP_EditionD
10		配置状态变化产生网络配置变化	OutP_DeployD
11		配置状态变化不产生具体信息变化	OutP_InvalidD
12	漏洞攻击有限状态机 LEFSM	漏洞变化产生漏洞所在主机变化	OutP_HostL
13		漏洞变化产生漏洞利用后果变化	OutP_AfterL
14		漏洞变化产生漏洞状态变化	OutP_ChangeL
15		漏洞变化不产生具体信息变化	OutP_InvalidL
16		受到攻击变化产生攻击发起主机变化	OutP_HostA
17		受到攻击变化产生攻击利用漏洞变化	OutP_UseA
18		受到攻击变化产生攻击状态变化	OutP_ChangeA
19		受到攻击变化产生攻击前提变化	OutP_PreA

这里描述的网络安全态势有限状态机包括三个:拓扑结构有限状态机、配置状态有限状态机和漏洞攻击有限状态机。

2.1.2　拓扑结构有限状态机

拓扑结构有限状态机(Topology Elements Finite State Machine,TEFSM)是一个用式(1)定义的网络安全有限状态机,描述网络系统拓扑状态的变化。其中:S、I、s_0、F、T 与式(1)网络安全有限状态机的定义相同。δ 是拓扑结构有限状态机的状态转移规则,简称拓扑状态转移规则,用于描述转移函数,定义不同状态发生转移的条件,包括初始状态、结构变化状态、节点信息状态和节点联系状态、结束状态之间的相互转移。

拓扑状态转移规则如下:

1)在某拓扑结构状态下,当网络系统拓扑结构未发生变化,而 IP 地址改变 OutP_IP 时,初始状态迁移到节点信息状态 St_Node;

2)当检测到拓扑结构变化,即输出拓扑变化产生拓扑结构变化 OutP_Structure,从初始状态 St_Initial 转移到结构变化状态 St_Structure;

3)当处于结构变化状态 St_Structure,若有节点增加或者减少,节点数目变化 OutP_Node,将转移到节点信息状态 St_Node;

4)当处于结构变化状态 St_Structure,若有节点联系增加或者减少,节点联系变化 OutP_Link,将迁移到节点联系状态 St_Link;

5)当处于节点信息状态 St_Node,若节点增加或者减少,则导致节点联系变化 OutP_Link,将迁移到节点联系状态 St_Link;

6)当处于节点信息状态 St_Node,若有 IP 地址改变 OutP_IP,将状态迁移到自身。

7)当处于节点信息状态 St_Node,若无具体信息变化产生 OutP_Invalid,将状态迁移到结束状态 St_End;

8)当处于节点联系状态 St_Link,若无具体信息变化产生 OutP_Invalid,将状态迁移到结束状态 St_End。

拓扑结构有限状态自动机 TEFSM 状态之间的转移图,如图 3 所示。

2.1.3　配置状态有限状态机

配置状态有限状态机(Deployments Finite State Machine,DEFSM)是一个用式(1)定义的网络安全有限状态机,描述网络系统配置状态的变化。其中:S、I、s_0、F、T 与式(1)网络安全有限状态机的定义相同。δ 是配置状态有限状态机的状态转移规则,简称配置状态转移规则,用于描述转移函数,定义不同状态发生转移的条件,包括初始状态、配置变化状态、端口状态、服务状态、操作系统状态、软件版本状态和结束状态之间的相互转移。

配置状态转移规则如下:

1)在某配置内容状态下,当网络配置发生变化 OutP_DeployD,将从初始状态 Dt_Initial 迁移到配置变化状态 Dt_Deploy;

2)当处于配置变化状态 Dt_Deploy,若端口开放或者关闭,导致端口数目变化 OutP_PortD,将从配置变化状态 Dt_Deploy 迁移到端口状态 Dt_Port;

3)当处于端口状态 Dt_Port,若由于端口开放关闭导致开放服务的增加或者减少,将导致服务开放变化 OutP_ServiceD,从端口状态 Dt_Port 迁移到服务状态 Dt_Service;

4)当处于配置变化状态 Dt_Deploy,若之间出现服务的开放或者关闭,将从配置变化状态 Dt_Deploy 迁移到服务状态 Dt_Service;

5)当处于服务状态 Dt_Service,若无具体信息变化产生 OutP_InvalidD,将状态迁移到结束状态 Dt_End;

6)当处于配置变化状态 Dt_Deploy,若出现操作系统更换 OutP_OSD,将从配置变化状态 Dt_Deploy 迁移到操作系统状态 Dt_OS;

7)当处于操作系统状态 Dt_OS,由于操作系统版本变化导致软件版本变化 OutP_EditionD,将从操作系统状态 Dt_OS 迁移到软件版本状态 Dt_Edition;

8)当处于软件版本状态 Dt_Edition,若无具体信息变化产生 OutP_InvalidD,将状态迁移到结束状态 Dt_End;

9)当处于配置变化状态 Dt_Deploy,若出现软件版本变化 OutP_EditionD,将从配置变化状态 Dt_Deploy 迁移到软件版本状态 Dt_Edition。

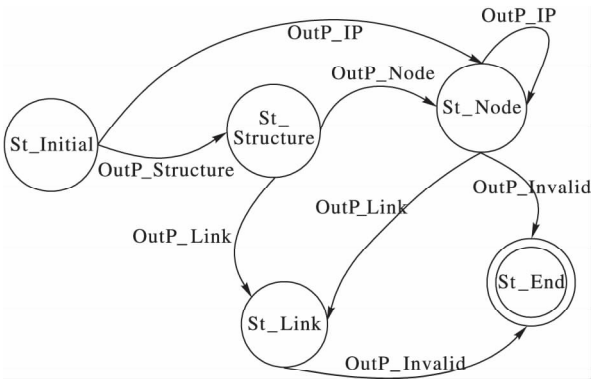

图3 拓扑结构有限状态自动机状态转移图

配置状态有限状态自动机 DEFSM 状态之间的转移图,如图4所示。

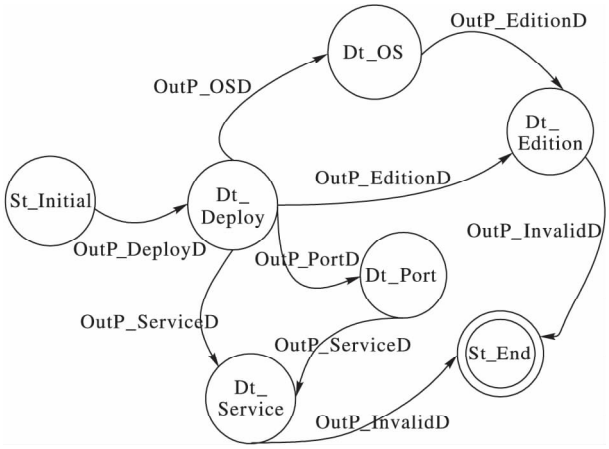

图4 配置状态有限状态自动机状态转移图

2.1.4 漏洞攻击有限状态机

漏洞攻击有限状态机(Leak Elements Finite State Machine,LEFSM)是一个用式(1)定义的网络安全有限状态机,描述网络系统安全状态的变化。其中:S、I、s_0、F、T 与式(1)网络安全有限状态机的定义相同。δ 表示状态转移规则,简称漏洞攻击状态转移规则,用于描述转移函数,定义不同状态发生转移的条件,包括初始状态、漏洞变化状态、主机状态、漏洞利用后果状态和结束状态等状态之间的相互转移。

漏洞攻击状态转移规则如下:

1)在某漏洞攻击状态下,当漏洞状态发生变化 OutP_ChangeL,将从初始状态 Lt_Initial 迁移到漏洞变化状态 Lt_Change;

2)当处于漏洞变化状态 Lt_Change,若漏洞所在主机发生变化 OutP_HostL,将从漏洞变化状态 Lt_Change 迁移到主机状态 Lt_Host;

3)当处于主机状态 Lt_Host,若由于主机的变化导致漏洞利用后果发生改变 OutP_AfterL,将从主机状态 Lt_Host 迁移到漏洞利用后果状态 Lt_After;

4)当处于漏洞利用后果状态 Lt_After,若无具体信息变化产生 OutP_InvalidL,将状态迁移到结束状态 Lt_End;

5)当处于漏洞变化状态 Lt_Change,若对漏洞采用不同的利用方式产生不同的漏洞利用后果发生改变 OutP_AfterL,将从漏洞变化状态 Lt_Change 迁移到漏洞利用后果状态 Lt_After;

6)当处于主机状态 Lt_Host,若无具体信息变化产生 OutP_InvalidL,将状态迁移到结束状态 Lt_End;

7)在某漏洞攻击状态下,当攻击状态发生变化 OutP_ChangeA,将从初始状态 Lt_Initial 迁移到攻击变化状态 Lt_ChangeA;

8)当处于攻击变化状态 Lt_ChangeA,若漏洞的攻击发起主机发生变化 OutP_HostA,将从攻击变化状态 Lt_ChangeA 迁移至攻击源状态 Lt_HostA;

9)当处于攻击源状态 Lt_HostA,通过检查发现由于攻击发起主机改变,导致攻击前提改变 OutP_PreA,将从攻击源状态 Lt_Hos 迁移至攻击前提状态 Lt_Pre;

10)当处于攻击前提状态 Lt_Pre,由于攻击前提发生改变,导致漏洞利用后果状态改变 OutP_AfterL,将从攻击前提状态 Lt_Pre 迁移至漏洞利用后果状态 Lt_After;

11)当处于攻击变化状态 Lt_ChangeA,若攻击发起主机未变,但攻击前提发生改变 OutP_PreA,将从攻击变化状态 Lt_ChangeA 迁移至攻击前提状态 Lt_Pre;

12)当处于攻击变化状态 Lt_ChangeA,若攻击发起主机未变,但攻击利用漏洞改变 OutP_UseA,将从攻击变化状态 Lt_ChangeA 迁移至漏洞利用状态 Lt_Use;

13)当处于漏洞利用状态 Lt_Use,由于漏洞改变,攻击前提条件随之改变 OutP_PreA,将从漏洞利用状态 Lt_Use 迁移至攻击前提状态 Lt_Pre;

14)当处于漏洞利用状态 Lt_Use,由于漏洞改变,导致漏洞利用后果状态改变 OutP_AfterL,将从漏洞利用状态 Lt_Use 迁移至漏洞利用后果状态 Lt_After;

15)当处于攻击源状态 Lt_HostA,若攻击利用漏洞改变 OutP_UseA,将从攻击源状态 Lt_HostA 迁移至漏洞利用状态 Lt_Use。

漏洞攻击有限状态自动机 LEFSM 状态之间的转移图,如图5所示。

2.2 态势理解

态势理解是指在获取网络安全态势信息数据的基础上,

通过分析计算状态建立的结果,获取网络安全态势,计算威胁存在概率、威胁状态概率、状态转移概率和威胁损失等态势组成值,综合得到网络安全态势,计算结果以数值形式呈现。

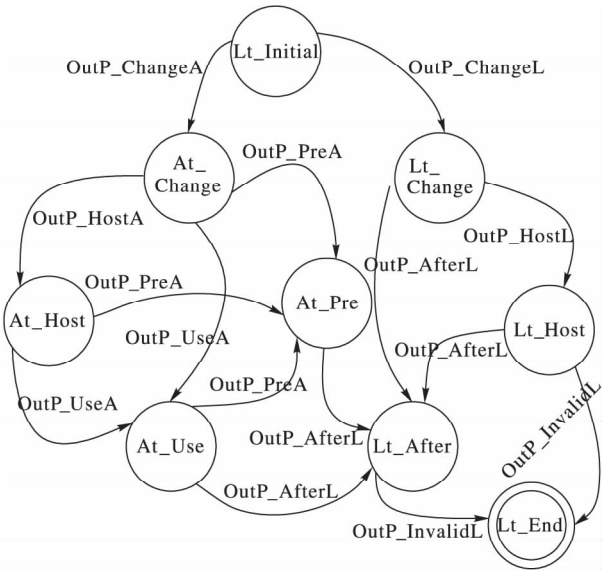

图5　漏洞攻击有限状态自动机状态转移图

定义2　威胁存在概率。指通过网络安全态势信息获取,得到某种漏洞、攻击或者威胁存在的可能性,用 I 表示。

威胁存在概率与获取到与该威胁的相关的态势信息 I_n 及其权重 w_n 相关,结合 DS 证据理论,可得威胁存在概率计算公式,公式表明威胁存在概率 I 与态势信息 I_n 成正比,且权重越大的对结果影响越大:

$$I = \frac{\sum_{\bigcap_{m=1}^{n} I_m = I} I_1^{w1} \cdot I_2^{w2} \cdot \cdots \cdot I_n^{wn}}{1 - a} \tag{2}$$

$$a = \sum_{\bigcap_{m-1}^{n} I_m = \varnothing} I_1^{w1} \cdot I_2^{w2} \cdot \cdots \cdot I_n^{wn} \tag{3}$$

其中: $I_1, I_2, \cdots, I_n$ 表示该威胁相关的态势信息; $w_1, w_2, \cdots, w_n$ 表示信息对应的权重,在信息获取时已经进行赋值计算; a 表示变量因素。

定义3　威胁状态概率。指通过网络安全态势信息获取,得到已经发生的攻击在网络安全状态转移图中处于某个中间状态的可能性,用 C 表示。

威胁状态概率由威胁存在概率、攻击相关度共同决定,威胁存在概率越大,受到同一攻击的可能性越大,则该节点处于越有可能威胁的状态,即:

$$C = \prod_{b=1}^{d} I(f_b) \cdot \prod_{b=1}^{d} rel(f_b, f_{b+1}) \tag{4}$$

其中: f_b 表示处于该状态与威胁相关的信息, rel 表示攻击相关度。

定义4　攻击相关度。指两个或者多个攻击信息之间的相关程度,用 $rel(x, y)$ 表示。

攻击相关度与信息获取时确定的特征关联度和权重有关,特征关联度越大,则权重越大,则 x, y 受到同一攻击的可能性越大,即:

$$rel(x, y) = \left[\sum_{j=1}^{d} \lambda_j \gamma_j(x, y)\right] / \sum_{j=1}^{d} \lambda_j \tag{5}$$

其中: λ_j 表示攻击信息中第 j 特征的权重, $\gamma_j(x, y)$ 表示特征关联度。

定义5　状态转移概率。指在网络安全状态转移图中,从当前状态转移到下一状态的可能性,用 E 表示。如果当前状态满足状态转移条件,则 $E = 1$,否则 $E = 0$。

定义6　威胁损失。指网络系统某个漏洞或者攻击影响,处于该状态时将带来的损失,用 L 表示。威胁损失 L 采用通用漏洞评分系统(Common Vulnerability Scoring System, CVSS)进行赋值。

网络安全态势分析计算,采用先局部后整体、自下向上的原则,通过分析计算网络系统中设备态势组成值,分类累加得到整个网络系统的安全态势值。

定义7　网络安全态势值。表示网络系统受威胁的程度,其值是用 0 ~ 1 的数字表示。

网络安全态势值的计算步骤如下:

1)计算设备态势组成值,将攻击状态概率 C、状态转移概率 E 与当前状态对应的威胁损失 L 相结合,得到该状态下设备的态势值 D:

$$D = C \cdot E \cdot L \tag{6}$$

2)当设备在同一状态下受到多个攻击时,则该状态下设备的态势值 Ac 需要进行累加。计算公式如下所示,其中 i 为受到攻击数:

$$Ac = \sum_{i=1}^{d} D_i \tag{7}$$

3)依据设备的安全态势组成值,考虑设备重要程度不一样,分别加以权重赋值,得到整个网络安全态势值 WAc:

$$WAc = \sum_{i=1}^{d} Ac_i \cdot w_i \tag{8}$$

这里需要说明的是,网络安全态势值反映了网络受攻击威胁的程度,网络安全态势值越大越容易受到威胁,网络的安全性越低。网络安全态势值与网络实际受威胁的程度间的对应关系如表 3 所示。

表3　网络安全态势值与网络安全威胁等级对应关系表

网络安全态势值	说明
$0 \leqslant WAc < 0.15$	网络系统正常运行,未受到严重漏洞或者攻击影响
$0.15 \leqslant WAc < 0.5$	网络系统基本正常运行,但受到少量攻击或者威胁,造成一定损失
$0.5 \leqslant WAc < 0.75$	网络系统不能正常运行,受到恶意攻击或者严重漏洞影响,关键设备遭到威胁
$0.75 \leqslant WAc < 1$	网络系统严重遭到破坏,受到大量严重恶意攻击,系统服务中断

算法　网络安全态势理解算法(Network Security Situation Understanding Algorithm, NSSUA)。

输入　网络安全态势有限状态机(NSSPFSM)拓扑、配置、漏洞攻击等安全状态,获取的网络安全态势信息数量 n,设备受攻击的数目 i;

输出　网络安全态势值 WAc。

1. Get 拓扑 and 配置信息,得到网络系统中设备信息 *Inf*
2. From NSSPFSM → *Phf* 生成有限状态图
3. for IP 地址 from 1 to n do

//遍历存活设备

4. if (*Phf* and *Inf*) then

```
        //综合设备信息与有限状态图,如果设备存在
5.        E = 1                          //状态转移概率为 1
6.      else WAc ← 0
        //设备不存在,状态转移概率为零,网络安全态势值为零
7.      end if
8.    end for
9.    compute D                  //计算存在状态转移的设备的态势值
10.   if (i > 1) then            //如果存活设受到攻击数量大于 1
11.     Ac ← ∑Ac                 //累加设备态势值
12.   else WAc ← ∑WAc
      //否则累加所有网络安全态势值
13.   compute WAc
      //累加设备的态势值,计算网络安全态势值
14.   WAc ← ∑WAc
15.   end if
16.   WAc ← 0
17. end
```

网络安全态势理解算法(NSSUA)时间复杂度由语句 2、3 ~ 7、10 ~ 13 和 14 确定,这些语句均为单重循环。假设设备信息数量为 n,其中拓扑、配置数量为 k,受到多个攻击的设备数量为 m,则其时间复杂度分别为 $O(n)$、$O(k)$ 和 $O(m)$,均为线性时间复杂度,整个算法的时间复杂度为三部分的和:$T = O(n) + O(k) + O(m)$,如果 $n > k > m$,则网络安全态势理解算法(NSSUA)时间复杂度为 $O(n)$。

2.3 示例

假设网络环境是由攻击主机、用户主机、服务器、交换机、路由器、集线器构成的网络系统,网络拓扑结构如图 6 所示。用户主机装有入侵检测系统(Intrusion Detection System, IDS),网络设置了防火墙。攻击者通过网络系统,判断存在普通用户主机 2,利用 SQL 注入漏洞攻击,获取主机的最高控制权限,通过主机 2 对文件服务器发起 UDP(User Datagram Protocol)泛洪攻击,获取文件服务器控制权限,获取重要文件信息,实现网络攻击过程。

通过态势感知模型,对图 6 所示网络系统以及假设的攻击过程进行网络安全态势感知,计算网络安全态势值。

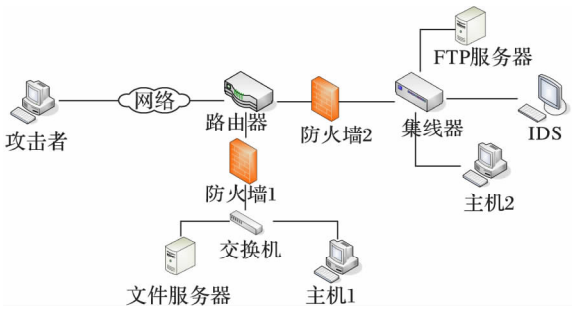

图 6 示例用网络拓扑

获取 IDS、防火墙和各个主机的安全日志信息以及通过拓扑扫描、端口扫描,发现网络的存活设备,获取网络的拓扑结构,对获取的信息构建状态转移图,如图 7 所示,网络系统从 St_Initial 初始状态,经过 5 次状态转化达到最终控制文件服务器的目的,5 个状态用是 s1 ~ s5 进行标记。

依据态势感知模型中态势理解计算公式(2) ~ (8),计算网络安全态势值。

计算时,以普通用户主机 2 且在检测到该主机受到 SQL 注入攻击后为例,说明网络安全态势值的计算过程。

1)由式(2)、(3)计算得到威胁存在概率 $I = 0.937$,而在此之前,网络拓扑扫描该主机且 $I = 0.915$,由式(5),计算这两次状态的攻击相关度 $rel = 1$;

2)依据攻击相关度、威胁存在概率和式(4),计算威胁状态概率 $C = 0.915 \times 0.937 \times 1 = 0.857$;

3)依据损失及威胁状态概率,采用通用漏洞评分系统(CVSS)对此处威胁损失进行赋值 $L = 0.2$;

4)由于处于 s2 状态,存在 s3 状态,并且实际过程中 s3 已经出现,状态转移概率 $E = 1$;

5)由式(6)、(7)、(8)计算该节点状态的网络安全态势值 $WAc = 0.171$。

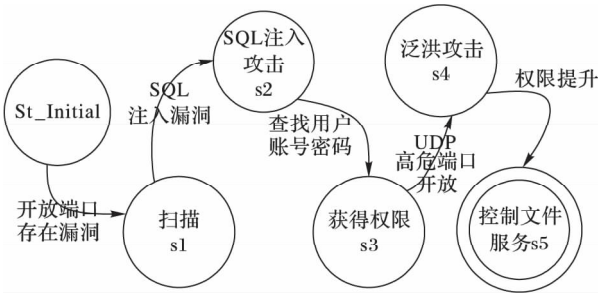

图 7 状态转移图

计算网络中所有状态节点的安全态势值,汇总于表 4。

表 4 网络安全态势计算数据

状态	威胁存在概率 I	威胁状态概率 C	状态转移概率 E	威胁损失 L	网络安全态势值 WAc
s1	0.915	0.872	1	0.5	0.136
s2	0.937	0.857	1	0.2	0.171
s3	0.886	0.830	1	0.3	0.237
s4	0.892	0.790	1	0.3	0.249
s5	0.831	0.741	1	0.5	0.371

3 验证与分析

对网络安全态势感知模型的正确性、有效性与优势进行实验验证。通过计算网络安全态势感知模型的“网络安全态势值”并与期望的“网络安全态势值”的比较,说明网络安全态势感知模型的正确性;通过计算网络安全态势感知模型的“网络安全态势值”并与层次分析模型、神经网络模型的“网络安全态势值”的比较,说明“网络安全态势感知模型”的有效性与优势。

实验用网络环境由主机、交换机、路由器、服务器等网络设备构成。

实验数据使用的是由国际计算机学会(Association for Computing Machinery, ACM)推荐 KDDcup99[16]。KDDcup99 数据集包含 41 个特征,共有 500 万条数据记录,是网络安全态势研究实验使用的数据集[17]。

网络安全态势感知模型正确性验证方法是从 KDDcup99 数据集中随机选取 100 个样本作为实验用数据,将 100 个样本数据集中的数据作为网络安全态势感知模型的输入数据,计算每一组实验数据的网络安全态势值;同时,选择 10 位网络安全态势专家对 100 个样本的测试数据集输入获得的网络安全态势结果进行评估,得到 100 组输出期望值。将网络安全态势感知模型的“网络安全态势值”与期望的“网络安全态势值”进行比较,对比的结果如图 8 所示。其中,初始状态网络系统的可能存在各设备未开机或者未运行,将初始状态网络安全态势值设置为零。

网络安全态势感知模型有效性验证方法是从 KDDcup99 数据集中已选定的 100 个样本数据中任意选取 12 组网络数

据作为实验用数据。将这 12 组网络数据作为层次分析模型、神经网络模型和态势感知模型的输入数据,计算每一个模型的每一组实验数据的网络安全态势值。将三个模型的"网络安全态势值"与期望的"网络安全态势值"进行比较,对比的结果如图 9 所示。

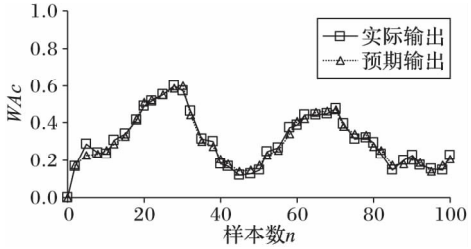

图 8　感知模型与期望的"网络安全态势值"对比

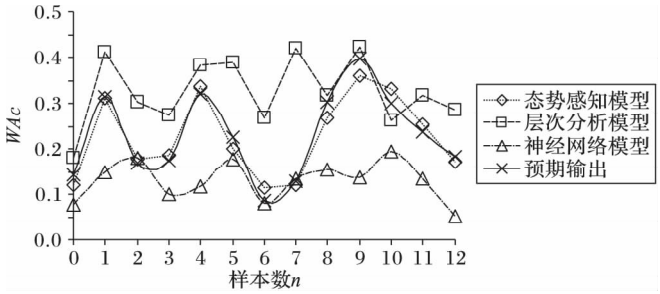

图 9　三个模型与期望的"网络安全态势值"对比图

为进一步说明网络安全态势感知模型与层次分析模型、神经网络模型比较的优势,计算网络安全态势感知模型、层次分析模型、神经网络模型与期望的均方差,计算结果如表 5 所示。

表 5　三种模型与期望的均方差对比

模型	均方差
态势感知模型	0.012
层次分析模型	0.033
神经网络模型	0.027

实验表明,网络安全态势感知模型的网络安全态势值与专家评估的期望值基本一致,说明网络安全态势感知模型是正确的;通过网络安全态势感知模型、层次分析模型、神经网络模型的"网络安全态势值"与期望的"网络安全态势值"分析对比,网络安全态势感知模型"网络安全态势值"与期望的"网络安全态势值"曲线走势更为贴近和重叠,网络安全态势感知模型与期望的均方差值最小,说明网络安全态势感知模型有效,且与层次分析模型、神经网络模型相比更具优势。

需要指出的是,图 8 所示的网络安全态势感知模型的网络安全态势值与专家评估的期望值在初始状态期间误差较大,原因在于网络安全态势感知模型在初始状态时被认为是不受任何网络攻击,网络安全态势值是 0,即初始状态设备均未受到威胁时的设备权重值与受攻击的值不同,需要使用与初始阶段相对应的权重值 w 计算 WAc。因此,在网络安全态势理解算法 NSSUA 算法中,将语句 13:"compute WAc "修改为:

if St_Initial then compute w

compute WAc

即判断该状态是否是初始状态阶段,如果是,计算初始状态网络设备的权重值 w,用这个 w 值计算网络安全态势值。如果不是,则按原权重直接计算网络安全态势值。

按照上述正确性验证方法,利用与上述实验相同的实验环境和数据,通过改进的网络安全态势感知模型计算"网络安全态势值",并与期望的"网络安全态势值"进行比较,对比的结果如图 10 所示。

从图 10 与图 8 对比可以看出,改进的网络安全态势感知模型的网络安全态势值与专家评估的期望值在初始状态期间基本相同,说明改进的方法有效,更适用于实际网络需求。

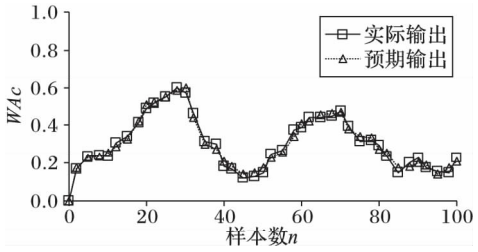

图 10　改进的感知模型与期望的"网络安全态势值"对比图

4　结语

针对基于神经网络的态势感知模型需要先验知识、反复训练神经网络消耗时间长,和层次分析法单独计算攻击态势值,提出了一种基于拓扑漏洞分析的网络安全态势感知模型,建立了网络安全态势理解有限状态机,设计了网络安全态势分析算法,解决了神经网络和层次分析模型存在的信息独立分析处理的问题。实验表明网络安全态势感知模型计算获取的网络安全态势值与专家评估的期望值更接近,误差小,从而验证了基于拓扑漏洞分析的网络安全态势感知模型的有效性和正确性。这说明,从网络安全态势信息获取入手,建立的基于拓扑结构有限状态机、配置状态有限状态机、漏洞攻击有限状态机的网络安全态势感知模型,可实现对网络安全态势的感知。

下一阶段研究的重点是进一步优化网络安全态势感知模型和网络安全态势分析计算方法,使之更加实用化和精准化;同时研究建立网络安全态势感知模型参数自适应理解和分析的机制,为网络安全态势的可视化展示提供技术支持和服务。

参考文献:

[1] BASS T. Multisensor data fusion for next generation distributed intrusion detection systems[C]// Proceedings of the 1999 Iris National Symposium on Sensor & Data Fusion. Laurel: [s. n.], 1999: 24 – 27.

[2] PATSOS D, MITROPOULOS S, DOULIGERIS C. Expanding topological vulnerability analysis to intrusion detection through the incident response intelligence system[J]. Information Management and Computer Security, 2010, 18(4): 291 – 309.

[3] 陈秀真,郑庆华,管晓宏,等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006,17(4): 885 – 897.

[4] 张勇,谭小彬,崔孝林,等. 基于 Markov 博弈模型的网络安全态势感知方法[J]. 软件学报, 2011,22(3): 495 – 508.

[5] JAJODIA S, NOEL S. Topological vulnerability analysis: a powerful new approach for network attack prevention, detection, and response [C]// Statistical Science and Interdisciplinary Research: Volume 3: Algorithms, Architectures and Information Systems Security. [S. l.]: World Scientific, 2008: 285 – 305.

[6] 谢丽霞,王亚超,于巾博. 基于神经网络的网络安全态势感知[J]. 清华大学学报(自然科学版),2013,53(12): 1750 – 1760.

[7] SWARUP V, JAJODIA S, PAMULA J. Rule-based topological vulnerability analysis[C]// Proceedings of the 3rd International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, LNCS 3685. Berlin: Springer, 2005: 23 – 37.

(下转第 169 页)

包,并修改其中要写入 RPMB 分区中的数据发送给 eMMC,观察结果;

读数据操作中,攻击者截获 eMMC 返回的数据读响应包,修改其中返回的数据并发送给安全世界,观察结果。

2)重放攻击测试。

写数据操作中,攻击者截获安全世界发送的数据写请求包,并在下一次安全世界请求写数据重新发送该数据包给 eMMC,观察结果;

读数据操作中,攻击者截获 eMMC 返回的数据读响应包,并在下一次安全世界请求读取数据时重新发送该响应包给安全世界,观察结果。

以上攻击测试的结果如表 1 所示。

表 1　隐私数据安全测试结果

攻击类型	结果	结果分析
写操作的篡改攻击	写数据失败	eMMC 根据返回数据计算 MAC 值,其与数据包中的 MAC 值不相等,说明数据包被篡改
读操作的篡改攻击	拒绝返回数据包	安全世界计算返回读取数据的 MAC 值,其与数据包中的 MAC 值不相等,说明数据包被篡改
写操作的重放攻击	写数据失败	eMMC 检查数据写请求包中的写计数,与自己写计数器中的值不相等,说明存在重放攻击,数据包失去时效性
读操作的重放攻击	拒绝返回数据包	安全世界检查数据读响应包中的随机数,与之前发送的随机数不相等,说明存在重放攻击,数据包失去时效性

测试结果表明,本方案可以很好地防止攻击者的篡改攻击和重放攻击,与一般的加密保护方案相比,能够更好地保护隐私数据的完整性、机密性和时效性。

4　结语

本文针对移动终端中缺乏有效隐私数据保护方案的问题,对 TrustZone 架构进行研究,并且基于终端中广泛使用的 eMMC 存储器,利用其中的 RPMB 分区提出了一种隐私数据保护方法。本方法对隐私数据进行加密保护,并且通过认证密钥以及写计数、随机数等机制实现对数据的认证读和认证写操作。经实验测试和分析,本方案可以防止攻击者的篡改攻击和重放攻击,有效地保证了隐私数据的完整性、机密性和时效性。

参考文献:

[1] ALVES T, FELTON D. Trustzone: Integrated hardware and software security[J]. ARM White Paper, 2004, 3(4): 18 – 24.

[2] BAILEY S A, FELTON D, GALINDO V, et al. TEE System Architecture Version 1.1[S]. Redwood City, USA: Global Platform, 2017: 18 – 33.

[3] BAILEY S A, FELTON D, GALINDO V, et al. The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market[S]. Redwood City, USA: Global Platform, 2011: 10 – 18.

[4] Trusted Computing Group. Trusted platform module summary[EB/OL]. [2017-04-30]. https://trustedcomputinggroup.org/trusted-platform-module-tpm-summary/.

[5] 魏兰. 基于 ARM TrustZone 的安全存储研究与实现[D]. 成都: 电子科技大学, 2015: 15 – 22.

[6] 刘艺. 移动设备安全系统的研究与设计[D]. 武汉: 华中师范大学, 2016: 16 – 22.

[7] ZHAO S, ZHANG Q, HU G, et al. Providing root of trust for ARM TrustZone using on-chip SRAM[C]// Proceedings of the 4th International Workshop on Trustworthy Embedded Devices. New York: ACM, 2014: 25 – 36.

[8] MAES R. Physically Unclonable Functions[M]. Berlin: Springer, 2013: 49 – 80.

[9] HEIN D, WINTER J, FITZEK A. Secure block device – Secure, flexible, and efficient data storage for ARM TrustZone systems[C]// Proceedings of the 2015 IEEETrustcom/BigDataSE/ISPA. Washington, DC: IEEE Computer Society, 2015, 1: 222 – 229.

[10] Embedded MultiMediaCard (eMMC) Mechanical Standard, JESD84-C43[S]. Arlington: JEDEC Solid State Technology Association, 2007: 1 – 14.

[11] ARM. ARM security technology: Building a secure system using TrustZone technology[EB/OL]. [2017-04-30]. http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf.

[12] Global Platform. GlobalPlatform made simple guide: Trusted Execution Environment (TEE) guide[EB/OL]. [2017-04-30]. http://www.globalplatform.org/mediaguidetee.asp.

[13] HANSEN T. US Secure Hash Algorithms (SHA and HMAC-SHA), RFC 4634[S]. [S.l.]: The Internet Society, 2006.7: 6 – 15.

[14] 崔建双, 李铁克, 张文新. 对称加密算法 Rijndael 及其编程实现[J]. 计算机工程, 2004, 30(13): 89 – 91.

[15] BELLARE M. Optimal asymmetric encryption — how to encrypt with RSA[C]// Advances in Cryptology – EUROCRYPT' 94, LNCS 950. Berlin: Springer-Verlag, 1995: 92 – 111.

(上接第 163 页)

[8] 唐成华,唐申生,强保华. DS 融合知识的网络安全态势评估及验证[J]. 计算机科学,2014,41(4): 107 – 110.

[9] 刘效武,王慧强,吕宏武,等. 网络安全态势认知融合感控模型[J]. 软件学报,2016,27(8): 2099 – 2114.

[10] 叶云,徐锡山,齐治昌,等. 大规模网络中攻击图自动构建算法研究[J]. 计算机研究与发展,2013,50(10): 2133 – 2139.

[11] 陈靖,王冬海,彭武. 基于动态攻击图的网络安全实时评估[J]. 计算机科学,2013,40(2): 133 – 138.

[12] 李庆朋,王布宏,王晓东,等. 基于安全状态约简的攻击图生成方法[J]. 计算机工程与设计,2013,34(5): 1589 – 1593.

[13] 谢丽霞,王亚超. 网络安全态势感知新方法[J]. 北京邮电大学学报,2014,37(5): 31 – 35.

[14] 蒋宗礼,姜守旭. 形式语言与自动机理论[M]. 北京: 清华大学出版社,2007: 12 – 43.

[15] 古天龙. 软件开发的形式化方法[M]. 北京: 高等教育出版社,2005: 67 – 91.

[16] University of CAlifornia, Irvine. KDD Cup 1999 Data[EB/OL]. [2018-01-10]. http://www.ics.edu/~kdd/databases/kddcup99.

[17] 张新有,曾华燊,贾磊. 入侵检测数据集 KDD CUP 99 研究[J]. 计算机工程与设计,2010,31(22): 4809 – 4813.