一种面向等保系统的轻量级攻防模拟方法

回赛男,胡 俊
(北京工业大学 信息学部,北京 100124)

摘 要:等级保护制度是国内网络安全领域的基本制度,需要对等保安全保障方案防护能力进行分析评估,要求安全保障机制形成体系,满足“可信、可控、可管”的要求。在等级保护信息系统的特点和能力要求下,针对信息系统时刻面临的网络安全问题,提出了一种以业务流程为保护对象,通过轻量级软件重建应用场景,在应用场景下,从安全属性和信息流角度模拟攻击行为和部署纵深防御机制,通过安全攻防的推演来判断系统安全防护能力的安全分析方法。该方法针对等级保护对网络系统安全防御的要求提出,可以低成本模拟多种应用场景,分析应用的安全性并尝试不同安全保障改进方案的效果。最后,通过工业控制系统震网病毒应用实例说明了该方法的实施方式和验证效果。

关键词:等级保护;轻量级;应用场景;攻击模拟;防御模拟
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2022)08-0096-07
doi:10.3969/j.issn.1673-629X.2022.08.016

A Lightweight Attack and Defense Simulation Method for Grade Protection System

HUI Sai-nan, HU Jun
(Faculty of Information, Beijing University of Technology, Beijing 100124, China)

Abstract: Graded protection system is the basic system of Cyberspace Security in China. It needs to analyze and evaluate the protection capability of peer-to-peer protection security scheme, and requires the security mechanism to form a system to meet the requirements of "credibility, controllability and manageability". Under the characteristics and capability requirements of graded protection information system, aiming at the network security problems faced by information system at all times, a security analysis method is proposed, which takes the business process as the protection object, reconstructs the application scenario through lightweight software, simulates the attack behavior and deploys the defense in depth mechanism from the perspective of security attributes and information flow, and judges the system security protection capability through the deduction of security attack and defense. This method is proposed in response to the requirements of graded protection for network system security defense, which can simulate a variety of application scenarios at low cost, analyze the security of the application and try the effect of different security improvement schemes. Finally, an application example of Stuxnet virus in an industrial control system is used to illustrate the implementation and verification effect of the method.

Key words: grade protection; lightweight; application scenario; attack simulation; defense simulation

0 引 言

近年来,系统信息安全事件屡见不鲜,这给国家安全和利益造成了严重危害。目前,等级保护已经发展到了 2.0 版,新的等级保护要求需要与其适配的网络系统安全分析方法[1]。常见的网络系统安全分析方法有态势感知方法、形式化方法和模拟真实环境测试等。态势感知技术主要通过采集网络原始数据与系统运行生成的动态安全数据等信息,再通过对数据进行实时分析实现,目前态势感知主要依托入侵检测、漏洞扫描等机制,与等保要求不符[2-3]。形式化方法是利用数学方法,从源头验证系统正确、无漏洞的有效手段,这种方法能够比较严格的论证安全性,但是因为研究过程过于复杂,一般用于比较简单的场景,不适合复杂场景[4]。模拟真实环境是在测试端未受到真实的网络攻击之前,提早对其进行攻击和防御模拟的一种测试方法,通过对被测试端进行攻击和防御效果检测与评估,

收稿日期:2021-09-29 **修回日期**:2022-01-31
基金项目:国家重点研发计划(2I007016202102)
作者简介:回赛男(1997-),女,硕士研究生,研究方向为可信计算;通讯作者:胡 俊(1972-),男,博士,讲师,研究方向为可信计算、云安全和安全操作系统。

并提出安全改进方案,以减小系统受到真实攻击的可能性和由此带来的影响,但是存在成本高、通用性低的问题[5-6]。

根据高安全级别等级保护系统的安全需求和技术特点,提出了一种新的安全分析方法。该方法以业务流程为保护对象,将业务流程抽象成信息流和计算逻辑的组合,搭建模拟场景,并通过该场景下对攻击机制和防御机制的抽象模拟,构造出类似“兵棋”的安全推演场景,通过攻防推演来判断系统的安全状况。该方法可以从信息流层面模拟系统的攻防对抗状况,推演系统面临的现实的安全威胁和防护效果,且具备通用、灵活、低成本等优势。

1　相关研究

常见的提供攻防模拟环境的平台是网络靶场,目标是尽量模拟真实环境,通过模拟仿真技术构建真实环境的仿真,并在仿真环境中模拟实际应用搭建攻防测试场景,进行攻防测试行为[7]。通过在靶场中进行各项渗透测试,可以探索目标系统可能存在的安全漏洞,同时模拟黑客攻击行为;攻击方对目标系统发起攻击,防御方通过加固系统来防御攻击,目的是通过网络靶场实战,掌握黑客的攻击过程和手段,从而部署最优防御措施[8]。

但在网络靶场中搭建攻防模拟环境,建设靶场的成本和在靶场中构建场景的成本较高[9];现有的靶场多是针对一些具体的应用场景而设立的,只能在这些设定好的场景中进行攻防,若想在其他应用场景下进行攻防测试,就要重新搭建一个对该应用场景的模拟,不具有通用性;而且许多场景不是真实系统中存在的。

网络仿真可以测试实际的系统,和外界真实网络有交互,所构造的虚拟网络和外界真实网络是需要进行同步的,攻防仿真实验环境可以对照真实系统来搭建应用场景,包括试验床和网络仿真器等方式。清华大学的刘武提出用 VMWare 构建高效的网络安全实验床,但是 VMWare 虚拟化技术在网络环境构建过程中需要手动操作,会随着网络规模的增大存在效率低下和成本高的问题[10]。L Stoller 等提出了使用 Emulab 构建大规模虚拟化环境,使用虚拟技术搭建攻防平台,配置步骤往往较为繁琐复杂,虚拟机文件往往较大,对个人用户来说并不友好,且环境搭建缺少灵活性,不便于扩展、管理和维护[11]。A Ezreik 等提出了使用 NS2 网络仿真器来设计网络并且使用加密算法来安全传输信息,描述了通过 NS2 网络仿真器来设计网络的方法构建实验需要的网络环境,使用网络仿真器构建实验环境简单高效,但是虚拟节点的真实性无法保证[12]。

2　信息系统安全分析方法的设计

该文提出的信息系统安全分析方法借鉴了军事学中兵棋的思路,基于已有的网络攻防知识,通过轻量级模拟方法,尝试对系统安全状况及安全防护方案的效果进行推断。

兵棋由地图、棋子和规则组成,地图是兵棋模拟的场景,棋子是参战单位的抽象表示,规则是根据战争规律设计的裁决方法。在等级保护环境中,本方法的保护对象是业务流程,攻击方可使用多种攻击手段组织攻击行为,防御方则使用多种安全机制配合实现安全保障机制以对抗攻击行为。在进行轻量级攻防模拟时,“地图”对应的就是业务流程的模拟,“棋子”则是模拟的攻击机制和防御机制,“规则”包括红方(攻击方)和蓝方(防御方)在地图上对“棋子”的使用方法,以及“棋子”在地图上的运作规则。以下对其进行具体说明:

(1)信息系统安全的保护对象为业务逻辑,因此,“地图”既包括环境,也包括在环境中运行的应用流程。环境(如系统中的各个计算节点)可以通过一组执行程序实体及程序实体间的连接关系来模拟,应用流程则可以通过构造与实际业务对应的信息流与数据处理模块,并根据实际情况来标识数据属性变化来抽象模拟。

(2)棋子为系统中的攻击机制和防御机制。攻击机制和防御机制都可以通过在业务流程中添加攻/防模拟过程来实现。其中攻击机制中的窃听行为和防御机制中的监视功能可通过复制业务流程数据进行处理来添加,攻击机制中的篡改数据和增加输入,防御机制中的访问控制、加解密等行为可以通过拦截业务流进行处理,再返回业务流的方式添加。

(3)规则是根据攻击机制和防御机制的特点,以及系统安全规律设计的。高安全级别等级保护的核心规则为强制访问控制规则,其本质为信息流控制的规则,因此,“兵棋”规则的基础是信息流限制。信息流限制可以由不同机制产生,其中根据系统网络拓扑给出的信息流限制可认为是模拟场景的背景,除考虑物理安全问题外,一般不应违反。而根据系统中的安全机制(包括安全隔离机制和访问控制机制)也可给出信息流限制,但这一信息流限制在进行攻防模拟时要考虑被绕过的可能。

在信息流规则基础上,还可以补充其他规则。在执行业务处理的节点上,根据攻击机制和防御机制的特点,可归纳攻击机制和防御机制的规则,以编程方式模拟该节点的攻防状况。对环境和人员安全状况的设定也可转化为系统安全分析时的规则,如威胁来自于外部对哪些设备的攻击,或来自于具有特定权限的某

内部人员等。

(4)红蓝双方的推演过程为:应用流程运行过程中,在设计的规则之下,红方利用攻击机制对系统发起攻击;蓝方则利用防御机制应对红方的攻击行为,对系统进行保护;通过观察红蓝双方攻防对抗的效果得到推演的结论。

信息系统安全分析方法的整体架构如图 1 所示。

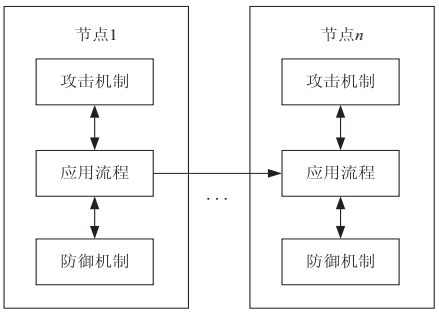

图 1 攻防模拟场景架构示意图

3 实现方法

本方法基于北京工业大学可信计算实验室自主开发的可信软件基原型架构[13]实现信息系统的攻防模拟。这个原型架构为分布式消息驱动架构,具备软件定义和模块载入功能,其提供的复制消息路由模式和切面消息路由模式可以用来模拟监视和拦截行为,可用来模拟攻击和防御机制。

3.1 应用场景重构

信息系统的应用场景采用轻量级的方法来重构。应用场景的模拟内容包括系统的节点拓扑结构和业务流程。可信软件基原型架构中,一个分布式运算进程为一个实例,实例可以加载多个模块,实例与模块间通过消息来交换信息和触发模块行为,消息通过预定义的消息路由进行传递。因此,本方法按照表 1 所示,建立可信软件基原型架构环境与应用场景之间的映射关系。

表 1 映射关系列表

业务系统中的对象	可信软件基础架构中对应的模拟实体
计算机节点和网络设备	实例
业务流程中的本地计算逻辑集合	模块
业务流程中的传输数据	消息
业务流程中的数据传输路径和计算逻辑组合顺序	消息路由
网络拓扑结构	实例间的网络连接
主体和客体的属性	消息的安全属性扩展数据结构

按照这一映射关系,本方法可以用可信软件基原型架构搭建出业务系统的网络拓扑环境,并模拟实现业务流程。这里不需要准确模拟业务的具体计算逻辑,只需要从属性上进行模拟,即模拟数据在经过了特定计算逻辑处理后,具备了何种属性。因为消息在消息路由中传播时,模拟的是一个处理过程,在该过程的某个环节既有特定的主体,也有具体的客体。因此,消息可以增添表达主客体属性的扩展项,来表示系统的处理过程。

3.2 攻击模拟

CC 标准(信息技术安全性评估标准)[14]规定:脆弱性+威胁 = 风险。当一个系统存在脆弱性、存在威胁,某种特定的威胁可以利用系统的脆弱性对系统造成损害,这个系统就存在着风险。因此,对攻击的模拟主要是模拟系统脆弱性被攻击者利用后产生的效果。

系统脆弱性可理解为系统中攻击者可以用来执行超越合法权限操作的权限的位置。而攻击者可以利用这些位置执行越权操作,获得更大的权限,并执行对业务系统的破坏行为。因此,对攻击的模拟,其核心是权限的模拟。可以在系统中多个节点上增加模拟脆弱性位置的模块,根据该位置脆弱性状况为其限定权限范围,攻击者在模块中按照规则编写攻击逻辑,模拟节点针对特定脆弱性的攻击行为,并通过在攻击模块之间配置攻击消息路由,将多个位置的攻击逻辑联系起来,模拟一个跨节点的完整攻击流程。

配置攻击消息路由时,可以通过可信软件基原型架构提供的复制路由和切面路由,将攻击机制接入系统中。其中,对系统进行窃听和数据分析的攻击行为可以通过可信软件基原型架构的复制路由,将数据从业务流程中可窃听位置复制下来后,执行攻击。对系统进行拦截和破坏的攻击行为,则可以通过可信软件基原型架构的切面路由,拦截正常的业务流程,并对业务数据进行篡改破坏,或在业务数据中附带恶意代码的模拟。

3.3 防御模拟

防御模拟主要模拟等保制度要求的访问控制、可信计算和密码保护等防御机制,并通过一个安全管理中心对这些防御机制进行统一管理,安全管理中心的管理方式为采集各防御机制的审计信息进行分析,并向各防御机制下发策略。防御机制接入业务流程的方法与攻击机制类似,也是采取复制和拦截等措施以在模拟业务流程的消息路由中加入安全机制。下面分别

描述不同安全机制的模拟方法:

(1)密码机制。

模拟数据加密机制时,可以在加密信道两端添加切面路由拦截消息,在加密端加密拦截的消息,在解密端解密被加密消息,加解密端通过另行定义的密钥管理机制和密钥管理消息路由实现密钥交换。这样,加密信道中的攻击者将无法窃听信息。模拟数据签名验证机制时实现方法类似。

(2)访问控制机制。

模拟访问控制机制时,可以在系统脆弱性的位置复制和拦截传输的消息。复制消息转发给监控模块,通过监控模块分析信息以模拟对系统的监控行为。拦截消息后,可根据监控结果对消息内容进行标记,标记该消息内容的属性(客体属性)和该消息操作者的属性(主体属性),访问控制机制则根据安全标记和访问控制策略实现访问控制操作,其中消息的扩展项为消息提供安全标记的添加,安全标记和访问控制策略通过切面路由接入到实例的消息路由中。

(3)可信度量机制。

模拟可信度量机制时,可以在每个实例处添加切面路由拦截消息,获取消息中主体和客体信息,并与历史记录汇总分析,进行可信度量,可信度量后可依据度量结果进行访问控制或审计操作。

3.4　攻防对抗演练

业务流程和攻防模拟准备好后,红蓝双方即可入场进行攻防对抗演练。演练时,双方选择合适位置部署攻击点和防御机制,编程实现攻击点和防御机制的攻防逻辑,通过配置攻防的消息路由,实现攻击和防御的执行流程,并在部署了攻防机制的环境中模拟业务流程,观察攻防对抗效果。此后双方可以修改攻防方案,进行下一轮攻防推演。

4　工程验证

基于提出的安全分析方法,以著名的工业控制系统震网病毒为实例[15],设计一个受震网威胁的网络环境作为此次攻防模拟的应用场景,来验证提出的安全分析方法的正确性。

4.1　应用场景重构

攻防模拟设想的网络拓扑环境[16]如图 2 所示。

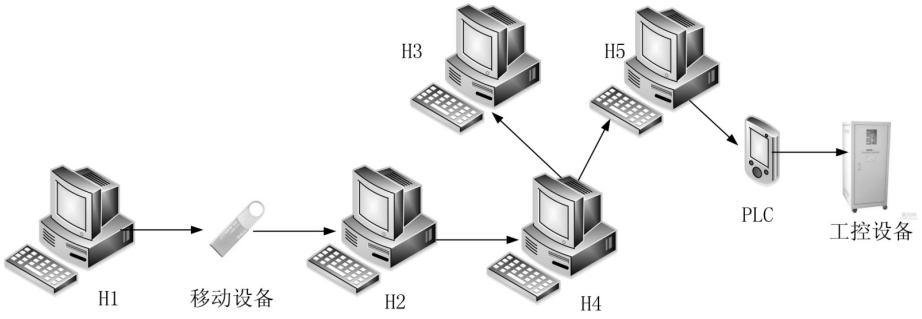

图 2　网络拓扑环境

在这一拓扑环境下,设计一个包含移动存储设备使用、打印、离心机控制等功能的工控业务流程,流程如下所述:

(1)用户 A 于外网在 H1 电脑上完成一个工作文档,并写入移动存储设备。

(2)用户 A 在 H2 电脑上插入移动存储设备,将工作文档复制到 H2 电脑。

(3)用户 A 将文件编辑处理后,传输到 H4 电脑。

(4)用户 B 在 H4 电脑编辑文件,并将文件传输到 H5 电脑。

(5)用户 B 将文件传输到 H3 电脑并打印。

(6)用户 C 在 H5 电脑处理文件,生成 PLC 控制命令。

(7)用户 C 发送 PLC 控制命令到工控设备,实现对工控设备的控制。

本方法建立 6 个实例,分别为 H1、H2、H3、H4、H5 和 PLC,其中 H1、H2 实例启动时,设定其属主为用户 A,H3、H4 启动时,设定其属主为用户 B,H5、PLC 启动时,设定其属主为用户 C。

可信软件基原型架构中,可定义不同的数据结构,并为数据结构的格式赋予(类型,子类型)对来唯一描述。定义业务流程相关记录结构类型为 STUXNET_PROC,并定义一些数据子类型以对应业务流程不同阶段的数据,如表 2 所示。

定义如表 3 所示的一些模块完成数据结构的处理。

在模块间定义的消息路由如图 3 所示。

启动各节点后,File_input 产生消息,将模拟可信软件基原型架构的行为。

4.2　攻击模拟

假设环境中各节点存在不同的漏洞,各个主机上的漏洞信息如表 4 所示。

表 2 数据结构列表

数据类型	数据子类型	内容	数据类型使用位置
STUXNET_PROC	INPUT	从 H1 输入的文件内容	H1,移动存储设备,H2
	IMPORT	H2 读取的文件内容	H2,H3
	EDIT	H4 节点编辑的文件内容	H4,H5,H3
	PRINT	H3 节点打印的文件内容	H3
	PLC_OUTPUT	H5 节点的输出内容	H5,PLC

表 3 业务流程模块列表

模块名称	输入数据结构类型	输出数据结构类型	模拟功能	所在位置
File_input	–	(STUXNET_PROC, INPUT)	H1 向移动存储设备输出数据	H1
File_import	(STUXNET_PROC, INPUT)	(STUXNET_PROC, IMPORT)	H2 从移动存储设备读入数据	H2
File_edit	(STUXNET_PROC, IMPORT)	(STUXNET_PROC, EDIT)	H4 编辑数据	H4
File_print	(STUXNET_PROC, EDIT)	(STUXNET_PROC, PRINT)	H3 打印数据	H3
Command_gen	(STUXNET_PROC, EDIT)	(STUXNET_PROC, PLC_OUTPUT)	H5 产生命令	H5
Command_plc	(STUXNET_PROC, PLC_OUTPUT)	–	PLC 执行命令	PLC

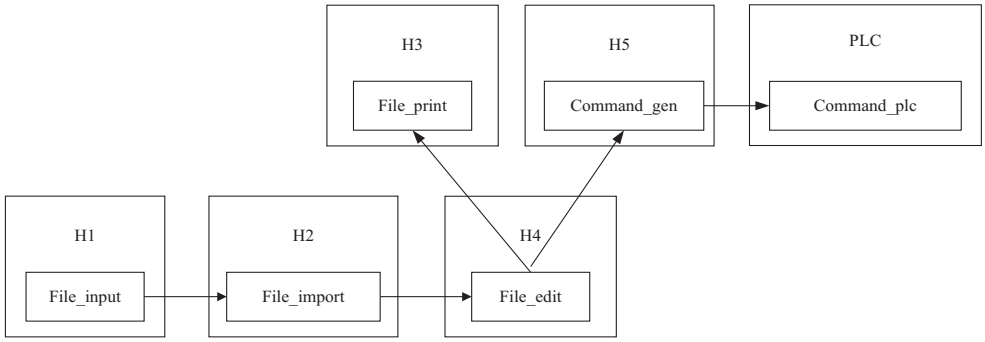

图 3 业务流程路由

表 4 主机漏洞信息

host	name	cve	right
H2	快捷方式文件解析漏洞	CVE-2010-2568	user
H3	快捷方式文件解析漏洞	CVE-2010-2568	user
H3	RPC 远程执行漏洞	CVE-2008-4250	root
H4	打印机后台程序服务漏洞	CVE-2010-2729	root
H5	内核模式驱动程序漏洞	CVE-2010-2743	root

为这四个漏洞分别设计不同的激活数据格式,这些数据格式定义类型为 STUXNET_VUL,可以作为扩展项添加在代表业务处理过程的正常消息内容中,见表 5。

表 5 数据结构列表

数据类型	数据子类型	内容
STUXNET_VUL	QUICK	快捷方式文件解析漏洞触发信息
	RPC	RPC 远程执行漏洞触发信息
	PRINT	打印机后台程序服务漏洞触发信息
	DRIVE	内核模式驱动程序漏洞触发信息

为这四个漏洞分别设计攻击模块(见表 6),攻击模块接收到相应的数据格式后就被激活,调用相应的攻击函数,攻击函数可以由红方进行编程实现。

表 6　攻击模块列表

模块名称	输入数据结构类型	模拟功能	所在位置
Att_quick	(STUXNET_VUL,QUICK)	快捷方式文件解析漏洞	H2,H3
Att_rpc	(STUXNET_VUL,RPC)	RPC 远程执行漏洞	H3
Att_print	(STUXNET_VUL,PRINT)	打印机后台程序服务漏洞	H4
Att_drive	(STUXNET_VUL,DRIVE)	内核模式驱动程序漏洞	H5

红方可以在业务流程中设计复制路由与切面路由,在合适点引入攻击模块,并在攻击模块编程实现攻击行为。攻击模块间定义的消息路由如图 4 所示。

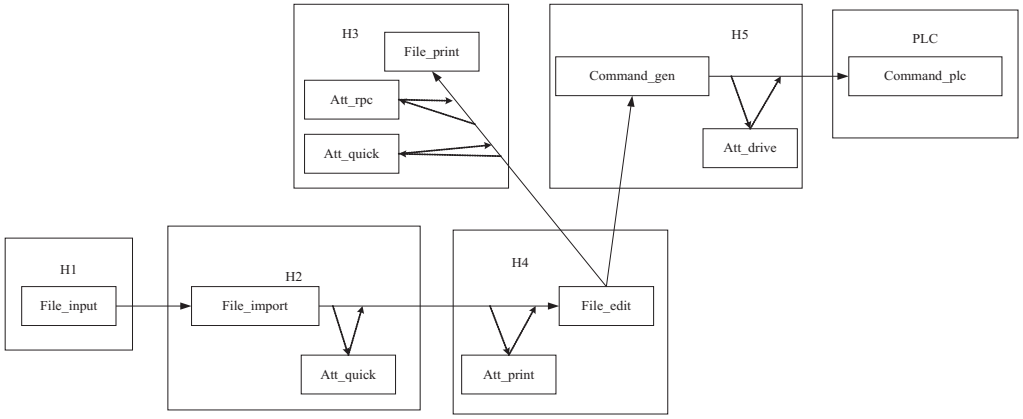

图 4　攻击模块路由

4.3　防御模拟

本方法分别设计了三种防御机制来实现对攻击行为的屏蔽,H1–H2 节点的文件检查,H4 节点的访问控制(攻击模块前置消息拦截机制),H5 节点的参数校验。

防御机制需要依据策略执行其功能,为三种防御机制定义的策略数据结构如表 7 所示。

表 7　数据结构列表

数据类型	数据子类型	内容
STUXNET_SEC	CHECK	文件检查策略
	ACC	访问控制策略
	VERIFY	参数校验策略

为这三种防御机制分别设计防御模块(见表 8),防御模块接收到策略后即按照策略执行相应的防御函数。

表 8　防御模块列表

模块名称	输入数据结构类型	模拟功能	所在位置
Def_check	(STUXNET_SEC,CHECK)	文件检查	H2
Def_acc	(STUXNET_SEC,ACC)	访问控制	H4
Def_verify	(STUXNET_SEC,VERIFY)	参数校验	H5

在防御模块间定义的消息路由如图 5 所示。

4.4　攻防对抗测试

(1)部署业务流程后,直接测试,业务流程可正常运行。

(2)部署攻击机制,再度运行业务流程,可看到验证 PLC 命令被篡改,插入非法参数。

(3)分别部署不同的防御机制,再运行业务流程,可看到文件检查、访问控制和参数校验均可阻断攻击行为对应用的影响。

(4)假设局域网其他机器已被攻击者入侵,则调整攻击场景为 H3 将受到 RPC 远程攻击行为,分别部署不同防御机制,再运行业务流程,可看到文件检查无效,访问控制和参数校验机制可阻断攻击行为对应用的影响。

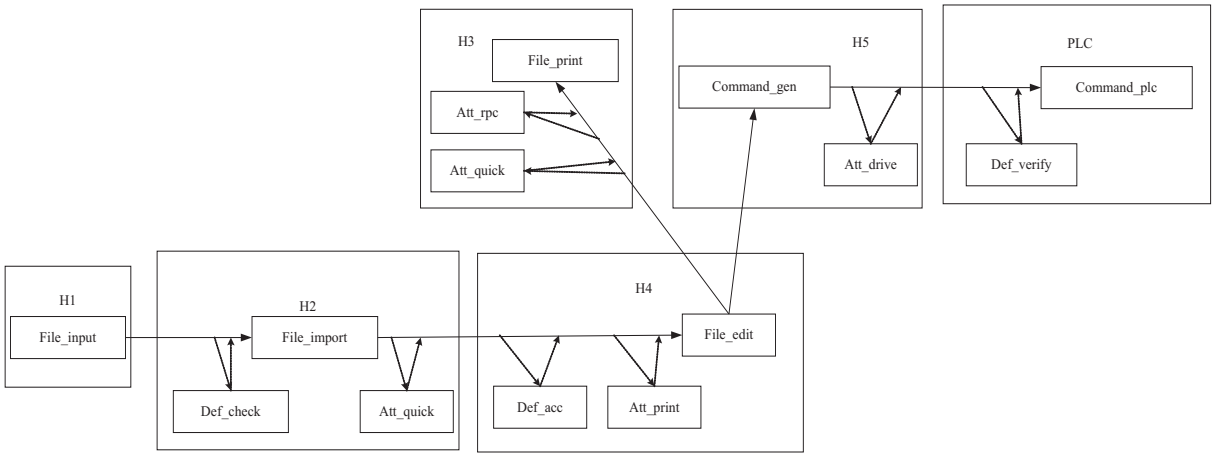

图 5 防御模块路由

5 结束语

一种通过轻量级软件模拟攻防对抗的安全分析方法旨在低成本地模拟工控系统攻防过程,来研究实际系统中的安全问题。该方法针对信息流进行轻量级的场景重构,将应用场景中的攻击手段和防御措施在该环境中进行模拟,通过攻防演练的结果来判断系统的安全状况。该方法通过轻量级的方式用少量计算机资源、搭建复杂环境;通过软件定义功能修改参数,改变节点安全属性,成本相对较低,且可以模拟任意应用场景,具有通用性。基于该方法,可以进行多种预设条件下的安全可信体系化攻防对抗,通过对抗来评测系统的防御能力,寻找更佳的防御方法。

参考文献:

[1] 全国信息安全标准化技术委员会. GB/T 22239-2019. 信息安全技术网络安全等级保护基本要求[S]. 2019.

[2] MAHALLE P N, THAKRE P A, PRASAD N R, et al. A fuzzy approach to trust based access control in internet of things[C]//2013 international conference on wireless communications, vehicular technology, information theory and aerospace and electronic systems technology. Atlantic City: IEEE, 2013: 1-5.

[3] CHEN R, BAO F, GUO J. Trust-based service management for social internet of things systems[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(6): 684-696.

[4] 陈 涛. 网络威胁检测模型及行为序列分析方法研究[D]. 西安:西安电子科技大学, 2010.

[5] GUPTA B B, CHHABRA M. An efficient scheme to prevent DDoS flooding attacks in mobile ad-hoc network (MANET)[J]. Research Journal of Applied Sciences Engineering & Technology, 2014, 7(10): 2033-2039.

[6] REGE A, OBRADOVIC Z, ASADI N, et al. Predicting adversarial cyber intrusion stages using autoregressive neural networks[J]. IEEE Intelligent Systems, 2018, 33(2): 29-39.

[7] 李 炜, 余慧英, 吴华颖. 网络空间博弈中的场景研究[J]. 信息安全研究, 2018, 4(5): 415-419.

[8] 吴怡晨, 王轶骏, 薛 质. 面向网络空间的攻防靶场设计[J]. 通信技术, 2017, 50(10): 2349-2356.

[9] RICCI R. The Flexlab approach to realistic evaluation of networked systems[C]//The 4th USENIX conference on networked systems design & implementation. Berkeley, CA: USENIX, 2007: 15-16.

[10] 刘 武, 吴建平, 段海新, 等. 用 VMware 构建高效的网络安全实验床[J]. 计算机应用研究, 2005, 22(2): 212-214.

[11] HIBLER M, RICCI R, STOLLER L, et al. Large-scale virtualization in the emulab network testbed[C]//2008 USENIX annual technical conference. Berkeley, CA: USENIX, 2008: 113-128.

[12] EZREIK A, GHERYANI A. Design and simulation of wireless network using NS-2[C]//2nd international conference on computer science and information technology. Singapore: ICCSIT, 2012: 139-143.

[13] 胡 俊, 沈昌祥, 公 备. 可信计算 3.0 工程初步[M]. 北京:人民邮电出版社, 2018: 13-35.

[14] 全国信息安全标准化技术委员会. GB/T 30270-2013. 信息技术安全性评估标准[S]. 2013.

[15] LI Muye, HUANG Yibin, PAN Heng. Research on attack mechanism of network intrusion in industrial control system[C]//2019 IEEE 4th advanced information technology, electronic and automation control conference. Piscataway, NJ: IEEE, 2019: 1904-1908.

[16] 谢嘉辰, 李新明. 震网病毒剖析[C]//2011 年全国电子信息技术与应用学术会议. 武汉:美国科研出版社, 2011: 195-199.