

文章编号:2095-6134(2023)06-0843-10

简 报

一种密码测评工具自动化调度方法及实现^{*}

张萌,王平建[†],陈天宇

(中国科学院数据与通信保护研究教育中心,北京 100093;中国科学院大学网络空间安全学院,北京 100049;
中国科学院信息工程研究所信息安全国家重点实验室,北京 100093)
(2021 年 10 月 26 日收稿;2022 年 4 月 21 日收修改稿)

Zhang M, Wang P J, Chen T Y. An automatic scheduling method and implementation of cryptographic evaluation tools[J]. Journal of University of Chinese Academy of Sciences, 2023, 40(6):843-852. DOI:10.7523/j.ucas.2022.043.

摘 要 提出一种密码测评工具自动化调度平台方案,该方案能够依据测评工具之间的依赖关系进行自动化装配,调度测评任务有序开展,归集测评中间数据并调度实时数据流转,根据模板输出报告,并支持产品接入、新建系统、系统运行 3 种测评场景。测评人员只需上传测评对象的应用场景拓扑图,在图中标识检查点选择所要使用的测评工具,然后通过调度平台向测评工具发送调度指令即可完成测评任务。调度平台采用网络接口调度测评工具,具有可扩展性,现有的测评工具只需依据本文提出的测评工具统一接口模型进行适配调整即可集成到调度平台中接受调度。

关键词 密码测评工具;自动调度;测评工具模型;调度平台

中图分类号:TP319 文献标志码:A DOI:10.7523/j.ucas.2022.043

An automatic scheduling method and implementation of cryptographic evaluation tools

ZHANG Meng, WANG Pingjian, CHEN Tianyu

(CAS Data Assurance & Communications Security Center, Beijing 100093, China; School of Cyberspace Security, University of Chinese Academy of Sciences, Beijing 100049, China; State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract In the process of cryptographic application evaluation, the evaluators complete the on-site evaluation and result analysis with the help of cryptographic evaluation tools. In practical application, the evaluators often need to use multiple evaluation tools in series. The output of one cryptographic evaluation tool needs to be used as the input of another tool to obtain further detection results. For example, when analyzing the SSL protocol, the digital certificate used for authentication should be extracted to complete the certificate format compliance verification. However, the existing evaluation tools are usually designed and developed independently for specific evaluation purposes, and they do not have the ability to work together with each other. The input and output data required

^{*} 国家重点研发计划(2018YFB0804303)资助

[†] 通信作者, E-mail: wangpingjian@iie.ac.cn

by each tool still need evaluators to carry out manual collection, data conversion, import and export, which is time-consuming and labor-consuming, and it is easy to introduce manual errors in the process of processing data. This paper proposes a scheme of automatic scheduling platform for cryptographic evaluation tools. The scheme can automatically assemble according to the dependency between evaluation tools, schedule evaluation tasks in an orderly manner, collect evaluation intermediate data and schedule real-time data flow, output reports according to templates, and support three evaluation scenarios: product access, new system and system operation. Evaluators only need to upload the application scenario topology map of the evaluation object, identify checkpoints in the map, select the evaluation tool to be used, and then send scheduling instructions to the evaluation tool through the scheduling platform to complete the evaluation task. The scheduling platform adopts the network interface scheduling evaluation tool, which has scalability. The existing evaluation tools only need to be adapted and adjusted according to the unified interface model of evaluation tools proposed in this paper, and can be integrated into the scheduling platform to accept scheduling.

Keywords cypher evaluation tool; automatic scheduling; evaluation tool model; dispatching platform

在当前网络互通的时代,大量数据通过互联网进行传输,其中不乏隐私数据和机密信息。密码技术能够实现加密、身份鉴别、签名验签等安全功能,保证传输数据的机密性、完整性,实体的真实性以及关键操作的不可否认性。但是,在密码算法应用过程中会出现各种各样的安全问题,比如密码技术的误用、密码算法 IV 值的错用等。一方面是由于密码学是一门相对专业的学科,而密码技术实现或使用人员可能缺乏相应培训;另一方面是由于密码应用安全性属于隐性指标,系统研发者可能通过“牺牲”或降低密码应用规格,获取更高的性能。不正确或无效的密码应用使得应用系统并没有获得应有的安全保障,反而存在很高的安全风险。

开展密码测评活动,能够对密码应用的合规性、正确性、有效性进行评估,有助于及时发现安全问题。2020 年 1 月开始实施的《中华人民共和国密码法》中明确规定,要求使用商用密码进行保护的关键信息基础设施必须使用国产密码算法,并定时开展商用密码应用安全性评估。

在密码测评过程中,测评人员需要进行大量标准符合性测试、密码算法运算等,使用专业的测评工具能够显著提高测评人员的工作效率和测评结果可靠性。一个测评实施可能需要使用多个测评工具,如验证通信数据中 SSL 协议建立过程密码应用安全性,通常需要使用安全协议捕获分析工具进行通信数据捕获,再由测评人员对协议建立过程中双方协定的密码套件、数字证书等关键

信息进行人工分析或者再次导入到其他工具中完成分析评价。由此可见,测评过程中往往涉及多个测评实施,每个实施结论可能需要多个测评工具协同联动对被测数据分析评价,但由于现有工具设计时并未考虑彼此之间的联动性,因此需要测评人员手动完成工具之间的调度、数据导入导出、格式转换等批量性工作,不仅增加了工作量,而且人工处理难免出现失误,最终会影响到测评结论的准确性。

针对以上问题,本文设计了一个密码测评工具自动化调度方案,并实现了密码测评工具调度平台(简称“调度平台”)。该方案通过建立测评工具统一接口模型,对测评工具进行统一化描述,随后在该模型基础上,建立测评工具间的依赖关系,最后依据调度策略有序调度测评工具,实现测评数据的自动采集和分析。测评人员只需要上传被测对象的应用场景拓扑图,标识工具接入位置,并选择需要使用的测评工具组合,便可以通过调度平台向测评工具发送测评指令完成测评任务。通过对平台进行功能性验证,平台发送测评指令的工具顺序以及指令中包含的调度信息是正确的。工具能够正确接收到其他工具发送的数据,并且能够将处理后的数据正确发送到下一个工具或者素材库,实现数据流转。

综上所述,本文的主要贡献如下:

1) 设计一个测评工具自动调度方案,能够支持产品接入、新建系统、系统运行 3 类测评场景,节省测评人员手动处理测评工具中间数据的时间

和精力,避免引入人工错误。

2) 提出一个测评工具统一接口模型,工具之间通过网络接口进行通信,具有良好扩展性。现有工具通过简单适配调整便可参与调度;借助调度平台中已有的测评工具功能,可减少新加入测评工具的开发量。

1 相关工作

首先简要阐述几类测评工具,随后对密码应用测评的场景等进行介绍。

1.1 测评工具

在开展商用密码应用安全性评估过程中,使用的测评工具可以依据应用范围划分为两类:专用测评工具和通用测评工具。专用测评工具主要用于检测和分析被测系统密码应用的合规性、正确性和有效性的一部分或全部环节^[1]。通用测评工具不限定应用的具体领域,具有通用性^[1]。由于通用测评工具不仅限于密码测评,故此不做详细介绍。接下来主要介绍专用测评工具。

专用测评工具可以分为 3 类:算法和随机性检测工具、密码安全协议检测工具、密码应用检测工具^[1],进一步分类如图 1 所示。下面对几类典型的专用测评工具进行介绍。

密码算法合规性检测工具 工具依据标准规范文档要求实现多个密码算法,包含分组密码算法、非对称密码算法以及流密码算法,能够实现加解密、签名验签的功能计算。用户将原始数据输

入到工具中,通过将工具产生的结果与被测结果相比较,验证密码算法实现的正确性。

数字证书格式合规性检测工具 依据数字证书标准规范,工具对数字证书的格式正确性、有效性和完整性进行验证^[2]。用户输入数字证书,获取证书的合规性验证结果。不同的工具可能支持不同格式的输入,检测结果的粗细程度也存在差异。

IPSec/SSL 协议检测工具 工具按照协议标准对通信数据进行解析,获取 IPSec/SSL 协议应用的密码算法,以及验证密码算法实现的正确性,进而判断协议中使用的密码算法和鉴别方式是否符合标准规范要求。用户输入通信数据,获得协议详细通信过程以及分析结果。现有的检测过程是测评人员从安全协议捕获工具的数据中挑选出协议建立过程的数据包,从中找到数字证书以及使用的密码套件等参数,并对照相关标准依次进行检验。

我国越来越多的密码应用方案中选择国产密码算法^[3]。但目前使用的一部分测评工具并不是为测评工作开发的或者不能支持国产密码算法,使用中需要测评人员依据标准规范和要求进行人工验证,对测评人员要求较高。在测评过程中,密码测评工具所需的输入数据,如密文、二进制格式的加密数据等,都需要测评人员从通信数据中进行手动查找、复制粘贴。测评工具的输入输出数据格式也没有明确的规范,测评人员在读取数据时,可能需要进行手动的格式转换。这些

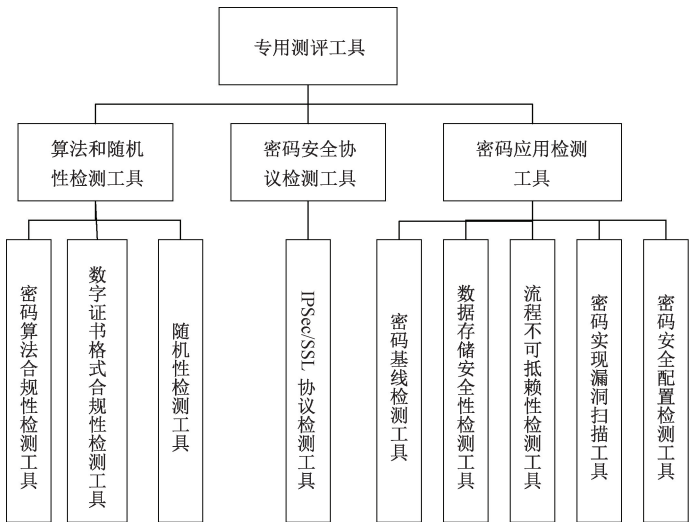


图 1 专用测评工具

Fig. 1 Special evaluation tools

过程会耗费大量的时间和精力,且容易引入人为错误。

1.2 密码应用测评

在密码应用测评中,商用密码应用安全性评估是一类必不可少的测评活动。依据《商用密码应用安全性评估管理办法(试行)》要求,涉及国家和社会公共利益的重要领域网络和信息系统的建设、使用、管理单位,应当在系统规划、建设和运行阶段,组织开展商用密码应用安全性评估工作。在规划阶段,测评机构需要对系统的密码应用方案开展多轮评估。在建设阶段,测评机构依据密码应用方案对建设完成的系统进行系统评估。通过后才可投入使用。在运行阶段,系统也应定期进行密码测评。此外,信息系统中使用的密码产品应该通过国家密码管理部门的认可和核准^[4]。对于已经取得证书的密码产品,测评时不需要对其本身进行检测,需要验证密码产品在接入系统环境后,是否能够符合系统所需的功能和性能要求。

密码测评的基本原则是避免对被测系统造成影响,并保证被测系统的通信数据等隐私数据不被泄露。被测系统一般会尽量减少与测评工具的直接接触,被测系统也会搭建模拟系统用于系统验证。在测评过程中,测评人员需要在每个测评点依次接入测评工具进行通信数据的采集和分析,判断被测系统使用的密码算法等是否合规、重要数据是否得到保护、密码产品是否被正确有效使用等。分析方式分为人工分析和工具分析两种。人工分析有些较为简单,比如在通信数据中找到管理员口令等鉴别信息,判断其是否在传输过程中得到了机密性保护。有些较为繁琐,比如从采集的通信数据中找到协议建立阶段双方使用的数字证书,并输入到对应的测评工具中。

如果这些重复的工作可以交由程序完成,使测评工具能够自动对通信数据进行处理,那么会给测评人员带来很大便利。近几年,一些人提出自动化测评的设计方案,并最终实现^[5-8]。苏昊欣等^[5-6]设计并实现了组件化的自动化测评系统,通过制定 XML 文件格式规范实现用户和测评系统通信,通过制定统一数据格式实现测评组件和密码算法组件通信,省去测评人员在密码算法测试中耗费的精力和时间。但通信数据格式规则过于复杂,并且测试只针对于密码算法组件,传入的输入数据相对固定,不适用多类功能组件的自动化

测评通信。罗世雄等^[7]设计了测评管理系统,能够使用漏洞扫描工具、数据库安全工具等自动收集被测系统的基本信息,如版本、补丁、安全配置等。但系统使用的工具需针对被测系统定制,接入工具不能重复使用,不易推广。李宇佳等^[8]提出一个调度自动化的软件测试平台,利用云计算提供 3 种测试模式对被测软件进行静态测试和性能兼容性等动态测试,省去了用户搭建测试环境所花费的成本和时间。但平台调度的对象是物理资源、虚拟资源和计算资源,且搭建此平台需要大量的硬件资源,不适合推广使用。

由此可见,自动化测评已在一些测评领域中应用,大大提高测评工作效率和质量。但针对现有密码测评活动中,多类别测评工具之间输入输出数据仍需要手动导入导出操作的问题,目前没有提出相应的测评工具自动化调度解决方案。

2 测评工具自动化调度方案

我们的工作就是设计一个测评工具自动化调度方案,并将其实现。自动化调度方案中,测评工具能够自动对其他工具输入或者测评人员上传的数据进行分析和处理,从而省去测评人员在测评过程中对测评工具输入输出数据进行手动采集、格式转换、导入导出、整理标记的时间和精力。测评工具自动化调度方案模型如图 2 所示,其中测评工具之间的连接关系以及被测对象场景拓扑图仅为示意。

在测评活动开始前,为满足测评对象可视化需求,测评人员需要上传被测对象的场景拓扑图。随后测评人员能够在场景图中标识测评点,并选择需要接入的测评工具组合,测评人员可以选择手动上传测试数据或者由测评工具自动采集通信数据。测评开始后,调度平台向测评任务中的每个测评工具发送包含调度信息的测评指令,测评工具可依据测评指令改变测评任务的运行状态,也可依据调度信息进行数据的自动采集和分发,无需由调度平台进行转发。测评结束后,测评工具上传到素材库中的测评数据和测评结果,可用于生成测评报告。本章我们首先介绍测评工具的部署方式、测评任务以及素材库,随后对测评指令和调度过程进行详细说明。

2.1 测评工具部署

相较于在被测系统的内网中安装一个可执行程序,外部接入服务器的方式更符合密码测评的

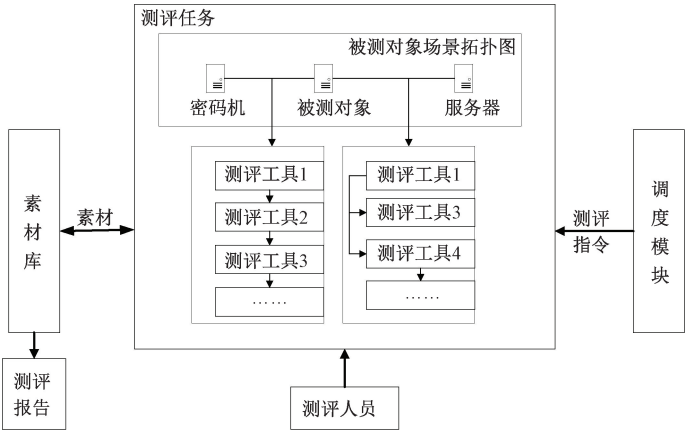


图 2 测评工具自动化调度模型

Fig. 2 Automatic scheduling model of evaluation tools

安全要求,对被测系统的影响更小。我们采用 WEB 开发中微服务架构的思想,使测评工具作为服务部署到服务器中。当有测评需求时,测评人员只需要将服务器接入被测系统的内网,便可以开启服务,采集内网通信数据用于测评分析。在调度过程中测评工具之间使用 WEB 服务接口采用 HTTP 协议进行通信,使用的传输数据格式为 JSON。这种方式在各个开发语言中都有相应的网络包或者开发框架可以直接使用,能大大减少现有工具和新接入测评工具的开发量。

测评工具需要暴露自己的接口访问地址供其他工具获取。我们使用配置文件来描述测评工具的访问地址,通过调度平台进行维护。其中每个测评工具对应一个配置文件。为研究测评工具对外所需要提供的接口类型,我们依据测评工具在调度过程中的位置和功能,将测评工具分为 3 类:采集工具、分析工具、关联工具。采集工具依据采集方式可分为交互测评工具和监听测评工具 2 类,通过与被测对象交互或者监听的方式采集通信数据,如 WireShark 工具。分析工具依据规范标准对被测数据进行分析验证,最终得出测评结果,如数字证书格式合规性检测工具。关联工具收集多个测评工具的测评结果,最终按照模板整理出测评报告。除基本的数据输入输出接口需求外,测评工具还需要包含接收调度信息的接口。为捕获通信数据以及与被测对象进行通信,采集工具还需要配置被测对象的 IP 地址等信息;部分分析工具需要配置参数信息,如数字证书格式合规性,检测工具为了验证数字证书的来源是否可信时,需要配置签发的上级证书参数等;部分分析工具之间存在依赖关系,如机密性分析工具的测

评结果需要依赖随机数分析工具对密文进行随机性检验的测评结果^[9]等。为能够满足上述 3 类测评工具的接口描述需求,我们提出了测评工具统一接口模型,如图 3 所示。

输入接口和输出接口 输入接口用于接收测评工具待处理的数据,可能由测评人员手动输入、也可能由其他测评工具产生。输出接口用于向调度平台发送测评结果,或者向其他测评工具发送处理后的数据。两个测评工具之间可以通过输入输出接口传输数据,如通用协议分析工具将采集到的数据输出给 IPSec/SSL 协议分析工具。

提供服务接口和依赖服务接口 提供服务接口用于接收其他工具发送的服务访问请求和参数,并将处理后的结果返回。依赖服务接口用于向其他工具发送服务访问请求和参数,并获取返回值。两个测评工具之间可以通过提供服务接口和依赖服务接口进行调用,如机密性分析工具调用随机数分析工具提供的随机性检验服务。

任务调度接口 任务调度接口用于接收调度平台发送的测评指令。测评工具从测评指令中获

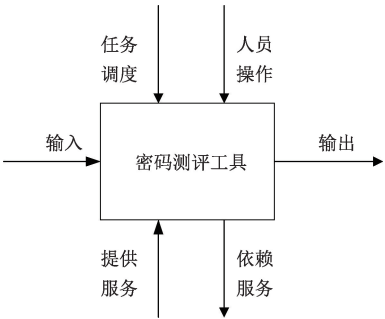


图 3 测评工具统一接口模型

Fig. 3 Unified interface model of evaluation tools

取调度信息,同时调整任务运行状态。

人员操作接口 人员操作接口用于展示测评工具提供的操作界面,测评人员可以在操作界面上配置测评工具的所需信息和运行参数,如采集数据的服务器 IP 地址、上级签发证书等。

对于每一个加入到调度平台的测评工具而言,都需要按照工具统一接口模型,定义具体的配置文件,便于与其他测评工具进行交互。配置文件中的每个接口类型都对应一个数据类型集合,代表这个接口所传入或者传出的数据结构信息。考虑到每个接口类型的输入数据和访问地址应该有很强的对应关系,测评工具使用伪静态页面接收请求^[10];测评工具加入到调度平台时,只需要提供工具的部署服务器地址,调度平台通过访问“服务器地址/meta”获取该工具的配置文件信息;通过访问“服务器地址/提供服务类型值”可以获得该工具提供的服务;通过访问“服务器地址/输入数据类型值”可以向该工具传输此输入类型的数据。由于配置文件可作为身份凭证,测评工具借助配置文件注册到调度平台中,以备后续的维护和使用。

2.2 素材库

将工具产生或者用户上传的一条数据,称为素材。调度平台使用素材库对素材进行存储管理。素材库支持将素材以文件、图片、JSON 等多种方式展现给测评人员。如果被测数据需要手动输入,测评人员可提前将被测数据上传到素材库中,进行保存管理,便于开启测评任务时进行选择。如果测评人员需要获取测评工具的某项输出数据,可以将输出数据上传到素材库中进行保存,便于后续查看。

2.3 测评任务

测评任务指对一个测评对象进行测评分析的过程,包含未开始、运行中、已结束 3 个运行状态。测评任务能够支持以下 3 类测评场景。

产品接入场景 采集工具能够捕获被测产品和调用方之间的实时通信数据,交由分析工具判断被测产品在接入系统的环境下,是否能够提供应有的密码服务;采集工具也可以向被测产品发送数据,采集被测产品的响应结果后交由分析工具,从而判断被测产品是否能够满足接入系统的功能、性能要求。

新建系统场景 测评人员在该场景下,可以选择测评数据由测评工具自动采集或者由测评人

员提前上传到素材库中。当选择自动采集时,采集工具能够捕获接入点的实时通信数据,交由分析工具判断被测系统的密码应用是否正确有效。

系统运行场景 测评人员无法选择采集工具,被测数据由测评人员提前上传到素材库中。

如果不同接入点的测试需求是相同的,则测评过程中使用的工具组合也是相同的。为此,我们增加工具链模块,对测评工具组合进行管理。测评人员在接入点选择所需使用的测评工具时,可以选择现有的工具链,也可以组合新的工具链。

2.4 调度过程

调度平台可以向该测评任务下的所有测评工具发送测评指令,包括新建测评任务指令、获取测评进度指令和释放测评任务指令 3 类。其中,依据调度策略对新建测评任务指令和释放测评任务指令的发送顺序做出了约束。测评工具从新建任务测评指令中获取运行和调度所需要的相关信息,最终实现自动调度。本节首先介绍 3 类测评指令,随后通过调度策略对整个调度过程进行详细介绍。

2.4.1 测评指令

测评指令中包含的信息有 2 类:调度信息和改变测评任务运行状态信息。测评工具需要根据调度信息实现数据自动采集和分发。依据测评工具统一接口模型,调度信息中应该包含测评工具对外的接口地址,包括测评工具输出数据以及依赖服务请求的接收地址。根据测评任务的 3 种运行状态,测评指令可分为以下 3 类。

新建测评任务指令 该指令中包含本次测评任务标识、每个依赖服务类型的访问地址以及每个输出数据类型的上传地址。其中,输出数据上传地址可能为空或者多个。

获取测评进度指令 测评工具收到指令后,返回信息包含:测评工具在该测评任务下接收的输入个数、处理后的输出个数和提供服务的个数。

释放测评任务指令 每个测评工具收到指令后,会立即终止指令中指定的测评任务,不再接受该任务下的输入数据以及访问请求。

2.4.2 调度策略

本小节内容主要介绍调度信息的来源,以及在进行调度过程中需要注意的细节。

调度信息获取 测评工具依据调度信息进行数据流转。调度平台需要明确和测评工具有数据流连接的下一个工具,从而获取该测评工具输出

数据以及依赖服务请求的接收地址。通过测评工具的配置文件内容,确定两个工具之间是否存在数据连接。如果测评工具 1 的某个输出类型和测评工具 2 的某个输入类型一致,认为这两个测评工具之间可以建立一条数据流连接,并记录下测评工具 2 该输入类型的接收地址,作为测评工具 1 该输出类型的上传地址。如果测评工具 1 的某个依赖服务类型与测评工具 2 的某个提供服务类型一致,认为这两个测评工具之间存在调用关系,可以建立一条数据流连接,并记录下测评工具 2 提供服务类型的地址,作为测评工具 1 依赖该服务类型的访问地址。这些记录下的内容会随新建测评任务指令一同发送给测评工具。

工具执行策略 在新建测评任务指令下发后,测评工具能够顺利开展测评任务、实现数据流转的前提是:测评工具能够访问所依赖的服务,并且输出的数据有工具能够接收。考虑到一个测评工具的输出和依赖服务可能是多个,对测评工具进行拓扑排序后,再依次向测评工具发送新建测评任务指令。拓扑排序的原则是先运行接收数据或者提供服务的一方。先收到新建测评任务指令的测评工具会先处于监听状态,这就使得它能够收到其他工具发送的输入数据或调用请求。需要注意的是,在释放测评任务时,发送测评指令的测评工具顺序与之相反,需要先关闭产生数据和调用服务的测评工具,从而切断数据源。由于采集工具的输出数据都交由分析工具进行分析验证,所以先开启分析工具等待数据输入。为能够采集到所有通信数据,在采集工具内部先开启监听测评工具,再开启交互测评工具。在测评任务结束后,调度平台开启关联工具,由关联工具到素材库中提取整合该任务下的所有素材,按照报告模板生成测评报告,上传到素材库并展示给用户。

综上所述,在新建测评任务指令下发前,调度平台通过匹配测评工具的配置文件,进行拓扑排序。这样使得在得到测评工具运行顺序的同时,也记录下了每个测评工具所需的调度信息,包含所有依赖服务的访问地址以及输出的上传地址。如果测评工具的输出数据需要保存到素材库中,则调度平台在拓扑排序时会直接将素材库对应数据类型的上传地址加入到该输出类型的上传地址集合中。最后,这些内容会随新建测评任务指令一同发送给测评工具。测评工具只需要将输出数据上传到指定地址,无需关注接收端是素材库还

是测评工具。该调度策略能够实现测评数据在测评工具之间自动采集与分发。

3 调度平台测试

调度平台基于广电项目需求进行开发。本节通过一个广电项目中的具体测评需求,对调度平台进行功能性验证,即验证调度平台是否能够向测评工具发送测评指令、测评指令中包含的调度信息是否正确、测评工具是否能够依据的调度信息输出数据或者调用服务,以及素材库是否能够接收测评素材,用于生成测评报告。调度平台和以下使用的测评工具均部署在便携式服务器上(CentOS Linux7 系统,CPU 为 Intel(R) Core(TM) i7-7700 3.60 GHz)。

3.1 实验设计

广电项目中包含多级广播平台,上下级广播平台之间相互通信。假设目前省级广播平台已经开发完毕,需要测试该广播平台的数字签名功能和数字签名验证功能实现是否正确,以及在签名过程中使用的数字证书是否合规。

为提高测评结果准确度,需要模拟被测平台的真实运行环境,使用模拟系统工具来模拟国家级广播平台所实现的功能,依据测评需求主动与被测平台进行特定内容的通信,提供测评数据。为了测试签名验证功能,模拟系统工具需要向被测平台发送正确的以及错误的签名数据,查看其是否能够正确验证。需要注意的是,模拟系统工具等同于模拟平台,不具有生成错误签名值的功能。因此由数字签名验证功能测评工具(简称“验签功能测评工具”)提供生成模拟签名服务,模拟系统工具通过调用此服务来获取正确或者错误的模拟签名值,发送给被测平台。模拟系统工具依据被测平台的响应信息可以判断被测平台的签名值验证结果,再由验签功能测评工具判断被测平台的验证结果是否正确。在通信过程中,被测平台发送的消息需要由协议捕获工具抓取,交由协议分析工具解析出签名数据和数字证书数据,最后由签名功能测评工具和数字证书格式合规性测评工具进行验证。被测平台的测评报告由报告生成工具整合测评数据后生成。

由上所述,该测评任务需要多个测评工具,对应的测评场景为新建系统场景。其中,模拟系统工具主动向被测平台发送包含模拟签名数据的消息,属于采集工具中的交互测评工具,与被测平台

交互的接口需要依据被测平台进行开发;协议捕获工具抓取被测平台和模拟系统工具之间的通信数据,为分析工具提供测评数据,属于采集工具中的监听测评工具。经过分析整理这些测评工具的接口模型描述如表 1 所示,数据流转过程如图 4 所示。除测评结果外,证书数据、签名数据和模拟签名值也需要上传到素材库中,便于再次查看以及使生成的测评报告更加完整。

3.2 实验过程及结果

首先将上述 7 个测评工具添加到调度平台上,部署服务器接入到被测平台的测试环境中,随后在测评任务中加入测评工具。根据测评需求,将被测平台和协议捕获工具、模拟系统工具进行物理连接。实验架构图如图 5 所示,其中调用服务数据连接未展示在图中。在测评任务开始前,依次填写上传测评工具所需要的各项参数。在测评任务开始 1 min 后,通过调度平台释放了这个测评任务。最终生成的测评报告如图 6 所示。

从测评报告中可以看出被测平台的签名功能

和签名验证功能实现正确,签名过程中使用的数字证书符合标准。测评人员使用调度平台能够解决测评需求,记录测评结果,同时省去了从通信数据中查找协议数据,再从中查找签名数据和证书数据等内容输入到对应测评工具的一系列操作过程。

报告生成工具能够从素材库中读取数据,生成测评报告,证明素材库能够正确接收测评工具的上传数据且上传数据的格式正确。测评工具能够输出正确格式的测评结果等数据,证明在测评任务执行过程中,测评工具收到了输入数据且运行成功,输入数据的格式正确。素材库和测评工具都能够接收到正确格式的数据,说明测评工具输出数据的上传地址正确,则调度平台向测评工具发送的测评指令中的调度信息正确。从调度平台发送的日志中可以得出结论:调度平台向测评工具发送新建测评任务指令的发送顺序符合调度策略,依次为数字签名验证功能测评工具、数字签名功能测评工具、数字证书格式合规性测评工具、

表 1 测评工具配置文件描述表
Table 1 Description table of evaluation tool configuration file

序号	名称	人员操作	输入	输出	提供服务	依赖服务
1	数字证书格式合规性测评工具	上传上级证书列表	证书数据	测评结果	生成模拟签名	生成模拟签名
2	数字签名功能测评工具	上传签发证书列表	签名数据	测评结果		
3	数字签名验证功能测评工具		验证结果	测评结果		
4	模拟系统工具	配置数量频率		验证结果		
		配置被测对象信息				
5	协议捕获工具	配置被测对象信息		数据包		
6	协议分析工具		数据包	证书数据		
				签名数据		
7	报告生成工具			测评报告		

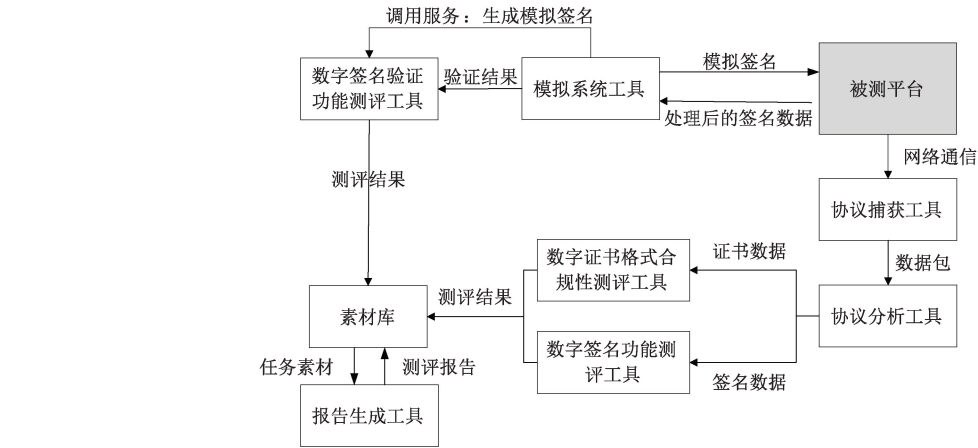


图 4 测评工具间数据流转示例

Fig. 4 Example of data flow between evaluation tools

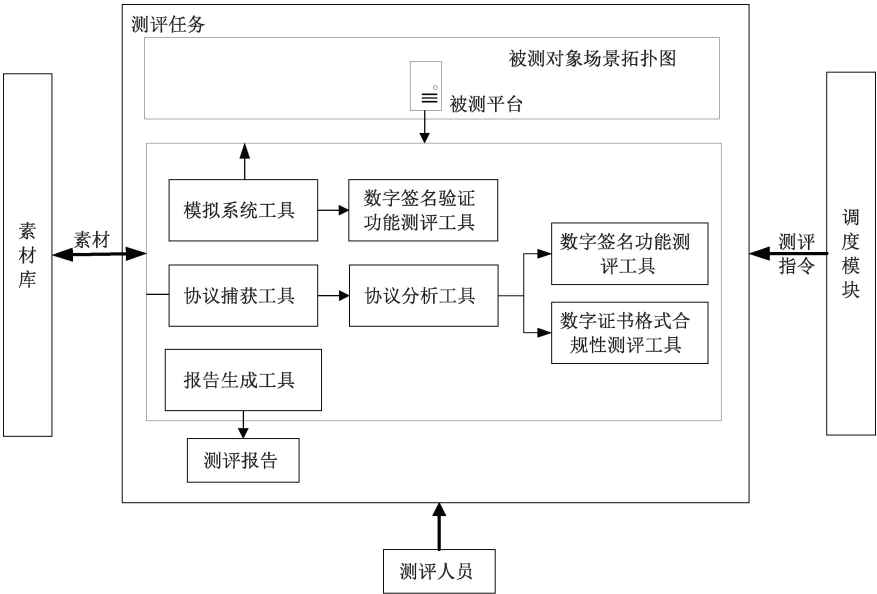


图 5 实验架构图

Fig. 5 Experimental architecture

测评报告				
被测对象	名称	省级广播平台		
	IP 地址	192.168.0.3		
签名功能	测评结果	<input checked="" type="checkbox"/> 通过 <input type="checkbox"/> 不通过		
	签名算法	SM2-SM3		
	签名值数量	1 个		
	详细测评过程	签名值	对应证书	验证结果
		1. MEQCIBJkrvhug3/BU+wV8ktBCBvze9M2pTtUFTg6dUqVDpyqAiA3sLJM6NwSLG2lL4vtQtnP4eRR1o1ENkg2MLuTaAt+Vg==	1. 00000000147d 合规	1. 正确
提供验证签名值证书	统计	<input checked="" type="checkbox"/> 合规, 有 1 个 <input type="checkbox"/> 不合规, 有 0 个		
	合规	证书 1: 颁发者: 000000000001 使用者: 00000000147d 有效期: 截止到 2072 年 9 月 公钥 HEX 进制: 2bc4c7c70b25f7e6b2ed7c20f02d5f4c22ae1a62ab5029c0d93053114a52163e04f606094d759863a42988b6ffcd9a0bba3d51327d53cbb9e7b2b68d4e945		
	不合规			
签名验证功能	测评结果	<input checked="" type="checkbox"/> 通过 <input type="checkbox"/> 不通过		
	验证模拟签名值使用的证书	颁发者: 000000000001 使用者: 000000005d17 有效期: 截止到 2081 年 10 月 公钥 HEX 进制: de4adfacc524fce81e883bb1a23f24d3bafd7f385796311af9fb2bc20586dd517482abcb39b57839c36d6858aefcd20085ff1bcd0adf480c8a2b658943bca22d4c		
	数量	1 个		
	详细测评过程	生成策略	模拟签名值	验证结果
		生成正确签名值	1. MEYCIQDF0iicn0PgABoWZeSfOhmthK m3lvO+QV7n/hh7hh7eglhAKGSaaYl.geltRXiBjfkntW3YXV06JvI4vE++MqNmamW	1. 正确
	生成错误签名值			

图 6 测评报告展示图

Fig. 6 Display diagram of evaluation report

协议分析工具、协议捕获工具、模拟系统工具。在测评任务执行过程中,测评工具都正常运行,数据自动采集和分发,没有出现数据丢失和请求失败的情况,调度策略正确可行。

3.3 方案对比

与前人工作相比,我们提出的方案更加适用于密码应用测评的自动化测评需求。苏昊欣等^[5-6]也使用配置文件来描述组件,实现被测组件的自动化测试。但是他们的配置文件描述的是被测组件,测评组件使用的测评方法只针对密码算法组件,传入的输入数据较为固定,不能满足多种密码应用测评需求。与之相比,我们的配置文件描述的是测评工具,并提出了适用于多类测评工具的统一接口模型,使得参与测评调度的测评工具种类多样,从而满足被测对象的多种密码应用测评需求。

罗世雄等^[7]使用本地数据库保存每个工具的扫描结果,供其他测评工具调用。在测评工具之间存在依赖关系的测评场景中,这种方案的效率较低。我们使用调度策略建立测评工具之间的依赖关系,并通过调度平台向测评工具发送调度信息,有序调度测评工具,使测评工具之间可以传输数据,而无需调度平台进行转发。此外,我们使用素材库来存储测评工具的测试结果,便于生成测评报告以及再次查看。

我们的方案不仅能够应用于商用密码应用安全性评估中,也可以应用在需要多个测评工具相互配合使用的密码应用测评过程中。

4 结论

本文设计了一个密码测评工具自动化调度方案,并实现了密码测评工具自动化调度平台。调度平台支持对产品接入、新建系统、系统运行 3 个测评场景下的测评任务进行测评,其中,被测数据可以由测评工具自动采集,也可以由测评人员手动上传。为使测评数据能够在多类测评工具之间实现自动流转分发,本文提出测评工具统一接口模型,对采集、分析、关联 3 类工具进行统一化描

述。现有测评工具只需要通过简单的适配调整,便可以集成到调度平台中,参与自动测评。最后,将其应用在广电项目中,实验结果表明,调度方案能够实现测评工具的自动组装,以及测评数据的自动采集和分发,从而有效减少测评人员在密码应用测评过程中对测评工具输入输出数据进行手动采集、格式转换、导入导出、整理标记的时间和精力,给测评人员带来很大便利。被测系统往往包含多个测评对象以及多个测评点,我们的工作目前只针对一个测评对象进行测评。后续将以被测系统为测评单位,进一步开展测评工具自动化调度方案的研究和探索。

参考文献

- [1] 霍伟,郭启全,马原.商用密码应用与安全性评估[M].北京:电子工业出版社,2020.
- [2] 邓福彪.数字证书格式合规性检测系统的设计与实现[J].福建电脑,2020,36(5):116-117. DOI:10.16707/j.cnki.fjpc.2020.05.041.
- [3] 林雪燕,林璟镔,管乐,等.在桌面虚拟化系统中实施国产密码算法[J].中国科学院大学学报,2015,32(5):701-707. DOI:10.7523/j.issn.2095-6134.2015.05.018.
- [4] 田敏求,傅大鹏,马原,等.面向等级保护的信息系统密码应用安全要求与测评实践[EB/OL].(2018-09-29)[2022-03-25]. <https://kns.cnki.net/KCMS/detail/detail.aspx?dbcode=CPFD&filename=HDJS201809001002>.
- [5] 苏昊欣.密码算法自动化测评系统[D].西安:西安电子科技大学,2010. DOI:10.7666/d.d100194.
- [6] 李风华,谢绒娜,苏昊欣,等.基于组件的密码算法自动化测评系统[J].计算机工程,2011,37(11):138-140,143. DOI:10.3969/j.issn.1000.3842.2011.11.047.
- [7] 罗世雄,刘晓强,刘振宇.面向等保 2.0 标准的测评管理系统设计与实现[J].信息技术与标准化,2019(10):76-78. DOI:CNKI:SUN:DZBZ.0.2019-10-024.
- [8] 李宇佳,李立新,狄方春,等.一种调度自动化主站系统软件测试方法及其平台:CN105677556B[P].2019-07-12.
- [9] 朱玉倩,王超,张艳.基于单因素方差分析的密码算法统计检验[J].电子技术应用,2021,47(9):43-45,50. DOI:10.16157/j.issn.0258-7998.211329.
- [10] 刘平.SEO 必知小知识 静态动态伪静态 URL 的特点[J].计算机与网络,2017,43(23):44. DOI:10.3969/j.issn.1008-1739.2017.23.052.