API接口安全运营研究

Research on API Interface Security Operations

韦峻峰[1]，李耀文[2]〔1. 中国联通河南分公司，河南 郑州 450008；2. 全知科技（杭州）有限责任公司，浙江 杭州 311100〕
Wei Junfeng[1], Li Yaowen[2]〔1. China Unicom Henan Branch, Zhengzhou 450008, China; 2. Quanzhi Technology (Hangzhou) Co., Ltd., Hangzhou 311100, China〕

摘　要：
根据当前API技术发展的趋势，从实际应用中发生的安全事件出发，分析并讨论相关API安全运营问题。从风险角度阐述了API接口安全存在的问题，探讨了API检测技术在安全运营中起到的作用，同时针对API安全运营实践，提出了几个方面的设想以及能够带来的运营价值。

关键词：
API接口；检测技术；安全运营
doi：10.12045/j.issn.1007-3043.2023.08.008
文章编号：1007-3043（2023）08-0033-05
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Based on the trends of current API technology development, it analyzes and discusses the research work related to API security operations from the security events encountered in practical applications. It elaborates on the security issues of API interface from the perspective of risk, explores the role of API detection technology in security operations, and proposes several ideas and potential operational value for API security operations.

Keywords：
API interface; Detection technology; Security operation

引用格式：韦峻峰，李耀文. API接口安全运营研究[J]. 邮电设计技术，2023（8）：33-37.

1 背景

近年来数据的价值逐渐凸显，数据应用场景不断拓展，数据交易持续增加。参与交易流通的数据类型从金融数据逐步扩展到医疗、交通、工业等多种类型的数据，数据需求方涉及公共服务、影视娱乐、交通、医疗、金融、广告营销等众多领域。然而，随着数据的集中汇聚及开放，数据共享面临着新的安全风险。相比传统的数据库层数据共享技术，当前大量数据通过各类API传输，传统的网络安全防护体系已经难以满足当前的数据安全保护需求，而针对API的安全防护和运营也引起了人们的高度关注。

收稿日期：2023-06-20

2 API及其安全风险

2.1 API概述

在应用编程实践中，由于系统的复杂性，在设计阶段就将其划为较小的部分，不同部分之间的规范约定就是应用程序接口（Application Programming Interface，API）。良好的接口设计可以降低系统各部分的相互依赖，提高组成单元的内聚性，降低组成单元间的耦合程度，从而提高系统的维护性和扩展性[1]。一方通过API发送远程请求，无需了解对方内部系统的逻辑，即可访问对方开放的资源，实现数据和服务的互动。目前，API已成为数据传输共享的重要手段。

2.2 API面临的挑战

2.2.1 API安全事件频发

API的数量急剧增长，与之相关的安全风险也在同步增加。近年来基于API安全所引发的事件屡屡发生：2018年Facebook公布了通过数据共享API被大规模网络攻击事件的细节，此次事件造成了3 000万用户的账号信息被泄漏；2020年淘宝报警称有黑产通过mtop订单评价API绕过平台风控批量爬取加密数据，共计11.8亿条。由此可见，API已经成为影响企业数据安全的重要风险来源。

2.2.2 API安全风险挑战

从API自身特点来看，除了常见的传统Web攻击威胁外，API还面临着越权访问、数据暴露、凭证失陷等威胁。同时，这些威胁检测涉及到了API接口发现、参数检测、行为识别、访问控制等多个环节，任何环节的缺失或不足都会影响到整体防护效果。所以，保护API安全的难点有以下几点。

a）场景复杂，无法通用。API应用业务场景十分丰富。在不同的业务场景下，一些风险特征或模型很难通用；同时，企业内部混合着十几年前的应用系统和新上线的系统，系统的实现可能不一致，API存在多样化的复杂性。

b）缺乏指导，难分主次。API安全防护虽然一直在发展，但目前还是处于探索阶段，业界对如何解决API安全问题，还没有形成一个普遍认可的最佳实践，所以在落地API运营建设的时候容易缺乏指导，难分主次。

c）能力分散，无法闭环。即使在一些安全建设比较领先的行业，也大多存在能力分散、产品孤岛的问题，产品能力、工作流程之间没有很好地打通，同时缺少对漏洞和风险的生命周期管理，没有形成闭环，实际运营的效率比较低。

2.3 安全风险分析

原生API大多从易用性、便利性等角度进行设计，往往缺乏对自身威胁的防护。而在API的设计实现中，也存在多种原因造成API之间的安全问题[2]。同时，敏感数据被封装在业务场景中，通过API进行交换，如果没有采用安全标记、多级授权、访问控制、安全审计等安全机制构建安全的交换空间，也难以确保数据的安全。

针对API的可利用性弱点、普遍性弱点、可检测性、技术影响、业务影响等方面，本文着重介绍其中影响较大的几个问题。

2.3.1 对象级授权失效

通常API采用令牌方式对用户请求进行鉴权，服务器会在用户登录之后生成一组不重复的字符作为令牌，在调用API时需要携带令牌由服务器进行校验[3]。这种机制的失效通常会导致未经授权的信息泄露、篡改或破坏。对象级授权失效如图1所示。

2.3.2 用户身份验证失效

如果身份认证机制出现问题，将使攻击者得以暂时甚至永久冒充其他用户身份，导致API的整体安全性降低。用户身份验证失效如图2所示。

2.3.3 对象属性级授权失效

当允许用户通过API接口访问数据时，需要验证用户是否具备访问对象的特定属性访问权限，如果API接口上存在用户不应该读取或访问的属性，即使是不敏感的数据，被大量收集后，也会暴露个人隐私，造成数据的泄露。对象属性级授权失效如图3所示。

3 API安全运营研究

3.1 API安全运营思路

API由于数量大、更新快且关联敏感数据和账号的变更，对其进行盘点和统计是后续安全防护的基

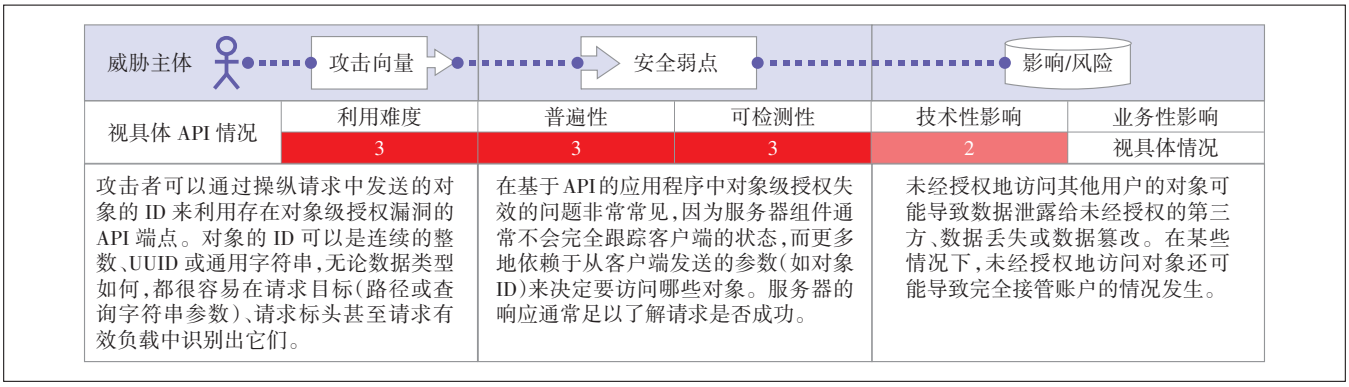

图1 对象级授权失效[4]

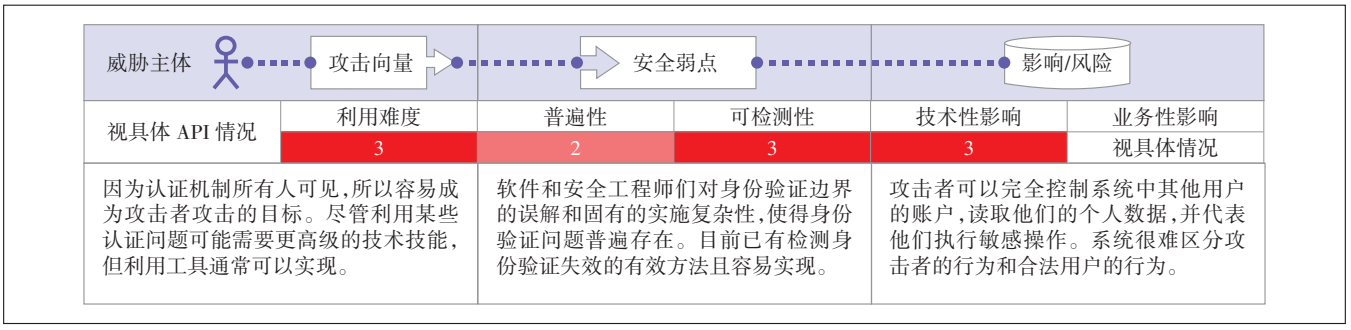

图2　用户身份验证失效[4]

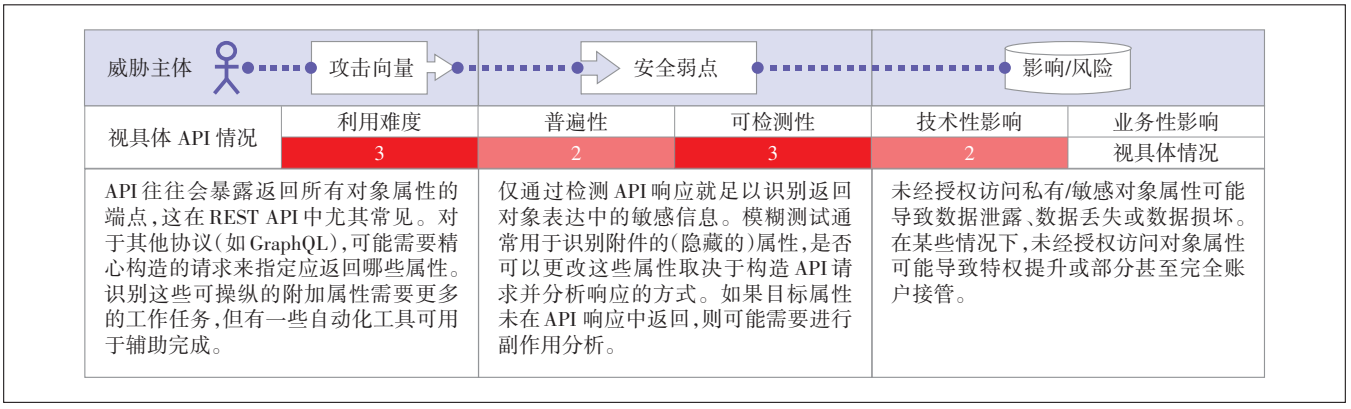

图3　对象属性级授权失效[4]

础。但大部分企业并没有把API资产纳入到资产盘点的范畴，未做好全面的资产梳理工作，会导致混乱、复杂的API资产台账。如应用API域名、IP、端口、路径的复用或拆分使用，呈现千“业务”千“API”的局面。

很多无用API没有及时下线，形成了僵尸API，可能导致严重的安全风险。传统上安全部门对API的盘点是依赖于业务部门的上报，但由于统计不全或更新不及时等种种原因，API资产很难通过有限人力以静态的方法来完成持续有效的梳理。并且由于安全技术人员对业务鲜有了解，难以准确理解API的各类业务属性，无法建立起资产、告警、业务、业务人员的逐一对应视图，因此必须借助API检测技术对API台账进行梳理。

API检测是一种软件测试实践，通常采用主动扫描的方式，直接测试API的功能表现、可靠性、性能表现和安全性。API测试可以通过工具模拟请求的发送与接收，如Postman、JMeter等；或者代码模拟请求的发送与接收，如JAVA自带的Web、HttpClient等。除此之外，还有以流量监测为基础的API流量分析技术，可实现对API数据暴露面的治理和对数据攻击行为持续发现[5]。

API的指数级应用使得API安全的条件变得异常严苛，也将企业推入了一个“高压”的局面，企业应该围绕闭环性、可持续性的API建设思路进行安全体系的设计和实施，基于均衡取舍研究的结果来定义系统安全设计元素，并且向系统安全设计元素分配安全机制，确定所期望的安全机制和实际有效的安全机制前端是否一致或相当，检验并最终确定设计元素和系统接口，制定安全规范等。

可以从以下几个方面开展API安全运营实践（见图4）。

a）全量API资产洞察。主动发现网站、小程序、APP等全量API资产，提供API类型、级别、形态、生命周期等全方位的API资产描述。从应用系统、数据标签组合、敏感等级、访问域、最近活跃时间、访问量等多种维度进行分析、筛选，形成重点API清单。

b）API暴露面管理。通过API数据暴露面管理、重点API清单筛选，辅助实现攻击面管理（ASM），完成泄露资产的发现及脆弱性检测。对接入侵&攻击模拟能力（BAS），评估企业安全技术措施的有效性，同时帮助渗透测试人员去更好更深度地渗透，持续加固API数据暴露面的管理。

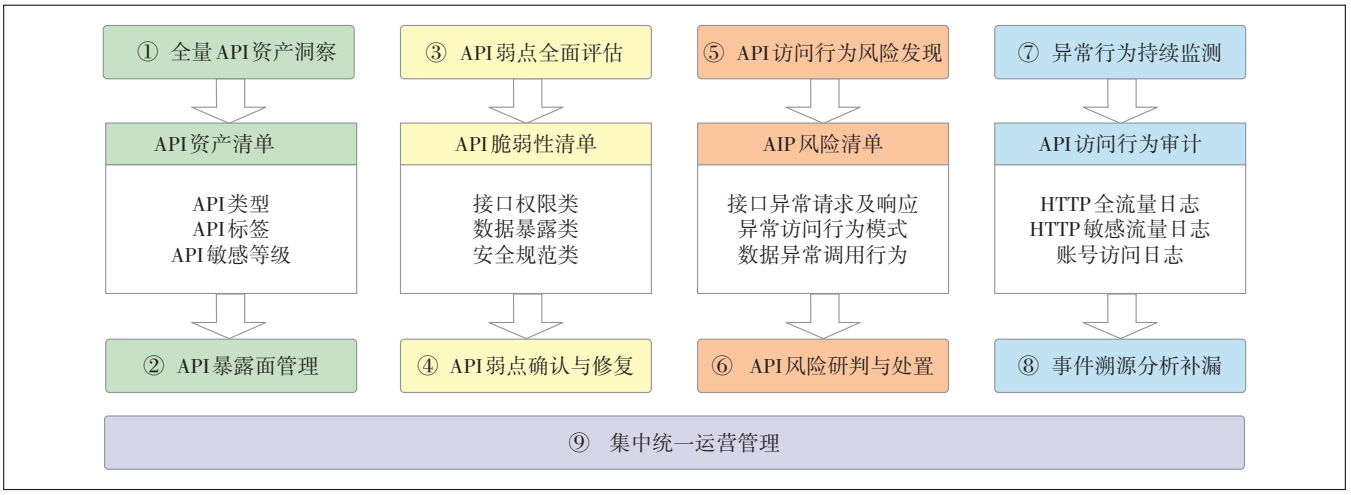

图4 API安全运营重点方向

c）API弱点全面评估。识别评估API脆弱性，包括接口权限类、数据暴露类、安全规范类、口令认证类、高危接口类等问题，能够覆盖OWASP API Top 10相关问题点，并满足主管部门及监管机构的合规要求。

d）API弱点确认与修复。对接企业的安全SOC平台，推动API的弱点修复流程；同时集成到企业现有的ITSM/SIEM工作流中，形成弱点/漏洞工单处理流程；也可以基于弱点的危害性和风险影响面，直接通过邮件、钉钉等IM软件推送给负责的业务部门去整改修复。在API弱点修复后，通过流量分析持续验证弱点是否完成修复，从而形成闭环。

e）API访问行为风险发现。由于在不同的业务场景下，一些风险特征或模型很难通用，因此在风险规则的基础上提出了新的解决思路：以接口为中心，针对业务安全场景，识别并刻画业务接口关键参数关系画像，从而能够以此画像为基线，发现接口的访问行为风险。能够识别的API新型攻击风险类型包括异常API请求/响应、异常访问行为模式、异常接口访问轨迹、异常数据调用行为等。

f）API风险研判与处置闭环。通过集成或对接威胁情报，实现可疑行为的进一步验证，通过旁路阻断、联动防护设备等方式完成验证后的风险处置。

g）事件溯源分析补漏。针对API的异常风险事件，通过下发溯源任务，主动进行关联事件的相关性检索分析，对数据行为进行精准审计并将结果汇总，便于及时补漏安全缺口。

h）异常行为持续分析。通过HTTP全流量日志存储检索与分析，对敏感API、人员账号、IP行为等要素进行组合检索，持续监测异常行为，将API安全运营做到更高的高度。

i）集中管理统一运营。通过威胁情报管理、暴露面治理、风险聚集性挖掘、异常行为审计分析等API运营手段，汇聚分析API风险并进行集中管理，打破孤岛效应，提升运营效率。

从企业视角来看，忽略API资产加剧了整个API风控运营体系的实施。建议企业结合自身的业务状况，打造API运营中心，以主动发现API资产、完成API接口资产清单为安全基建，逐步打造API弱点评估、风险监测、威胁拦截、异常行为审计、集中管理等能力，最终实现API安全运营闭环的落地。API风险运营流程如图5所示。

3.2 API安全运营价值

3.2.1 数据流动态势识别

可识别自定义的流入、流出应用系统的敏感数据（包括Web页面内和传输文件内的敏感数据）的种类和数量，记录存储访问系统传输敏感数据的详细信息，包括用户IP、姓名、部门、访问对象、访问时间以及访问内容等详情，构建应用系统的敏感数据流动地图，提供记录的多维度查询功能，可以快速、全面地知晓什么人在什么时间通过什么方式获取了什么敏感数据。

3.2.2 应用系统接口管理

针对每个业务系统，梳理其接口数量和情况，形成应用接口清单。从是否传输敏感数据、接口的活跃程度、上传/下载等方面将接口进行分类分级，检测接

图5　API风险运营流程

口存在的无鉴权访问、后门接口等暴露面，并进行分类汇总展示，实现暴露面可还原，帮助安全人员摸清接口的脆弱性，推动系统侧进行应用系统设计和运维方面的问题整改。

3.2.3 敏感数据风险预警

建立各类敏感数据风险监控指标，构建分析模型，对数据行为建立用户基线、接口基线、系统基线等，实时监控多个维度的运行状态，实时发现非正常时间访问、大量数据异常下载、敏感数据未脱敏、伪脱敏等各类异常行为，并及时告警，防止大规模的敏感数据泄露、窃取、滥用等风险。

3.2.4 数据泄露事件溯源

实现敏感数据流动地图的可视化展示，能够清晰地展示应用系统、接口等清单报表和运行安全性，自定义敏感数据标签和风险指标，详细记录日志并针对脆弱性、风险事件进行分类统计、分析和展示。在完整记录敏感数据流动、访问操作的基础上，做好数据内容、账号、接口等多维度的溯源，还原风险路径、评估影响面。

4 API安全运营总结

从长远来看，可以通过将本文的解决方案与用户现有的工作流程无缝集成以及与用户现有的平台/技术紧密融合，从而建立一个有效的闭环验证机制。同时，还可以利用API接口上下文画像，建立正常行为的基线，并检测异常和离群的风险，实现风险规则的自动调整，加强风险自动化运营能力。考虑到企业内部职责边界的情况，设计清晰的用户使用路径，使参数配置可视化并实现精细化运营。这些举措将提升API风险管控机制的建设与运营实践水平，真正实现API安全运营落地，为企业发展带来持续的收益和效益。

参考文献：

[1] 中国信通院. 应用程序接口（API）数据安全研究报告（2020年）[EB/OL]. [2023-04-25]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202007/t20200727_287193.htm.

[2] 董之光，冯梅，柏东明. 常用API接口安全防护研究[J]. 网络安全技术与应用，2023(4)：52-54.

[3] 崔喜萌，陈明. 软件开发开放API接口的安全处理[J]. 网络安全技术与应用，2020(4)：80-81.

[4] OWSAP. OWASP API Security Top 10 (2023)[EB/OL]. [2023-06-05]. https://owasp.org/API-Security/editions/2023/en/.

[5] 全知科技. API风险监测系统[EB/OL]. [2023-04-25]. https://data-sec.com/product/api/.

作者简介：
韦峻峰，高级工程师，硕士，主要从事IT系统及网络信息安全相关技术及运营研究；李耀文，工程师，学士，主要从事数据安全相关的方案规划及安全运营等工作。