基于ATT&CK的入侵检测与防御体系建设实践

Practice of Intrusion Detection and Prevention System Construction Based on ATT&CK

郭新海，徐　雷，张曼君，刘　安，蓝鑫冲，丁　攀（中国联通研究院，北京 100048）
Guo Xinhai，Xu Lei，Zhang Manjun，Liu An，Lan Xinchong，Ding Pan（China Unicom Research Institute，Beijing 100048，China）

摘　要：
数字化转型和云形态日新月异的变化，给网络安全领域带来了各种各样的新式挑战，有效的保证网络空间安全，开展攻击溯源及反制，已经成为新形势下网络安全行业所面临的新任务。网络安全防护人员如何在当今攻守不对称的情况下做好入侵检测与防御，已经成为每个组织需要重点解决的问题。分析了当前入侵检测与防御体系存在的问题，结合ATT&CK框架，讨论了如何构建入侵检测与防御体系，才能更好地应对攻击行为。

关键词：
ATT&CK；网络空间安全；入侵检测；入侵防御
doi：10.12045/j.issn.1007-3043.2022.09.016
文章编号：1007-3043（2022）09-0077-05
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：
Digital transformation and rapid changes in cloud morphology have brought a variety of new challenges to the network security . Effectively ensuring the security of cyberspace and carrying out attack source tracing and countermeasures have become the new tasks faced by the network security industry under the new situation. How the network security protection personnel do well in intrusion detection and prevention under the situation of asymmetric attack and defense has become a key problem to be solved by each organization. It analyzes the existing problems of current intrusion detection and prevention system，combined with ATT&CK framework，it discusses how to construct intrusion detection and prevention system，in order to better deal with the attack behavior.

Keywords：
ATT&CK；Cyberspace security；Intrusion detection；Intrusion prevention

引用格式：郭新海，徐雷，张曼君，等. 基于ATT&CK的入侵检测与防御体系建设实践[J]. 邮电设计技术，2022（9）：77-81.

0 前言

当今时代，随着数字化转型的推进和云计算技术的普遍应用，进入了开源和云原生时代。在这个时代背景下，开源组件和云原生技术得到广泛应用，并且已成为软件应用系统快速开发、发布部署和持续运营的必要条件。据中国信息通信技术研究院统计，软件应用中开源代码占软件代码的比例从2015年的36%增长到2019年的70%，近2年又增长到80%~90%，而容器、Docker和Kubernetes等技术的应用改变了传统软件交付的方式，Docker和Kubernetes则进一步成为了新型的基础设施。新技术的普遍应用和相应防御措施建设的滞后，使企业面临着更多的新型攻击，攻击者不断地利用开源组件漏洞、镜像漏洞、微服务漏洞、容器漏洞发起更多的攻击。

因此，在这个时代背景下，网络空间防守方既要面对传统的安全攻击行为，又要面对新兴的软件供应链攻击、APT攻击、开源组件攻击以及基于云原生技术发起的攻击。在这种攻守不对称的情况下，如何做到对入侵行为的有效检测与防御，构建更加有效的安全

收稿日期：2022-07-25

体系，是保护组织机构安全进而保护国家安全的迫切需求。

1 当前检测与防御体系面临的问题

1.1 基于攻击者视角的研判分析体系不足

目前针对网络攻击的检测与防御体系仍然以被动响应为主，在被动响应的基础上，逐渐开展纵深安全防御体系的建设，增强主动防御的能力。同时，很多机构也开始了建设自有的SOC运营中心、安全大脑、安全统一指挥平台等，这些平台在平时以及护网的网络安全检测与防御中发挥了重要的作用，但是由于其在推广使用的过程中存在系统过多集成困难、报警过多不易分析、攻击行为缺乏上下文语境等问题，并未发挥出最大的作用。根据痛苦金字塔模型（见图1）分析，目前这些系统平台仍以分析哈希值、IP、域名、网络和主机进程等信息为主，基于攻击者视角分析其TTPs（Tactics、Techniques、Procedures）的能力仍然偏低。但是，TTPs却是分析攻击者行为的重要信息，其描述了攻击者从侦查、信息收集、攻击到获取数据这一过程中每一步是如何进行的，因此，TTPs也是痛苦金字塔中对防守方最有价值的信息。ATT&CK（Adversarial Tactics、Techniques and Common Knowledge）是有效分析攻击行为的威胁模型，基于ATT&CK框架体系，通过结合多种情报对攻击者进行画像，有效识别攻击者，增强基于攻击者视角的研判分析水平，能够有效提高企业的攻击检测与防御能力。

1.2 软件应用自我防护能力需要提高

目前数字化软件应用系统都在大量的使用开源组件，开源组件的使用大大提高了软件应用系统的开发效率，但是也带来了更多的安全风险。从2021年的log4j2漏洞，到2022年的spring框架漏洞，都说明开源组件存在着很多未知的安全漏洞，2021年版本的OWASP TOP 10（见表1）中针对风险组件发起的攻击行为也从第9位上升至第6位。新型漏洞风险的不断出现，导致攻击方的攻击手段日益多样，软件应用的安全防护所依赖的检测防御却仍然以传统的基于规则的防御体系为主，这些防御措施很难有效地拦截新型攻击行为，在应对0DAY漏洞攻击方面也存在天然的缺陷。如何更有效地实时阻断针对软件应用的攻击行为，贴身保护软件应用，提升应用的自我免疫能力，增强应用应对0DAY攻击的能力，准确发现开源组件中的风险并进行修复，已经成为各个企业组织亟待解决的问题。

1.3 云原生安全防御手段建设滞后

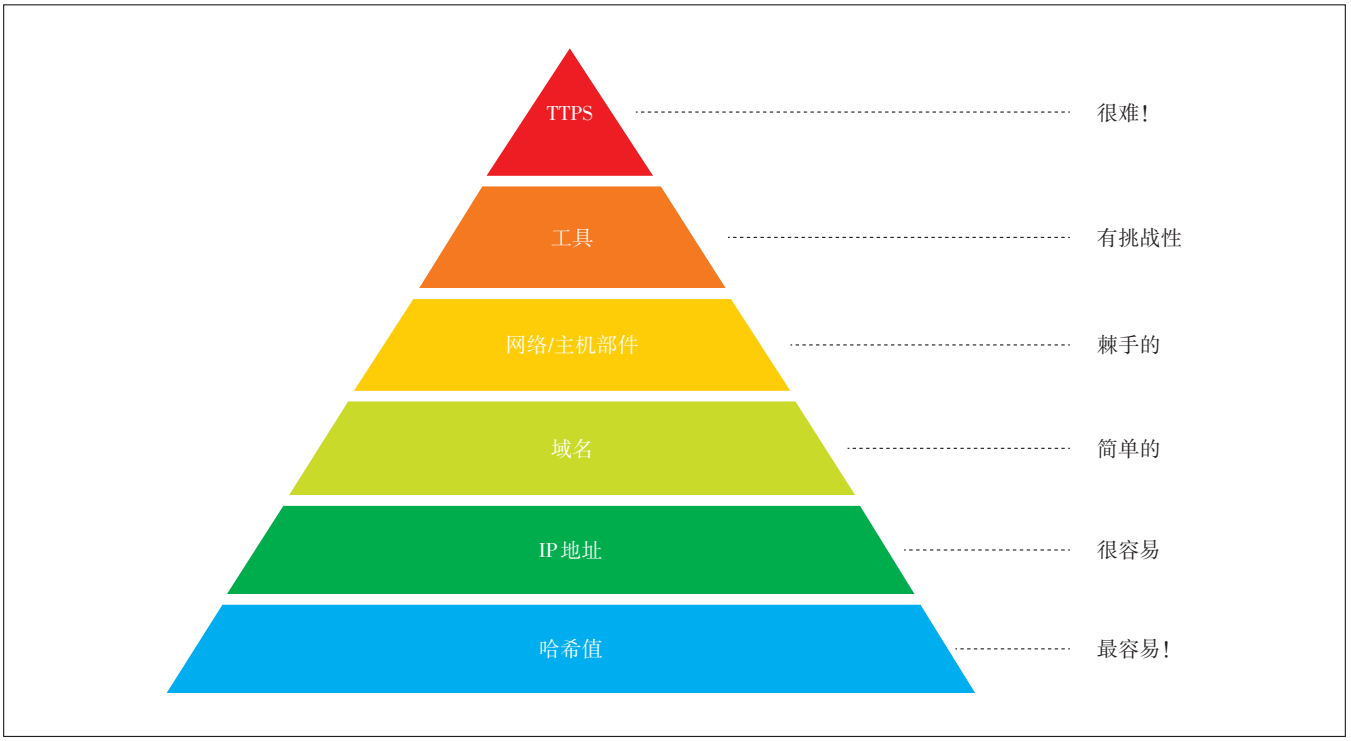

图1　Bianco提出的痛苦金字塔

表1　OWASP TOP 10（2021）

序号	漏洞类型
A01	失效的访问控制
A02	加密失败
A03	注入漏洞
A04	不安全的设计
A05	安全配置错误
A06	易受攻击和过时的组件
A07	认证和授权失败
A08	软件和数据完整性故障
A09	不足的日志记录和监控
A10	服务器请求伪造

云原生技术中广泛采用了持续交付、DevOps、微服务和容器化，并且以容器、微服务、DevOps等技术为基础建立了一套云技术产品体系，在这套体系中容器和Kubernetes成为了新型的基础设施。这些技术发展的同时，也带来了安全方面的诸多挑战，如在搭建应用的过程中，镜像的使用可能会导致将存在风险的镜像引入到内网环境中；容器和Kubernetes的不安全配置，可能会导致攻击者通过容器攻击宿主机、通过容器攻击集群等风险的发生；微服务的增多、暴露的端口数量难以梳理，增大了风险暴露面；微服务框架的使用，也可能会将开源组件的风险漏洞引入应用系统中。

在云原生的体系中，传统的安全防护手段无法深入识别容器和镜像的安全问题，因此需要加快相应安全检测与防御体系的建设进度。结合容器的ATT&CK框架，打造基于攻击行为的容器安全防御与检测能力，实现新型基础设施、容器、镜像的安全可视和综合风险感知。

2 ATT&CK框架介绍

2013年，MITRE公司为了摆脱网络安全治理中防守方所面临的困境，基于现实中发生的真实攻击事件，创建了一个丰富的对抗战术和技术知识库，即ATT&CK。目前，ATT&CK最新版本为11.1，该版本的ATT&CK框架包含了企业矩阵、移动端矩阵、工业控制系统矩阵，每类矩阵中都包含攻击者发起攻击所采用的战术、技术和子技术，并且战术、技术和子技术的种类一直处在迭代增加的过程中。

2.1 企业的ATT&CK攻防矩阵

企业的ATT&CK矩阵涵盖了攻击者进行攻击的常用技术，适用于Windows、MacOS、Linux等平台，并且随着云计算技术的广泛应用引入了云环境的内容，包含office 365、Azure AD、Google Workspace、SaaS、IaaS等平台，另外还对网络环境和容器环境进行了覆盖。企业矩阵中介绍了攻击者在攻击过程中使用的14项战术，分别是侦察、资源部署、初始访问、执行、持久化、提权、防御绕过、凭证访问、发现、横向移动、收集、命令与控制、数据窃取和影响，这14项战术又包含了220多项技术以及500多项子技术。

2.2 容器的ATT&CK攻防矩阵

容器的ATT&CK攻防矩阵，涵盖了容器层的攻击技术，还介绍了一系列与容器相关的恶意软件，包括攻击者在对容器环境进行攻击时所采用的8项战术和29项技术，8项战术分别为初始访问、执行、持久化、权限提升、防御绕过、凭证访问、发现和影响。具体的ATT&CK容器攻防矩阵如图2所示。

3 基于ATT&CK框架构建检测与防御体系

3.1 对应ATT&CK矩阵形成安全能力图谱

根据ATT&CK矩阵，打造企业自身的安全能力图谱，能够更好地提升企业的安全防护能力，充分发挥已建设系统的防御效果，发现欠缺的安全防护能力，指导未来的系统建设方向。

企业在建设自己的安全能力时应该保障运营安全，按需打造安全能力，重视安全管理。企业可根据实际需要建设自有的综合态势感知平台、资产和漏洞集中管理平台、安全运营中台、软件系统测绘平台、威胁狩猎平台等，通过建设这些平台能够保证内网全部网络资产的可视化，及时发现攻击行为，形成内网网络拓扑和软件依赖的关系图谱，记录攻击行为的攻击信息，完成攻击者的身份信息获取和画像，为开展攻击者的溯源反制提供参考；根据实际需要打造自己的安全能力，安全能力覆盖网络及边界安全、主机安全、云安全、软件应用安全、安全审计和数据安全等，能够做到全方位的安全防护；另外，安全管理作为保证企业安全的重要方面，需要制定符合企业自身的安全管理制度，安全管理可包括开发管理、运营管理、系统上线管理以及员工的安全意识培训等。图3给出了安全能力建设图谱示例，可为企业或组织的安全能力建设提供参考。

3.2 打造软件应用自我防护能力

软件应用系统在当前形势下面临着攻击日益增

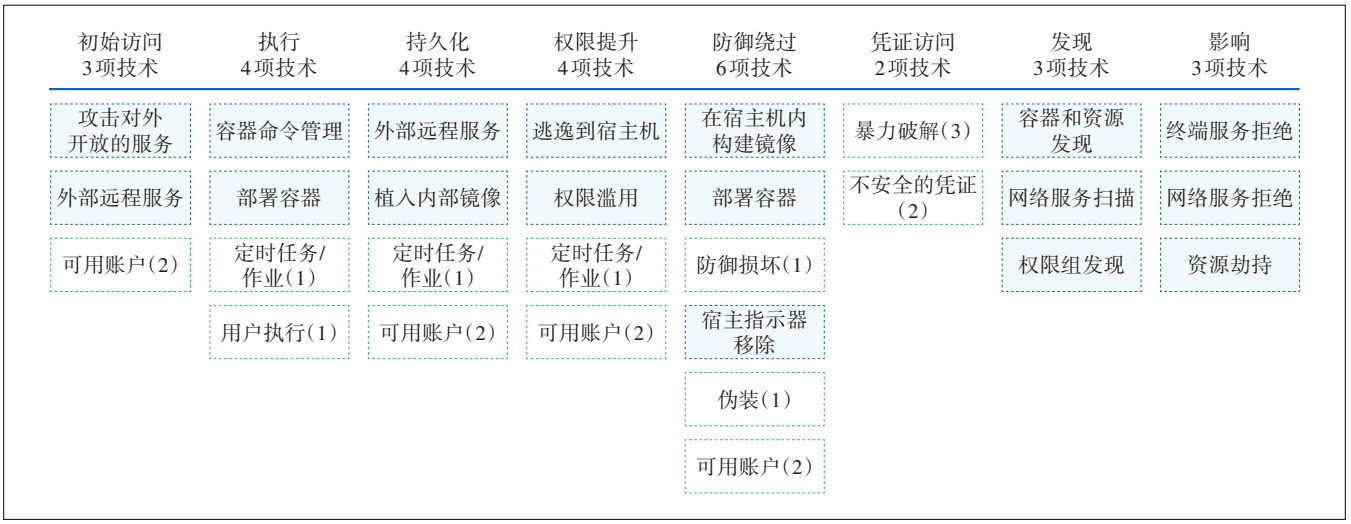

图2　ATT&CK容器攻防矩阵

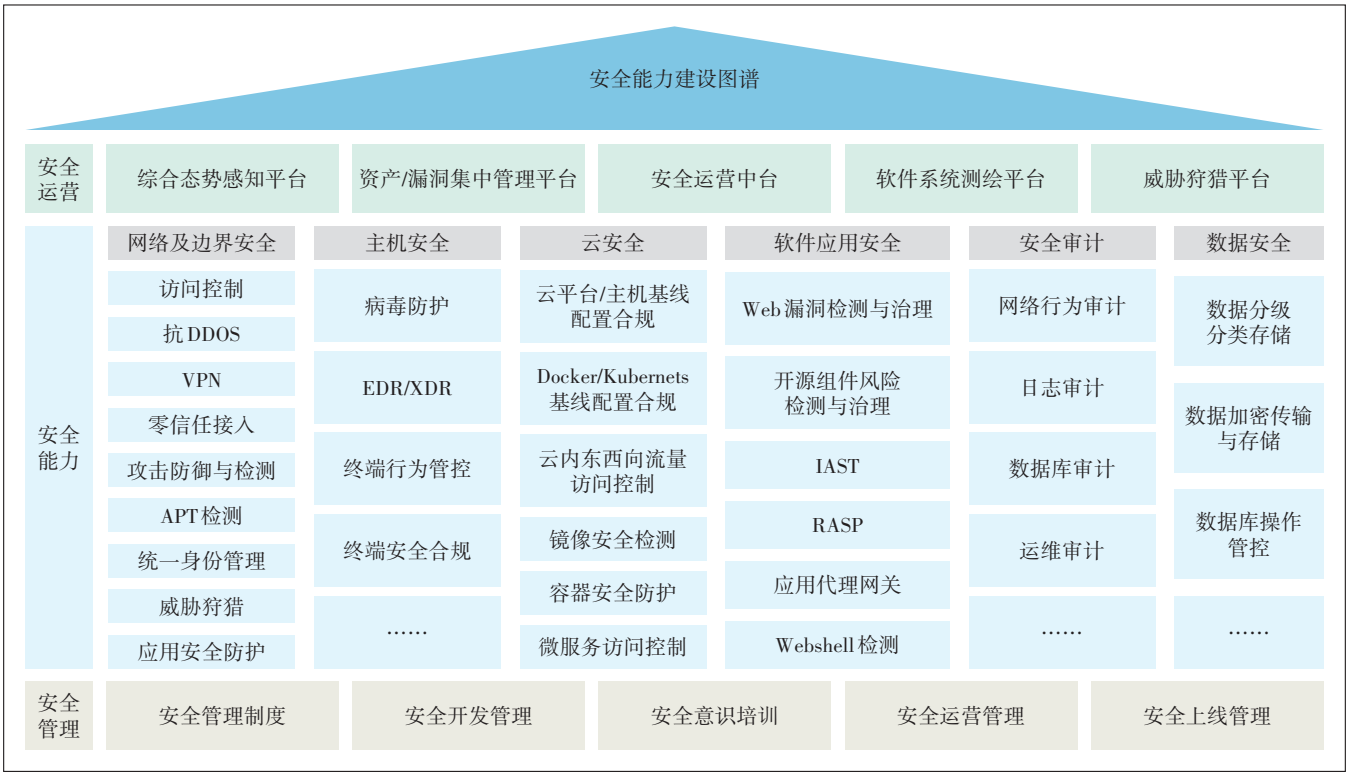

图3　安全能力建设图谱示例

多以及难以获取攻击者网络身份信息并进行有效溯源反制的问题。因此，在依托原来软件应用纵深安全检测与防御体系进行防护的同时，需要重点打造软件应用自身的免疫力，增强其动态防御和风险组件的检测能力，构建白名单防护、动态补丁分发和应用自身防护多级联动机制。

开发运行时应用程序自我保护（Runtime application self-protection，RASP）能力，将防御逻辑注入到Java底层API和Web应用程序中，实现防御手段与应用程序融为一体，实时分析和检测Web攻击，使应用程序具备自我保护能力，能够有效弥补原来防护体系的不足，补上现网软件应用系统多级防御体系中的最后一环，让穿透后的攻击无法落地形成危害。RASP技术能够有效地发现并防御多种已知的Web应用攻

击行为和未知的针对0DAY漏洞发起的攻击，并能够梳理应用系统的开源组件信息，发现开源组件的风险。因此，依托RASP打造软件的自我防护能力，能够增强企业应对0DAY漏洞攻击、开源组件攻击的能力，更好地保护应用系统和内网的安全。软件应用自免疫防御能力如图4所示。

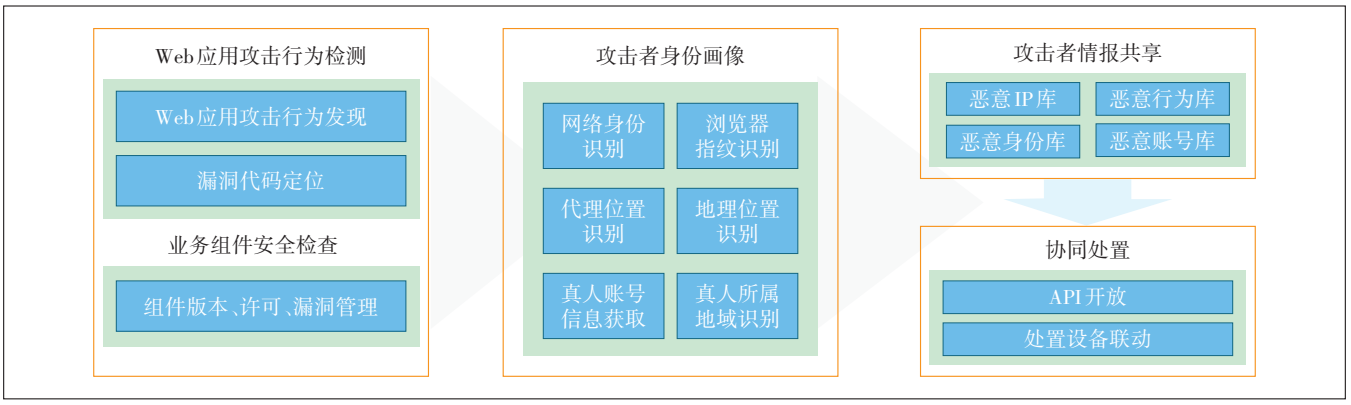

图4　软件应用自免疫防御能力

3.3 加快推进云原生安全防御能力建设

面对云原生技术中广泛采用微服务和容器化所带来的安全问题，需要加快推进相应的云原生安全防御能力建设，构建云原生安全防御系统，针对容器、Kubernetes和云主机提供安全基线配置核查能力，保证新型基础设施的基础安全水平；针对容器镜像中存在的安全风险，提供镜像安全检测能力，快速地定位发现镜像中存在的风险；针对容器运行时可能存在的容器逃逸、容器网络攻击等行为，提供容器进程监控、行为监控与审计、风险行为检测与阻断等功能，保证容器的安全运行；针对微服务的使用所带来的风险暴露面增加，精细化微隔离策略，根据业务需要控制不同业务属性相互访问需求等。

4 结束语

ATT&CK自发布以来就一直在促进着红队、蓝队和管理层之间的沟通交流，其中防守方能够使用该框架进行攻防演习和评估自己的安全能力建设情况，攻击方能够使用该矩阵寻求自身可以使用的技术。企业基于ATT&CK矩阵建设入侵检测与防御体系能够更全面、更有针对性地应对攻击者，更好地保护自己企业内网的安全。但是，攻击和防守方的技术能力都始终处于不断发展之中，ATT&CK矩阵也一直处于更新之中，因此企业的入侵检测与防御体系也应该根据攻守方的态势进行快速更新，只有这样才能更好地检测并防御攻击行为，进而更好地保证自己企业的网络安全。

参考文献：

[1] 张莹. 基于ATT & CK的中国蓝云一体化威胁防御系统建设[J]. 中国有线电视，2021(12)：1208-1214.
[2] 何树果，袁瑗，朱震，等. 基于ATT&CK框架的域威胁检测[J]. 信息技术与网络安全，2021，40(12)：15-18，25.
[3] 李璇，黄俊，袁帅. 基于ATT & CK + SOAR的运营实践[J]. 网络安全和信息化，2021(2)：52-53.
[4] 冀俊涛，石磊. 基于ATT&CK框架的实战分析[J]. 网络安全技术与应用，2021(2)：6-8.
[5] 郭新海，张小梅，刘安，等. 云原生应用供应链安全风险防护方案探讨[J]. 信息通信技术，2021，15(4)：39-43.
[6] 贵重. 基于ATT&CK的多源数据深度安全检测技术研究[J]. 电信工程技术与标准化，2020，33(10)：81-86.
[7] 徐嘉涔，王轶骏，薛质. 网络空间威胁狩猎的研究综述[J]. 通信技术，2020，53(1)：1-8.
[8] 葛文翰，王俊峰，唐宾徽，等. 基于关联增强的网络威胁情报技战术分类[J]. 四川大学学报(自然科学版)，2022，59(2)：94-102.
[9] 刘高，郝龙，赵东东. 基于“ATT&CK”战术框架的网络安全单兵侦测系统[C]//2021年国家网络安全宣传周网络安全产业发展论坛论文集. 西安：中国网络安全产业联盟 中国电子技术标准化研究院，2021：41-45.
[10] 庞进，王景初，郝龙. 基于ATT & CK战术框架的自动化渗透攻击研究[J]. 网络安全和信息化，2021(10)：120-124.

作者简介：
郭新海，毕业于北京交通大学，工程师，硕士，主要从事网络与信息安全研究工作；徐雷，毕业于北京理工大学，教授级高级工程师，博士，主要从事网络与信息安全研究工作；张曼君，毕业于西安电子科技大学，高级工程师，博士，主要从事网络与信息安全研究工作；刘安，毕业于哈尔滨工程大学，工程师，硕士，主要从事网络与信息安全研究工作；蓝鑫冲，毕业于中国科学院大学，工程师，硕士，主要从事网络与信息安全研究工作；丁攀，毕业于北京化工大学，工程师，硕士，主要从事网络与信息安全研究工作。