安全+
SECURITY
2023/12 总第 059
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

SecLLM在外部攻击面管理中的应用之道

大模型与软件供应链安全结合调研与总结

车联网移动应用安全攻守道

基于风险量化的网络安全保险实践

机密计算的崭露头角与未来前景

NSFOCUS

本期看点 HEADLINES

主办：绿盟科技
策划：《安全+》编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-5462
传真：(010)6872 8708
网址：www.nsfocus.com

2023/12 总第 059

欢迎您来信nsmagazine@nsfocus.com 与我们交流，
分享您的建议和评论。（《安全+》部分图片来源于网络）

安全+ SECURITY

目录 CONTENTS

数字经济时代网络安全环境风云多变，需要技术持续创新。网络安全是基础的安全保障力量，只有有效地保障网络安全，才能为网络空间中运行的各种业务和数据的安全稳固提供支撑，保障业务平稳运行。

本期《安全+》将继续着眼网络安全趋势，从前沿技术发展、能力构建、政策解读等视角出发，分享网络安全发展和安全的路径思考。

安全产业的发展没有终点，如何在不断涌现的新技术中找到正确方向、释放安全能量？绿盟科技一直在路上。面对网络空间的高度不确定性，绿盟科技积极推动数字技术在网络安全领域的创新应用，以先进技术解决安全风险难题，重构数智时代的数字安全新方案，秉承智慧安全3.0理念，构建“全场景、可信任、实战化”的安全运营能力，实现“全面防护、智能分析、自动响应”的防护效果，为夯实数字中国建设框架的数字安全屏障发力。

数字化发展需要坚实的安全底座，未来，绿盟科技将持续聚焦优势资源，坚持技术长期主义，不断深耕求索，从国家网络安全的整体和大局出发，为网络安全设计全面可信的防御体系，为用户提供全生命周期安全防护，为推动网信事业高质量发展持续赋能。

叶晓虎

SecLLM在外部攻击面管理中的应用之道

绿盟科技 创新研究院 袁军

摘要：安全大模型 SecLLM 在网络安全领域扮演了关键角色，特别是在攻防模拟和外部攻击面管理（EASM）方面。首先，它能模拟各种复杂的攻防场景，例如供应链攻击、钓鱼攻击和零日漏洞攻击，多维数据分析，辅助安全运营人员全面评估特定情况下的安全风险。其次，SecLLM 较强的生成和识别能力能够检测多样化的攻击载荷、恶意代码等数据，其研判能力不仅提高了检出率并降低了误报。本文从外部攻击面管理、攻防演练角度讲述安全大模型 SecLLM 如何做好智能辅助工作。

关键词：安全大模型 外部攻击面管理 智能攻防

1. 外部攻击面管理——EASM

外部攻击面管理（External Attack Surface Management，EASM）是一种网络安全实践，是指识别、监控和管理组织的外部攻击面（攻击入口）。外部攻击面包括互联网暴露的服务器资产、凭证、公有云服务、源代码、暗网信息披露以及可能被攻击者利用的第三方合作伙伴软件代码等。通过 EASM 跟踪和评估这些潜在的攻击面来帮助组织更好地了解面临的风险，并采取措施来减少潜在威胁，企业安全做到“比攻击者更懂您的外部风险”。

EASM 任务包含泛资产普查、攻击触点识别和评估、攻击面分析、风险评估及预警等一系列的安全实践。具体实践如下：

1.1 泛资产普查

通过分布式探测引擎，持续扫描和监控外部环境，对网络空间的泛资产进行搜索普查，识别一切可能被潜在攻击者利用的数字资产、敏感数据、Email 情报等，为弱点检测和风险分析打好基础。

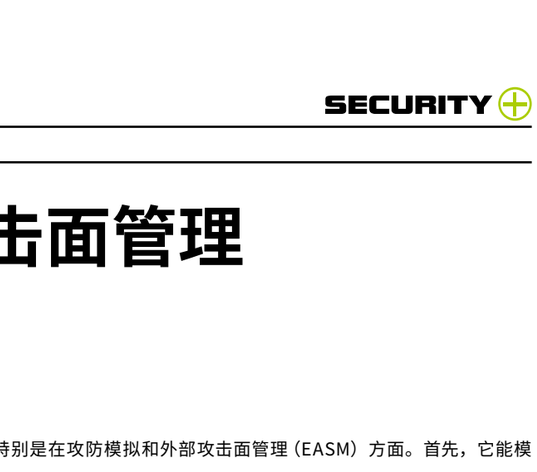


图 1 泛资产识别与发现

1.2 攻击触点识别和评估

在攻防视角下，依托强大的指纹库、情报库对外部泛资产进

行弱点检测。对关键信息基础设施、业务系统、数据库、物联网等资产进行弱口令检测和漏洞扫描。基于关键字匹配或正则匹配，识别网站 JS 代码中敏感数据。利用 Email 情报信息发现易被钓鱼利用的弱点。结合攻防情报、供应链情报等信息进行智能分析，检测易被攻击者利用的供应商高风险资产。

图 2 攻击点识别与管理

1.3 攻击面分析

基于弱点检测结果进行综合分析研判，确定是否存在社工利用风险、漏洞利用风险、供应链风险、数据泄露风险、勒索利用等风险。通过对风险统一研判，识别外部攻击面，评估一旦发生安全事件客户业务受影响范围，并提供风险收敛优先级，以便及时进行处置闭环。

1.4 风险评估及预警

一旦确定了外部攻击面上的风险，组织可以采取措施来缓解这些风险。这可能包括修复漏洞、配置安全策略、限制访问权限等。

持续监控和维护

定期监控其外部攻击面，以检测新的或变化的资产、漏洞和威胁。这种监控可以通过实时扫描、漏洞管理和威胁情报源来实现。

报告和合规

生成报告和记录，以跟踪外部攻击面的状态、风险和改进措施的执行情况。对于组织安全合规性要求和安全审计也同等重要。

2. 安全行业大模型（SecLLM）助力 EASM

利用 SecLLM 开展 EASM 外部攻击面管理是一种创新尝试，

该应用旨在更好地识别、评估和管理外部攻击面，从而提高网络安全的整体防御能力。如图 3 所示：

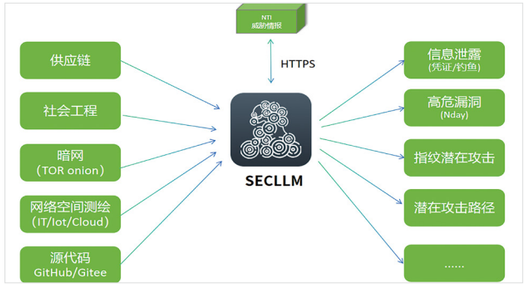


图 3 SecLLM 应用于 EASM

SecLLM 站在潜在攻击者的角度来持续不断地审视与管理组织资产和薄弱环节，包括以下三部分：

2.1 持续监控和全面收集数据

SecLLM 具备的自然语言处理能力能够有效地应用到多源数据的信息提取中，如从批量的资讯文本中提取重要安全实体和关系，同时进行自动化数据分类；能够帮助组织监控和处理多种数据，包括识别社交媒体、SSL 证书、域名信息、漏洞数据库、违规数据集、深网 / 暗网数据、代码存储库等。通过 SecLLM 可以快速识别多源数据中的关键数据，清理无效信息，仅收集和整理与组织相关的公开可见信息。

图 4 外部攻击面数据分析

2.2 SecLLM 与威胁情报分析

将 SecLLM 与威胁情报数据相结合，对外部攻击面进行威胁分析。这些情报源可能包括开源情报、商业情报、政府情报等，大模型可以分析这些信息，识别与组织相关的潜在威胁，并为每个威胁提供上下文信息。大模型可以整合来自不同威胁情报源的信息，识别新的威胁并生成实时告警，丰富威胁情报库；同时安全运营中通过与威胁情报数据对比，及时发现可能受到攻击的系统和服务，有效协助组织及时进行攻击面收敛。

2.3 外部攻击面评估

利用大模型进行数据分析和挖掘，对组织的外部攻击面进行

评估。(1) 风险排序：SecLLM 将合适的数据和技术工具结合起来，可以分析各种风险因素，包括漏洞、威胁情报、网络活动、系统配置等，然后将它们排序，以确定哪些风险对组织的安全性构成最大威胁。(2) 漏洞发现：SecLLM 分析外部暴露信息数据和漏洞数据库，识别可能存在的漏洞和已知的安全问题。它可以与漏洞扫描工具集成，帮助自动化漏洞检测。(3) 攻击路径分析：SecLLM 可以模拟攻击路径，从外部攻击者的角度分析组织的网络和系统，识别潜在的攻击入口和攻击路径，有助于安全团队理解攻击者的思维方式和行动方式。(4) EASM 评估和报告：SecLLM 可以自动生成安全风险和漏洞的报告，包括风险级别、建议的行动计划和优先级，以帮助安全团队决策和通信。

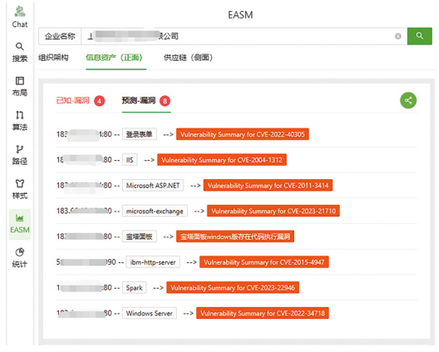


图 5 SecLLM 应用指纹攻击漏洞预测

通过上述 SecLLM 在企业安全评估 EASM 中尝试应用，可以帮助组织发现潜在的威胁，评估系统的安全性，优化安全措施，保护重要数据和资产的安全。后续利用 SecLLM 在数据处理能力、智能威胁识别、威胁情报整合以及攻击面可视化等方面的技术优势，对攻击面进行细分和分层评估，提高 EASM 评估的效率、准确性和全面性。

3. 安全行业大模型助力攻防演练更智能

安全行业大模型（SecLLM）作为安全分析的大脑，较强的数据分析能力能够很好地解决安全数据的信息识别抽取、分类以及上下文综合分析的问题；高质量的数据生成能力解决了威胁情报整合，脆弱性评估报告的产出；结合上下文分析能力可结合威胁情报、知识图谱等多源数据进行预测性分析，识别未来可能的威胁趋势。

攻防对抗是一场不断演进的博弈过程，涉及网络安全领域的攻击者与防御者之间的智力对抗。攻击者寻求发现和利用漏洞、渗透系统、窃取敏感信息或者破坏关键基础设施，而防御者则努力检测、阻止、纠正和回应这些攻击。这场博弈不仅要求防御者不断改进安全措施，还需攻击者不断寻找新的攻击方式。在这个不断升级的竞赛中，创新、智能分析和持续学习成为攻防双方的关键筹码。安全行业大模型（SecLLM）作为安全专家，可以不断转换角色并应用于攻防对抗中，能够更加灵活和高效地应对不断变化的威胁和攻击，助力解决安全运营中的大部分问题。可以在以下几个方面充分利用安全行业大模型：

3.1 威胁检测与分析

作为防御者，安全专家可以使用大模型来分析网络流量和日志数据，快速检测异常行为和潜在威胁。模型可以帮助他们识别攻击迹象、异常模式和威胁指标，从而及早发现攻击事件。

3.2 威胁情报整合

安全专家可以利用大模型整合多个威胁情报源的信息，分析新的威胁趋势，识别可能的攻击者行为，并根据情报数据改进安全策略。

3.3 漏洞管理和脆弱性评估

在防御角色下，安全专家可以使用大模型和已有工具或系统来管理漏洞和系统脆弱性评估。大模型可以帮助他们自动化漏洞扫描，评估漏洞的严重性，并提供修复建议。

3.4 攻击路径分析

作为防御者，安全专家可以利用大模型来模拟攻击路径，理解攻击者如何渗透系统，识别可能的攻击入口，并采取相应的防御措施。

3.5 自动化决策支持

大模型可以为安全专家提供自动化的决策支持，根据威胁严重性和影响程度，建议采取适当的措施，加速对攻击事件的应对。

3.6 威胁模拟与演练

安全专家可以使用大模型来模拟攻击，测试其安全防御措施的有效性，并识别弱点，这有助于改进安全策略和培训团队。

3.7 数据可视化和报告生成

大模型可以帮助安全专家将复杂的安全数据可视化，生成易于理解的报告和仪表板，提供实时的安全信息。

综合来看，大模型在安全专家的支持下可以适应多种角色，帮助他们更好地应对不同类型的安全挑战，提高攻防对抗的效率和精度。这种灵活性和自动化能力对于在不断变化的威胁环境中保护组织的网络和信息安全至关重要。

大模型与软件供应链安全结合调研与总结

绿盟科技 创新研究院 王永吉

摘要：目前大模型与软件供应链安全领域的多个方向进行了初步融合，尤其是软件供应链中的漏洞检出与大模型供应的代码安全。多个团队对大模型在漏洞检测方面与传统方法进行比较，发现大模型的检测效果非常优秀。有研究团队对其结构进行改进，使之漏洞检测能力更加优秀。此外，大模型在生成代码方面具有一定的安全问题。不过大模型生成的代码优于人工编写的代码，并且能够意识到自身漏洞代码的危害并加以纠正。有研究团队对此进行微调和纠正，使之生成更安全代码。此外，大模型还能够对软件供应链事件进行分类，但准确率一般。尽管目前处于初步尝试阶段，但已经取得不错的效果，未来有望在软件供应链安全中的逻辑漏洞检测、安全培训等方面发挥更大优势。

关键词：大模型 软件供应链安全 漏洞检测 大模型生成代码安全

1. 软件供应链安全

软件供应链安全指的是确保软件供应链中的各个环节和组件不受恶意攻击或未经授权的篡改，以保证软件交付的完整性、可信性和可靠性。软件供应链是指涉及开发、测试、集成、部署等多个环节的软件开发和交付过程，其中包括了供应商、开发者、第三方库、依赖组件、工具和用户等各种参与者。

软件供应链安全面临多种威胁和风险，其中包括以下几个方面：

恶意代码注入：黑客可以在软件开发过程中注入恶意代码，这些代码可能会在软件运行时执行恶意操作，如窃取敏感信息、破坏系统功能等。依赖关系风险：软件通常会依赖于许多第三方库和组件，而这些依赖可能存在漏洞或被滥用。如果攻击者能够操纵或替换这些依赖，就可能导致整个软件链的安全问题。开发环境恶意篡改：黑客可以通过恶意修改开发工具、框架或编译器，来操纵或损害软件的构建过程，从而在软件中插入后门或漏洞。不安全的交付渠道：软件交付过程中，如果传输渠道不安全，攻击者可能利用中间人攻击、篡改软件包等手段，在传递过程中对软件进行恶意篡改或注入恶意代码。

2. 软件供应链安全与大模型结合点

由于大模型拥有一定的检测能力、生成能力、理解能力，与软件供应链安全摩擦出新的火花。软件供应链的威胁检测拥有了新的检测手段，大模型供应的代码安全性得到了注重，对软件供应链事件分析等高复杂度任务，大模型也有部分能力进行处理。

2.1 软件供应链漏洞检测

在软件供应链中，往往需要针对引入的他人代码进行安全检测，针对已知漏洞往往使用 SCA 技术来进行识别，针对未知漏洞需要加以静态分析、动态分析等技术判断代码质量。在大模型出现之后，有学者使用大模型对代码中的漏洞进行检测，本文主要研究目前学术界使用大模型的方法以及效果，不对研究细节进行探究。大模型目前在漏洞检测方面应用效果较好，将漏洞数据投喂大模型，表现出较好的检测效果，有学者研究大模型生成的代码的安全性，或使之更可靠。

Ferrag M A 等人 [7] 创造了一种基于大型语言模型（LLMs）的创新模型架构 SecureFalcon，用于软件漏洞检测和网络安全应用。SecureFalcon 是在 FalconLLM 基础上进行微调优化训练而成的，通过区分易受攻击和非易受攻击的 C 代码样本来检测软件漏洞，具体架构如图 1 所示。研究团队构建了一个新的训练数据集 FormAI，利用生成式人工智能（AI）和形式验证的方法进行构建，以评估 SecureFalcon 的性能。研究结果显示，SecureFalcon 在软件漏洞检测方面的准确率达到了 94%，突显了其在重新定义网络安全中的软件漏洞检测方法方面的重要潜力。

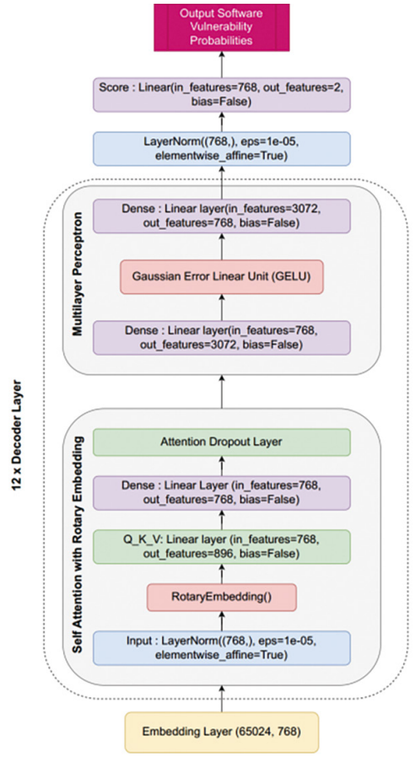


图 1 SecureFalcon 模型架构图

Bakhshandeh A 等人 [2] 提出了使用 ChatGPT 进行 Python 漏洞检测的方法，将适当的提示以及易受攻击的数据提供给 ChatGPT3.5，并将其与三种静态应用程序安全测试工具（Bandit、Semgrep 和 SonarQube）进行了比较。实验结果表明，ChatGPT 具有降低误报率和漏报率的潜力，有望用于 Python 源码的漏洞检测。这为利用自然语言处理技术进行代码安全性分析提供了一种新的思路和方法。

Omar M 等人 [10] 提出了一种新颖的基于 Transformer 的漏洞检测框架 VulDetect。现有的深度学习模型，如卷积神经网络（CNN）和长短期记忆网络（LSTM），虽然能够准确识别易受攻击的代码模式，但需要大量计算资源，导致实时部署的可行性不高。为此，Omar M 等人通过对预训练的大型语言模型（GPT）在多个易受攻击代码基准数据集上进行微调，提出了一种基于 Transformer 的漏洞检测框架 VulDetect，具体检测架构如图 2 所示。实证结果显示，该框架能够以高达 92.65% 的准确率识别易受攻击的软件代码。与两种最先进的漏洞检测技术 SyseVR 和 VulDeBERT 相比，Omar M 等人提出的技术表现更优。这一研究为基于 Transformer 的漏洞检测方法提供了新的思路，并取得了令人满意的实验结果。

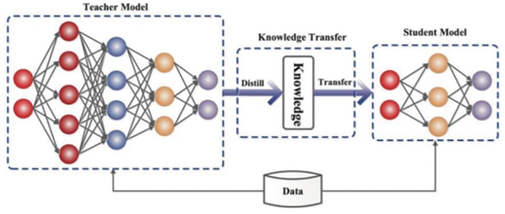


图 2 VulDetect 检测器检测过程图

Cheshkov A 等人 [5] 基于真实世界数据集，使用 CWE 漏洞的二元分类和多标签分类任务进行了评估。由于 ChatGPT 模型在编程挑战和高层次代码理解等其他基于代码的任务中表现良好，因此 Cheshkov A 等人选择了该模型进行评估。然而，Cheshkov A 等人发现 ChatGPT 模型在代码漏洞检测的二元分类和多标签分类任务中表现不如一个普通分类器。

Zhang C 等人 [18] 研究了使用 ChatGPT 进行软件漏洞检测的性能，并通过设计不同的提示信息来改进模型的性能。与之前的研究相比，Zhang C 等人充分考虑到了大型语言模型（LLM）的特点，并提供了针对漏洞检测的具体提示设计。在基本提示的基础上，通过引入结构和顺序辅助信息来改进提示设计，并利用 ChatGPT 记忆多轮对话的能力，设计了适合漏洞检测的提示。研究团队在两个漏洞数据集上进行了大量实验，证明了使用加强版的提示信息进行漏洞检测的有效性，同时，还对使用 ChatGPT 进行漏洞检测的优点和缺点进行了分析。这一研究为利用 ChatGPT 进行漏洞检测提供了新的思路和改进方法。

Chen Y 等人 [4] 制作了一种新的漏洞源代码数据集，对使用深度学习和 LLMs 等 11 种模型进行对比，研究结果如图 3 所示，由于高误报率、低 F1 得分以及难以检测复杂 CWE，深度学习在漏洞检测方面仍然不够成熟。基于深度学习模型泛化挑战仍是重要难点，增加训练数据量可能不会进一步提高深度学习模型在漏洞检测方面的性能，但可能有助于提高对未见项目的泛化能力。Chen Y 等人证明了大型语言模型（LLMs）是基于机器学习的漏洞检测的有希望的研究方向，在实验中表现优于具有代码结构特征的图神经网络（GNNs）。

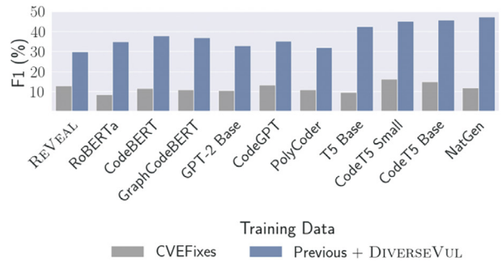


图 3 11 种模型对比结果图

Ahmad B 等人 [1] 研究了一种名为 FLAG 的新方法，旨在协助人工调试员识别和定位代码中的安全和功能缺陷。FLAG 基于生成式人工智能，特别是大型语言模型（LLMs）的词法能力，该方法输入一个代码文件，然后提取并重新生成文件中的每一行代码以进行自我比较。通过将原始代码与 LLM 生成的替代代码进行比较，可以将显著差异标记为异常，以供进一步检查，其中包括与注释的距离和 LLM 的置信度等特征也有助于这种分类，具体过程如图 4 所示。这减少了设计人员对代码的检查搜索空间。与该领域的其他自动化方法不同，FLAG 不依赖于编程语言，可以处理不完整（甚至无法编译）的代码，并且不需要创建安全属性、功能测试或规则定义。Ahmad B 等人探讨了帮助 LLMs 进行这种分类的特征，并评估了 FLAG 在已知漏洞上的性能。研究人员使用 C、Python 和 Verilog 的 121 个基准测试，每个基准测试都包含已知的安全或功能弱点。Ahmad B 等人使用 OpenAI 的 code-davinci-002 和 gpt-3.5-turbo 两种最新的 LLMs 进行实验，他们的方法也可以被其他模型使用。FLAG 能够识别出 101 个缺陷，并将源代码的搜索空间减少到 12% ～ 17%。

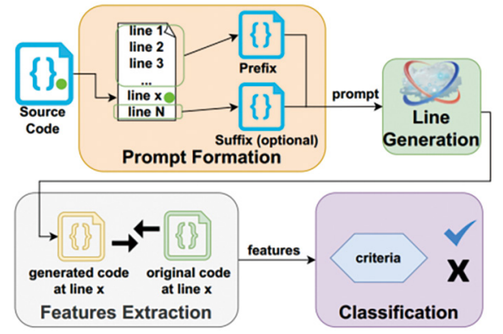


图 4 FLAG 查询代码行异常过程图

Deng Y 等人 [6] 研究了一种名为 FuzzGPT 的技术，旨在改进使用大型语言模型（LLMs）进行深度学习库模糊测试的能力。传统的技术需要人工设计生成器，并确保生成的程序在语法和语义上是有效的，而 FuzzGPT 通过利用 LLMs 的内在能力（包括微调和上下文学习）将这个过程完全自动化，同时具有普适性和适用性。LLMs 生成的程序往往遵循与它们训练语料库中的典型程序相似的模式和标记，而模糊测试则偏向于涵盖边界情况或不太可能

人工产生的异常输入。为了解决这个问题，FuzzGPT 提出了一种新的方法，利用历史的 Bug 触发程序作为参考，以引导 LLMs 合成不寻常的程序测试用例用于模糊测试，具体实现方法如图 5 所示。Deng Y 等人介绍了 FuzzGPT 在不同 LLMs 上的应用，重点关注了强大的 GPT 风格模型：Codex 和 CodeGen。此外，还展示了最近的 ChatGPT 的指导跟随能力在有效进行模糊测试时的潜力。通过在两个流行的深度学习库（PyTorch 和 TensorFlow）上进行的实验研究，FuzzGPT 表现出比之前的 TitanFuzz 更好的性能，检测到 76 个 Bug，其中 49 个被确认为以前未知的 Bug，包括 11 个高优先级的 Bug 或安全漏洞。总结起来，FuzzGPT 利用 LLMs 的能力自动生成异常输入程序用于深度学习库的模糊测试，提高了 Bug 检测的效果。它通过引导 LLMs 合成不寻常的程序，并利用历史 Bug 触发程序作为参考，提高了模糊测试的覆盖率和发现率。

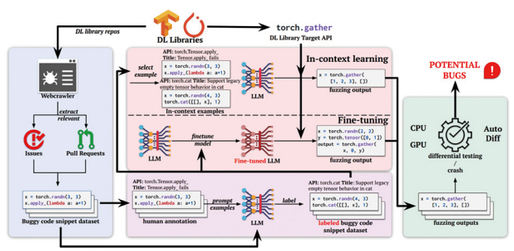


图 5 FuzzGPT 实现方法图

2.2 大模型供应代码的安全性检查

大模型能够为人们编写代码提供以下几种方式的帮助：

自动完成：大模型可以根据输入的部分代码，预测并推荐接下来可能的代码片段。这对于减少编码过程中的手动敲击和减少常见代码片段的输入时间非常有用。

错误修正：大模型可以检测到潜在的语法错误、逻辑错误或潜在的错误做法，并提供相关建议和修复策略。这可以帮助开发人员更快地发现和纠正错误，提高代码的质量和可靠性。

代码生成：大模型可以根据开发人员提供的高级指令或意图，生成相应的代码。使用这种方式，开发人员可以通过提供高级描述，而无须冗长的手动编码来实现复杂的功能或任务。

文档和注释：大模型可以帮助编写文档和注释，提供关于代码功能、参数和用法的提示和建议。这可以改善代码的可读性，并帮助其他开发人员更好地理解和使用代码。

然而大模型供应的代码也会伴随着一系列的安全问题，有学者研究大模型生成的代码质量，或如何调教大模型生成更加安全可靠的代码。

为此，Tony C 等人 [16] 提出了一个名为 LLMSecEval 的数据集，其中包含 150 个自然语言提示，可用于评估这些模型的安全性能。这些提示是针对 MITRE 的 Top 25 Common Weakness Enumeration（CWE）排名中列出的各种安全漏洞的代码片段的自然语言描述。数据集中还提供了安全实现示例，以便对比分析 LLMs 生成的代码。最后，Tony C 等人展示了如何利用 LLMSecEval 来自动评估由自然语言描述自动生成的代码片段的安全性。

Copilot 是使用大模型基于开源 GitHub 代码进行训练的语言模型，但由于代码经常存在漏洞，因此考虑到 Copilot 处理的大量非审查代码，该语言模型肯定会从易受攻击的有缺陷代码中学习。Pearce H 等人 [21] 研究通过在与高风险网络安全弱点相关的场景下提示 Copilot 生成代码，并从 MITRE 的“Top 25”常见弱点枚举（CWE）清单中选择。通过探索 Copilot 在弱点多样性、提示多样性和领域多样性等三个不同的代码生成方面的表现，共产生 89 个不同的场景，生成 1,689 个程序，最终发现大约 40% 的程序存在漏洞。

Perry N 等人 [12] 进行了第一项大规模用户研究，考察用户与 AI 代码助手在不同编程语言下解决各种安全相关任务的互动的代码安全性。总体而言，发现有 AI 助手（基于 OpenAI 的 codex-davinci-002 模型）的参与者编写的代码明显不够安全，而没有 AI 助手的参与者编写的代码更加安全。此外，有 AI 助手的参与者更容易相信他们编写的代码是安全的，相比之下没有 AI 助手的参与者则相对较少，还发现对 AI 的信任程度较低且更多地与提示语言和格式进行交互（例如重新表述、调整温度），所提供的代码中安全漏洞较少。最后，为了更好地指导未来基于 AI 的代码助手的设计，对参与者的语言和互动行为进行了深入分析，并将用户界面发布为工具，以便未来进行类似的研究。

Khoury R 等人 [9] 通过实验来探究 ChatGPT 生成的代码究竟是否安全的问题，具体地要求 ChatGPT 生成一些程序，并评估所得源代码的安全性，进一步探讨了通过适当的提示是否可以促使 ChatGPT 改善安全性，讨论了使用 AI 生成代码的伦理方面的问题。结果表明，ChatGPT 意识到潜在的漏洞，但往往生成的源代码对某些攻击不够健壮。在研究中，对 ChatGPT 从 GPT-3.5 系列的模型微调后生成的代码进行了安全性评估实验。具体而言，要求 ChatGPT 生成 5 种不同编程语言（C、C++、Python、html 和 Java）的 21 个程序，然后评估生成的程序并询问 ChatGPT 代码中是否存在任何漏洞，发现在多个情况下，ChatGPT 生成的代码远低于大多数场景下的最低安全标准。事实上，当被询问生成的代码是否安全时，ChatGPT 能够识别出不安全。然而，如果明确要求，聊天机器人在许多情况下可以提供更安全的代码版本。

Sandoval G 等人 [13] 讨论了使用大型语言模型（LLMs）作为人工智能编码助手的影响，特别是最近的研究显示 LLMs 可能会提供含有网络安全漏洞的建议。研究者进行了一项安全驱动的用户研究，通过此研究考察了学生程序员在 LLMs 的协助下编写代码时的情况。他们要求参与者在 C 语言中实现单向链接列表结构，并对完成的代码进行了功能和安全性方面的评估，使用了手动和自动方法来检查代码。结果显示，在这种低层次的 C 语言中使用指针和数组操作时，LLMs 的使用对安全影响很小，参与者编写出的代码的安全漏洞率不会比未经过 AI 协助的控制组高出 10%。研究者还发现，63% 的漏洞源于人类编写的代码，36% 的漏洞位于给出的建议中。

Storhaug A 等人 [15] 提出了一种新的漏洞约束解码方法，以减少由基于 transformer 的大型语言模型（LLM）生成的代码中

存在的漏洞数量。通过使用一个小型的标记漏洞代码数据集，对 LLM 进行微调，使其在生成代码时包含漏洞标签，充当嵌入式分类器。然后，在解码过程中，禁止模型生成这些标签，以避免生成存在漏洞的代码。该方法的评估选择了以以太坊区块链智能合约（SCs）的自动完成为案例研究，因为 SC 安全性要求严格。首先，在从 2,217,692 个 SC 中去除重复后，使用 186,397 个以太坊 SC 对具有 60 亿参数的 GPT-J 模型进行了微调，微调过程使用了 10 个 GPU，耗时超过一周。结果显示，微调后的模型可以生成具有平均 BLEU（双语评估协助下的理解）得分为 0.557 的 SCs。然而，自动完成的 SC 中的许多代码都存在漏洞。通过使用包含不同类型漏洞的 176 个 SC 中漏洞行之前的代码来自动完成代码，Storhaug A 等人发现超过 70% 的自动完成代码存在安全问题。因此，Storhaug A 等人进一步在其他 941 个包含相同类型漏洞的易受攻击 SC 上进行了微调，并应用了漏洞约束解码。微调过程只需 4 个 GPU，耗时仅一个小时，然后，再次自动完成了 176 个 SC，并发现该方法可以识别出 62% 的待生成代码存在漏洞，并避免生成其中的 67%，表明该方法可以高效地避免自动完成代码中的漏洞。

Pearce H 等人 [11] 研究了利用大型语言模型（LLMs）来修复程序中的网络安全漏洞。该团队使用了多个商用和开源的 LLMs，以及自己训练的模型，对多种合成、手工制作和真实世界的安全漏洞场景进行了测试，并检查了设计合适提示用于引导 LLMs 生成修复后的不安全代码的挑战。虽然该方法在修复方面表现出了很大的潜力，例如在执行手工制作或合成数据时，LLMs 可以共同修复 100% 的测试场景，但在评估大量历史真实世界示例代码时，其功能正确性尚存在着一些挑战。

2.3 大模型与其他软件供应链安全技术结合点

软件物料清单（SBOM）通过提供软件开发中不可或缺的组件和依赖项的详细清单，成为确保软件供应链安全的关键支柱。然而，共享 SBOM 存在大量挑战，包括潜在的数据窜改以及软件供应商在披露 SBOM 全面信息方面参差不齐。这些障碍阻碍了 SBOM 的广泛采用和使用，凸显了对更安全、更灵活的 SBOM 共享机制的需求。

Xia B 等人 [17] 针对这些挑战提出了一种新颖的解决方案，通过引入区块链支持的 SBOM 共享架构，架构细节如图 6 所示，利用可验证的凭证来允许选择性披露。这种策略不仅提高了安全性，而且提供了灵活性。此外，Xia B 等人扩大了 SBOM 的范围以涵盖人工智能系统，从而创造了人工智能物料清单（AIBOM）这一术语。这一扩展的动机是人工智能技术的快速发展以及跟踪人工智能软件和系统的谱系和组成的需求不断升级。Xia B 等人的解决方案的评估表明了所提出的 SBOM 共享机制的可行性和灵活性，为保护（AI）软件供应链提供了一种新的解决方案。

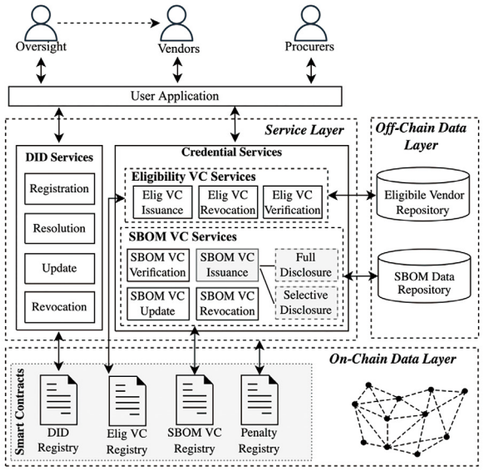


图 6 区块链应用在 SBOM 架构图

“软件供应链事故”指的是发生在软件供应链中的安全事件或漏洞。软件供应链是一个涉及多个环节的过程，包括软件的开发、测试、交付和维护等阶段。如果在这些环节中存在安全漏洞或被恶意攻击，就会导致软件供应链事故。

Singla T 等人 [14] 使用大型语言模型（LLMs）来分析历史上发生的软件供应链事故。他们使用 LLMs 来复制 Cloud Native Computing Foundation（CNCF）成员对 69 起软件供应链安全失败的手动分析过程，分析过程如图 7 所示。为了对这些故障进行分类，作者为 LLMs 开发了一些提示，包括四个维度：威胁类型、意图、性质和影响。研究结果表明，GPT-3.5 对这些维度的分类准确率平均为 68%，而 Bard 的准确率为 58%。研究结果表明，LLMs 可以有效地对软件供应链事件进行分类、描述，但尚不能取代人工分析师的角色。

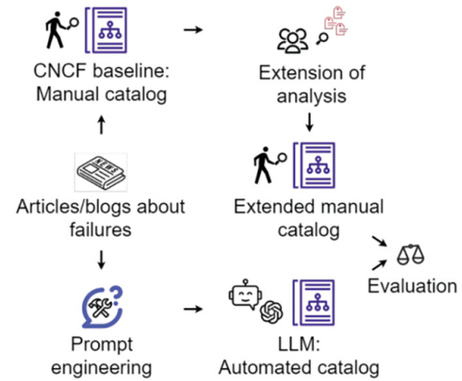


图 7 使用大型语言模型分析软件供应链事件过程图

在软件供应过程中，检测供应代码进行漏洞检测具有重大意义，静态分析工具是最常用的，并且具有固有的误报率，对开发人员的生产力提出了严峻的挑战。大型语言模型（LLM）为这些长期存在的问题提供了一个有希望的解决方案，FalconLLM 在识别复杂模式和复杂漏洞方面显示出巨大潜力。

第三方包在软件供应链中供应关系非常庞大，Chen T 等人 [3] 提出了一种名为 VulLibGen 的生成方法，旨在解决现有 SCA 漏洞报告中缺乏记录受影响库名称列表的问题。该方法利用大型语言模型（LLM）的巨大进展，通过漏洞的描述来生成与之相关的可能受影响的库名称列表，以实现高准确性。VulLibGen 还包括输入扩充技术，用于帮助识别训练过程中未出现的零样本受影响库，以及后处理技术，用于处理 VulLibGen 的错误识别。Chen T 等人使用三种最新的漏洞识别方法对开源数据集 VulLib 进行了评估，结果显示 VulLibGen 的平均 F1 得分为 0.626，而其他方法仅为 0.561。通过后处理技术，VulLibGen 的 F1@1 平均改进率为 9.3%。

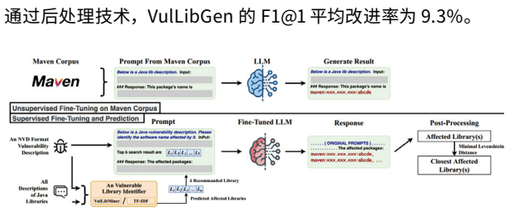


图 8 使用大模型分析供应链漏洞影响的组件列表过程图

Jin M 等人 [8] 针对软件开发生命周期中缺陷的引入、识别和解决等问题，提出了一种基于 Transformer 的程序修复框架 InferFix。该方法结合 Retriever-Transformer 编码器模型和 Generator- 大型语言模型，通过增加语义类型注释和从外部检索的语义相似修复来细化程序修复过程，有错误的 commit 由 Infer 静态分析器检测到，该分析器用于制作一个提示，其中包含错误类型注释、位置信息、相关语法层次结构（eWASH）在大模型的支持下修复严重安全和性能缺陷，修复过程如图 9 所示。Jin M 等人构建了 InferredBugs 作为测试数据集，经过实验证明，InferFix 比强大的 LLM 基线方法表现更好，C# 生成修复的 Top-1 准确率为 65.6%，Java 为 76.8%。同时，Jin M 等人还讨论了 InferFix 在 Microsoft 的部署情况，将其与 Infer 整合，提供端到端的解决方案以及自动化软件开发流程。

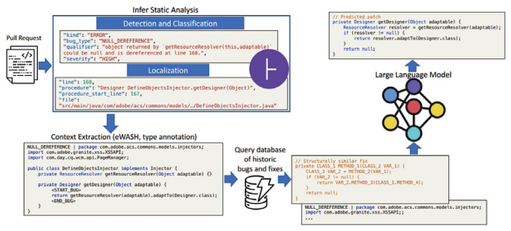


图 9 使用大模型解决软件开发工作流程缺陷自动化过程图

3. 总结

在漏洞检测方面，多个团队对大模型以及普通静态分析检测方法、最新深度学习检测方法进行比较，绝大部分团队的实验结果中对大模型检测效果非常优秀，甚至高达 92.65% 的准确率，但有实验结果表明基于 ChatGPT 和 GPT-3 的大模型在分类任务上表现不如一个普通分类器。最新部分团队，对大模型的改进结构进行漏洞检测优化。有研究团队甚至将大模型使用在 FUZZ 测试工具优化方面，使用历史的 Bug 触发程序作为参考，引导变异种子的生成，将源代码的搜索空间减少到 12% ～ 17%。

大模型在生成代码方面，在容易触发漏洞场景下，2021 年，所生成的代码 40% 含有漏洞；在 2022 年，有人实验论证生成的代码远低于大多数场景下的最低安全标准，而有人研究结果为 63% 的漏洞源于人类编写的代码，36% 的漏洞位于给出的代码中，认为生成的代码优于人工代码。很多试验结果表明，虽然给出很多不安全的代码，但是在明确要求下，大模型能够写安全的代码；大模型能够认识到自己的漏洞代码有危害并加以纠正。

因此有人对大模型在写代码方面进行纠正微调，使用漏洞代码生成负标签，在大模型解码过程中，不允许生成含有这些标签的代码；有团队添加提示词，设计、引导大模型对自己生成的漏洞代码进行修改，并达到 100% 修复的效果。

针对软件供应链安全其他方面，大模型的供应链也需要保护，例如：维护 AIBoms；大模型能够对软件供应链事件进行分类（威胁类型、意图、性质和影响），但仍然不能帮助人们对事件进行分析；大模型在软件开发生命周期中能够对缺陷的引入进行识别和解决，但是准确率一般。大模型还能够针对使用的第三方软件进行缺陷检测，但效果只比经典静态分析方法好一点点。

将大模型应用于软件供应链安全领域目前处于初步尝试阶段，但经过测试，总体已取得不错的效果，假以时日进行调整优化，大模型能发挥出超长的水平。笔者认为，在未来大模型能够在软件供应链逻辑漏洞方面发挥出更大的优势，例如在软件集成过程对于他人 API 误用造成的逻辑漏洞；将模型进行调用图生成、理解等定向训练，降低静态分析固有的误报率；或扮演安全培训工程师的角色，定向生成特殊场景的漏洞代码及相关文档，完成对开发人员的培训。

参考文献

[1] Ahmad B, Tan B, Karri R, et al. FLAG: Finding Line Anomalies (in code) with Generative AI[J]. arXiv preprint arXiv:2306.12643, 2023.

[2] Bakhshandeh A, Keramatfar A, Norouzi A, et al. Using ChatGPT as a Static Application Security Testing Tool[J]. arXiv preprint arXiv:2308.14434, 2023.

[3] Chen T, Li L, Zhu L, et al. VulLibGen: Identifying Vulnerable Third-Party Libraries via Generative Pre-Trained Model[J]. arXiv preprint arXiv:2308.04662, 2023.

[4] Chen Y, Ding Z, Chen X, et al. DiverseVul: A New Vulnerable Source Code Dataset for Deep Learning Based Vulnerability Detection[J]. arXiv preprint arXiv:2304.00409, 2023.

[5] Cheshkov A, Zadorozhny P, Levichev R. Evaluation of ChatGPT Model for Vulnerability Detection[J]. arXiv preprint arXiv:2304.07232, 2023.

[6] Deng Y, Xia C S, Yang C, et al. Large language models

are edge-case fuzzers: Testing deep learning libraries via fuzzgpt[J]. arXiv preprint arXiv:2304.02014, 2023.

[7] Ferrag M A, Battah A, Tihanyi N, et al. SecureFalcon: The Next Cyber Reasoning System for Cyber Security[J]. arXiv preprint arXiv:2307.06616, 2023.

[8] Jin M, Shahriar S, Tufano M, et al. Inferfix: End-to-end program repair with llms[J]. arXiv preprint arXiv:2303.07263, 2023.

[9] Khoury R, Avila A R, Brunelle J, et al. How Secure is Code Generated by ChatGPT?[J]. arXiv preprint arXiv:2304.09655, 2023.

[10] Omar M. Detecting software vulnerabilities using Language Models[J]. arXiv preprint arXiv:2302.11773, 2023.

[11] Pearce H, Tan B, Ahmad B, et al. Examining zero-shot vulnerability repair with large language models[C]//2023 IEEE Symposium on Security and Privacy (SP). IEEE, 2023: 2339-2356.

[12] Perry N, Srivastava M, Kumar D, et al. Do users write more insecure code with AI assistants?[J]. arXiv preprint arXiv:2211.03622, 2022.

[13] Sandoval G, Pearce H, Nys T, et al. Lost at c: A user study on the security implications of large language model code assistants[J]. arXiv preprint arXiv:2208.09727, 2023.

[14] Singla T, Anandayuvaraj D, Kalu K G, et al. An Empirical Study on Using Large Language Models to Analyze Software Supply Chain Security Failures[J]. arXiv preprint arXiv:2308.04898, 2023.

[15] Storhaug A, Li J, Hu T. Efficient Avoidance of Vulnerabilities in Auto-completed Smart Contract Code Using Vulnerability-constrained Decoding[J]. arXiv preprint arXiv:2309.09826, 2023.

[16] Tony C, Mutas M, Ferreyra N E D, et al. LLMSecEval: A Dataset of Natural Language Prompts for Security Evaluations[J]. arXiv preprint arXiv:2303.09384, 2023.

[17] Xia B, Zhang D, Liu Y, et al. Trust in Software Supply Chains: Blockchain-Enabled SBOM and the AIBOM Future[J]. arXiv preprint arXiv:2307.02088, 2023.

[18] Zhang C, Liu H, Zeng J, et al. Prompt-Enhanced Software Vulnerability Detection Using ChatGPT[J]. arXiv preprint arXiv:2308.12697, 2023.

车联网移动应用安全攻守道

绿盟科技 创新研究院 李智科

摘要：移动应用在助力车联网发展成熟的同时，也带来了新的安全挑战，本文立足攻防，洞见车联网移动应用安全的攻守之道。

关键词：车联网 移动应用 逆向分析 恶意代理

1. 引言

车联网实现了车与车、车与人、车与路、车与服务平台之间的网络连接，提升了交通服务的智能化水平，使得汽车不再只是孤立的交通工具。而移动应用（APP）作为智能汽车的标配，承载着车与人之间的连接，各品牌汽车手机 / 车机 APP 不仅可以提供商城、维修、保养等基础服务，还能够实现汽车的远程启动、车门解锁、空调开关以及自动驾驶等功能，为用户提供安全、舒适、智能、高效的驾驶感受与用车体验，显著提高车辆整体的智能驾驶水平。

但移动应用在丰富汽车功能、提升用户体验的同时也扩展了网络攻击者的攻击面，由手机 / 车机 APP 引发的汽车网络安全事件屡见不鲜。根据 Upstream 发布的《2023 年全球汽车行业网络安全报告》显示 [1]，过去五年中，全球汽车行业因为网络攻击造成的损失高达 5050 亿美元，而在所有汽车网络安全事件中，由远程攻击行为引发的安全事件占比超过了 70%。其中，与汽车 APP 相关的车联网安全事件排在第六位，汽车网络安全事件攻击面分布如图 1 所示。

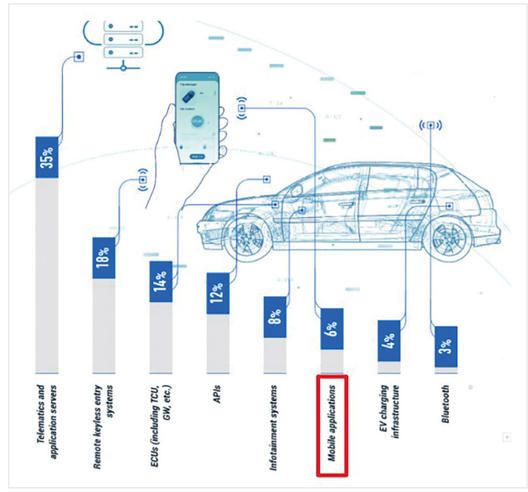


图 1 汽车网络安全事件攻击面分布

本文从传统移动应用安全出发，站在攻击者视角对手机 / 车机 APP 展开研究分析，通过剖析攻击手段来向读者阐明车联网移动应用面临的安全威胁和挑战，并且在文章最后，我们将给出相应防护措施。

2. 传统应用 VS 车联网应用

移动互联网的快速发展，为移动应用生态提供了巨大的发展空间，凭借着智能便携、互联互通的特性，各类 APP 数量呈爆发式增长，推动移动端用户数快速增加，在产生巨大经济效益的同时也带来了诸多安全隐患。移动应用安全风险不容忽视，本章将对比介绍传统移动应用安全与车联网移动应用安全。

2.1 传统移动应用安全

移动应用顾名思义是指可以在移动设备上运行的应用程序，这些移动设备通常包括智能手机、平板电脑以及其他便携式设备。根据《全国移动 App 风险监测评估报告》数据显示 [2]，在对移动应用大数据平台提供的 338 万款 Android 移动 App 进行监测分析后发现，其中 70% 以上的 App 存在高危漏洞，容易遭受反编译、二次打包、恶意代码植入等攻击；34.17% 的 App 嵌入了第三方工具类 SDK，而第三方 SDK 通常是造成用户个人信息在网上“裸奔”的罪魁祸首；若在百度搜索中输入 App 破解等关键字，相关检索结果高达 50300000 条，检索结果如图 2 所示。由此可见，移动 App 在为用户带来数字化、智能化体验的同时，亦隐藏着巨大的网络安全风险，这些风险不仅会损害到用户利益，也会对 App 提供者的数据平台造成安全威胁。

图 2 App 破解检索结果

2.2 车联网移动应用安全

在车联网环境下，除传统移动设备（手机）外，应用程序还运行在汽车系统（车机）中，为用户提供位置、导航、媒体、天气、资讯、车辆诊断、车辆控制等个性化服务，以提升汽车的智能化水平。但同手机 App 一样，车机 App 也面临着反编译、动态调试、进程注入、密码爆破、ROOT 运行环境等一系列安全风险，而且车机 App 通常会收集车主的隐私信息，包括姓名、联系方式、家庭住址、行车轨迹等，如果这些信息未得到妥善保护，极易导致用户隐私泄露，进而引发盗窃、诈骗等事件。并且相较于常规移动应用程序，汽车 App 往往具备远程控制车辆的功能，如远程启动、解锁、导航等，一旦攻击者利用 App 漏洞获得汽车操控权，便会直接对车主人身安全构成威胁。

3 车联网应用安全威胁

手机 / 车机 App 作为用户与汽车交互的主要入口，攻击者可通过逆向分析、动态调试、恶意代理等手段从该攻击面入侵汽车、破解应用、篡改程序、窃取数据，接下来我们将通过三种攻击技术来揭示车联网应用面临的安全威胁。

3.1 应用逆向破解

信息收集往往是攻击者发起攻击的第一步，通过对市面上主流车企的 50 款移动端 App 进行分析(App 版本更新至 2023 年 8 月)，我们发现约有 1/3（17 款）的 App 并未采取软件加固措施，攻击者可直接通过各类反编译工具，如 Jadx、dex2jar、apktool，将 Android 应用程序（APK、DEX、AAR）中的 Dalvik 字节码转换为 Java 类文件，快速解析 Android 应用程序源代码进行分析并寻找可利用漏洞。而在其余采取了安全加固措施的汽车 App 中，有 16 款 App 在启动时未执行环境校验，因此可以利用各类 FART 脱壳机 [3] 通过 Dump 内存的方式来获得类列表和 DEX 文件，再辅之主动调用技术，便可轻松实现指令抽取，完成对应用的脱壳操作，以支持攻击者进一步的逆向分析。车企手机端 App 加固统计结果如图 3 所示。

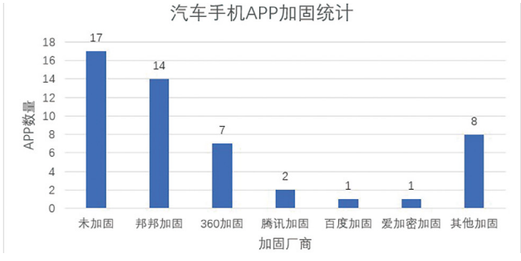


图 3 车企手机端 App 加固统计

通过收集到的信息不难发现，相当一部分汽车 App 并未采取混淆或加固措施。我们随机对某车企未加固 App 进行反编译分析，通过简单的信息检索，就可从中获取大量敏感信息，图 4 为某车企移动端 App 泄露的敏感服务信息（MQTT 服务），由此可见，移动应用极易成为企业泄露敏感信息的门户。

```
1  package [redacted];
2
3  /* loaded from: classes3.dex */
4  public class MqttConstant {
5      public static final String MQTT_BROKER = "t[redacted]";
6      public static final String MQTT_ENVTYPE = "1";
7      public static final String MQTT_PASSWORD = "d[redacted]";
8      public static final String MQTT_SDK_PASSWORD = "[redacted]
9      public static final String MQTT_SDK_PCODE = "[redacted]
10     public static final String MQTT_SDK_USERNAME = "[redacted]";
11     public static final String MQTT_USERNAME = "
12     public static final int QOS_LEVEL_0 = 0;
13     public static final int QOS_LEVEL_1 = 1;
14     public static final int QOS_LEVEL_2 = 2;
15 }
```

图 4 汽车手机 App 泄露敏感服务信息

3.2 函数劫持调用

攻击者在利用逆向手段获得汽车 App 源代码后，便可完整分析出 App 的运行逻辑、通信协议、业务接口以及功能实现，此时再结合程序漏洞发起攻击，将会给用户造成极大的安全危害。通常情况下，汽车 App 大量依赖第三方 API（Application Programming Interface）来实现其功能，如位置服务 API、支付 API 等，如果这些 API 被暴露出来，攻击者便可通过攻击 API 来获取敏感数据或者利用 API 漏洞进行其他恶意活动。

此外，对手机 / 车机 App 使用基于动态二进制插桩技术（DBI）的代码注入工具 Frida[4]，通过其功能强大的 API（JavaScript API、C API、Swift API、Go API），攻击者可以轻松编写脚本来

Hook 应用程序中的目标函数，并将恶意代码注入其中，对系统或进程中的各消息事件进行拦截篡改，从而执行恶意操作。图 5 中遭到破解的汽车车机空调 App，其功能函数可被攻击者任意劫持调用，由此可见，Android 系统开源的特性使其应用极易成为黑客的攻击目标。

图 5 汽车车机空调 App 遭遇非法劫持

3.3 恶意代理环境

移动代理通常是指在通信网络中充当中间人的实体，负责转发用户请求至目标服务器，一般用于网络优化、安全检查、流量管理等目的，可以为用户提供更加便捷、可靠的网络连接。而运行在不安全网络环境中的手机 / 车机 App，所有通信数据都处于“裸奔”状态，攻击者利用恶意代理不仅可以截获窃取用户敏感信息，还能够篡改请求或伪造服务器响应，欺骗用户进行恶意操作，严重扰乱用户与目标服务器间的正常通信流程。我们以 Charles 工具为例进行演示 [5]，攻击者利用移动设备系统漏洞，安装证书并设置 Charles 为汽车的网络访问代理服务器，迫使所有用户网络访问请求都必须通过该代理，进而实现对应用程序与服务器之间通信数据包的监控拦截，对于使用 TLS/SSL 协议加密后的通信流量，配合 Charles 证书即可实现对加密数据的解密，其详细工作流程如图 6 所示。由此可见，安全的网络环境对于加密数据传输至关重要。

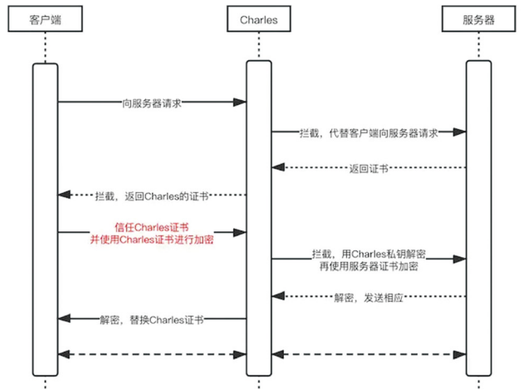


图 6 Charles 代理工作流程

4. 车联网应用安全防护

在前一章节中，我们通过脱壳、逆向、劫持、恶意代理等攻击手段展示了车联网移动应用面临的安全威胁与挑战，本章节我们将以车联网应用安全风险管控为核心目标，向大家介绍如何构建具备检测评估、安全加固以及持续监测能力的车联网应用安全防护体系。

4.1 安全检测评估

安全测试和隐私合规评估不仅可以帮助车企更好地把控自研 App 的代码安全，还能加强对第三方供应商提供 App 的质量监管，通过代码审计、漏洞扫描、渗透测试等一系列技术手段，再辅之以对应的安全意识培训可以在开发阶段有效提升车联网应用的安全性，预防可能存在的安全风险。

4.2 安全加固防护

为了解决移动应用普遍面临的破解、篡改、盗版、调试、数据窃取等各类安全风险，对已经设计开发完成的 App 进行安全加固和重点功能模块保护，使其具备防二次打包、防反编译、防 Hook、防 Dump、防注入、反调试的安全防护能力，可以有效保护移动应用的代码安全、文件安全、数据安全、通信安全以及业务系统安全，显著提高手机 / 车机 App 的抗攻击能力，APK 文件的常见安全加固流程如图 7 所示。

图 7 APK 安全加固

4.3 持续运营监测

对于移动设备中运行的车联网应用来说，持续的安全监控和完善的安全运营机制亦是不可或缺的。通过对用户手机 / 车机 App 提供风险行为、攻击行为以及其他异常行为的安全监测和应急响应服务，可以及时发现并消除威胁隐患，切实保障广大用户 / 车主的合法权益。

5. 总结

在逐渐开放的车联网生态中，暴露的风险面和大量的漏洞往往会给整个车联网服务造成难以估量的安全危害，移动应用在为智能汽车产业发展注入活力的同时，也引入了新的安全挑战。本篇文章立足攻防，以移动应用为切入点，详细介绍了车联网应用面临的安全威胁以及相应防护体系的构建思路。

类似于 App 加固与脱壳之间的持续博弈，移动应用安全作为一个长期且将持续存在的挑战，车企应该给予足够的重视，不断提升安全技术手段来实现防逆向、防篡改、防调试和防窃取的安全目标，对自身手机 / 车机 App 的业务场景及运行环境建立全方位的安全防护。

参考文献

[1] 2023 年全球汽车行业网络安全报告，https://www.tripwire.com/state-of-security/global-automotive-cybersecurity-report.

[2] 全国移动 App 风险监测评估报告，https://www.anquanke.com/post/id/248544.

[3] https://github.com/hanbinglengyue/FART.

[4] https://frida.re/docs/home/.

[5] https://www.charlesproxy.com/.

2024年网络安全趋势简析

绿盟科技 总工办 王强

摘要：Gartner® 每年 10 月左右发布次年未来战略趋势，次年 3 月左右发布和网络安全相关的趋势。我们通过将近 3 年的趋势文章进行分组对比分析，发现除了众人皆知的 AI 外，数据模块化、身份优先安全、行业云平台也会成为未来主流趋势。

关键词：Gartner® 技术趋势 安全

2023 年 10 月 16 日，Gartner® 在官网发布了 Gartner Identifies the Top 10 Strategic Technology Trends for 2024 一篇推文，介绍了分析师在奥兰多 IT Symposium/Xpo 2023 峰会上发布的 2024 年的十大战略技术趋势。我们汇总下最近 3 年的技术趋势做个整理，详见表 1。

表 1：Top 战略技术趋势

2022年	2023年	2024年
Generative AI 生成式AI	Digital Immune System 数字免疫系统	Platform Engineering 平台工程
Autonomic Systems 自治系统技术	Applied Observability 应用可观察性	AI-Augmented Development 人工智能增强开发
Total Experience 整体经验	AI Trust, Risk and Security Management 人工智能信任、风险和安全管理	AI Trust, Risk and Security Management 人工智能信任、风险和安全管理
Distributed Enterprise 分布式企业	Industry Cloud Platforms 行业云平台	Continuous Threat Exposure Management 持续威胁暴露管理
AI Engineering 人工智能工程	Platform Engineering 平台工程	Industry Cloud Platforms 行业云平台
Hyper automation 超自动化	Wireless Value Realization 无线价值实现	Intelligent Applications 智能应用程序
Decision Intelligence 决策智能	Superapps 超级应用程序	Sustainable Technology 可持续技术
Composable Applications 可组合应用程序	Adaptive AI 自适应AI	Machine Customers 机器客户
Cloud-Native Platforms 云原生平台	Metaverse 元宇宙	Augmented Connected Workforce 增强的互联员工队伍
Privacy-Enhancing Computation 隐私增强计算		Democratized Generative AI 民主化的生成式AI
Cybersecurity Mesh 网络安全网格		
Data Fabric 数据结构		

我们把 3 年的趋势做个分组归类，可以发现：3 年的整体体趋势类似，共性趋势很多；三年发展上趋势变化缓慢，逐渐递进。下面逐一描述。

1. 与 AI 相关趋势关键词：生成式 AI，Autonomic Systems 自治系统技术、AI Engineering、人工智能工程 Hyper automation、超自动化 Decision Intelligence 决策智能。AI Trust, Risk and Security Management 人工智能信任、风险和安全管理、Adaptive AI 自适应 AI、AI-Augmented Development 人工智能增强开发、Intelligent Applications 智能应用程序、Democratized Generative AI 民主化的生成式 AI.Digital Immune System 数字免疫系统。

在 2021 年发布的 2022 技术趋势中就提及到生成式 AI，只不过那个时候还没有 ChatGPT，ChatGPT 从 2023 年年初开始爆发，AI 相关话题成为讨论最多的一年，各大媒体机构高校研究院等密集发表相关洞察成果；而事物都具有两面性，新的技术发展带来便利的同时必然随之带来风险，AI 的发展涉及的安全问题也成为新的趋势。

2. 与分布式、模块化、可组装相关趋势关键词：Distributed Enterprise 分布式企业、Composable Applications 可组合应用程序、Cybersecurity Mesh 网络安全网格、Data Fabric 数据结构、Digital Immune System 数字免疫系统。

随着远程和混合工作模式的兴起，传统的以办公室为中心的组织正在演变为由地理位置分散的员工组成的分布式企业。

在不断变化的业务环境中，对业务适应性的需求将组织引导到支持快速、安全和高效的应用程序更改的技术架构。可组合应用程序架构增强了这种适应性，而那些采用可组合方法的应用程序在新功能实现速度上将比竞争对手快 80%。

网络安全网格（架构）Gartner 的描述是“传统的安全架构方法是为上一代计算而设计的，在上一代计算中，我们几乎可以对所有内容进行物理控制。然而，现在我们的数字资产广泛分布在许多地点和许多云中，因此我们需要一种新的方法来实施分布式控制。典型的安全方法建立在孤岛中运行的专用单点产品之上，以被动和专业的方式保护资产，这会增加成本，并在覆盖范围和可见性方面留下相当大的差距。这不适合大多数现代企业的快速、分布式特性。保护现代企业需要一种新的方法，将安全视为一个生态系统，而不是孤立的解决方案的集合。而网络安全网格架构（CSMA）是一个由工具和控制组成的协作生态系统，用于保护现代分布式企业。它建立在集成可组合的分布式安全工具的策略之上，通过集中数据和控制平面来实现工具之间更有效的协作。结果包括增强的检测功能、更高效的响应、一致的策略、态势和行动手册管理，以及更具适应性和精细的访问控制，所有这些都可以提高安全性。”那么，最小单位已经从传统意义上企业内外环境以防火墙为边界，逐渐打散，以每个数据集作为最小单位。

数据结构是为解决数据的量或者维度的增加，及现有数据孤岛的问题，通过一个跨平台，将已有的数据弹性集成，以满足不同的业务需求。这种强调灵活性、可扩展性。同时，也能减缓因为人才短缺导致的业务效率降低的问题。

数字免疫系统结合了可观察性、AI 增强测试、混沌工程、自修复、站点可靠性工程和软件供应链安全等实践和技术，以提高产品、服务和系统的弹性，同时降低业务风险。强大的数字免疫系统可以让应用程序更富弹性，能够快速从故障中恢复，从而保护应用和服务免受异常影响，例如软件故障或安全问题等。在关键应用和服务遭受严重损害或完全停止工作时，数字免疫系统降低业务连续性风险。企业在确保弹性运营环境、加速数字交付和可靠的用户体验方面面临前所未有的挑战，他们希望能够快速响应市场变化和迅速创新。用户所期望的不仅仅是健全的功能，他们更想要的是高性能、交易和数据的安全以及令人满意的交互。那么，相当于让产品带有原生的安全性、适应性、自我诊断修复能力。特别是在业务中断风险情况下，有了新的缓和能力。

3. 与平台工程相关趋势关键词：平台工程 Platform Engineering（出现 2 次）。

互联网的时代，使得软件开发、软件工程变得更加普及，涉及敏捷迭代、DevOps 等新的开发交付模式也有这越来越多的接受度。Gartner 对于平台工程的描述是“是构建和运营自助服务内部开发平台的学科。每个平台都是一个层，由专门的产品团队创建和维护，

旨在通过与工具和流程交互来支持其用户的需求。平台工程的目标是优化生产力、用户体验并加速业务价值的交付。基本上，产品开发人员、测试人员、运维人员完全在一个大平台上实现了协作，简化了因为各自工具独立而导致的信息、工作流、协作的壁垒，大大提高了交付的频率和效率。”

4. 与行业云平台相关趋势关键词 :Cloud-Native Platforms 云原生平台、Industry Cloud Platforms 行业云平台（出现 2 次）。

这个连续 3 年都完整的体现出来。过去理解的行业云平台大多指的是 SaaS 或者 PaaS 单一服务的行业属性，而 Gartner 所描述的行业云平台是“将底层 SaaS、PaaS 和 IaaS 服务组合到具有可组合功能的完整产品中，实现与行业相关的业务成果。”是 3 个层次的融合。这个属性我个人认为具有中国特色，并且逐渐壮大。国外几朵公有云的垄断使得客户有较少的选择及意愿去重新搭建新的云。而在国内，法律体系的不同、大家对数据安全的关注以及央国企与腾讯阿里等并行竞争的情况下，健康云、金融云、政务云等具有强行业属性与特色的云共同发展。而我认为这些云建设的背景大多与 Gartner 描述的 3 个层次的融合具有更好的契合度。

一个趋势的诞生到爆发变热在 Hype Cycle 中大约需要 3 年左右的时间，这在表 2 也能看出来，一个趋势的持续火爆是会连续出现的。而以当前来看我们好像在走 2022 年的趋势。那么，我们通过推理也可以自行预测出明年什么可能会是热点。

2023 年 3 月，Gartner 在官网发布 Top Cybersecurity Trends for 2023 推文，我们用同样的方法把 Gartner 最近 3 年针对网络安全方面的趋势汇总归类，详见表 2：

表 2：Top 安全趋势

2021年	2022年	2023年
Cybersecurity Mesh	Attack Surface Expansion	Threat Exposure Management
网格安全网格	攻击面扩展	威胁暴露管理
Identity-First Security	Identity Threat Detection and Response	Identity Fabric Immunity
身份优先安全	身份威胁检测和响应	身份结构免疫
Security Support for Remote Work is Here to Stay	Digital Supply Chain Risk	Cybersecurity Validation
远程工作的安全支持将继续存在	数字供应链风险	网络安全验证
Cyber-Savvy Board of Directors	Vendor Consolidation	Cybersecurity Platform Consolidation
精通网络的董事会	供应商合并	网络安全平台整合
Security Vendor Consolidation	Cybersecurity Mesh	Security Operating Model Transformation
安全供应商整合	网络安全网格	安全操作模式转换
Privacy-Enhancing Computation	Distributing Decisions	Composable Security
隐私增强计算	分发决策	可组合安全
Breach and Attack Simulation	Beyond Awareness	Human-Centric Security Design
入侵和攻击模拟	超越意识	以人为本的安全设计
Managing Machine Identities		Enhancing People Management
管理机器标识		加强人员管理
		Increasing Board Oversight
		加强董事会监督

再次将与安全趋势里面的关键词做个简单分组归类，有共性趋势的大致分为 3 组。

1. 与分布式、模块化、可组装相关趋势关键词：Cybersecurity Mesh 网络安全网格（出现 2 次）、Composable Security

可组合安全：该关键词在上文战略技术趋势中有提及。不再赘述。

2. 与身份（Identity）相关趋势关键词 :Identity-First Security 身份优先安全、Managing Machine Identities 管理机器标识、Identity Threat Detection and Response 身份威胁检测和响应、Identity Fabric Immunity 身份结构免疫。

以身份（Identity）为主的安全趋势变的尤为重要，特别是在刚刚提到的分布式的、去中心化的、模块化的发展下，过去以往的以边界安全的场景逐渐向以最小单位为数据为边界，那么第一步就

是识别数据使用相关的身份信息，好比在银行柜台办业务之前，出示身份证成为办业务的首要环节。而在安全攻击事件发生时，首要任务也是要获得合法身份信息、进行提权。随着量子计算等新技术的发展，和身份相关的发展不再局限于验证，而是由被动的使用变为主动的检测和响应。可见，和身份相关的产品方案（如 IAM、PAM、零信任等）会逐渐成为行业新热点。而 2023 年提出的身份结构免疫，更是在配置之初就以安全目的做了相关的加强，更像个原生状态下的安全能力。如下 4 个和身份相关的趋势点：

- 身份优先安全：多年来，任何用户、任何时间、任何地点的访问愿景（通常称为“身份作为新的安全边界”）是一种理想。由于技术和文化的转变，加上 COVID-19 期间现在大多数远程劳动力，它现在已成为现实。身份优先的安全性将身份置于安全设计的中心，并要求从传统的 LAN 边缘设计思维中做出重大转变。
- 身份威胁检测与响应：狡猾的威胁行为者正在积极针对身份和访问管理 （IAM） 基础设施，而凭据滥用现在是主要的攻击媒介。Gartner 引入了术语“身份威胁检测和响应（ITDR）”，用于描述用于保护身份系统的工具和最佳实践的集合。

“组织已经花费了相当大的精力来改进 IAM 功能，但其中大部分都集中在改进用户身份验证的技术上，这实际上增加了网络安全基础设施基础部分的攻击面，”Firstbrook 说，“ITDR 工具可以帮助保护身份系统，检测它们何时受到损害并实现有效的补救措施。”

- 身份结构免疫：脆弱的身份基础结构是由身份结构中的不完整、配置错误或易受攻击的元素引起的。到 2027 年，身份结构免疫原则将阻止 85% 的新攻击，从而将违规的财务影响减少 80%。

Addiscott 表示：“身份结构免疫不仅通过身份威胁和检测响应（ITDR）保护结构中的现有和新 IAM 组件，而且还通过完成和正确配置它来加强它。”

- 管理计算机标识：机器身份管理旨在建立和管理对与其他实体（如设备、应用程序、云服务或网关）交互的机器身份的信任。现在组织中存在的非人类实体数量越来越多，这意味着管理机器身份已成为安全策略的重要组成部分。

3. 与供应商整合相关趋势关键词：Security Vendor Consolidation 安全供应商整合、Vendor Consolidation 供应商合并、Cybersecurity Platform Consolidation 网络安全平台整合。

这个整合涉及 2 个层面，或者是同一家公司内部不同产品方案侧的合并，或者是涉及为了获得一个综合的方案牵扯到的投资并购整合。这种方案如 XDR，如 SASE 等。当然，整合背后的驱动力还因为安全分支过多过细，而涉及的安全能力的联动发展需要驱动跨方案跨产品的协作协同。特别是在俄乌战争、巴以冲突的背景下，网络战变的频繁多样，及时发现快速响应和阻断变的尤为重要。而对于最终用户来说，同时和多个厂商交易也是费力费神的事儿，牵扯到方案联动的情况下不仅消耗大量的精力钱财，在投入运营后能否解决真的问题，或面临事件后责任划分的问题也是模糊的，容易扯皮的。

总结一下针对整体战略趋势和安全趋势背后的原因，有如下几点：

1. 在疫情的背景下，远程办公、混合办公成为趋势，而对应的，

公司内部的业务系统需要支持灵活办公的需求。分布式、模块化的发展方向得到促进与加强。疫情也促进了企业应用和数据的逐渐上云，不管是私有云还是公有云，抑或是混合云，上云的步伐前进了一步，涉及相关的发展、敏捷、DevOps、协作平台、行业云平台成为新的趋势。数据的流转变的自由起来，传统边界变得不清晰了，数据需要自带身份，更需要主动检测身份。新的形态尚未完全熟悉，已经存在了许多需要做的事情，需要修补的漏洞，需要完善的机制，这些尚未解决的事情都是潜在的风险，潜在的暴露面。只要黑客比你专业，轻松拿捏你的弱点。

2. 国内安全公司上千家，安全类别复杂多样，每次看到全景图，密密麻麻的公司 logo 拥挤在一个小框框内，感觉到拥挤，感觉到压力，也感觉到竞争，这个不仅给客户带来选择困难，也给厂商带来迷茫，这么多的行业从业者，能否坚持到最后，能否能收获一杯羹？因此，厂商的整合，也代表者方案的整合，化繁为简，显而易见，这对于大公司来说是优势。

3. 世界区域性的战争也促进了网络战的发生频率，如何保证业务连续性，安全重要，韧性更重要。如果安全太复杂，在安全能力较为薄弱的情况下，关机重启是简单，但仍然不能解决连续性本质问题，加强安全能力建设，提高安全意识，仍然是当前需要重点投入的，虽然，当前看不到利益和效果，但看不到就是获得，只是无感罢了。

4. 科技变化迅速，人才永远跟不上科技的发展，AI 能帮一些忙，虽然是重复性的低级的替代，但也解决了很大一部分问题。从历史的发展来看，变革替代总是慢慢的、小步的、一点点的，AI 的进步就像婴儿成长为小学生、中学生，至少有了一定的学习能力和判断能力，只不过三观仍然需要修正，而三观，我的理解，就是告诉他道德底线在哪儿，红线在哪儿，法律在哪儿，这就是 AI 相关的风险信任管理。一旦这些逐渐获得了，那就是大学毕业了。

参考来源

[1]Gartner Press Release, Gartner Identifies the Top 10 Strategic Technology Trends for 2024, October 16, 2023 (https://www.gartner.com/en/newsroom/press-releases/2023-10-16-gartner-identifies-the-top-10-strategic-technology-trends-for-2024)

[2]Gartner Press Release, Gartner Identifies the Top Cybersecurity Trends for 2023 , April 12, 2023 (https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023)

[3]https://www.youtube.com/watch?v=N_sQbYJl820

[4]https://www.gartner.com/en/newsroom/press-releases/2021-10-18-gartner-identifies-the-top-strategic-technology-trends-for-2022(archived, for historical reference only)

[5]https://www.gartner.com/en/newsroom/press-releases/2022-10-17-gartner-identifies-the-top-10-strategic-technology-trends-for-2023(archived, for historical reference only)

[6]https://www.gartner.com/en/newsroom/press-releases/2021-03-23-gartner-identifies-top-security-and-risk-management-t(archived, for historical reference only)

[7]https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022(for historical reference only)

[8]GARTNER 是 Gartner, Inc. 和 / 或其关联公司在美国和国际上的商标和服务标识，并在获得许可的情况下在此使用。保留所有权利。

基于风险量化的网络安全保险实践

绿盟科技 专业服务产品部 欧阳周婷 工程交付部 郝少硕 企业安全运营产品部 刘钊

摘要：网络安全风险量化对网络安全保险的方案设计、产品定价等环节具有重要影响。本文通过分析网络安全保险中的风险量化难点与价值，提出网络安全风险量化模型设计思路，并以勒索场景为例着重介绍风险量化的实践应用。

关键词：网络安全 保险 风险量化 勒索评估

2023 年 7 月，工业和信息化部、国家金融监督管理总局联合印发《关于促进网络安全保险规范健康发展的意见》（以下简称《意见》）。《意见》作为我国网络安全保险领域的首份政策文件，立足我国网络安全保险发展现状和亟待解决的问题，其中对开展网络安全风险量化评估，给出探索建立网络安全风险量化评估模型、支持研发网络安全风险量化评估技术等具体意见。绿盟科技聚焦网络安全保险领域，自 2018 年开始该服务探索，目前已在网络安全风险量化模型设计、评估工具支撑、实践应用等方面积累了丰富经验。

1. 解决网络安全风险量化问题迫在眉睫

网络安全风险量化作为网络安全保险的关键要素，对保险方案设计、产品定价等环节具有重要影响，然而对于网络安全保险业务流程中涉及的各方而言，网络安全风险量化存在着诸多难点：

- 对于保险公司而言，导致网络安全事件发生的原因多样，造成量化过程需要取舍、考虑权重等，如数据泄密责任险种，可触发数据泄露的网络安全事件可能有勒索、数据未加密等，量化指标过严会导致购置门槛高，过低会加大保险公司的风险。
- 对于投保企业而言，无法量化被投保系统（包括基础设施、信息资产等）可能面临的风险，意味着难以平衡保费与成本之间的关系，无法预测的投入产出比，加剧了对于网络安全保险产品的不信任。
- 对于安全厂商而言，以渗透测试、管理咨询为主的安全服务作为支撑网络安全风险量化的主要手段，投入成本高，实施周期长，无法满足网络安全风险量化在网络安全保险中的应用需求。

2. 网络安全风险量化促进产业融合发展

网络安全风险量化模型作为网络安全技术与网络安全保险的纽带，促进着产业间的融合发展。网络安全风险量化模型，可用于指导构建详细的量化评估指标；量化指标促进投保企业对安全查漏补缺并形成更加体系化的安全防御能力，辅助保险公司灵活定价，进一步形成更贴合企业安全需求的保险产品，并为安全厂商提供风险数据输入以刻画用户安全画像，细化安全需求点；保险公司、投保企业、安全厂商三方得益于网络安全风险量化的不断迭代，持续促进安全产业和保险产业的需求释放与高质量发展。

绿盟科技基于常见的网络安全保险险种定义和承保范围，将险种与安全事件关联（如开放端口、人员安全意识、数据管控等），形成了安全能力指标，并与应急响应等外部影响因素相结合，构建了网络安全风险量化模型。

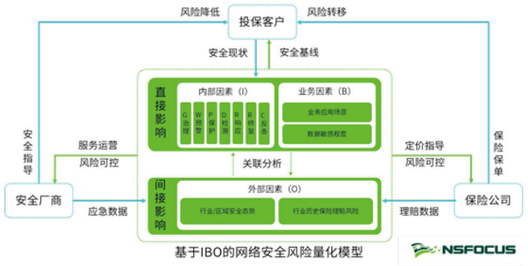


图 1 网络安全风险量化模型

- 内部因素（I），关注企业自身安全防护能力建设，以等保2.0、数据安全成熟度模型、个人信息安全评估等合规要求为支撑，结合保险场景出险的根因分析和绿盟科技应急经验，从治理能力、预警能力、保护能力、检测能力、响应能力、修复能力和反击能力7大能力域，建立60+项企业安全能力指标。各项能力指标由1个或多个评价项组成，评价项以问题形式呈现，且因评价项与网络安全保险的险种相关联，所以评价项赋予了不同权重；评价项的答案（即能力现状）也给出不同分值，各项能力指标的分值由评价项权重与能力现状得分相乘而得。

能力域	能力项	能力指标	评价项	评价项权重	能力现状	能力现状得分
E（响应）	应急响应	制定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容，重要事件的应急预案应包括应急处理流程、系统恢复流程等内容。	是否根据国家、行业或地方有关部门应急管理相关规定，制定安全事件的总体应急预案以进行应急处理、恢复？	1.5	是	1
					否	0
			是否具有针对明显病毒、勒索等安全事件场景下的专项应急预案？	1.5	是	1
					否	0
		测试组织事件响应能力。	是否对安全事件应急预案定期进行演练？	1.5	是，一年多次，或覆盖3个及以上的安全场景作演练且会通过培训让大家掌握相关能力和流程	1
					是，一年1次，或一年只对1个安全事件场景作演练，如Web安全事件、主机安全事件、网络安全事件等	0.5
					否	0
			是否有专业的第三方服务提供商来帮助提供应急响应服务？	1.5	是	1
					否	0

图 2 内部因素（I）的某安全能力指标示例

- 外部因素（O），关注企业潜在安全事件发生可能性，包括企业所在行业和区域的应急事件比重、企业所在行业的历史保险理赔风险等级等，形成多个指标项。例如针对近12个月企业所在行业、区域的应急事件占比统计，排名不同则赋予不同分值。

区域事件占比排名	赋值
Top 1-10	3
Top 11-20	2
Top 21之后	1

图 3 外部因素（O）的某指标赋值示例

- 业务因素（B），关注企业受损后的业务影响程度，从系统外联与应用场景、数据敏感程度、短信接口应用场景等方面考虑事后影响，形成多个指标项。例如针对系统外联与应用场景，按照系统是否互联网可访问，是否存在线上交易等敏感业务场景，进行赋值。

系统外联与应用场景	赋值
所有系统可互联网访问，且存在线上交易业务场景	2
所有系统均可互联网访问；部分系统可互联网访问，且存在线上交易业务场景	1.5
部分系统可互联网访问	1.2
均为内网系统	1

图 4 业务因素（B）的某指标赋值示例

企业综合风险分值（R），作为企业最终风险量化结果，在分别对内部因素、外部因素、业务因素的分值统计基础上，对上述三大因素进行权重分配，最终通过公式计算输出企业综合风险值（R区间为 3 至 11），完成风险量化工作，并可映射到企业综合风险参考等级。在网络安全保险应用场景中，则可进一步向保险公司提供核保建议。

风险等级	风险分值（R）	风险描述	核保建议
极高	11	风险发生可能性很高，存在极严重的安全问题	不建议承保
高	8~10	风险发生可能性高，存在较严重的安全问题	加固后承保
中	6~7	风险发生可能性中，存在部分安全问题	加固后承保
低	3~5	风险发生可能性很低，安全风险较小	可承保

图 5 企业综合风险分值（R）示例

3. 绿盟基于勒索场景的网络安全保险 2.0 实践

为更好应对勒索这类网络安全保险关联度最高的事件场景，绿盟科技围绕“保险 + 风险管控 + 服务”的服务理念，以网络安全风险量化模型为指导，考虑攻击团伙可能的入侵路径，形成勒索专项风险量化指标，引入自动化的评估流程工具链，对路径上防御手段的有效性进行验证和评估，并在某国有控股上市金融企业进行风险量化实践。

锁定评估范围，形成勒索专项评估指标。基于客户调研结果，选用了 2022 年国内外五大活跃勒索家族关联的技战术进行测试用例构建和剧本设计，完成评估工作分解。

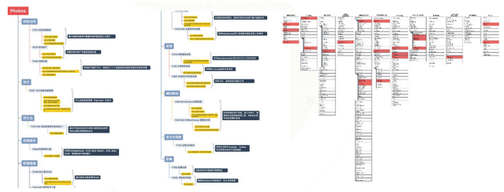


图 6 构建勒索专项评估指标

轻量化评估资产风险，无害化模拟真实场景。根据商定的评估工作分解步骤开展勒索防护能力评估，引入 SaaS 服务，如以外部攻击面管理服务（EASM）梳理内部资产面临的外部攻击风险，以轻量化渗透测试服务（PTaaS）快速评估互联网资产安全态势，以轻量化安全意识测评服务（InSAAS）量化安全意识水平；同时，针对国内外五大活跃勒索家族关联的技战术进行了无害化模拟测试，输出量化的风险评估结果，实现勒索场景下的网络安全风险量化。

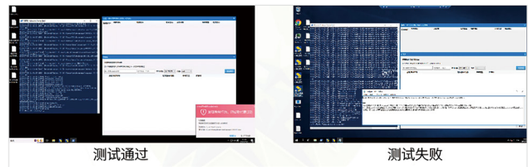


图 7 轻量化评估资产风险

综合分析安全能力，完成网络安全风险量化。使用用例集定义的目标行为和实际评估测试结果，计算各过程域评估得分，映射评估等级。根据当前评估等级和目标评估等级，提供差距分析和改进建议，并输出勒索防护能力评估报告。

图 8 形成网络安全风险量化结果

4. 展望

随着安全大模型正在越来越多的行业应用场景发挥效能，网络安全风险量化不仅促进着网络安全技术和保险行业的融合发展，也会对整个社会在网络安全领域的认知和应用产生积极影响。相信随着大模型与网络安全、保险行业的垂直应用，也将为网络安全保险产业创新带来新动能。绿盟科技后续将携手金融、保险和企业相关机构共同探索网络安全保险领域的智能化安全，为推进网络安全保险的产业发展持续贡献力量。

基于虚实结合技术的工控安全实训靶场设计

绿盟科技 解决方案销售中心 马跃强 陕西办事处 韩皓 内蒙古办事处 尹天助

摘要：针对目前实体工控安全实训靶场不能开展多人同时在线操作的实验教学、攻防比赛、红蓝对抗等问题，以及虚拟工控安全实训靶场不能基于应用层和实体设备开展攻击演示、漏洞扫描与挖掘、安全研究等问题。本文设计了一种虚实结合的工控安全实训靶场平台，通过融合实体设备仿真和虚拟化应用层仿真的能力，来满足用户开展实验教学、攻防演练、红蓝对抗、漏洞扫描与挖掘、攻击效果演示以及安全研究等工作，为今后我国工控安全实训靶场建设提供参考依据。

关键词：工控安全实训靶场 靶场平台 虚拟化 人才培养 攻防演练 科研测试

随着《网络安全法》《数据安全法》以及《关键信息基础设施安全保护条例》等法律法规相继落地实施，驱动网络安全产业高速发展，导致对网络安全人才的大量需求[1]，据《网络安全产业人才发展报告》（2021 版）预估[2]“我国网络安全人才整体上供需失衡，人才累计缺口 140 万以上，而每年高校毕业生不足 2 万，其中工控安全人才缺口比例更高”，已经不能满足工控安全快速发展的需要。2023 年，国家能源局印发《2023 年电力安全监管重点任务》中明确要求：“推进国家级电力网络安全靶场建设，并加强攻防演练、教育培训等内容。”

目前，培养工控安全人才最有效的方式是建设工控安全实训靶场[3-5]。依托工控安全实训靶场，开展理论学习、实操训练、竞技比赛、攻防演练、红蓝对抗、安全测试、安全研究等内容，从而达到快速培养人才的目的[6]。

1. 工控安全实训靶场发展现状

目前，国内工控安全实训靶场主要有实体工控安全实训靶场和虚拟工控安全实训靶场[7]。所谓实体工控安全实训靶场，就是业务场景、攻击渗透、防护验证以及效果展示都是以实体的形式呈现，未集成在虚拟化平台中[8]。这种实训靶场，主要优点是真实的仿真环境，体验效果好，可以基于实体设备开展诸如漏洞扫描、利用、挖掘、Fuzzing 以及防护验证等应用研究。但其缺点是不能支持基于多人同时开展的实验操作，攻防比赛、红蓝对抗以及建设成本高等问题。所谓虚拟工控安全靶场，就是业务场景、渗透攻击、防护验证以及攻击效果演示等集成在一个虚拟平台中[9]。这种实训靶场，主要优点是建设成本低，可以支持多人同时开展实验教学、攻防比赛、红蓝对抗等比赛以及扩展灵活、资源弹性等。其缺点主要是基于实体设备开展的应用研究能力弱、场景不逼真、体验效果差等问题[10]。

从以上分析来看，能将实体实训靶场与虚拟实训靶场各自优点集合在一起的工控安全实训靶场尤为重要，但是，目前能将二者有效集合在一起的工控安全实训靶场并不理想。这种靶场对业务场景的仿真，只能对网络层面实现仿真，即把 DCS、PLC、HMI、工业交换机、操作员站、工程师站、SCADA 实时服务器以及接口机等工控组件看成一个网络节点。一个 IP 节点，不能基于应用层面仿真[11-12]，所以对开展安全实训、竞技比赛、攻防渗透、红蓝对抗以及实体设备安全研究等，并不理想。

因此，设计一种能将实体实训靶场与虚拟实训靶场各自优点集合在一起，且还能基于应用层的仿真的工控安全实训靶场尤为重要。

2. 工控安全实训靶场平台设计

2.1. 设计思路

本文设计一种既可以基于虚拟化场景开展实验教学、攻防演练、红蓝对抗等工作，又可以基于实体场景开展攻击演示、漏洞挖掘、Fuzzing、防护验证以及安全研究等工作的工控安全实训靶场平台。即通过虚拟化、虚实结合、安全资源编排与调度、自适应接入、工业设备虚拟化、工业协议模拟器以及工业组态等技术构建各类工控虚拟化应用层仿真场景，开展相关教学培训、攻防演练、竞技比赛、红蓝对抗等实训工作。同时，搭建基于实体设备的工业仿真场景、防护设备、演示沙盘等，满足用户攻击演示、漏洞挖掘、Fuzzing、防护验证以及安全研究等工作。

2.2 整体架构设计

工控安全实训靶场主要包括业务场景仿真、虚拟化靶场平台、安全防护设备以及沙盘演示系统等共四大部分内容，整体设计如下图所示：

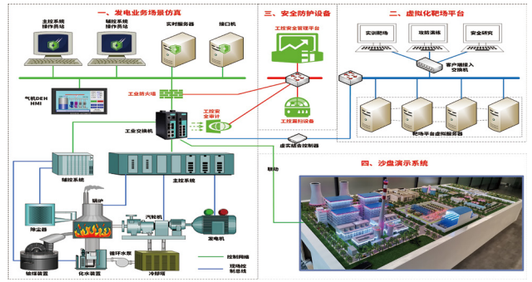


图 1 工控安全实训靶场整体架构设计

场景仿真：根据实际业务场景，从真实场景中抽取出一部分典型业务进行模拟。本论文选取火力发电厂为例，以汽轮机、发电机、锅炉、冷却塔以及化水装置、除尘器和输煤装置等典型业务，来模拟火力发电厂的主控和辅控系统。

虚拟化靶场平台：本论文利用 OpenStack 云架构和 Docker、NFV、虚实结合等技术，对虚拟资源进行统一调度编排管理与弹性扩展，设计 1 套虚拟化靶场平台，作为靶场应用的底座。同时将生产设备、DCS/PLC 模拟器、工业交换机、工业协议模拟工具、组态软件、编程软件以及攻击渗透工具、流量发生器等资源进行虚拟化部署，构建虚拟化工控仿真场景、攻击渗透场景以及开展实训

教学、竞技比赛、科研测试等应用。

安全防护设备：本论文主要选取工业防火墙、工控安全审计系统、工控主机防护系统、工控漏洞扫描以及工控安全管理平台等产品，进行实训教学、安全分析以及验证防护有效性等。

沙盘演示系统：本论文设计 1 套物理实体沙盘，用于对仿真业务场景攻击效果的沉浸式体验。

2.3 业务场景仿真设计

2.3.1 实体仿真

利用生产设备（模具 + 灯带 + 声光传感器）+ 控制器（DCS/PLC/RTU）+工业主机（操作员站 +工程师站 + 实时服务器）+HMI+ 工业交换机 +工业软件（编程软件 + 组态软件）等工具，对火力发电业务场景仿真。

主控系统模拟仿真：在汽轮机、发电机、锅炉、冷却塔等模具上安装灯带、开关以及声光传感器。这些传感器通过信号线与控制器 DCS 连接，在 DCS 控制器中编写梯形图程序，模拟发电过程中对汽轮机、发电机、锅炉、冷却塔等设备的控制逻辑、运行参数和运转状态；在主控操作员站上安装组态软件，设计发电工艺组态画面、实时曲线以及报表，并通过组态软件集成的设备驱动与 DCS 通信，将 DCS 中的模拟数据在工艺图上显示；在 SCADA 实时服务器上部署工业实时数据库，模拟数据实时采集；在接口机上部署数据采集接口软件，模拟与 II 区的 SIS 系统数据交互功能。

辅控系统模拟仿真：在输煤装置、化水装置以及除尘器等模具上安装灯带、开关以及声光传感器。这些传感器通过信号线与控制器 PLC 连接，在 PLC 中编写控制程序，模拟发电过程中对输煤、化水、除尘等工艺控制和生产运行数据，并在辅控操作员站安装部署组态软件，并设计输煤、化水以及除尘等工艺组态画面、实时曲线以及报表，并与 PLC 建立通信连接，将 PLC 中模拟的数据以及传感器的数据在组态画面显示。

通过实体场景的仿真，可以满足基于实体设备开展诸如漏洞扫描、利用、挖掘、Fuzzing 以及防护验证等应用研究。

2.3.2 虚拟化仿真

通过将 DCS/PLC 模拟器、协议模拟软件以及编程软件、组态软件等模拟工具，部署在虚拟化平台中，利用 DCS/PLC 模拟器模拟火力发电站的主控和辅控系统的控制器；利用协议模拟软件模拟汽轮机、发电机、冷却塔以及输煤、化水、除尘等生产设备运行状态和参数；利用编程软件、组态软件模拟上位机，并进行组态画面。在 DCS/PLC 模拟器和协议模拟软件中进行编程和设置，产生模拟数据，并与组态软件进行通信，在监控画面中实时显示这些数据、运行曲线以及报表。

通过虚拟化的应用层场景仿真，满足多人同时开展实验教学、攻防比赛、红蓝对抗等比赛需要的实验环境和靶标系统。同时，还可以根据实际要模拟的仿真场景以及场景数量，进行任意组合、编排以及弹性拓展。

2.4 虚拟化靶场平台设计

2.4.1靶场平台功能架构

通过 OpenStack 框架搭建虚拟化靶场平台，其整体功能架构设计如下：

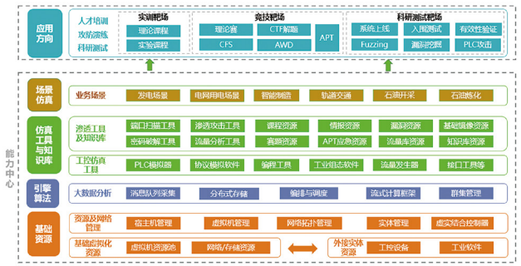


图 2 靶场平台功能架构设计

基础资源：主要为靶场平台提供网络、存储、计算等虚拟化资源以及进行宿主机、虚拟机和虚实结合控制管理等功能。

引擎算法：主要采用大数据分析技术，通过群集管理多个计算节点，使用消息队列实时采集多种来源的仿真数据，并使用流式计算框架进行数据处理，以及以分布式存储技术为整个平台提供存储、编排与调度能力。

仿真工具与知识库：通过虚拟化技术，将攻击渗透类工具（如端口扫描 Nmap，漏洞利用工具 Metasploit，流量分析工具 Wireshark、自动化渗透工具，如绿盟 EZ 工具等）和工控仿真工具（如 PLC 模拟器、工业协议模拟软件、编程工具、组态软件、流量发生器等）以及知识库资源（如课程、赛题、情报、APT、漏洞、流量库等资源）部署在虚拟化平台中，为场景仿真提供灵活的应用工具。

场景仿真，基于虚拟化资源、引擎算法以及仿真工具与知识库资源，根据实际业务场景需求，进行基于应用层的仿真，如发电场景、用电场景、智能制造、石油开采等场景。

同时，将基础资源、引擎算法、仿真工具与知识库以及场景仿真这四个层级看成一个能力中心，作为整个靶场平台的能力底座，提供实训靶场、竞技靶场以及科研测试靶场的能力。

2.4.2实训靶场

实训靶场功能主要实现对学员进行理论知识和实操技能的训练及考核过程的管理，包括对不同培养方案的编排、过程监控、考核评价、效果评估等。实训流程如图 3 所示：

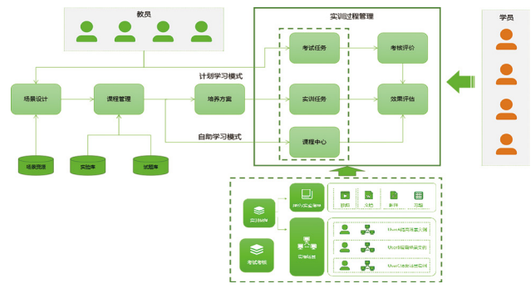


图 3 实训靶场业务流程设计

针对不同学员，教员编排不同的培养方案，根据培养方案的内容进行特定的场景设计、课程设计。培养方案完成后，向学员发布实训和考核任务，学员登录靶场系统领取任务，并开

展相应的训练和考核。

靶场对学生的整个实验过程实时监控，包括实验场景状态、实验结果和操作记录等，并可以通过 VNC 等方式以第三人称视角实时查看受训者的实验过程。

学员完成实训和考核任务后，系统对实训和考核任务的结果进行效果评估，通过收集的学员学习记录、考核记录等数据，并结合人才能力评估模型进行多维度多方位的综合能力评估，给出最终的评估结果和能力评估雷达图。

2.4.3 竞技靶场

竞技靶场功能主要实现竞赛过程的管理，能够对一场竞赛的全生命周期进行全方位的过程管理，包括试前、试中、试后三个阶段。系统内置多种竞赛模式，包括理论赛、CTF、AWD、CFS 四种竞赛模式，并为每种模式配备高区分度的赛题，同时根据竞赛的具体需求进行自定义场景。竞赛演练流程如图 4 所示：

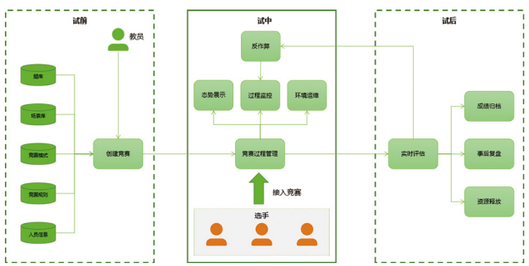


图 4 竞技靶场业务流程设计

通过设定竞赛名称、LOGO、开始时间、结束时间、人员信息、竞赛规则等信息，并选择相应的参赛队伍来新建一场比赛。

比赛中对每个参赛队伍的赛题状态进行实时监控，并远程维护比赛双方主机。同时系统以用户指定的可视化模式对竞赛过程进行态势展示。

比赛结束后系统对参赛队伍提交的答案进行实时评判，对当前和历史竞赛信息进行统计展示，并对数据进行归档、事后复盘、资源释放等。

2.4.4 科研测试靶场

科研测试靶场功能主要实现对目标环境的模拟仿真，科研主要依据实体仿真场景开展，测试流程如下图所示：

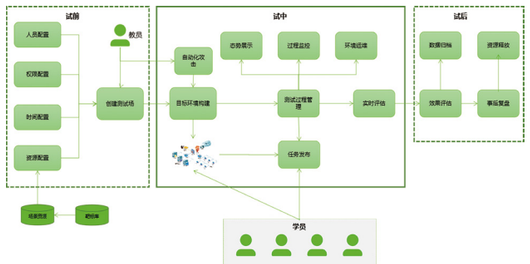


图 5 科研测试业务流程设计

教员根据需求自定义测试场，包括测试场名称、开始时间、结束时间、人员配置、权限配置、资源配置等。创建测试场完成之后，对目标环境进行构建，通过虚实集合将虚拟设备和实物设备进

行柔性混合组网，同时将任务发布给对应的人员。学员登录系统接受任务，并进行测试操作。

靶场平台对测试过程中的数据进行采集和评估，并对测试的数据进行态势展示，对测试过程进行监控，对目标环境进行运维操作。在测试过程中，教员可以对目标环境进行自动化攻击，为目标环境产生攻击流量和背景流量。

靶场平台对测试的数据和报告进行效果评估，测试结束之后对数据进行归档、资源释放、事后复盘等。

2.5 安全防护设备

主要包括工业防火墙、工控安全审计系统、工控主机防护系统、工控漏洞扫描以及工控安全管理平台等产品的功能验证，验证其防护的有效性。

表 1 工业防火墙功能验证设计

功能	***验证设计***
工业协议识别与解析	对主流工控协议（MODBUS、OPC、S7、IEC61850、IEC60870、DNP3、Fins 等）识别与深度解析验证
白名单基线	对机器自学习建立白名单安全基线模型；对操作行为的细粒度控制、检测和阻断异常操作行为验证
基于应用层访问控制	对工控协议的功能码、寄存器范围、寄存器地址、寄存器内容等进行指令读写、阈值等应用控制验证
IPSec VPN	对 IPSec VPN 功能，为通信双方提供数据加密、防篡改等安全策略防护验证
DOS 攻击	对各类 DoS 攻击，如 Icmp-flood、land、ping of death、udp-flood 等扫描攻击以及漏洞利用攻击进行防护验证
高可用性	对 HA 双机热备和 Bypass 等可靠性机制验证

表 2 工控安全审计系统功能验证设计

功能	***验证设计***
流量审计	对工控网络通信回溯验证，根据 IP 地址、端口号、时间等条件查询通信记录；对工控协议审计、流量审计，生成完整记录验证
安全检测	实时检测工控网络中的误操作、恶意攻击、违规行为、漏洞利用以及非法设备接入行为进行验证
关键操作	对 PLC 程序下载、上传以及 CPU 启停、硬件组态变更等关键操作进行识别验证
工业协议识别与深度解析	对常见的 MODBUS、OPC、S7、FINS、DNP3，以及 IEC-60870/61850 电力规约协议的识别与深度解析进行验证，包括功能码、寄存器、值域、指令等应用层内容的验证
白名单模型	验证其机器自学习白名单功能，对工业网络中的合法行为进行学习记录，形成白名单模型，然后增加非法行为，验证其能否识别告警

表 3 工控主机防护系统功能验证设计

功能	***验证设计***
应用程序白名单防护	验证非白名单中的应用程序是否能正常运行
进程白名单防护	验证非白名单中的进程是否能启动
脚本白名单防护	验证 bat、cmd、vbs 等脚本格式，白名单之外的脚本文件被禁止执行
USB 防护	验证移动存储介质可读、读写、禁用等功能以及非白名单中的移动存储介质是否可用
工控机加固防护	验证对工控机操作系统的关键文件、目录、注册表以及重要应用服务、进程的防护能力，被保护的文件、注册表、应用服务、进程是否被恶意代码篡改、破坏、删除

表 4 工控漏洞功能验证设计

功能	***验证设计***
工控设备漏洞扫描	对西门子、施耐德、罗克韦尔、霍尼韦尔、欧姆龙、亚控、三维力控、和利时、浙大中控等主流工控厂商以及工控漏洞扫描验证
工业协议 Fuzzing 漏洞挖掘	对厂商设备出厂自检，工业现场环境入围测评，检测机构设备送检安全测试提供 Fuzzing 漏洞挖掘功能，对工控协议进行漏洞挖掘验证
无损漏洞扫描	对轻量化扫描（端口探测、协议识别、资产识别、知识库）和无损扫描验证（设备指纹库+漏洞库）
基线配置核查	对工业主机（操作员站、工程师站以及 SCADA 实时服务器、OPC 接口机等）、工业交换机、操作系统、数据库、中间件等资产基线配置核查验证
工控资产识别与网络拓扑绘制	验证对工控资产（包括但不限于 DCS、PLC、HMI、工控机、编程软件、组态软件等）的品牌、版本以及固件号进行识别与管理，并根据资产通信流量绘制网络拓扑

2.6 沙盘演示系统设计

本论文设计 1 套物理实体沙盘系统，通过工业 ABS 板、亚克力等材料和灯带、报警器、传感器等电控组件模拟发电汽轮机、锅炉、冷却塔等装置的运行状态。整个沙盘独立控制，提供标准接口，与发电仿真系统进行联动，对汽轮机、冷却塔等正常生产状态和受到攻击的异常状态进行动画显示。沙盘效果如图 6 所示：

图 6 发电沙盘效果图

3. 工控安全实训靶场应用设计

3.1 人才培养

理论培训：工控安全实训靶场平台内置基础的工控课件，包括工业网络、工业协议、工控系统、工业软件、工控安全产品以及网络安全法律法规、标准等，可在线学习、在线点播语音教程、在线练习，全面提升安全人才的工控网络安全与网络安全知识与技能。

技能培训：基于虚拟化仿真场景，开展多人同时在线的实训教学工作。比如对工控设备(PLC、RTU、传感器、阀门等)、业务系统(组态软件、工控机、SCADA 实时服务器等)、网络设备（工业交换机、路由器、无线设备等）以及网络安全产品（工业防火墙、工控安全审计、工控漏扫、工控主机防护系统、安全管理平台等）进行操作训练，根据业务需要，学员能够独立完成基本配置、参数设定、安全策略配置以及运行维护。

应急培训：基于工控安全实训靶场平台，对学员开展应急处置方面培训，使学员达到对工控设备、网络设备、工控机、SCADA 实时服务器以及网络安全产品功能的熟练操作，报警信息查看、日志关联分析、安全事件识别与研判，并根据事件发展势态能够进行策略调整、加固，以及必要的应急处置手段。

3.2 攻防演练

通过工控安全实训靶场平台提供的理论赛、CTF、AWD、CFS 四种竞赛模式，开展竞赛演练、应急演练或实战对抗等赛事。

理论赛题：提供单选、多选和判断等多种题型，内容涉及工控网络、工控设备、工控系统以及工控安全、网络安全的各个方向，考察学员的理论知识掌握程度。

CTF 解题：参赛队员通过直接访问靶机或者下载相关附件进行解题。内容涉及 WEB、密码学、隐写、溢出、逆向、固件提取、梯形图编程、工业组态、工业协议分析等方向。CTF 赛题考察学员对单一网络安全技术的掌握能力。

CFS 竞赛：为每个参赛队提供相同的模拟真实企业内部架构的实训环境。环境由若干存在漏洞的靶机组成，在靶机的关键位置存有 Flag 文件。参数队伍需要按照网络拓扑情况对此环境进行逐层渗透得到 Flag 文件并提交。

AWD 混战：为每支参赛队伍提供具有相同漏洞的网络靶机。每支队伍在加固自己网络靶机的同时，要攻击其他队伍的网络靶机。攻击成功后，攻击方得分，防守方减分。

3.3 科研测试

可根据用户需求场景各种应用层仿真场景，并依托靶场平台提供的攻防工具库、靶标资源、漏洞资源、自动化测试工具，流量仿真等资源，开展漏洞研究、装备测试、技术验证等工作。在测试

方面，比如开展入围测试、供应链安全评估、系统上线测试、标准验证以及安全防护有效性验证测试等；在科研方面，依托实体仿真场景，开展诸如工控资产识别、漏洞挖掘，协议分析、PLC 中间人、拒绝服务、缓存溢出等渗透攻击以及成果孵化、专利申报、发表论文、撰写著作等。

4. 总结

本论文针对实体工控安全实训靶场和虚拟工控安全实训靶场存在的问题，设计了一种既可以基于虚拟化场景开展实验教学、攻防演练、红蓝对抗等工作，又可以基于实体场景开展攻击演示、漏洞挖掘、Fuzzing、防护验证以及安全研究等工作的工控安全实训靶场平台。该设计方案，已在某大学落地应用，在成本投入有限的情况下，满足了教师既要开展实验教学、攻防演练又要开展安全研究、漏洞挖掘、攻击演示等需求，为今后我国开展工控安全实训靶场建设提供参考依据。

参考文献

[1] 孙翔 . 绿盟网络空间安全仿真平台助力数字经济发展 [J]. 数字经济 ,2022,3(17):44-47.

[2] 王海涛 , 宋丽华 . 浅析网络靶场的概念、分类与体系架构 [J]. 保密科学技术 ,2021,1(2):04-09.

[3] 李秋香 , 郝文江 , 李翠翠 , 等 . 电网工控安全实验室建设及运行管理探讨 [J]. 信息网络安全 ,2014,2(09):63-68.

[4] 蒋焱 . 电力行业高仿真工控安全实验室建设 [J].2022,4(4):50-56.

[5] 方滨兴 , 贾焰 , 李爱平 , 等 . 网络空间靶场技术研究 [J]. 信息安全学报 ,2016,1(3):1-9.

[6] 刘若琳 . 网络攻防虚拟场景构建技术的研究与实现 [D]. 北京邮电大学 ,2019.

[7] 朱辰 , 孙斌 , 金心宇 , 等 . 网络空间安全攻防实验教学与实训平台的构建 [J]. 实验室研究与探索 ,2021,(6):265-267,275.

[8] 唐颖 , 余愿 . 基于虚拟现实技术的沉浸式教学实践探索 [J]. 进展 : 科学视界 ,2022,(4):92-94.

[9] 王群 , 李馥娟 , 郭向民 , 等 . 网络靶场实训平台的规划与实践 [J]. 火力与指挥控制 ,2021,46(07):136-141.

[10] 孙健 , 翟健宏 . 工控网络仿真靶场虚拟化场景的构建 [J]. 智能计算机与应用 ,2021,9(11):191-199.

[11] 龙九清 . 工控安全攻防演练平台的设计与实现 [J]. 现代信息科技 ,2020,6(11)171-174.

[12] 孙彦斌 , 徐俐 , 陈晓 , 等 . 工业控制系统网络靶场发展及应用 [J]. 保密科学与技术 ,2021,6(4)37-41.

容器镜像仓库泄露风险分析

绿盟科技 创新研究院 程章

摘要：本文主要分析了 Docker 镜像仓库中公共镜像仓库和私有镜像仓库的数据泄露风险。首先对公共镜像仓库 Docker Hub 的镜像泄露情况进行了分析和讨论，然后分别对私有镜像仓库 Harbor 和 Docker Registry 在公网的暴露情况以及镜像泄露的风险进行了讨论和分析，并给出了建议的配置方法。在使用 Docker 镜像仓库时，由于镜像泄露敏感信息的事件经常发生，因此我们应该始终关注其安全性，并采取必要的措施来保护敏感信息和数据的安全。

关键词：容器 云上风险 数据安全

1. 概述

Docker 提供了一种快速、灵活和可移植的方式来构建和交付应用程序，Docker 镜像仓库使得用户能够更加方便地存储和共享 Docker 镜像。然而，镜像泄露敏感信息事件屡有发生，因此，在使用 Docker 镜像仓库过程中，我们应该始终关注其安全性，并且采取必要的措施以保护敏感信息和数据的安全。

Docker 镜像仓库分为公共镜像仓库和私有镜像仓库，**公共镜像仓库**主要是由一些官方机构提供给用户免费使用的存储和共享 Docker 镜像的平台，常见的公共镜像仓库有 Docker Hub、阿里云镜像仓库、Google 镜像仓库等，都包含了广泛的公共镜像供用户使用。**私有镜像仓库**是用户自己搭建用于存储和共享 Docker 镜像的平台。用户可以在私有镜像仓库中存储自己的镜像，并控制访问权限，使其只能被特定的用户或组织使用。常见的私有镜像仓库有 Harbor 和 Docker Registry，其中 Harbor 提供了企业级的镜像仓库管理功能，包括镜像复制、安全扫描等功能。

本文主要对公共镜像仓库 Docker Hub、私有镜像仓库 Harbor、Docker Registry 的数据泄露风险进行了分析。

文中涉及的技术仅供教学、研究使用，禁止用于非法用途，文中所涉及漏洞验证，均使用本地服务器。

2. Docker Hub 镜像泄露分析

2.1 Docker Hub 镜像密钥泄露情况

今年 7 月，德国亚琛工业大学 (RWTH-Aachen University) 的研究人员在 Docker Hub 上发现了数万个暴露敏感数据、源代码的镜像 [1]。他们在分析了 337171 个镜像，包含了 1647300 层的复杂数据集后，最终在 28621 个镜像（占比 8.5%）中发现了 52107 个有效的私钥和 3158 个 API 密钥。

		Regular Expressions (Section 5.1.1 / Appendix C)	(Distinct) Matches (Sec. 5.1.2)		Valid Secrets (Section 5.1.3)		
Domain		Potential Threat / (Service) Type	Images	Variables	Images	Variables	Total
Private Key		Perform man-in-the-middle attacks, fake identity, … *PEM Private Key, PEM Private Key Block, PEM PKCS7, XML Private Key*	1,377,336 (62,282)	2 (1)	52,107	0	52,107
API	Cloud	Manage services, create new API keys, reconfigure DNS, access emails / SMS, control voice calls, read / alter private repositories, … *Alibaba[76], Amazon AWS[76], Azure[76], DigitalOcean[76], Github[76], Gitlab (v1, v2)[76], Google Cloud[76], Google Services[76], Heroku[76], IBM Cloud Identity Service[76], Login Radius[76], MailChimp[76], MailGun[76], Microsoft Teams[76], Netlify[76], Twilio[76]*	6,208,995 (74,460)	416 (84)	2,880	67	2,920
	Financial	List / perform payments, inspect / alter invoices, … *Amazon MWS[76], Bitfinex[76], Coinbase[76], Currency Cloud[76], Paydirt[76], Paymd[76], Paymongo[76], Paypal Braintree[76], Picatic[76], Stripe[76], Square[76], Ticketmaster[76], WePay[76]*	42,901 (343)	4 (2)	23	2	25
	Social Media	Tweet, access direct messages, retrieve relationships, … *Facebook[76,198], Twitter[76]*	6,365,854 (439,822)	14 (8)	209	4	213
	IoT	Retrieve (privacy-sensitive) IoT data, e.g., track cars, … *Accuweather[76], Adafruit IO[76], OpenUV[76], Tomtom[76]*	297 (117)	0 (0)	0	0	0

图 1 研究人员最终获取的敏感信息汇总

从图 1 中可以看出，私钥的泄露可能会导致中间人攻击、身份伪造等后果，主要私钥类型有 PEM Private Key、PEM Private Key Block 等。API 敏感信息主要包括公有云服务凭证、金融支付凭证、社交媒体凭证和物联网凭证，其中泄露的公有云服务凭证类型包括了阿里云、亚马逊云、Azure 等多个大型公有云服务，金融支付凭证则包含了亚马逊 MWS、Bitfinex、Coinbase 等大型国外交易网站或加密货币的交易凭证，社交媒体的凭证主要包含了 Facebook 和 Twitter，物联网设备的凭证数量相对较少，但也可能会导致物联网设备数据被窃取的严重后果，例如汽车位置信息的跟踪定位。

2.2 暴露敏感信息分析

另外，德国亚琛工业大学的研究人员还对暴露的敏感信息进行了分析，确定其实际用途进而了解所暴露的攻击面的大小。结果根据泄露的密钥发现了 22082 个证书，其中还包括 7546 个私有签名证书和 1060 个公共 CA 签名证书，研究者对这些 CA 证书进行了深入分析后，发现仍有 141 个证书有效。

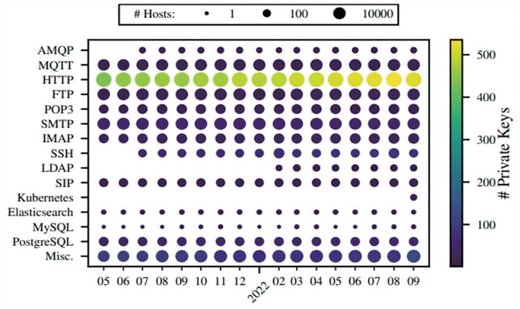


图 2 Docker Hub 泄露信息类型汇总

研究人员进一步通过 Censys 数据库 [2] 对密钥进行分析，发现了存在 275269 个主机使用了这些泄露的密钥。如图 2 所示，其中包括了可能传输物联网敏感数据的 MQTT 资产以及 AMQP 资产，存储重要敏感数据的 FTP 资产、PostgreSQL 资产和 MYSQL 资产，还包括上万台用于 SMTP、POP3、IMAP 等邮件系统服务器。

对于 SSH 服务器和 Kubernetes 服务器，泄露的密钥可能会带来远程恶意 shell 访问、僵尸网络扩张等威胁。

（备注：基于白帽原则，研究人员并未对暴露的服务验证其密钥）

Docker Hub 免费版只支持公开镜像的托管，因此只能使用其公共镜像仓库的功能。如果用户缺乏安全意识，将带有敏感信息的镜像上传至公共镜像仓库，将导致镜像和敏感信息泄露的风险。因此，建议避免将存储敏感信息的镜像上传至 Docker Hub 公共镜像仓库，而是选择自建 Harbor 或 Docker Registry 私有镜像仓库。同时，使用自建私有镜像仓库时也需要注意安全性。接下来的内容将分析私有镜像仓库的安全性。

3. Harbor 镜像泄露分析

3.1 Harbor 组件公网暴露情况

截至 2023 年 11 月，在 Shodan 上可以检测到 12379 个暴露的 Harbor 资产，如图 3 所示，其中检测到国内 3377 个 Harbor 资产、国外 9002 个资产。值得一提的是，在 2022 年 4 月，国内的 Harbor 资产暴露数量仅为 2557[4]，在近一年半的时间内增长了 820 个，增长率为 32%。这些资产都是暴露在公网上，且大量资产都处于存活状态。

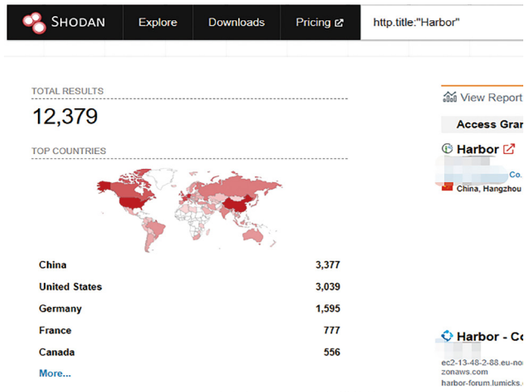


图 3 Harbor 资产在 Shodan 上扫描的结果

3.2 镜像泄露风险分析

既然 Harbor 在公网上暴露了这么多资产，且暴露资产的数量增长如此迅猛，公网上的 Harbor 资产是否也存在镜像泄露风险呢？本文将逐步进行分析。

3.2.1 CVE-2022-46463导致镜像泄露过程验证

提到 Harbor 镜像泄露风险，不得不说其近年来频频爆出漏洞，如 CVE-2022-46463，NVD 对该漏洞的描述如图 4 所示 [5]，我们可以得出攻击者可在无认证情况下，访问公开和私有的镜像仓库。

图 4 NVD 对 CVE-2022-46463 的描述

虽然图 4 的公告中明确指出了该漏洞所影响的范围是 2.5.3 以下的版本，但经过实际安装测试，笔者发现截至 2023 年 11 月，Harbor 最新 Release 版本 2.9.1，以及之前发布的 2.8.4 及更老的版本，依然存在该镜像泄露风险。利用该 Harbor 特性获取镜像信息的验证过程如下：

首先在服务器上安装 harbor 目前的最新 release 版本 2.9.1，如图 5 所示。

图 5 测试环境的 Harbor 版本为 2.9.1

之后任意上传测试镜像至 Harbor，并将其设置为公开，如图 6、图 7 所示。

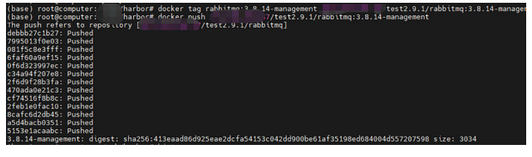


图 6 将测试镜像打标签，并上传到 Harbor

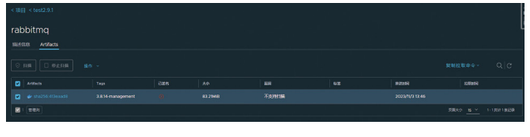


图 7 Harbor 上可以查询到该镜像

最后，在另外一台服务器上，依然可以现通过 Harbor 的 API 接口获取服务器上存储的镜像信息，再进一步获取某个镜像的 digest 等具体信息后，可以组装出该镜像的拉取命令，并对该镜像进行拉取，结果成功拉取了该测试镜像。具体过程如图 8 到图 10 所示。

图 8 通过 CVE-2022-46463 发现了上传的镜像仓库名称

图 9 通过 Harbor 的 API 接口进一步获取该镜像的 digest

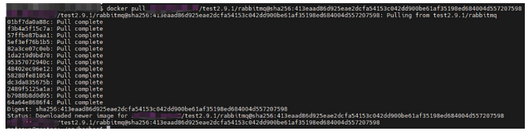


图 10 通过镜像的 digest 组装出镜像拉取命令，并成功拉取该镜像

上述过程是在没有任何认证前提下，从目前最新 Release 版本（2.9.1）Harbor 项目中获取镜像信息的过程，可以看出我们能够获取 Harbor 私有仓库中被设置为“公开”的镜像仓库的信息，甚至能够进行拉取。

行文至此，想必读者一定会好奇，为何如此严重的漏洞，官方迟迟不修复呢？

3.2.2 “假漏洞”乌龙事件

细心一点的读者可以发现，NVD 对该漏洞的描述（如图 4）中最后的 NOTE 对该漏洞做出了补充说明：官方认为这个“漏洞”是 Harbor 的一个特性。

官方具体的回应如图 11 所示。

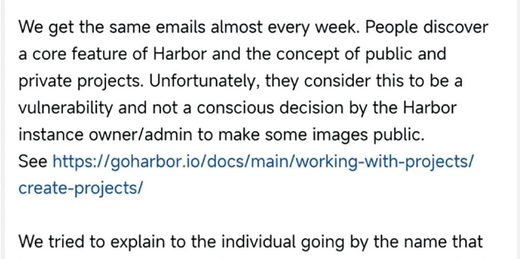


图 11 Harbor 官方对此漏洞的回复

官方回应明确指出，他们不认为公开的 CVE-2022-46463 是 Harbor 的一个漏洞，而是 Harbor 官方文档中所明确定义的特性之一，即用户可以设置一些镜像为公开，该特性导致 Harbor 上的

所有被设置为公开的项目都通过相应的 API 接口被列举，获取详细信息，甚至被拉取。

笔者在测试过程中，确实发现在新建项目时可以对项目的访问级别进行勾选，如图 12 所示。

图 12 新建项目界面

而且，在访问级别后面的说明也对项目公开做出了详细且明确的描述，当项目设置为公开时，任何人都有该项目下的读权限，且命令行用户不需要“docker login”就可拉取该项目下的镜像。

测试过程中，如果用户不对项目访问级别勾选“公开”项，则只有项目设置所属账户和 admin 账户可以看到此类项目，因而所有未认证的用户均无法通过 API 或前端查询到任何信息，如图 13 所示。

```
@master:~$ curl http://                    /api/v2.0/projects/test/repositories?page_size=15&page=1
14629
@master:~$ {"errors":[{"code":"UNAUTHORIZED","message":"unauthorized"}]}
```

图 13 未认证用户无法通过 API 获取到该项目的任何信息

尽管该项目对“公开”的描述已经很翔实，但由于 Harbor 的前端界面需要登录认证，针对使用 Harbor 不熟悉的用户在操作时仍有可能会误用该功能，从而使包含敏感信息的镜像仓库对所有人开放，而用户的初衷可能只是对认证用户开放。

通过上述实验可以看出，几乎所有版本的 Harbor 都存在通过特定方式获取镜像的风险，这可能导致敏感信息泄露。因此，在使用 Harbor 进行镜像管理时，特别是在部署在公网上的情况下，建议用户先熟悉 Harbor 的使用方式和特性，并严格控制镜像仓库的公开范围。同时，重视对镜像仓库中的敏感信息和相关配置信息的管理，以避免因公开包含敏感信息的镜像而导致敏感信息泄露的风险。

4. Docker Registry 镜像泄露分析

4.1 Docker Registry 组件公网暴露情况

截至 2023 年 11 月，在 Shodan 上可以检测到 12920 个暴露的 Docker Registry 资产，如图 14 所示，其中检测到国内 2902 个 Harbor 资产、国外 10018 个。

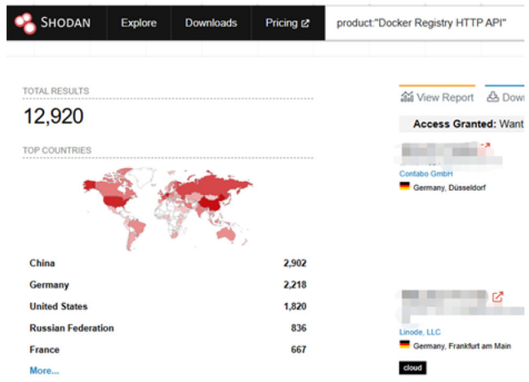


图 14 Docker Registry 资产在 Shodan 上扫描的结果

4.2 镜像泄露风险分析

在默认情况下，可以直接获取到 Docker Registry 私有镜像仓库列表和版本信息，进而获取详情信息，具体过程如下：

当使用命令 docker run -p 5000:5000 --restart=always --name registry -v /var/lib/registry:/var/lib/registry -d registry 进行 Docker Registry 私有仓库的构建时，默认不会开启认证服务。若该镜像仓库服务暴露在公网时，任意用户可以通过官方 API 对镜像列表进行获取，如图 15 所示。


```
root@test:~# curl                    5:5000/v2/_catalog
{"repositories":["rabbitmq"]}
```

图 15 通过 API 对资产的镜像仓库列表进行读取

在获取到镜像仓库列表后，进一步通过官方 API 获取 tag 信息，如图 16 所示。

```
root@test:~# curl                    5000/v2/rabbitmq/tags/list
{"name":"rabbitmq","tags":["latest"]}
```

图 16 通过 API 获取镜像仓库的 tag 列表

通过获取仓库名称和 tag，我们不仅可以获取镜像构建的详细信息，还能够根据名称和 tag 信息组合出镜像拉取命令并进行拉取，如图 17 所示。

```
root@test:~# docker pull                    .5000/rabbitmq:latest
```

图 17 组合出来的镜像仓库拉取代码

首先创建 Docker Registry 认证文件目录和认证文件，并使用 Apache 的 htpasswd 来创建加密文件，容器的启动方式如图 18 所示。

```
root@master:~# htpasswd -Bbn admin admin > /var/lib/registry_auth/htpasswd
root@master:~# docker run -p 5000:5000 \
> --restart=always \
> --name registry \
> -v /var/lib/registry:/var/lib/registry \
> -v /var/lib/registry_auth/:/auth/ \
> -e "REGISTRY_AUTH=htpasswd" \
> -e "REGISTRY_AUTH_HTPASSWD_REALM=Registry Realm" \
> -e "REGISTRY_AUTH_HTPASSWD_PATH=/auth/htpasswd" \
> -d registry
```

图 18 开启认证服务时的 Docker Registry 启动方式（示例）

当给 Docker Registry 添加了认证机制后，再通过其 API 接口获取镜像列表时将返回未认证的提示，如图 19 所示，因此添加认证机制的 Docker Registry 将可以对私有镜像仓库进行保护。

```
                ~$ curl                    :5000/v2/_catalog
{"errors":[{"code":"UNAUTHORIZED","message":"authentication required",
"detail":[{"Type":"registry","Class":"","Name":"catalog","Action":"*"}
]}]}
```

图 19 具有认证机制的 Docker Registry 将可以对私有镜像仓库进行保护

由此得出，虽然 Docker Registry 的安装部署和使用起来非常方便，但是直接使用 Docker Registry 身份认证服务的默认配置并不安全。而且由于 Docker Registry 没有前端界面，缺少 Harbor 中直观的用户认证与配置方式，导致用户在使用 Docker Registry 时，不安全配置的可能性较大。

笔者建议在使用 Docker Registry 进行私人镜像管理时，应首先开启其认证机制后再进行镜像的传输，从而避免镜像信息的泄露。

5. 总结

本篇文章主要介绍和分析了公共镜像仓库 Docker Hub 中镜像和敏感信息泄露情况，以及 Harbor、Docker Registry 两个私有镜像仓库中镜像和敏感信息的泄露风险。

近年来云上数据泄露事件屡见不鲜，公有镜像仓库泄露大量密钥已是事实，私有镜像仓库的安全风险依然存在，因此，建议大家在使用镜像仓库过程中密切关注其安全性，并且采取必要的措施以保护敏感信息和数据的安全，在构建镜像时，避免直接将密钥设置在环境变量中，避免在镜像中直接添加包含源代码、敏感配置信息等。

参考文献

[1]Thousands of images on Docker Hub leak auth secrets, private keys (bleepingcomputer.com)https://www.bleepingcomputer.com/news/security/thousands-of-images-on-docker-hub-leak-auth-secrets-private-keys/

[2]https://search.censys.io/

[3]https://www.docker.com/pricing/

[4] 云原生服务风险测绘分析（二）：Harbor– 绿盟科技技术博客 (nsfocus.net)

[5]https://nvd.nist.gov/vuln/detail/CVE-2022-46463

[6]https://docs.docker.com/registry/

机密计算的崭露头角与未来前景

绿盟科技 创新研究院 陈佛忠

摘要：传统的加密技术已经在数据传输和存储方面提供了一定的保护，但在数据分析和处理过程中，数据通常需要被解密，这增加了潜在的风险。正是在这个背景下，机密计算技术崭露头角。它代表了一项创新性的计算科学领域，旨在保护数据的机密性，即使在计算过程中也是如此。机密计算使用先进的加密技术，使数据在计算和分析中保持加密状态，只有授权的用户可以访问和使用数据，而其他人无法窥探其内容。这一技术的潜力不仅局限于个人隐私保护，还扩展到金融、医疗、科学研究和国家安全等众多领域，为解决数据保护难题提供了创新的解决方案。

关键词：机密计算 数据安全 数据共享 隐私计算

1. 数据保护的未来：机密计算的崭露头角

在当今信息时代，数据已经成了无处不在的宝贵资源。从金融机构到医疗保健领域，从科学研究到政府机构，巨大的数据集用于支持决策制定、创新发展和提供各种服务。然而，随着数据的不断增长，数据隐私和安全问题也变得日益突出。

数据泄露、黑客入侵和滥用个人信息的事件屡见不鲜，这引发了关于如何更好地保护敏感信息的担忧。传统的加密技术已经在数据传输和存储方面提供了一定的保护，但在数据分析和处理过程中，数据通常需要被解密，这增加了潜在的风险。

正是在这个背景下，机密计算技术崭露头角。它代表了一项创新性的计算科学领域，旨在保护数据的机密性，即使在计算过程中也是如此。机密计算使用先进的加密技术，使数据在计算和分析中保持加密状态，只有授权的用户可以访问和使用数据，而其他人无法窥探其内容。这为数据隐私和安全提供了强大的保障，同时仍允许数据在不暴露其内容的情况下进行分析和计算。这一技术的潜力不仅局限于个人隐私保护，还扩展到金融、医疗、科学研究和国家安全等众多领域，为解决数据保护难题提供了创新的解决方案。

2. 机密计算介绍

2.1 技术概述

机密计算是隐私增强计算技术之一，其关键点是保护正在使用的数据。这一技术的核心思想是通过在硬件级别的可信执行环境（Trusted Execution Environments，TEE）中执行计算，以确保数据的安全性 [1]。通常情况下，计算机上的计算组件和内存中的数据是以解密状态存在的，这会使它们容易受到未经授权的软件或管理员的查看或篡改。TEE 提供了一个受保护的环境，确保只有经过授权的计算进程能够访问和操作数据，而不会受到外部干扰或泄露的影响。因此，TEE 的主要作用是防止未经授权的访问或修改正在使用的应用程序和数据，从而提高了管理敏感或受监管数据的安全级别。

机密计算联盟（Confidential Computing Consortium，CCC）表示机密计算应该至少有如下三种属性来保护使用中的数据 [2]：

- 数据机密性：“未经授权的实体无法查看TEE中使用的数据”。
- 数据完整性：“未经授权的实体无法添加、删除或更改TEE中使用的数据”。
- 代码完整性：“未经授权的实体无法添加、删除或更改TEE中执行的代码”。

2.2 机密计算常见的类型

“信任边界”界定了哪些元素有可能访问机密数据（无论它们是善意的还是恶意的），根据“信任边界”定义的不同，机密计算的技术方法会有所不同，主要会有如下三种类型 [3][4]：

- 虚拟机级隔离：仅允许基础设施上运行的虚拟机内的元素访问潜在的数据。
- 进程级隔离：仅允许授权的软件应用程序或进程访问数据。
- 函数隔离：仅允许大型应用程序中的授权子例程或模块访问数据，阻止任何其他系统元素的访问，包括大型应用程序中未经授权的代码。

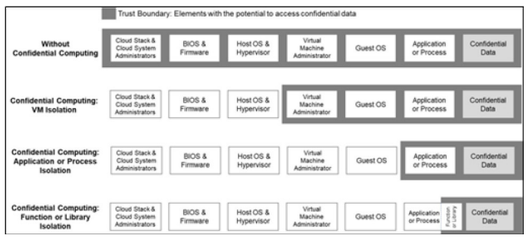


图 1 机密计算三种常见类型对比图 [5]

其中虚拟机级隔离 TEE 代表的 CPU 厂商有：海光 CSV、AMD SEV 等。进程级隔离 TEE 代表的 CPU 厂商有：Intel SGX 等。

2.3 相关技术的对比

机密计算技术经常与其他隐私增强计算技术进行比较，包括全同态加密、安全多方计算、可信计算和联邦学习等。这些技术都旨在实现数据的可用不可见，但它们在安全性、性能开销、通用性和支持的计算类型上都各有不同。

- 全同态加密技术允许数据在加密状态下进行计算，所有的计算都是基于密文的，这提供了极高的隐私保护，但该技术计算开销非常大，且需要了解密码学原理来进行编码，通用性较低。
- 安全多方计算技术使多个参与者能够在不泄露各自私有数据的情况下合作进行计算，整个过程中保障除计算结果外的任何信息都不会被泄露，实现了数据的可用不可见，但该技术计算开销也非常大，且通信耗时长，在实现层面上也需要大量特定于应用程序的编码，通用性较低。
- 可信计算旨在通过使用基于标准化硬件的机制（例如可信平台模块）来建立对计算系统的信任。从技术角度来看，可信计算和机密计算依赖于相似的安全概念（例如信任架构和远程证明协议），然而可信计算的内存不是加密的，机密计算是通过内存加密保证了所使用代码和数据的机密性和完整性。
- 联邦学习是一种分散式机器学习技术，它允许多个参与者在不共享原始数据的情况下合作训练人工智能模型。这一方法的关键

优势是各参与者之间无须传递敏感数据，而只需互相传递模型梯度信息，从而有效降低了数据泄露的风险。然而，联邦学习的分散性质可能引入一些性能开销。需要注意的是，联邦学习并不适用于所有计算类型。该技术主要支持多方数据的协同建模，而不支持通常的计算任务。最终，各方共同构建的模型可用于进行预测，以满足业务需求。预测准确性通常取决于数据的数量和质量，因此数据的丰富性和准确性对于联邦学习的成功至关重要。

	安全性	性能开销	通用性	支持的计算类型
机密计算	较高	低	高	任意计算
全同态加密	高	高	低	任意计算
安全多方计算	高	高	低	任意计算
可信计算	中	低	高	任意计算
联邦学习	较高	中	中	AI预测

图 2 五种隐私增强计算技术的对比

3. 机密计算的应用场景

机密计算的应用场景可以主要归纳为以下三个：安全外包计算及云计算、多方协同计算以及数据安全共享。下面将对这三个应用场景进行详细阐述。

3.1 安全外包计算及云计算

企业通常需要进行诸如数据清洗和数据分析等大量计算资源的任务。在这种情况下，企业可以选择将数据处理任务外包给第三方服务提供商，以降低硬件、人力和运营成本。然而，这样做也会增加数据泄露的风险，因为外包计算服务提供商可以访问企业的处理数据。为了解决这一难题，机密计算技术应运而生。它允许企业在外包计算的同时保持数据的隐私和安全。使用机密计算技术，外包计算服务提供商无法获取到企业进行处理的数据，因为数据在计算过程中会进行加密处理，从而保护数据的机密性，而不会暴露数据的明文内容。这使企业能够在降低成本和提高效率的同时，不必担心数据泄露的风险。

云计算则是外包计算中最常见的一种形式。在传统的云计算环境中，云服务提供商通常可以获取到用户在其平台上处理的数据。然而，如果在云计算环境中使用机密计算技术，企业则无须担心云服务提供商或其他用户能够访问其在云中处理的数据，这有助于提高数据隐私和安全性。例如，企业可以借助机密计算来保护其机器学习模型，允许其在云环境中进行训练，而不会泄露敏感的训练数据。同样，金融机构可以将客户交易数据上传至云中，以进行风险评估和欺诈检测，同时确保云服务提供商无法访问客户的隐私数据。

3.2 多方协同计算

当多个组织或个体需要合作进行数据分析或计算时，机密计算允许各方在不共享原始数据的情况下合作完成任务，以下举四个例子：

- 医疗研究与合作：多个医疗研究机构可以共同分析大规模的医疗数据，如基因组数据、病例记录等，以研究疾病治疗和预防。使用机密计算，这些机构可以在不泄露患者身份和敏感信息的情况下分享数据和分析结果。
- 金融风险评估：不同的金融机构和保险公司可以合作进行风险评估，共享客户信用数据，以确定贷款或保险的条件。机密计算允许他们进行这种合作，同时保护客户隐私。
- 供应链管理：多个供应链的参与者，如制造商、供应商和物流公司，可以共同协作以提高供应链的效率和可见性。他们可以使用机密计算来共享关键的供应链数据，如库存、运输和订单信息，同时保持商业机密。
- 多方数据建模：机密计算技术赋能多方数据建模，这意味着多个数据参与者可以合作创建模型，而不必共享原始数据。这对于保护数据隐私和合规性非常重要，因为数据可以保持加密状态，无须暴露给其他合作方。这有助于确保数据的安全性和隐私，同时允许多方共同合作，以创建更准确的模型。

3.3 数据安全共享

对于运营商、政府等数据量丰富的机构来说，数据在新时代中扮演着双重角色。一方面，数据成了宝贵的资产，可以促进社会的发展和行业进步；另一方面，这些机构必须肩负起保护数据资产的责任。它们既需要实现数据共享以推动社会发展，又必须确保共享数据的安全。以下举两个例子：

- 运营商向广告公司共享用户的位置数据，广告公司可以借助这些数据向用户提供与他们当前位置相关的广告，例如在用户手机APP上给用户推荐目前附近的餐厅或商店。通过采用机密计算技术，可以实现数据的安全共享，这不仅有助于广告公司提供更精准的广告服务，也确保了运营商数据的安全性，避免个人隐私数据的泄露。
- 政府向金融机构共享反洗钱数据：政府机构，如金融情报单位，向金融机构提供有关可疑交易、账户和客户的信息，其中可能包括大额交易、频繁现金存款和跨国转账等可能涉及洗钱的迹象。金融机构可以借助这些数据加强对客户的尽职调查，并报告可疑交易，以确保他们符合反洗钱法规。采用机密计算技术可以确保数据的安全共享，不仅有助于金融机构的反洗钱工作，也保护了政府数据的安全，避免了个人隐私数据的泄露。

4. 机密计算的未来前景

4.1 机密计算联盟

机密计算技术主要由机密计算联盟（Confidential Computing Consortium，CCC）来推动，CCC 是 Linux 基金会的一个项目社区，旨在通过开放协作来加速机密计算的应用 [6]。该联盟汇集了硬件提供商、云计算提供商和机密计算服务提供商，其主要成员单位如下图所示。

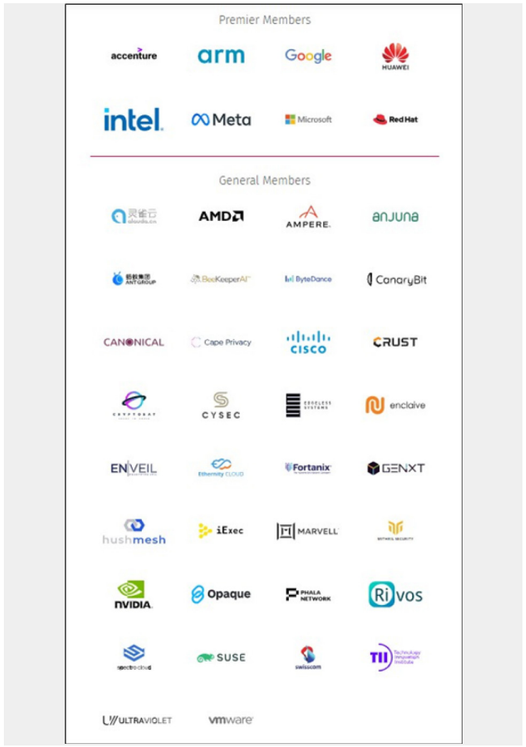


图 3 CCC 主要成员单位

4.2 未来市场预估

在 2020 年，Gartner 就在其年度云安全技术成熟度曲线中，将机密计算列为 33 种关键安全技术之一 [7]。近些年来，多家市场研究和咨询机构认为，未来机密计算市场的增长将非常迅猛。

MarketsandMarkets 公司成立于 2009 年，是美国著名的咨询公司之一 [8]。该公司于 2023 年 5 月发布了一份有关机密计算市场分析的报告 [9]。该报告预测了在 2023 至 2028 年期间，北美、欧洲、东亚、中东 & 非洲以及拉丁美洲五个地区的机密计算市场份额（份额组成为：机密计算相关的硬件、软件和服务）。据报告预测，在 2023 年，全球机密计算市场份额将达到 53 亿美元，而到 2028 年，该份额将增长至 594 亿美元，年复合增长率达到 62.1%。

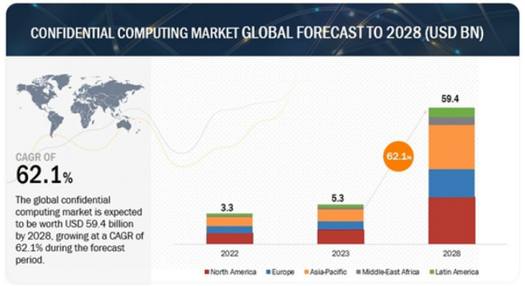


图 4 机密计算市场份额预测（MarketsandMarkets 公司）

Allied Market Research 公司成立于 2013 年，也是美国著名的咨询公司之一 [10]。该公司在 2023 年发布了一份有关机密计算市场分析的报告 [11]，与 MarketsandMarkets 公司不同，Allied Market Research 公司在这份报告中预测了 2023 年至 2032 年全球机密计算市场的份额（份额组成为：机密计算相关的硬件、软件和服务）。据报告预测，在 2032 年，全球机密计算市场份额将达到 1845 亿美元，年复合增长率将达到 46.8%。

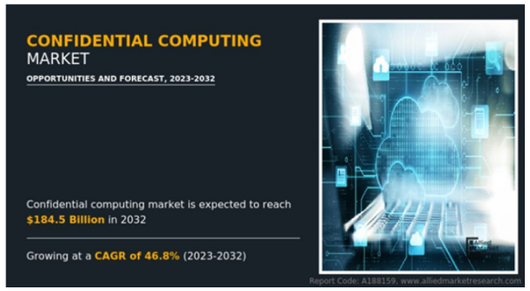


图 5 机密计算市场份额预测（Allied Market Research 公司）

Aspects	Details
Market Size By 2032	USD 184.5 billion
Growth Rate	CAGR of 46.8%
Forecast period	2022 - 2032
Report Pages	341
By Component	• Service • Hardware • Software
By Deployment Mode	• On-premise • Cloud
By End User	• BFSI • IT and Telecom • Healthcare • Retail and E-commerce • Manufacturing • Government and Public Sector • Others
By Application	• Data Security • Secure Enclaves • Pellucidity between Users • Others
By Region	• **North America** (U.S., Canada) • **Europe** (UK, Germany, France, Italy, Spain, Rest of Europe) • **Asia-Pacific** (China, Japan, India, Australia, South Korea, Rest of Asia-Pacific) • **LAMEA** (Latin America, Middle East, Africa)
Key Market Players	Advanced Micro Devices, Inc., Amazon Web Services, Inc., International Business Machines Corporation, Microsoft Corporation, Ovh SAS, fortanix, Cyxtera Technologies Inc., Alibaba Cloud, Intel Corporation, Google LLC

图 6 报告关键要素一览图（Allied Market Research 公司）

5. 总结

本文首先介绍了机密计算技术诞生的背景，然后详细阐述了该技术的特点、常见类型以及与其他类似技术的比较。在第三部分，我们总结了机密计算的三个主要应用领域，包括安全外包计算及云计算、多方协同计算以及数据安全共享。最后，我们介绍了机密计算领域的主要组织 CCC 联盟及其成员，并讨论了对未来机密计算市场的预测(机密计算的市场在未来 5 至 8 年内的增长将非常迅猛)。

综上所述，机密计算技术的崭新前景正在改变我们的数字世界。在数据安全和隐私保护方面，它提供了前所未有的机会。未来，我们可以期待看到机密计算在各个领域的广泛应用，从金融到医疗，从云计算到物联网。让我们紧密关注这一技术的演进，为更加安全的数字未来做出贡献。

参考文献

[1]https://ieeexplore.ieee.org/document/9935045.

[2]https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.3_unlocked.pdf.

[3]https://infohub.delltechnologies.com/p/understanding-confidential-computing-with-trusted-execution-environments-and-trusted-computing-base-models/.

[4]https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/Common-Terminology-for-Confidential-Computing.pdf.

[5]https://en.wikipedia.org/wiki/Confidential_computing

1.https://confidentialcomputing.io/about/.

2.https://www.gartner.com/cn/information-technology/articles/top-actions-from-gartner-hype-cycle-for-cloud-security-2020.

3.https://www.marketsandmarkets.com/AboutUs-8.html.

4.https://www.marketsandmarkets.com/Market-Reports/confidential-computing-market-27796261.html.

5.https://www.alliedmarketresearch.com/about-us.

6.https://www.alliedmarketresearch.com/confidential-computing-market-A188159.

5G视角下的数据安全

绿盟科技 运营商售前技术二部 许国昊

摘要：随着 5G 网络与应用的大力推广，5G 数据安全的重要性也越发明显，5G 带来了便利性，也带来了新的数据安全风险。本文以 5G 数据安全的整体防护框架为切入点，从 5G 通用数据安全、5G 网络数据安全、5G 业务数据安全等多维度进行探讨，并结合绿盟自身探索分享基于流量分析的 MEC 数据安全防护方案。

关键词：5G 数据安全 NFV/SDN MEC

1. 概述

5G 技术自逐步推广应用后，对经济发展和数字化转型提供了新思路，5G 融合应用是促进经济社会数字化、网络化、智能化转型的重要引擎。国家为推动 5G 全面协同发展，深入推进 5G 赋能千行百业，促进形成“需求牵引供给，供给创造需求”的高水平发展模式，驱动生产方式、生活方式和治理方式升级，培育壮大经济社会发展新动能，工信部等十部门关于印发《5G 应用“扬帆”行动计划（2021—2023 年）》的通知。

国家“十四五”规划、中央网信办、工信部、全国信安标委等提出了数据安全管理与保护相关制度及要求。针对 5G 安全，工信部于 2020 年 3 月 24 日印发《关于推动 5G 加快发展的通知》，明确要强化 5G 网络数据安全保护。其中提出了四项要求，即：

- 典型场景数据安全：围绕典型应用场景，健全完善数据安全管理制度与标准规范。
- 明确数据安全责任：合理划分各方数据安全和用户个人信息保护责任。
- 明确数据安全基线：明确5G环境下数据安全建设要求，加强监督执法。
- 完善技术保障体系：推动数据安全合规性评估认证，构建完善技术保障体系。

1.1 5G 数据安全相关监管要求

工信部于 2021 年印发《5G 网络建设与应用安全实施指南》，提出“强化 5G 网络数据安全保护”“强化 5G 行业应用数据安全保护”“深化 5G 数据合作管理”等要求。

1.1.1 强化5G网络数据安全保护要求

结合信息通信行业数据安全有关工作部署，建立健全 5G 数据资产分类分级、重要数据目录、权限管理合作管理、安全评估等制度规范。

适应 5G 网络云网协同特点，基于 5G 数据采集、传输、加工、使用、共享和删除等环节，开展数据安全技术手段云化部署，提升监测、溯源和处置等能力。

1.1.2 强化 5G 行业应用数据安全保护要求

针对 5G 典型应用场景和数据特性，按照“谁运营、谁负责”的原则，梳理形成相关业务应用场景数据资产清单，围绕数据分类分级、数据脱敏、权限管理、备份恢复、安全审计等方面，明确全管理措施和技术。

1.1.3 深化5G数据合作管理要求

建立健全 5G 数据使用风险管理机制，采取合同约束、信用管理等多种措施规范相关数据合作使用行为。对于行业重要数据合作，数据合作方安全保护能力原则上不能低于数据提供方现有水平。

1.2 5G 数据安全风险

5G 网络与业务的快速发展，使企业和个人的数据安全风险将会面临更严峻的挑战。而且随着 5G SA 组网、核心网 NFV/SDN 新技术使用和 MEC 移动边缘计算的接入点下沉和分散，会进一步提高 5G 终端被劫持、数据泄露、过度采集滥用、数据欺诈、非法交易等数据安全风险。

- 终端设备及无线接入数据安全：5G大规模连接，将会有大量的弱终端接入，大大增加了易受攻击点及数据泄露点。多种无线接入技术，可能因中间人攻击、鉴权机制问题等造成用户隐私泄露。
- MEC数据安全：移动边缘计算模式使得网络及用户数据下沉到网络边缘，数据安全管理责任界定、网络边缘数据隔离与保护存在挑战。
- 核心网、切片数据安全：NFV/SDN计算、存储及网络资源虚拟化开放共享，网络边界模糊提高了数据保护的难度，网络切片技术对数据的安全隔离与保护提出了双重挑战。
- 5G垂直业务数据安全：各类5G垂直行业数据安全与隐私泄露风险不一，亟须开展针对特定行业领域的数据资产与隐私保护。

2. 5G 数据安全防护

5G 数据安全的防护，重点不应聚焦于应用的数据安全，这部分其实在通用的数据安全防护中已经可以得到保障，而应重点关注 5G 自身带来的风险，比如控制信令风险、网络切片风险、管理平面风险、MEC 边缘云风险，等等。5G 数据安全防护旨在通过加固 5G 自身数据安全防护能力，进而提升整体 5G 应用的数据安全能力。

2.1 5G 数据特征

我们在探讨如何在各环节保护数据安全前，首先需要了解 5G 网络中的数据，即 5G 数据有什么特征。5G 数据在包含移动网络既有数据属性之外，还具备哪些特有属性。

从数据内容特性上来看，5G 数据一方面增加 5G 网络标识属性数据，例如网络切片，另一方面增加面向 5G 的垂直行业的业务数据。

从数据形式上看，具有如下特性：

（1）数据量大，内容丰富。包括消费者生活、工作信息以及 5G 网络承载的我国工业制造、基础设施控制（如电网）等重要领域数据。

（2）数据传播速度更快。为满足局部热点区域网络极高的流量密度需求，5G 网络提供极高的数据传输速率。

（3）数据分散和下沉。为满足 5G 低时延业务等需求，5G 网络用户面数据下沉到网络边缘，贴近应用业务并分散到各个

边缘计算节点。

（4）数据开放。5G 网络能力开放的特性，允许第三方应用服务通过接口调用，访问包括用户位置等信息。

从种类上看，5G 核心网内新增具有个人敏感数据或重要数据种类：

数据种类	内容
UDM	用户标识、鉴权数据、签约数据、UE 上下文
UDR	用户数据、营账/开销户操作日志
AMF	个人敏感 ID、位置信息、UE 上下文、鉴权数据、签约数据
SMF	个人敏感 ID、会话管理数据、签约数据、计费数据
UPF	用户个人信息、流量使用报告、策略规则、业务配置、认证数据
NSSF	切片配置数据
NRF	NFProfile 信息、密钥
SMSF	配置数据、签约数据、位置、用户上下文
PCF	管理面认证数据、签约数据、位置等

2.2 5G 数据安全防护框架

5G 采用的网络切片、服务化架构等新技术带来了新的安全威胁，通过 5G 的应用，传导到应用场景，与应用场景原有的安全问题叠加，带来了新的安全挑战。要保障 5G 场景下的数据安全，就得从源头入手，根据 5G 自身制订特定防护方案。根据《5G 数据安全防护白皮书》[1] 中对数据安全防护框架的定义，数据安全技术防护框架从 5G 通用数据安全、5G 网络数据安全、5G 业务数据安全等多维度进行建设，适用于 5G 各种业务场景的数据安全防护。

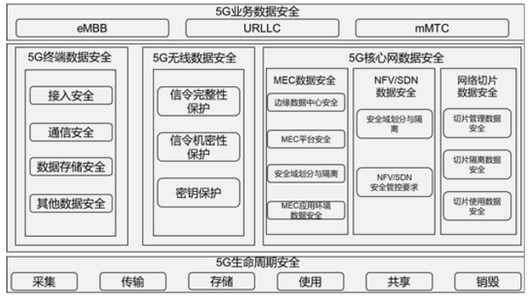


图 1 5G 数据安全防护框架

5G 数据安全防护体系架构包括：

- 5G通用数据安全：数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据销毁安全。
- 5G基础设施安全：物理安全、云平台安全、网络安全。
- 终端设备数据安全：接入安全、通信安全、数据存储安全、其他数据安全。
- 无线数据安全：信令完整性保护、信令机密性保护、密钥保护。
- 核心网数据安全：MEC数据安全、NFV/SDN数据安全、网络切片数据安全。
- 5G业务数据安全：车联网、工业互联网等5G垂直行业数据安全。

2.3 5G 通用数据安全防护措施

针对 5G 数据的防护，宜按照数据采集、数据传输、数据存储、数据处理、数据共享、数据销毁等生命周期各维度进行防护，同时对各个阶段的数据安全风险进行集中检测与预警处置。

- 数据采集安全

①对人、设备、接口强化认证鉴权机制；

②强化人员管理，分类分级防护；

③采集通道做好流向控制和区域隔离。

- 数据传输安全

①加强安全可靠性保障及分类分级管控；

②针对安全域传输，应对敏感信息的传输通道和数据内容进行加密保护和完整性校验。

- 数据存储安全

①差异化安全存储，针对多租户数据的共享存储需求，建立安全策略。

- 数据处理安全

①坚持最小授权原则；

②高风险操作管控；

③接口鉴权和使用监控。

- 数据共享安全

①严格落实内部审批，明确共享责任；

②数据共享设备、接口做好鉴权管理、账号管理。

- 数据销毁安全

①建立针对各种数据销毁场景下的数据销毁管理规章和安全机制；

②落实安全销毁措施，保障数据不可被还原。

图 2 5G 数据全生命周期防护

2.4 5G 核心网数据安全防护措施

5G 核心网较 4G 网络使用了大量的新技术，如 NFV/SDN、网络切片、MEC 等，这些新技术也带来了新的安全威胁和暴露面。因此，针对 5G 核心网的数据安全防护，主要针对 NFV/SDN 数据安全、网络切片数据安全、MEC 数据安全采取防护措施。

- NFV/SDN 数据安全

通过系统安全加固、安全隔离、安全管控等技术手段保障好虚拟化平台安全，通过数据加密存储、完整性校验、数据加密传输等技术手段保障数据传输和内容安全，由于云计算平台的运维特性，须在迁移或单性扩缩过程中采用分布式杂凑算法等网络数据分布式存储的销毁策略与机制。

- MEC数据安全

根据不同敏感级别的数据，针对 MEC 部署差异化的安全策略；对边缘计算环境下的敏感数据出园区、出厂区等行为进行监管、分析与处置；对安全要求高的数据，建设安全传输层协议等加密传输

的方法，防止通信过程中数据泄露。

- 网络切片数据安全

加强切片管理组件的身份信息权限管控、数据访问控制等安全措施；做好切片安全隔离，对高安全要求的行业实施物理隔离；针对不同安全需求的业务提供不同级别的数据传输，选取各种切片隔离机制。

2.5 5G 无线数据安全防护措施

5G 无线数据安全主要针对信令数据安全、数据传输安全、敏感数据安全采取防护措施。

信令数据安全：对于 5G 终端无线接入过程中用户数据和信令数据的安全，可从信令完整性保护、信令机密性保护、密钥保护和抗重放保护等方面进行。

数据传输安全：基于密钥技术在 5G 终端与 5G 基站之间以及 5G 基站与业务管理功能之间进行数据传输加密保护，保障重要信息（用户数据、信令数据）的机密性、完整性。

敏感数据安全：对于无线接入侧的个人敏感信息数据可运用加密算法进行传输加密，避免敏感数据泄露风险。

2.6 5G 业务数据安全防护措施

5G 业务数据安全主要包含通用数据安全和承载在 5G 网络上的垂直行业特定的数据安全两部分内容。5G 业务可明确自己的关键数据清单，针对关键数据清单，做针对性的数据安全防护。

- eMBB业务应用场景安全措施

建立业务流量数据内容监控与识别能力，综合考虑终端与 eMBB 业务服务平台的认证以及传输安全，保障网元间的用户数据传输安全，通过物理隔离或加密手段确保 5G 用户面安全。

- URLLC业务应用场景安全措施

优化安全算法以减少数据传输安全保护所带来的额外开销；采取异构多层接入网络统一认证机制；使用轻便的加密算法，使用并行的加解密。

- mMTC业务应用场景安全措施

分布式身份管理和接入安全认证链条实现快速安全接入，适当地使用轻量级的安全算法、简单的安全协议。

2.7 绿盟 5G+ 数据安全探索

绿盟科技积极在 5G+ 数据安全领域探索，除自身持续投入研究外，还与信通院联合先后成立 5G 安全实验室与数据安全实验室，共同探索 5G 应用场景和应用下的数据安全防护，并在 MEC 数据安全领域获得了一些研究成果。

边缘 MEC 作为 5G 应用承载园区的近源接入点和计算节点，往往面临着多种风险。从 5G 业务层面看，我们需要面对以下安全问题的考验：业务链路（N3、N6）如何保障数据不出园区？如何保障信令链路（N1/N2/N4）没有数据泄露的风险？是否存在通过信令链路攻击园区专网以及内网的可能？如何防范？管理平面是否存在上述风险？信令数据安全如何保障？

绿盟提出基于流量分析的数据安全方案来解决以上问题。通过在 MEC 各节点部署全流量探针，流量镜像的方式采集来自 5G 专网与 5GC 核心网之间的信令流量（N1/N2/N4）以及可能存在的网络流量，管理平面流量，将这些数据接入信令安全网关进行数据安全事件分析，再经过数据处理层的数据关联处理，对数据安全事件进行统计分析及呈现，形成一套信令安全监测、处置系统。通过对 5G 专网与 5GC 核心网之间的信令数据、网络数据、管理平面数据的解析和识别，实现对信令攻击安全事件、网络攻击安全事件、敏感数据泄露事件、非法接入事件等进行安全监测和分析。对网络的实时监测可发现出现安全事件的网元并结合园区资产监测，发现敏感数据泄露风险。

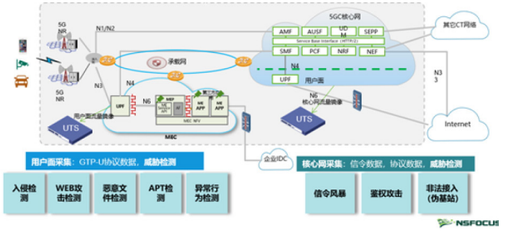


图 3 5G 流量检测数据安全防护方案

3. 结语与展望

5G 应用在国家大力推广下，5G 数据安全也得到了相当多的安全实践。如果把当前以构建 5G 基础设施为核心的应用推广看作 5G 数据安全的上半场的话，那下半场则大概率会是以算力网络为核心的服务体系，算力网络同样会引入新架构、应用新技术、提供新服务，也会带来数据安全新风险，在国家东数西算建设的大前提下，5G+ 数据安全还将迎来更大的发展。

参考文献

[1] 中国通信学会《5G 数据安全防护白皮书》,2022-04-22.

[2] 张滨 .5G 数据安全防护技术研究 [J]. 电信工程技术与标准化 ,2021.

[3] 董宏伟 , 苗运卫 , 袁艺 .《个人信息保护法（草案）》视角下 5G 数据安全的挑战及应对 [J]. 中国电信业 ,2021(1):5.

[4] CCSA 2020-0147T-YD《5G 数据安全总体技术要求（报批稿）》

[5] CCSA H-2020011185《5G 数据安全评估规范（送审稿）》

[6] 西佳平 .5G 网络信息安全威胁及防护技术研究探索 [J].2021.

智慧矿山工业融合安全解决方案设计

绿盟科技 解决方案销售中心 马跃强 云南办事处 肖毅 西藏办事处 库朝才

摘要：随着智慧矿山不断建设，生产环境被打破，网络互联互通，随之而来面临了各种勒索软件、挖矿病毒、黑客、敌对势力等威胁。本文通过对客户存在的资产不清、网络安全看不懂，生产网安全监测预警能力差，云主机缺乏微隔离与防护，通信链路多、数据出口不收敛以及远程访问和远程诊断带来的安全风险等痛点进行分析，并给出了对应的解决方案。

关键词：智慧矿山 网络安全 数据中转缓冲区 监测预警

1. 方案概述

2020 年 3 月，由国家发改委、能源局、煤监局等 8 部委联合印发了《关于加快煤矿智能化发展的指导意见》，意见指出到 2035 年，各类煤矿基本实现智能化，建成能够智慧感知、智能决策、自动执行的安全、高效、绿色煤矿 [1]。

在此背景下，煤矿企业开始进行数字化转型升级，不断加快智慧矿山建设试点示范，但同时也面临了新的挑战，各种勒索软件、挖矿病毒、不法分子甚至敌对势力等威胁对煤矿生产环境进行网络攻击，给煤矿企业带来了巨大的安全隐患 [2]。

2. 客户痛点

主要有以下几点：

①资产不清，网络安全看不懂。本煤矿生产综合自动化系统已运行十余年，工控资产台账陈旧，与实际相差较大。同时，本煤矿在办公内网和互联网区进行了网络安全建设，但由于各安全产品以及安全管理平台，并没有结合业务，以用户的习惯去呈现安全事件，导致用户看不懂、不愿看以及误报多等问题，最终没用起来。

②生产网无防护，安全监测预警能力差。在生产控制网内部，如井下环网、地面环网、调度中心缺少边界防护，私拉网线、违规接入、非法外联现象屡有发生。生产网中缺少威胁入侵、漏洞利用、关键操作等状态监测手段；工控机、SCADA 服务器、数据服务器等主机无恶意代码防范能力，以及无法从整体层面进行集中管理、关联分析、监测感知、研判分析、预警。

③一体化智能管控平台，云主机缺乏微隔离与防护。一体化智能管控平台采用云架构设计，云主机 100+ 个，且缺少东西向流量检测、微隔离以及安全防护机制。

④通信链路多、数据出口不收敛、安全管理难度大。受能源局、煤监局、集团以及随着智慧矿山推进过程中，越来越多的单位、部门需要从生产环境中获取人员定位、安全监视、工业视频、产量等相关数据，导致通路链路多，数据出口不收敛，安全管理难度大。

⑤远程访问，导致相关应用频繁遭受网络攻击。上级领导、生产主管，需要通过办公 PC 机、手机、iPad 等终端设备，远程访问 WEB 和 APP 应用服务器，查看生产状态、安全情况，经常导致相关应用遭受网络攻击，无法正常提供服务。

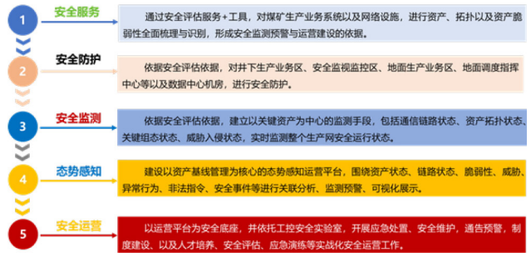
⑥大型生产设备远程诊断，可能导致数据外泄和出境风险。通风机、运输皮带机、采煤机等关键大型生产设备，远程诊断，可能导致产量、工艺图纸、核心控制程序、GIS 以及智能应用的高价值数据，泄露，甚至出境。

⑦安全管理落后。人员安全意识弱、无相应的组织机构、无岗位职责，无体系化安全管理制度和流程等问题。

3. 解决方案设计

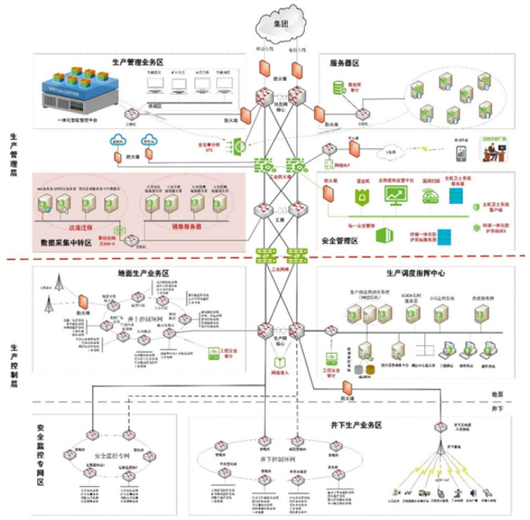
3.1 设计思路

在国家法律法规、政策、标准的框架体系下，从安全技术和安全管理，建设纵深防御体系，设计思路如下：



3.2 整体安全架构设计

依据客户痛点、实施思路以及风险评估报告，进行如下架构设计：



3.3 详细设计

3.3.1 安全服务

通过人工服务 +工控漏扫工具，梳理出的业务系统及资产清单的隶属关系、属性以及脆弱性对应关系，并将每个资产生产 1 个二维码（资产隶属关系、资产属性、资产脆弱性），进行标识、设备粘贴，同时将二维码导入态势感知运营平台中，进行管理维护。

3.3.2 安全防护

首先，针对通信链路多，数据出口不收敛问题，利用工业网闸

和防火墙隔离出一个安全区（数据中转缓冲区），将需要外发的人员定位、工业视频、安全监测等数据镜像到该区；将 WEB 发布、APP 应用服务器以及信息发布系统等服务器迁移到该区。该区作为统一对外转发数据的窗口，加强对该区的重点防护，降低直接对煤矿自动化系统的防护力度。

其次，针对各安全区网络边界，利用现有防火墙，优化访问控制策略；针对井下环网、地面环网等生产网违规接入问题，在生产网核心部署网络准入 1 台，对管理型交换机进行管控；同时对非管理型工业交换机闲置端口进行物理封堵。针对煤矿工业主机，通过部署主机卫士系统，利用工控安全卫士，解决工控主机恶意代码防范能力不强的问题。针对上级领导、生产主管通过办公 PC 机、手机、iPad 等终端设备远程访问生产网 WEB、APP 应用等产生的安全问题，通过零信任技术，在数据中转区，应用服务器前部署零信任安全网关一体机 SDP-U+ 客户端，对网络端口和 WEB 应用进行隐藏，不对外开发一切端口和 TCP 连接，实现对终端进行身份认证，访问行为、过程管控等，解决远程访问带来的安全风险；针对采煤机、通风设备、压缩机等大型生产设备远程诊断，可能导致高价值数据外泄、甚至出境等问题，在生产网到互联网出口处，部署网络 DLP 设备 1 台，对敏感内容、关键词进行检测、过滤、阻断。同时通过管理制度要求，远程诊断定期远程数据文件，不能被加密，确保被 DLP 识别与解析。针对一体化智能管控平台的虚拟机缺乏微隔离及东西向流量检测与防护问题，在虚拟机部署终端一体化防护系统，对虚拟机进行行为检测与防护。同时将虚拟机间的东西向流量牵引到全流量分析设备 UTS，实现对东西向流量检测。针对一体化智能管控平台的数据服务器区，通过部署数据库审计，对用户访问数据库行为，进行记录、分析和告警、溯源追踪等。

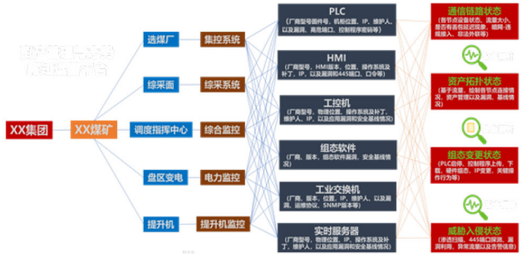
3.3.3 安全监测

在地面生产业务区和生产调度指挥中心各部署工控安全审计设备 1 台，对流经生产综合监控系统的网络流量进行安全监测与审计。

3.3.4 态势感知

新建安全管理区，并建设安全管理网。在安全管理区部署统一管理平台和态势感知运营平台等产品，实现从整体视角进行实时感知、事件分析、研判等，提升煤矿整体安全防护预警水平和运维效率。

同时，提升用户可读性、易用性和误报，对态势感知运营平台与安全探针设备进行如下映射：



通过将资产的隶属关系、属性以及脆弱性与安全探针检测的数据进行关联映射，使可读性增强。让用户一目了然看得懂安全，以及对误报有了判断依据和修正手段，解决用户看不懂和误报问题。

3.3.5 安全运营

首先，进行组织治理。明确了本企业网络安全负责人和管理组织，关键岗位和职责等。

其次，进行管理制度建设。一共制定安全管理办法 7 项，流程 22 个，操作模板 89 个。

最后，进行轻量化安全运营。主要包括如下：资产安全管理、脆弱性管理、威胁管理、应急响应、安全培训等运营工作。

4. 方案价值与亮点

价值 1：解决用户关于网络安全看不懂、用不起来问题

将资产的隶属关系、属性以及脆弱性与安全探针检测的数据，通过 IP 进行关联映射，态势感知运营平台以业务视角和用户习惯方式来呈现安全信息和安全事件，这样使得用户一目了然看懂安全，同时还具备误报的研判和修正机制。

价值 2:应用零信任安全技术，解决远程访问带来的安全风险。

煤矿上级主管单位领导、生产主管人员，需要通过办公 PC 机、手机、iPad 等终端设备，远程访问 WEB 和 APP 应用服务器，查看生产状态、安全情况，导致相关应用频繁遭受网络攻击。通过零信任技术，部署零信任安全网关一体机 SDP-U+ 客户端，对网络端口和 WEB 应用进行隐藏，利用 UDP 的 SPA 单包授权技术，实现先认证后访问，解决远程访问带来的安全风险。

价值 3：利用数据防泄露技术，解决远程诊断带来的高价值数据外泄、出境的问题。

通过在远程诊断网络边界出口，部署网络 DLP 设备，对采煤机、

通风设备、压缩机等大型生产设备远程诊断回传的数据，基于关键字、正则表达式、文档指纹等多种数据识别能力，对敏感内容、关键词进行检测、过滤、阻断。

价值 4：利用微隔离技术，解决一体化智能管控平台和虚拟机间微隔离以及东西向流量检测。

利用微隔离技术，在体化智能管控平台和虚拟机部署终端一体化防护系统，对虚拟机进行行为检测与防护。检测 APT 攻击、勒索病毒、挖矿、僵木蠕、0day 漏洞等已知和未知威胁，同时将虚拟机间的东西向流量牵引到全流量分析设备 UTS，实现对东西向流量安全检测。

亮点 1：资产映射管理

通过资产梳理，将每个资产的隶属关系（集团—二级单位—煤矿—矿井—系统），资产属性（物理位置、品牌型号、使用人 / 运维人 / 责任人、联系电话、资产编号、IP、数据流向等），资产脆弱性（139、445、3389 高危端口、弱口令、默认共享等安全配置基线以及漏洞），与二维码进行关联，并进行粘贴。同时在态势感知运营平台进行管理，形成数字空间与物理空间的映射。

亮点 2：数据中转缓冲区理念

通信链路多、数据出口不收敛问题，设计了数据中转缓冲区理念。利用工业网闸和防火墙隔离出一个安全区（数据中转缓冲区），将需要外发的人员定位、工业视频、安全监测等数据镜像到该区；将 WEB 发布、APP 应用服务器以及信息发布系统等服务器迁移到该区，该区作为统一对外转发数据的窗口，重点加强对该区的安全防护建设，从而降低对生产控制系统进行安全防护带来的影响。

5. 参考文献

[1] 牛世刚 , 关于井下矿山建设智慧矿山的思考 [J], 新疆钢铁 ,2019,3(151):53-56.

[2] 赵华山 , 高斌 , 如何加强煤炭企业信息基础设施保护与网络安全等级保护制度的有效衔接 [J], 电子元器件与信息技术 ,2020,4(5):31-34.

为什么云原生环境下需要零信任安全

绿盟科技 创新研究院 刘文新

摘要：云原生化大势所趋，云原生帮助企业快速构建高度可扩展、灵活且具有弹性的应用。由于云原生动态、无固定安全边界的特性，传统安全策略已无法适应云原生环境。而零信任安全的核心是持续地身份验证和授权，这种基于身份验证和授权的安全策略能够更加细致地管理和监控每一个访问请求，更好地适应系统的动态性和多样性。零信任安全为安全策略提供了更大的灵活性和可扩展性，能够有效地降低安全风险，降低企业 IT 成本，提高访问灵活性，以适应不断演变的云原生环境。

关键词：云原生 零信任 网络安全

1. 零信任安全是什么

零信任安全不是一种特定技术、产品，而是一种基于“不相信任何人”理念的安全模型。Forrester[1] 将零信任定义为“默认情况下拒绝访问应用程序和数据的信息安全模型。威胁预防是通过仅使用策略授予对网络和工作负载的访问权限来实现的，并通过跨用户及其相关设备的持续、上下文、基于风险的验证来通知”，包含以下四个原则：

最小化信任：假设任何用户、设备、应用程序不可信，将所有请求视为潜在的威胁，并进行验证和授权。

多重身份验证和授权：使用多因素验证用户、设备、程序身份，进行细粒度的授权，使其只能访问所需的资源和数据。

实时监控和审计：实时监控和审计所有用户、设备和程序行为，及其访问的资源和数据。

动态安全策略：安全策略随用户、设备、数据及外部风险的变化动态更新。

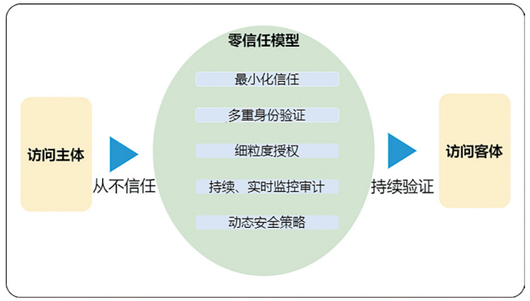


图 1 零信任安全模型中的访问过程

2. 云原生环境特点

云原生环境是一个现代化基础架构，面向云计算基础设施及应用程序，倡导以容器为核心的轻量级应用程序开发和交付模式。它具有以下特点 [2]：

- 容器化：云原生环境以容器技术为核心，将应用程序及依赖打包进容器，实现跨平台运行和快速部署。

• 自动化：云原生环境倡导自动化，包括自动化部署、自动化扩缩容、自动化监控等，以提高效率，降低成本。

• 弹性伸缩：云原生环境具有弹性伸缩能力，可以根据负载和需求实时增加或减少资源，以应对不同的业务场景。

• 微服务架构：云原生环境以微服务架构为基础，将程序拆分成独立微服务，并通过轻量级的通信机制通信，提高灵活性、可伸缩性及可维护性。

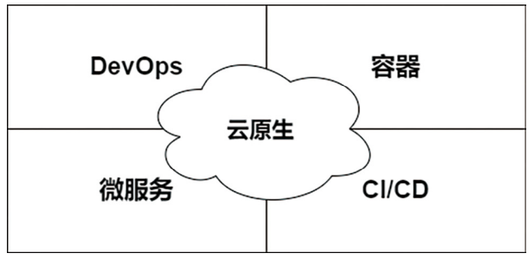


图 2 云原生环境

3. 为什么云原生环境下需要零信任安全

由于云原生环境具有动态、容器化、微服务等特点，传统的边界型安全防护策略已无法完全适应。云原生环境下安全防护策略面临以下挑战[3-4]：

• 网络安全边界消失：传统网络架构中的网络安全边界通常由防火墙、网关等硬件设备实现。随着公有云、私有云及混合云技术的发展，云原生程序可能被部署到任何地方，甚至跨越多个云服务提供商和地区，传统的安全边界正在消失。

• 不可信因素增多：云原生环境中，容器的数量和位置不断变化，其运行状态会因外部攻击、软件缺陷等原因异常，这将对云原生环境的安全产生不利影响。此外，云原生应用程序在自动化部署、管理过程中依赖多种开源工具，越多的工具意味着其中的不可信因素数量越多。

• 统一授权机制复杂：云原生应用通常由运行在不同容器中的微服务构成，这意味着每个微服务需要配置不同的身份认证、鉴权、授权机制，并确保它们之间的相互作用是安全的。此外，云原生环境下通常使用多种技术栈来构建和部署应用程序，需要为每个技术栈配置不同的身份验证和授权机制。

• 基础设施共享的复杂性：云原生应用的部署和运行可能需要依赖同一组计算资源、存储资源、网络资源等。为了提高资源利用效率，对这些资源进行了多层次的管理和共享。在管理和共享的过程中容易出现越权、资源挤兑等问题，影响其他正常服务运行。

• 数据安全和合规性要求：云原生应用程序的部署和运行可能会跨越不同的安全域，数据安全和合规性有了更高的标准，如《个人信息保护法》[5]、GDPR[6]、PIPEDA[7]等。

• 综上，云原生环境中需要一种更为灵活、精细、可扩展的安全模型——零信任。零信任安全模型的本质诉求是以身份为中心的访问控制，它引导安全体系架构从网络中心化走向身份中心化，建立更加高效、全面、灵活的安全防御体系，减少云原生环境中的攻击面，降低云原生环境中的安全风险，增加访问控制的细粒度，避免信息、数据泄露等。

4. 云原生环境下的零信任安全实践

云原生环境下零信任安全实践可从以下几个方面开展[8-9]：

• 云原生环境资产清点：资产清点能够及时发现未知或未授权的资产，确定哪些资产应该被授权或禁止访问，提升云原生环境的安全性和可控性。

• 最小权限原则：限制用户和云原生服务的访问权限，确保其只能访问所需的资源和数据，以降低攻击面和减少潜在的攻击风险。

• 精细的访问控制和授权机制：采用强制、精细的身份认证和授权机制，如多因素身份验证（MFA）和单点登录（SSO），能够减少未授权的访问。

• 数据加密：云原生应用程序通常需要处理敏感数据，在数据存储、传输和处理过程中均需要使用加密和解密技术，以确保数据安全。此外，也需要采用安全的密钥管理和分发策略，确保密钥安全。

• 风险面和威胁管理：云原生环境会依赖其他开源组件、框架，这些组件、框架或多或少会存在漏洞和安全风险。通过实施云原生环境下的风险面管理，能够减少开源组件、框架带来的安全风险。

• 持续安全监控和审计：持续的安全监控和审计可确保用户、服务对敏感数据和应用访问的合法性，实时监控潜在的威胁，降低未授权访问的危险。

• 凭证自动化轮换：自动化的凭证轮换可以减少人为错误和疏漏，降低凭证泄露、被盗窃带来的安全风险。在勒索软件事件频发的现在，这点尤为重要。

• 动态的安全策略：安全风险日益增加，需要可动态更新的安全防护策略，以应对层出不穷的安全威胁。

• 安全培训：对员工进行定期的安全培训，帮助员工了解安全风险和防范措施，可以有效提高企业的整体安全水平。

5. 总结

由于云原生环境动态、无固定安全边界等特性，传统安全策略无法有效解决云原生环境下的诸多安全问题。零信任安全模型的核心原则是身份验证和授权，只有经过验证和授权后的设备、用户才能访问特定的资源。以身份为核心的零信任安全模型可以更加动态、精细、有效地解决一些传统安全策略无法解决的问题。但是，零信任安全模型仍无法完全替代传统安全策略，应结合两者构建具备“纵深防御”能力的安全体系，多角度、全方位地保护服务、数据、网络及系统的安全。

参考文献

[1] https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/

[2] https://www.simplilearn.com/cloud-native-application-article

[3] https://www.suse.com/c/rancher_blog/zero-trust-the-new-security-model-for-cloud-native-applications-and-infrastructure/

[4] https://thenewstack.io/why-the-castle-and-moat-approach-to-security-is-obsolete/

[5] http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[6] https://gdpr.eu/what-is-gdpr/

[7] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda

[8] https://knowtechie.com/how-to-implement-zero-trust-security-in-your-cloud-native-environment/

[9] https://thenewstack.io/why-cloud-native-systems-demand-a-zero-trust-approach/

网络安全政策导读

绿盟科技 总体技术部 林涛 张文辉

栏目说明：

本专栏基于绿盟科技团队在网络安全政策法规方面的日常跟踪，筛选国内外近期热点政策法规文件，并重点结合网络安全产业发展，对其内容和影响等进行分析。

本期研究的国内外政策法规的发布时间为 2023 年 8 月－ 9 月。

限于篇幅，本文仅刊载部分篇目，完整内容请关注“网络安全罗盘”和“绿盟科技”微信公众号。

1. 国内篇

1.1 工业和信息化部发布《关于开展移动互联网应用程序备案工作的通知》，启动移动互联网信息服务准入管理

【内容概述】2023 年 8 月 8 日，工业和信息化部发布《关于开展移动互联网应用程序备案工作的通知》（以下简称《通知》）。《通知》适用于在中国境内从事互联网信息服务的 APP 主办者。《通知》规定，APP 备案通过 APP 主办者在填写有关备案材料并实名核验后，由其网络接入服务提供者或应用分发平台通过“国家互联网基础资源管理系统”（ICP/IP 地址 / 域名信息备案管理系统），向 APP 主办者住所所在地通信管理局在线提交备案申请。

【导读分析】APP 备案是移动互联网监督管理的一项重要制度，其意义堪称移动互联网领域的“网站备案”。该监管机制源于《中华人民共和国反电信网络诈骗法》第二十三条“设立移动互联网应用程序应当按照国家有关规定向电信主管部门办理许可或者备案手续”。本次《通知》的发布旨在落实《反电信网络诈骗法》的规定，并进一步细化移动互联网应用程序备案制度相关要求。除了申请备案需提交相关资料外，《通知》尤其开宗明义地明确了“未履行备案手续的，不得从事 APP 互联网信息服务”。可见，对“APP 主办者”而言，备案是从业的“起始动作”，否则无法开展相关业务。与此同时，从《通知》的立法依据来看，《互联网信息服务管理办法》（国务院令第 292 号）将是实施备案工作的重要操作准则之一。

对网络安全行业来说，有两点需要重点关注。一是备案实施工作中的能力匹配和保障，如支撑相关备案实施机构强化数据安全监测和防护、开展相关突发事件的应急处置等。二是密切关注相关法规的修订衔接，《互联网信息服务管理办法》（国务院令第 292 号）上次修订距今已超过十年，此间已有多部有关移动互联网监管的法规和政策文件发布，如《移动互联网应用程序信息服务管理规定》，等等。如何强化这些法规政策间的协调衔接，或将是备案领域法规清理的一项重要工作。

1.2 国家认证认可监督管理委员会发布《关于修订〈网络关键设备和网络安全专用产品安全认证实施规则〉的公告》，相关安全认证工作迎来重大更新。

【内容概述】2023 年 8 月 10 日，国家认证认可监督管理委员会发布《关于修订〈网络关键设备和网络安全专用产品安全认证实施规则〉的公告》（以下简称《公告》）。《公告》规定，此前已经颁发的有效安全认证证书可继续使用，证书转换工作采取到期换证、产品变更、标准换版等自然过渡的方式完成。同时发布的还有修订后的《网络关键设备和网络安全专用产品安全认证实施规则》（以下简称新版《实施规则》），自发布之日起实施。

【导读分析】长久以来，网络安全产品重复检测认证问题是有关部门着力解决的困扰企业发展的突出问题之一。此前，国家网信办已会同有关部门先后发布了《关于调整网络安全专用产品安全管理有关事项的公告》《网络关键设备和网络安全专用产品目录》等政策文件，分别就检测认证工作机制衔接、产品范围等问题做出专门规定。本次《公告》的发布，对实施规则进行了明确，又朝着优化并推进认证工作迈出了坚实一步，也为后续认证工作的实际落地奠定了基础。

与 2018 版《实施规则》相比，新版《实施规则》在认证模式、认证流程、认证时限等方面进行了全面更新。如认证模式减少“工厂检查”环节，变为“型式试验 + 获证后监督”；认证流程将“认证申请及受理、文档审核”等简化为“认证委托”程序；认证时限由 90 个工作日缩短为 60 天等。此外，该规则还要求认证机构编制认证实施细则，包括细化监督频次、评价内容及评价方式等方面。

统一检测认证事关产品资质，因此《信息安全技术 网络安全专用产品安全技术要求》（GB 42250）、《网络关键设备和网络安全专用产品目录》等相关要求的落地，以及后续或将出台的相关检测认证实施细则、机构管理办法等，都无疑会成为引导网络安全厂商乃至网络安全产业发展的重要风向标，值得认真学习领会。

1.3 全国信息安全标准化技术委员会发布《信息安全技术 网络安全保险应用指南》（征求意见稿），推进网络安全保险规范化

【内容概述】2023 年 9 月 13 日，全国信息安全标准化技术委员会发布《信息安全技术 网络安全保险应用指南》（征求意见稿）（以下简称《征求意见稿》）。《征求意见稿》概述了网络安全保险的概念、作用和主要应用阶段，提出了网络安全保险应用各阶段的流程和方法。该文件适用于指导采用网络安全保险转移风险的组织，也可为保险人和服务方提供参考。

【导读分析】伴随数字经济的蓬勃发展，企业面临越发严峻的网络安全威胁态势，网络安全保险新业态应运而生。近年来，我国积极探索网络安全保险管理体制建设，出台了相关政策文件。2021 年 7 月，工信部在《网络安全产业高质量发展三年行动计划（2021—2023 年）》（征求意见稿）中明确提出，要“探索开展网络安全保险，开展网络安全保险服务试点，加快网络安全保险政策引导和标准制定”；2023 年 7 月，工信部、国家金融监管总局联合印发《关于促进网络安全保险规范健康发展的意见》，提出了网络安全保险标准体系的基本构成，包括：网络安全保险行业术语规范、

风险量化评估标准、监测管理服务标准、理赔实施标准等。

《征求意见稿》是网络安全保险领域的首个国家标准（稿），该稿主要从风险管理角度描述了网络安全保险中各方的主要行为及网络安全保险的基本流程。对于推进网络安全保险的落地实施勾画了基本框架。而对于网络安全保险中的风险量化、检测管理、理赔实施等重点内容，或将成为网络安全保险标准领域未来关注的核心问题。

对网络安全行业来说，《征求意见稿》或将为推动网络安全产业发展带来新机会。一是服务于保险人，开展保险标的风险评估和风险控制，包括风险量化评估产品、风险监测预警工具的开发等。二是服务于被保险人，开展风险整改及发生网络安全事件时提供应急响应和技术取证等。三是由网络安全保险政策标准制订、生态机制建设等带来的衍生类市场需求，如咨询规划、方案设计服务等。

1.4 国务院常务会议审议通过《未成年人网络保护条例》，强化未成年人特殊群体的网络保护

【内容概述】2023 年 9 月 20 日，国务院第 15 次常务会议通过《未成年人网络保护条例》（以下简称《条例》）。《条例》共 7 章 60 条，旨在营造有利于未成年人身心健康的网络环境，保障未成年人合法权益，将于 2024 年 1 月 1 日起施行。

【导读分析】随着移动互联网的普及发展，未成年人使用互联网的比例迅速提升。与此同时，网络攻击、个人信息滥用等传统网络安全问题也加速向未成年人群体扩散。国家网信部门将未成年人网络保护工作列入部门重要监管任务之一，并组织开展“清朗·2023 年暑期未成年人网络环境整治”等专项行动。此前发布的《未成年人保护法》《关于规范网络直播打赏 加强未成年人保护的意见》《移动互联网未成年人模式建设指南（征求意见稿）》等政策法规，均对未成年人网络保护提出相应要求。本次《未成年人网络保护条例》以行政法规的形式出台，进一步明确了相关要求，也体现出党中央、国务院对未成年人网络保护工作的高度重视。

2022 年 3 月，国家网信办发布《未成年人网络保护条例（征求意见稿）》（以下简称《征求意见稿》）。与《征求意见稿》相比，《条例》主要有以下 3 方面修改。一是进一步明确相关管理制度和依据，如明确授权制定“网络平台服务提供者认定办法”等；二是加强与《个人信息保护法》等上位法制度衔接，如与《个人信息保护法》中“网络产品和服务提供者不得通过自动化决策方式向未成年人进行商业营销”等规定衔接；三是加强新兴技术手段应用，如要求网络产品和服务提供者采用人工智能、大数据等技术手段和人工审核相结合的方式加强对网络欺凌信息的识别监测等。

对网络安全行业来说，在未成年人网络安全保护方面有以下业务机会值得重点关注。一是定制开发针对未成年人的上网行为安全管理产品，加入防沉迷、过滤有害信息等功能。二是与政府主管部门、学校、专业机构合作，开发针对未成年人网络安全意识培训的课程或者配套安全培训服务。三是在个人信息保护解决方案的基础上，结合相关法律法规的具体化要求，制定针对未成年人等特定人群的隐私保护解决方案。

1.5 中央网信办发布《云计算服务安全评估专业技术机构》，持续完善云计算服务安全评估机制

【内容概述】2023 年 9 月 25 日，中央网络安全和信息化办公室（以下简称“中央网信办”）发布《云计算服务安全评估专业技术机构》（以下简称《技术机构》）。新版《技术机构》在原有的国家信息技术安全研究中心、中国信息安全测评中心、中国信息通信研究院、中国电子技术标准化研究院等 4 家评估机构基础上，又增加了 4 家机构，分别是国家计算机网络与信息安全管理中心、国家信息中心、中国电子科技集团公司第十五研究所、国家工业信息安全发展研究中心。此外，中央网信办还公布《云计算服务安全评估专家组成员名单》，共 23 人入选。（原文链接：http://www.cac.gov.cn/2023-09/25/c_1697301645483790.htm）

【导读分析】2019 年 7 月，国家互联网信息办公室、工业和信息化部等四部门联合印发《云计算服务安全评估办法》，旨在“提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平”。云计算服务安全评估的一般流程是：申报—受理—专业技术机构评估—专家组评价—协调机制审议—网信办核准—发布—持续监督。截止到 2023 年 7 月底，通过云计算服务安全评估的云平台已有 70 余家。

云计算服务安全评估由国家市场监管总局下属的中国网络安全审查技术与认证中心牵头组织开展，最初专业技术机构有四家。此次专业技术机构新增四家，或主要反映两方面情况：一是云计算安全评估业务量增长的需要；二是与目前的“云计算服务安全评估工作协调机制”“专家组”机制等相适应。

对网络安全行业来说，云计算服务安全评估或将带来以下两方面市场机遇。一方面，服务于云服务提供商，开展云计算服务系统安全自评，提供云安全相关技术产品和服务支撑等。另一方面，服务于云安全评估机构，提供专业安全技术、工具支持、开展云平台威胁情报监测等。

2. 国外篇

2.1 美国网络安全和基础设施安全局发布《2024—2026 财年网络安全战略规划》，落实顶层规划要求

【内容概述】2023 年 8 月 4 日，美国网络安全和基础设施安

全局（CISA）发布《2024—2026 财年网络安全战略规划》（CISA Cybersecurity Strategic Plan FY 2024—2026）（以下简称《战略规划》）。《战略规划》旨在落实 2023 年《国家网络安全战略》及《2023—2025 财年 CISA 战略规划》提出的有关要求，为 CISA 履行网络安全保护责任及提升网络安全能力提供指导。

【导读分析】近年来，美国政府高度重视网络安全顶层设计，加紧制定一系列网络安全相关战略，如《国家网络安全战略》（美国白宫）《国家网络安全战略实施计划》（美国白宫）、《2023 年国防部网络战略》（美国国防部）等。

本次发布的《2024—2026 财年网络安全战略规划》，不仅是落实联邦政府相关网络安全顶层设计的部门举措，也是明确网络安全工作方向的重要载体，具有对内和对外两方面作用。对 CISA 内部来说，该规划将作为实施、投资和运营计划的蓝本，并将通过年度工作计划进一步分解执行；对外部组织来说，该计划将帮助利益相关方了解并参与 CISA 长期网络安全规划和优先事项。

总体来看，《战略规划》明确了 CISA 未来 3 年网络安全工作的重心，可成为外部评估美国网络安全战略动向的一个重要参考。同时，其提出的强化协同和生态发展的思路和举措，对于完善我国网络安全保障体系也具有一定的参考意义。

2.2 美国国家标准和技术委员会发布《网络安全框架 2.0》草案，加强网络安全风险管理

【内容概述】2023 年 8 月 8 日，美国国家标准和技术委员会（NIST）发布《网络安全框架 2.0》（Cybersecurity Framework 2.0）草案（以下简称《框架 2.0》）。《框架 2.0》旨在帮助行业、政府机构和其他组织更好地理解、评估和部署其网络安全工作。

【导读分析】伴随新形势下网络安全风险的变化，NIST《网络安全框架》也随之进行动态更新。2014 年 2 月，NIST 发布《改进关键基础设施网络安全框架》（《框架 1.0》）；2018 年 4 月，NIST 发布《框架 1.1》版本；2023 年 4 月，NIST 发布《框架 2.0》核心讨论草案。

本次发布的《框架 2.0》主要对《框架 1.0》进行了如下三方面的更新。第一，扩大了覆盖范围。《框架 2.0》直接更名为“网络安全框架”，此前两个版本的官方名字都是以关键基础设施为对象，体现该框架进一步扩大了适用范围。第二，强化网络安全治理。在《框架 2.0》中，“治理”调整到与其他的 5 个核心功能平级，反映了美国政府对于网络安全治理的重要性认知。第三，强调供应链风险管理。《框架 2.0》提供了更多关于如何评估和管理供应链中的安全风险的内容，反映了美国政府日益加强对供应链安全的重视程度，并致力于从供应商和合作伙伴处获取的产品和服务的安全性。

《框架 2.0》是网络安全不断适应环境变化和各方最新需求的体现，也反映出美国政府通过扩大标准适用范围，来推进其网络安全国内标准国际化的意图。网络安全标准化建设一向是我国网络安全保障体系和能力建设的重要工作内容，而就目前来看，我国尚未出台指导用户做好网络安全举措的一般性操作指南和规范。《框架 2.0》在此方面对于我们具有参考价值。

2.3 美国网络安全和基础设施安全局发布《为供水公司提供免费的网络漏洞扫描》情况说明书，加强供水关键基础设施信息安全

【内容概述】2023 年 9 月 11 日，美国网络安全和基础设施安全局（CISA）发布《为供水公司提供免费的网络漏洞扫描》（*Free Cyber Vulnerability Scanning for Water Utilities*）情况说明书（以下简称《情况说明书》），旨在识别和解决饮用水和废水处理系统漏洞，降低供水系统遭受网络攻击的风险。

【导读分析】供水系统事关民众基本生活，近年来针对城市供水系统的网络攻击日益增加，如以色列中部供水设施遭遇国家级黑客组织网络攻击、美国佛罗里达州自来水厂系统遭黑客入侵等。美国政府此前开展一系列监管行动审查供水行业网络安全，如针对水和废水部门的百日行动计划、环境保护署提高公共供水系统的网络安全弹性专项行动、NIST 提出《确保水和污水公共服务的安全：水和污水系统部门的网络安全》草案等。

“水及污水处理系统”是美国政府认定的 16 类关键基础设施部门之一（奥巴马总统行政令 PPD-21，2013）。在水及污水处理网络系统中推行免费漏洞扫描服务，是美国加强水及污水处理系统关键基础设施安全的一项重要举措。

对此，一方面，我国的水及污水处理系统是否属于关键信息基础设施范畴值得主管部门深入探讨和研判；另一方面，在关键信息基础设施系统推行免费漏洞扫描的机制，或可为我国关键信息基础设施保护带来思考借鉴。此外，对于网络安全行业而言，美国的这种做法无疑也是潜在拉动网络安全需求的一种实践。

2.4 美国国防部发布《2023 年国防部网络战略》摘要，延续“以攻为守”网络安全思想

【内容概述】2023 年 9 月 12 日，美国国防部发布《2023 年国防部网络战略》摘要（*2023 Cyber Strategy of the Department of Defense*）（以下简称《2023 战略》）。《2023 战略》概述了美国国防部如何最大限度地发挥其网络能力，以支持综合威慑，并与其他国家力量工具协同运用于网络空间行动，并明确提出了该战略的总体优先事项。

【导读分析】美国于 2011 年发布了首份《国防部网络空间行动战略》（*Department of Defense Strategy for Operating in Cyberspace*），此后又发布了《2015 年国防部网络战略》《2018

年国防部网络战略》。《2023 战略》贯彻了美国网络安全战略的“综合威慑、国际合作、投资引领”等指导思想，并对美国国防领域的具体网络行动进行了明确，如开展前出防御（Defend Forward）、前出狩猎（Hunt Forward）等。

《2023 战略》反映出美国网络军事化的两个特点。一方面，进一步强化“以攻为守”的网络安全策略。《2023 战略》体现出更强的“进攻性防御”属性，后续或将对美国国防领域网络安全的监管方式、合作路径等方面产生影响。另一方面，网络安全对产业、外交等领域的溢出效应将持续显现。《2023 战略》所涉及的网络安全重点领域建设方向、管理思路等，可能引起相关国家效仿；而在网络安全建设管理模式、技术路线和重点工作等方面的趋同，反过来也会强化以美国为首的国防、网络、技术乃至外交领域同盟、联盟的发展。

美国防部每年发布的网络战略可以视为其网络空间军事化发展的一个风向标。从中，不仅可以观察美军的网络武器储备、网络攻防技术研发等领域的大致情况，也能对其发展目标、战略布局、重点工作和举措等有一个大概的了解。对于我国业界的产品技术创新、市场前瞻等相关研究也能起到一定参考作用。

2.5 欧盟《数据治理法案》正式施行，为欧盟提供数据共享新模式

【内容概述】2023 年 9 月 24 日，欧盟《数据治理法案》正式施行。《数据治理法案》旨在促进整个欧盟内部和跨部门之间的数据共享，并为主要技术平台的数据处理实践提供一种新的欧洲模式，帮助释放人工智能的潜力。

【导读分析】《数据治理法案》于 2020 年 11 月正式提出，并于 2023 年 6 月达成政治协议（political agreement），是落实《欧洲数据战略》的重要立法举措之一，进一步革新了欧洲数据治理模式，旨在为欧盟打造统一的数据市场，使欧盟科技企业能够更为有效地转化和利用数据。

我国正在全面推进数字战略，数据要素作为一种战略资源的重要价值也日益凸显。欧盟《数据治理法案》所提出的建设数据中介机构的思路，对于我国构建和完善数据要素开发利用机制具有借鉴意义。我国目前在促进数据开发利用方面，以规范数据合法、合规利用为侧重点，在发挥第三方中介力量问题上也较多同数据交易平台的建设发展相关联。下一步如何充分发挥第三方中介尤其是非盈利组织的作用，促进和完善数据开发层面的良性发展，或是一个具有较大意义的新研究方向。

NSFOCUS

绿盟数据安全检查工具箱

NSFOCUS Data Security Inspection Toolkit

主动检查，快速发现数据安全风险。
自检自查，评估自身数据安全隐患。

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、金融、运营商、能源、交通、科教文卫等行业用户和各类型企业用户，
提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的后面，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技