网络空间安全工程技术人才培养体系指南

（综合版）

中国网络空间安全人才教育论坛

二〇二四年八月

编 委 会 主 任：方滨兴

编委会副主任：贾　焰 田志宏

执 行 编 委：王　乐 鲁　辉 崔　翔

本版编写单位：

广州大学

杭州安恒信息技术股份有限公司

安天科技集团股份有限公司

北京神州绿盟科技有限公司

北京天融信网络安全技术有限公司

任子行网络技术股份有限公司

（以上单位按参编内容量和名称字母序排列）

版权声明

免责声明

本指南仅供参考。对于本文档中的信息，网教盟及编写单位不作明示、默示保证。在指南中的信息和意见，均可能会改变，不另行通知。您需自行承担使用风险。

词汇说明

文中“网安人才”特指网络空间安全工程技术人才。

引 言

网络空间作为人类社会生存和发展的新空间，成为了“陆、海、空、天、网”中的第五维新疆域，网络空间安全进入到国家战略强势介入的全新阶段。

面对我国目前对有实践经历和实战能力的网络空间安全工程技术人才（以下及正文简称“网安人才”）需求缺口巨大、需求增速不断加快的现实，中国网络空间安全人才教育论坛汇聚成员单位提出了我国网安人才知识及能力框架并持续改进，在《网络空间安全工程技术人才培养体系指南》（以下简称“指南”）中对框架的网安人才层次化体系、知识技能体系、培养体系等主体部分进行了论述。其中的“知识技能体系”，按照从业人员业务标签这一全新角度，参考学科专业体系，对网安人才的知识技能进行了梳理，突出以“人”为核心、以“业务内容”为标签、以“知识技能”为内容，为网安人才培养、考核、认证以及招聘等提供参考。

“指南”前期采取迭代补充更新的发布方式，完成了4个版本共14 个一级标签的知识技能体系的梳理。本次“综合版”是在前序版本（1.0、2.0、3.0、4.0）基础上修订编写而成，完善了已有 14 个一级标签并新增“人工智能安全”一级标签，形成了 15 个一级标签、123 个二级标签的知识技能体系。

本指南（综合版）的设计和编写是由中国网络空间安全人才教育论坛发起，广州大学受托组织统编。

目 录

第一章 网络空间安全人才培养的特殊性

1.1 网络空间安全特性

网络空间安全涉及在网络空间中电磁设备、信息通信系统、运行数据、系统应用中所存在的安全问题，即设备层安全、系统层安全、数据层安全和应用层安全。其中，设备层安全需应对网络空间中信息系统设备所面对的安全问题，包括物理安全、环境安全、设备安全等；系统层安全需应对网络空间中信息系统自身所面对的安全问题，包括网络安全、软件安全等；数据层安全需应对在网络空间中处理数据的同时所带来的安全问题，包括数据安全、身份安全、隐私保护等；应用层安全需应对在信息应用的过程中所形成的安全问题，包括内容安全、应用安全等。

由于网络信息技术所具有的支撑和工具特性，以及安全问题的伴随本性，网络空间安全具有与生俱来的伴生性。一项网络信息技术的诞生之日，就无法避免地催生出其可能存在的安全问题，随着技术的发展和应用，其安全问题也会逐渐引起人们关注、得到研究和重视。因此，伴生性是网络空间安全的本质性特征之一。

网络空间本身涉及到物理空间的电磁信号、信息设备、运行环境，逻辑空间的软件、数据、信息，虚拟空间的身份、隐私、行为等不同空间维度的不同层次类型的对象；不同对象的安全问题及安全技术之间，具有复杂交错的关联关系。因此，交叉性是网络空间安全的另一个本质特征。

安全问题本质上是一种博弈关系，存在于人与人、人与自然乃至自然事物之间。网络空间的安全也符合这一客观规律，并且由于网络空间是人类基于网络信息技术构建的集物理、逻辑、虚拟于一

体的复合空间，其所展现的博弈关系更多体现在人与人之间，以及人所基于的网络信息技术或工具而进行的“人+技术”的对抗，包括行为对抗和认知对抗。因此，对抗性也是网络空间安全的本质特征之一。

综上，网络空间安全是伴随着网络信息技术的出现、发展和应用而出现和发展的，新的网络信息技术必然会丰富网络空间安全的内涵、拓展其外延；而网络空间安全在内容逻辑上，具有极强的交叉关联关系，强化了其技术范畴的交错关联性；由人类的构建和交互行为打造的网络空间，其安全问题在本源上形成于人与人之间的行为和认知对抗，需要用博弈对抗的视角审视和应对。

1.2 网安人才培养的特殊性

（1）安全保障强技能

物理世界中的安保人员追求身强力壮，拼的是体力，物理世界的军人首先要求具备过硬的身体素质。网络空间的安保人员追求 IT 技能高超，拼的是智力，网安工程技术人才作为网络空间的“捍卫者”，首先要求具备娴熟的网络攻防技能。这种断崖式的安保人才门槛，导致了网络安全人员的紧缺。

（2）攻易防难非对称

物理世界的攻击者和攻击手段具有鲜明的局域特点，单点攻击只引发局部防范，区域戒备就可以解决问题。网络空间攻击可以直接扫描国际互联网或间接触及任何“物理隔离”的目标网络，单点攻击会引发全球防范，防御人员的需求规模与系统规模成比例关系，攻击者则与规模无关。网络攻击者的培养相对简单，重在实践；网络防御者的培养过程复杂，需要理论与实践结合。攻易防难的非对称性，加重了网安工程技术人才尤其是高层次防御人员培养的难度。

（3）触及法律高风险

网络攻击技能的培养如同武术技能的传授，受训者的自律程度成为造福人类还是危及社会的分水岭。与武术技能的提高相同，网络攻防的技术能力建立在不断实践的基础之上，闭门造车无法真正提高实战能力。如何在不断“挑战高手”的同时避免触及法律红线是难以两全的问题。

（4）技能学术弱关联

攻击技能可以通过经验的积累而迅速提高，但防范能力则需要深厚的理论积累，尤其是对利用非配置漏洞而发起的攻击的防范，简单的实践不能掌握其要领。因此，技能型人才不一定依赖学术水平，技能与学术没有直接的强相关性。攻击能力往往呈现实践性，防御人才往往首先呈现学术性，两种人才培养不尽相同。

（5）宿主技术后伴生

任何新兴的网络空间技术所对应的安全技术一定是与相应的网络空间技术相伴生的，新兴网络空间安全技术本质上是寄生在新兴宿主网络空间技术之上，不了解所要保护的网络空间技术，就不可能了解相应的网络空间安全技术。任何新兴网络空间安全技术出现之后，一定会存在相应的安全问题，因此，也一定会伴生出现相应的新型网络空间安全技术。

（6）技能水平难鉴别

由于社会上对安全人才需求与供给关系严重失衡，因此存在大量的转行人才。网络安全技能缺少显式的展现方法，一般机构难以通过简单的卷面测试、短时的面试考核等方法判断出一名网安人员的技能水平，使得急需网安人才的机构面临两难的境地。

1.3 网安工程技术人才培养体系

目前，国内网安人才成长主要包括院校教育、职业培训、自学成才三种渠道。其中，院校教育包括普通大学、高职高专、民办高校等以学校为单位组织的网安人才培养形式，内涵上包括其培养目标、课程体系和培养模式等。院校培养体系在人才培养路线上一般具有系统化、理论化和学术化等特点，需着重根据网安人才的特殊性和人才需求特点，结合培养机构人才出口、去向等个性情况，强化层次化、方向化的实践教学和实战能力培养。

职业培训和自学成才包括用人单位组织的有计划的定制化在岗培训、网安职业培训机构面向社会个体人员的方向性、层次化的网络安全工程技术和技能的培训，以及社会个体参照方向性的考核认证内容、自学实训计划、实训实践指南等进行的层次化分级、兴趣型分类自学实践。这些培训或自学具有目标性强但系统性不足、短期内见效但成长性不足等特点，需要根据国家网络空间安全战略规划、网络空间安全学科内容、网安知识技能体系等客观性和科学性要求，进行层次化、体系化规范和指导。

根据上述分析，通过不同渠道成长的网安人才，其在学习的方式、路线、周期、手段等方面，有较大的差异；另外，国家和社会的行业、单位、岗位的分工不同，对网络安全工程技术人才的知识技能需求在内容上会各有侧重，在层次上体现不同。因此，面向适应网安人才特殊性和满足国家网安人才需求，参考网络空间安全学科知识体系，以“人”为核心，以行业对从业人员知识、技能、素质等的要求为出发点，研究梳理网络安全工程技术人才的分类分层体系，以及网络安全知识技能体系，从而衔接人才培养与行业需求间的纽带，为不同渠道网安工程技术人才培养、能力考核评估、求职招聘和岗位设置等提供技术参考。

第二章 网络安全工程技术人才分类与评价体系

2.1 网安人才评价机制的目的和需求现状

对网络空间安全人才评价的目的是评判从业人员是否达到网络空间安全专业技术人员独立从事某种网络空间安全专业技术工作知识、技术和能力的要求。建立网络空间安全人才评价体系有利于加快网安人才培养，指导院校培养体系、社会培训、自学成才等多渠道人才培养和成长活动，促进专业人才队伍素质和业务水平的提高，有利于引导用人单位设置合理、务实的招聘、考核，完善人才队伍。

发达国家高度重视网络空间安全评价，在国家层面上不断地出台相应的战略计划，以完善其评价体系，从而支撑和推动培训体系发展。2012 年美国正式发布了《NICE 战略计划》，指出由 DHS 负责统一领导制定网安人才框架，以评估工作人员的专业化水平，为预测未来网络空间安全需求推荐最佳的实践活动，为招募和挽留人才制定国家策略。该计划的目的是建立和维护一个具有全球竞争力的网安人才队伍。2014 年美国发布了最新版本的《NICE 网络安全人才框架》，目前该框架仍在持续更新。

我国网安人才需求迫切，数量奇缺，但目前以高校培养、社会培训、自学成才三种方式成长起来的网安人才，在知识技能水平上，与社会现实需求间的匹配度还很低。高校网络空间安全毕业生无法快速适应岗位实际工作需求，往往需要用人单位进行一年甚至更长时间的二次培训才能满足实际工作需求；社会培训结业人员，在职业发展、业务能力提升方面，存在知识储备不足、缺少系统性理论能力支撑等问题；自学成才的“奇才”，在职业早期进步很快，但在后期业务拓展、体系性实战能力提升，特别是团队协作、团队管

理等方面，存在明显“力不从心”。

综上，迫切需要通过制定规范统一的评价机制，发挥认证评价指挥棒作用，明确网安人才出口标准，解决缺人才、缺合适的人才、缺可持续发展的复合型人才问题。

2.2 网安人才层次化分类体系

1. 一线安全运营人员

网络空间安全的一线安全运营人员通常包括安全分析师、安全运维工程师、威胁狩猎人员、安全响应团队成员等。其中，安全分析师负责监视和分析网络安全事件，以便及时检测和应对潜在的安全威胁，主要工作内容包括分析日志数据、网络流量和其他安全事件数据，调查潜在的安全漏洞或攻击行为，提供应对建议和解决方案；安全运维工程师负责维护安全设备和系统，确保网络安全措施的有效性和可靠性，主要工作内容包括配置和管理安全设备（如防火墙、入侵检测系统等）、执行安全补丁管理、协助应急响应等工作；威胁狩猎人员负责主动寻找网络中的未知威胁，发现潜在的安全漏洞和攻击活动，主要工作内容包括利用安全工具和技术进行系统审查和分析，识别异常行为和潜在的威胁，提供安全建议和改进方案；安全响应团队成员负责应对网络安全事件和紧急情况，迅速采取行动限制损失并恢复正常运行，主要工作内容包括制定和执行应急响应计划，收集证据、分析攻击手法、修复受影响系统等工作。

这些一线安全运营人员通常需要具备网络安全相关的技术知识和技能，熟悉常见的安全工具和技术，具备良好的问题解决能力和团队合作精神。他们需要密切关注网络安全威胁的动态变化，及时做出反应并保护组织的信息资产安全。

2. 工程技术开发人员

网络空间安全的工程技术开发人员主要包括安全工程师、安全研究员、加密工程师、安全测试工程师等。其中，安全工程师负责设计、开发和维护安全解决方案和系统，保障系统和数据的安全性，主要工作内容包括开发安全工具和软件，设计安全架构，评估系统漏洞和风险，制定安全策略和标准；安全研究员负责研究最新的安全漏洞、攻击技术和威胁情报，为安全产品和解决方案提供技术支持，主要工作内容包括分析恶意代码、漏洞利用技术，进行安全漏洞挖掘和利用研究，撰写安全报告和建议；加密工程师负责设计和实现加密算法、协议和安全通信系统，保障数据的机密性和完整性，工作内容包括开发和优化加密算法、实现安全协议，评估加密方案的安全性和性能等；安全测试工程师负责进行安全测试和渗透测试，评估系统和应用程序的安全性，发现潜在的漏洞和弱点，工作内容包括进行渗透测试、代码审计、漏洞扫描等活动，提供漏洞修复建议和安全加固方案。

这些工程技术开发人员通常需要具备扎实的计算机科学和网络安全知识，熟练掌握编程语言和安全工具，具有创新思维和问题解决能力。他们致力于提升系统的安全性和防御能力，对抗不断演进的网络安全威胁，为组织和用户提供可靠的安全保障。

3. 安全研究创新人员

网络空间安全的安全研究创新人员包括高级安全研究员、安全顾问、安全架构师、安全创新专家等。其中，高级安全研究员负责探索网络安全领域的新技术、新方法和新思路，发现并分析最新的安全漏洞和攻击手法，工作内容包括研究安全漏洞、恶意软件、漏洞利用技术等，开展安全研究项目，发表研究成果和安全报告；安全顾问负责为组织和企业提供安全咨询服务，评估安全风险、制定

安全策略和解决方案，工作内容包括安全评估、风险分析和安全咨询，帮助客户建立健全的安全体系和应对安全挑战；安全架构师负责设计和规划安全架构，确保系统和应用程序在设计阶段就具备安全性，工作内容包括制定安全架构设计方案，评估安全需求和风险，指导开发团队实施安全设计和实施；安全创新专家负责推动网络安全领域的创新发展，探索新的安全技术和解决方案，工作内容包括研究和开发新的安全技术、工具和方法，参与安全创新项目，推动安全领域的技术前沿。

这些安全研究创新人员通常需要具备扎实的网络安全和计算机科学知识，具有创新意识和研究能力，能够跟踪和理解安全技术的最新发展趋势，为解决网络安全挑战提供创新的思路和解决方案。他们的工作对于推动网络安全领域的进步和发展至关重要。

4. 安全规划治理人员

网络空间安全的安全规划治理人员主要涉及制定网络安全规划、策略和政策，监督和管理网络安全实施，确保组织网络资产的安全和持续运营。他们是高层次的管理或治理人员，是政策、制度、规范的制定者和监督实施人员，包括安全项目经理、首席安全官、安全规划师、安全治理专家、安全风险管理专家等。其中，安全项目经理负责管理和协调网络安全项目，确保项目按时完成、符合预期目标，工作内容包括制定项目计划和进度，分配资源，协调团队工作，监督项目执行过程，报告项目进展和风险；首席安全官负责整体网络安全战略的制定和实施，监督组织的网络安全管理和治理工作，工作内容包括领导网络安全团队，制定安全战略和政策，监督安全控制措施的实施和维护，应对安全事件和威胁；安全规划师负责制定组织的网络安全规划和战略，评估安全风险和需求，规划安全措施和应对策略，工作内容包括制定安全规划和策略文件，分析

安全需求和风险，协调安全实施计划，监督安全项目的执行；安全治理专家负责制定组织的网络安全政策、标准和流程，研究制定法规和行业标准，并确保组织符合这些法规标准，工作内容包括制定安全政策文件，指导员工遵守安全政策，监督政策执行情况，对政策进行定期评估和更新；风险管理专家负责评估和管理组织的安全风险，制定风险管理策略，确保组织的网络资产受到有效保护，工作内容包括评估和分析风险，制定风险管理计划，建立风险控制措施，监督风险管理的执行和监控。

这些安全规划治理人员需要具备网络安全、风险管理、合规和治理等领域的专业知识和技能，能够全面考虑组织的安全需求和挑战，制定有效的安全规划和管理策略，监督安全控制措施的实施，确保网络安全工作的持续改进和有效实施。他们在保障组织网络安全和数据安全方面发挥着关键作用。

2.3 构建层次化的网安人才分类评价体系

结合网络空间安全人才岗位、领域和层次，建立分类化评价指标体系，在指标体系的构成或权重上，应体现岗位和层次的区别。综合分析，考评指标应该包括技术能力、问题解决能力、沟通能力、主动性与效率、团队合作或组织管理能力、胜任力等六个方面。

1. 技术能力

对一线安全运营人员，重点考查熟练使用工具的种类水平、应急响应方法和效率；对工程技术开发人员，重点考查安全编码、安全规则实现和安全架构设计等方面达到的认知与实践水平；对安全研究创新人员，考查其学术背景和专业知识水平，以及安全理论、技术创新和新技术开发成果，转化效果等；对安全规划治理人员，重点考查其制定战略和规范的合理性、有效性和效率，以及相关验

证、检验、评测等工具和技术的熟练应用能力。

2. 问题解决能力

对一线安全运营人员，重点考查其解决网络安全问题和故障的能力，以及分析和评估网络系统安全风险的能力；对工程技术开发人员，重点考查解决方案的设计与实现能力，以及漏洞发现、分析和修复能力，兼顾新的安全工具、自动化工具的设计与实现能力；对安全研究创新人员，考查其发现安全问题、建立问题求解模型、提出新理论、新技术及成果转化能力等；对安全规划治理人员，重点考查其发现系统性风险、聚焦核心性问题、提出全局性解决方案能力，以及溯源组织和管理问题并建立针对性规则制定能力。

3. 沟通能力

对一线安全运营人员，重点考查评估其撰写事件报告、风险分析报告等文档的表达能力，以及评估其与团队成员和其他部门进行有效沟通和协作的能力；对工程技术开发人员，重点考查评估其与其他技术团队或非技术团队之间有效沟通和协作的能力，以及编写技术文档、设计文档和开发文档的能力；对安全研究创新人员，考查评估其在学术期刊、会议上发表论文的能力，以及在学术或行业会议上进行有效交流和分享研究成果的能力；对安全规划治理人员，重点考查评估其向高层管理层传达安全风险和建议的能力，以及评估其与团队成员和其他部门有效沟通和协作的能力。

4. 主动性与效率

对一线安全运营人员，重点考查评估其持续学习新技术和工具，保持对网络安全领域的更新认识，以及高效完成任务和处理工作事务的能力，包括时间管理和优先级处理能力；对工程技术开发人员，重点考查评估其自主学习新技术和工具的意愿和行动力，以及在开

发项目中的时间管理和任务分配能力；对安全研究创新人员，考查评估其制定和执行研究计划的能力，包括时间管理和资源规划，以及持续学习新技术和理论知识的主动性和效率；对安全规划治理人员，重点考查其了解新技术能力，以及调研发现新问题新需求并付诸决策的效率。

5. 团队合作或组织管理能力

对一线安全运营人员，重点考查评估其在团队中积极参与、协作和支持他人的团队合作精神，以及在日常安全运营工作中的组织协调和管理能力；对工程技术开发人员，重点考查评估其在团队中积极参与、协作和支持他人的团队合作精神，以及在项目中的组织协调和管理能力，包括进度管理和风险控制；对安全研究创新人员，考查评估其与团队成员合作开展研究的能力，以及在多人合作项目中的组织管理和任务协调能力；对安全规划治理人员，重点考查评估其在不同团队间协调和合作的能力，以及领导团队实施安全规划和治理的能力。

6. 胜任力

对一线安全运营人员，重点考查评估其解决实际网络安全问题的能力和成效；对工程技术开发人员，重点考查评估其在项目中的贡献和成果，包括项目交付质量和效率；对安全研究创新人员，考查评估其研究成果的影响力和贡献度；对安全规划治理人员，重点考查评估其安全规划和治理成果对组织安全的影响和贡献。

第三章 网络安全工程技术人才知识技能体系

3.1 体系分类方法

网安人才知识技能分类方法在国际上一直没有公认标准。可参考的相关工作有美国发布的《NICE 网络安全人才框架》、美国国家安全局和国土安全部联合主持成立的国家信息保障/网络防御学术卓越中心（CAE）发布的“基于知识单元的课程体系”、Gartner 近年发布的新兴技术成熟度曲线和信息安全技术列表，以及国内如智联招聘、360 互联网安全中心、安恒信息等单位组织发布的网络安全人才相关市场状况研究报告等。

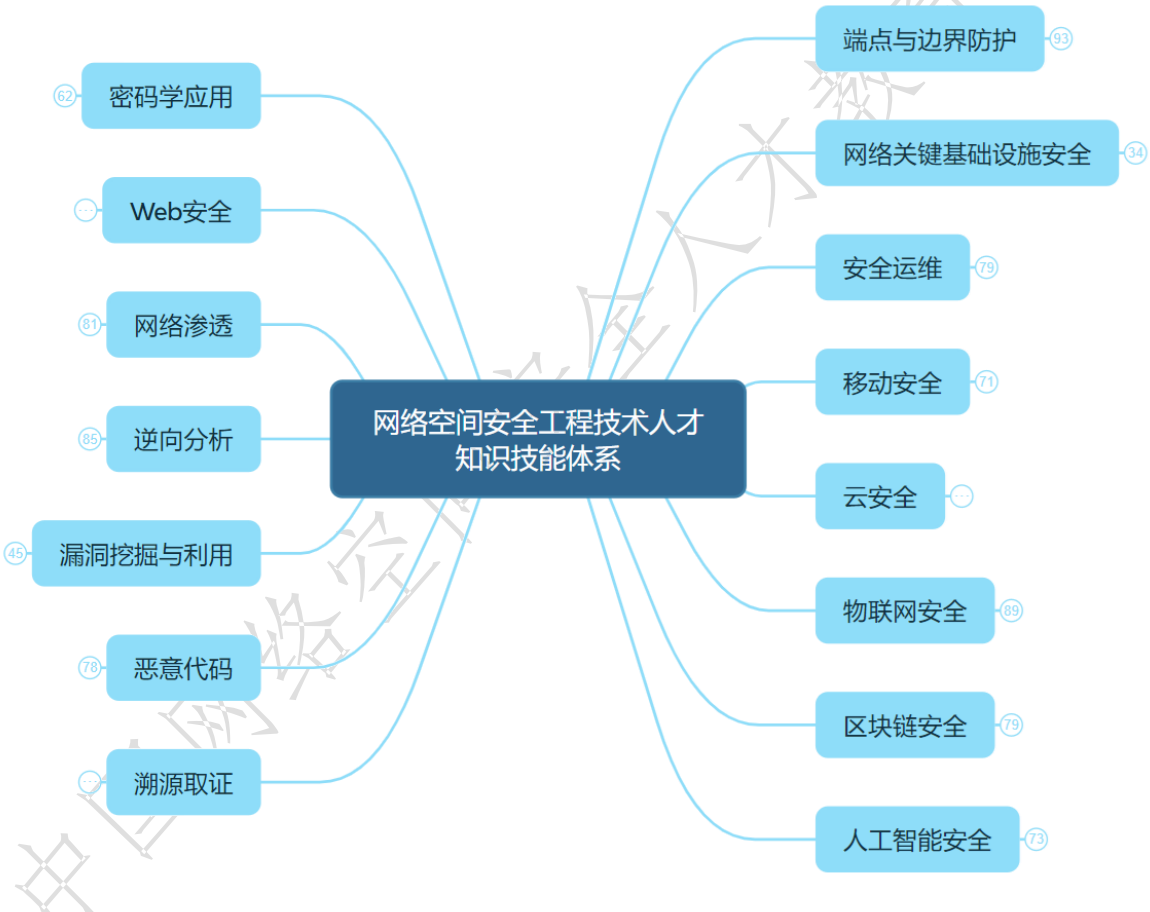
鉴于网络空间安全工程技术人才培养的特殊性，在借鉴国内外相关工作的基础上，延续了本指南前序版本所提出的以“网安人才标签”为主维度的分类法及知识技能体系，以满足聚焦实战能力的网安人才培养需求。之所以没有将“网安岗位”作为分类主维度，是因为对每个岗位的理解，因人而异、因培养单位而异、因用人单位而异、因认证机构而异，存在很大的个体差异性。同时，我们注意到一个现象，当谈及网安从业人员“做什么方向的工作？”，得到的回答往往既不是自己所在网安岗位，也不是工作所需核心技术，而是从业人员给自己打上的一个标签（如“Web”、“渗透”、“运维”），标签的默认含义也已基本形成共识。

因此，设计一个面向网络空间安全工程技术人才的知识技能体系，为学校授课、网安培训、人才认证、岗位招聘以及个人自学成才等提供参考依据，为相关方提供公共可理解的概念、分类体系，成为本指南的初衷之一。此外，鉴于知识技能体系所服务的对象、涵盖的内容是围绕“网安人才培养”，所以，与信息安全管理相关

的政策和法律等内容未列入到体系内。

3.2 标签化知识技能体系

本指南将网安人才知识技能体系划分为 15 个子体系（也称为网安人才标签或一级节点），分别为密码学应用、Web 安全、网络渗透、逆向分析、漏洞挖掘与利用、恶意代码、溯源取证、端点与边界防护、网络关键基础设施安全、安全运维、移动安全、云安全、物联网安全、区块链安全、人工智能安全。



其中，密码学是网络安全的重要基础，“密码学应用”关注网络安全中常用的密码算法实现、加解密技术应用等，不包括与密码学自身紧密相关的如数学理论、加解密算法设计、密码算法安全等；“Web 安全”关注 Web 服务端和浏览器客户端安全，虽然 Web 安全属于应用安全且与“网络渗透”等一级节点有交集，但因其重要性

和标志性而自成一类；“网络渗透”关注攻击者综合运用社工和技术手段对特定目标实施渗透以获得远程目标上的代码执行权的行为过程；“逆向分析”是网络攻防中“变未知为已知”的有效手段，涵盖了文件格式、动态分析、脱壳和相关工具运用等技术；漏洞是网络安全中最受关注的技术之一，也常常是攻击者的“先遣部队”，“漏洞挖掘与利用”关注汇编语言、符号执行、二进制插桩和相关工具运用等技术；“恶意代码”关注从自动传播到规避对抗的全生命周期关键技术；“溯源取证”关注 APT 攻击追踪溯源和网络犯罪取证；“端点与边界防护”关注终端防护平台、端点检测和响应等端点安全技术，入侵检测与防御系统、安全审计系统等边界安全技术，以及威胁猎杀、数据防泄漏等相关防护技术与产品；“网络关键基础设施安全”关注芯片、操作系统、核心应用软件、域名系统等的安全；“安全运维”是信息安全建设不可或缺的一部分，通过安全运维力保 IT 信息系统安全、稳定和可靠运行；“移动安全”关注移动设备、移动无线网络安全；“云安全”关注数据丢失与泄露、虚拟化安全等云计算平台面临的主要威胁和常用防御手段；“物联网安全”关注 IoT 设备安全、通信协议安全和隐私泄露等；“区块链安全”关注矿机与矿池、智能合约和数字钱包等安全技术；“人工智能安全”关注人工智能技术内生安全及人工智能应用业务安全。

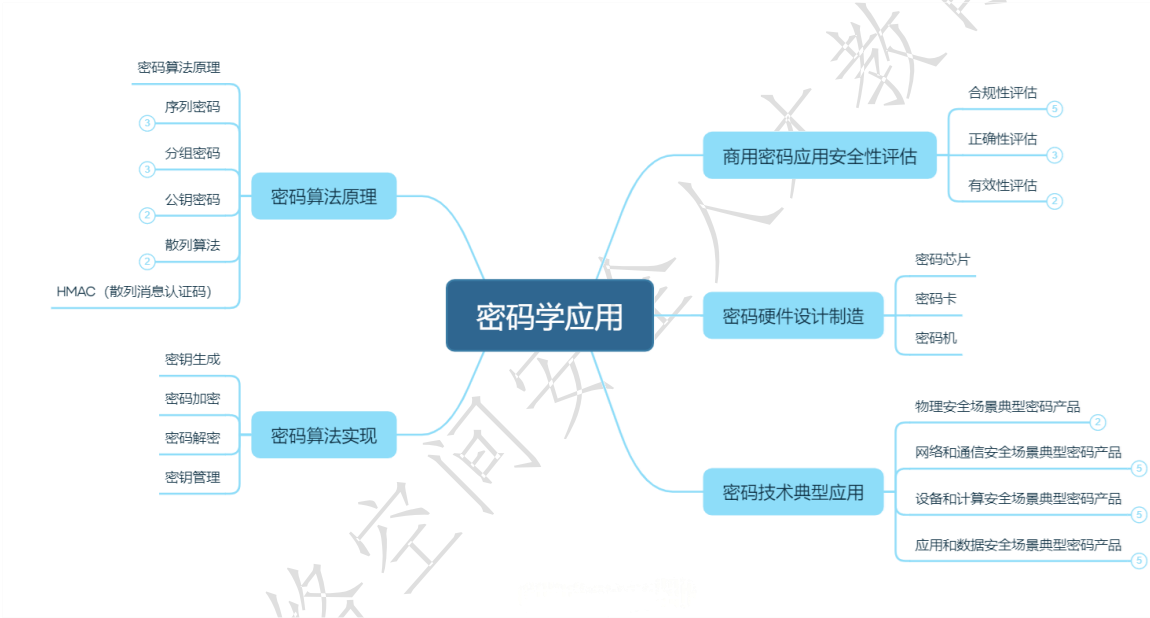
每个子体系（一级节点）又分为多个二级节点，二级节点分类为多个三级节点，最多不超过四级节点。

3.3 体系展开实例

本指南对 15 个一级标签逐一进行了子体系展开描述，并在指南前序版本基础上，主体依托国内网络空间安全行业某一规模性公司资深专家提出框架和建议内容，邀请国内知名网安高校资深学科专家提供修订意见，最终统稿成文。

1. 密码学应用知识技能体系

密码技术是目前世界上公认的、保障网络和信息安全最高效、最可靠、最经济的关键核心技术，在信息化、网络化、数字化高度发展的今天，密码技术的应用已经渗透到社会生产生活的各个方面，政府、金融、医疗、运营商等各行业均积极推动密码应用相关建设。本指南聚焦密码学常见的应用领域，密码学应用知识技能包括密码算法原理、密码算法实现、密码硬件设计制造、商用密码应用安全性评估、密码技术典型应用等。



（1）密码算法原理。密码算法是用于加密和解密的数学函数，密码算法是密码协议的基础。现行的密码算法主要包括序列密码、分组密码、公钥密码、散列函数等，用于保证信息的安全，提供机密性、完整性、不可否认性等能力。序列密码是一种基于密钥和明文流逐位异或的加密方式，常见的序列密码算法包括 RC4、Salsa20、Serpent、ZUC（祖冲之算法）等，其密钥空间相对较小，安全性相对较低，但实现简单、加解密速度快，适用于对速度要求高、安全性要求较低的场景；分组密码是一种将明文数据分成固定长度的块

进行加密的密码算法，也称为块密码，常见的算法包括 DES、3DES、AES、SM1、SM4 等，其对每个密码块独立进行加密和解密操作，具有较高的安全性和较强的适应性；公钥密码是一种基于非对称加密的密码算法，其中加密和解密使用不同的密钥，常见算法包括 RSA、Elliptic Curve Cryptography（ECC）、SM2 等，其应用范围涵盖了网络通信、电子邮件、数字签名、电子支付等领域；散列算法主要作用是将任意长度的消息映射为固定长度的消息，常见算法包括 SHA-2、SHA-3、SHA-256、SM3 等；散列消息认证码（HMAC）是一种常用的消息认证码，它将散列函数和密钥结合起来，从而保证消息的完整性和真实性。

（2）密码算法实现。密码算法的实现方式可以分为密钥生成、加密、解密、密钥管理等几个步骤。密钥生成方式可以是由随机数生成器生成一个随机密钥，也可以是由用户设置一个密钥；加密是根据密钥，将明文数据使用密码算法进行转换，生成密文数据；解密是使用与加密密钥相同或相关的解密密钥，将密文数据转换为对应或相同的明文数据；密钥管理包括密钥的存储、备份和使用，保证密钥的安全性，避免密钥泄露、丢失、损坏。

（3）商用密码应用安全性评估。商用密码应用安全性评估是指对采用商用密码技术、产品和服务集成建设的网络和信息系统，对其商用密码应用的合规性、正确性和有效性进行评估。商用密码应用合规性评估是指判定信息系统使用的密码算法、密码协议、密钥管理是否符合法律法规的规定和相关国家标准、行业标准的有关要求，使用的密码产品和密码服务是否经过国家密码管理部门核准或由具备资格的机构认证合格；商用密码应用正确性评估是指判定密码算法、密码协议、密钥管理、密码产品和服务使用是否正确，即系统中采用的标准密码算法、协议和密钥管理机制是否按照相应的

密码国家和行业标准进行正确的设计和实现，自定义密码协议、密钥管理机制的设计和实现是否正确，安全性是否满足要求，密码保障系统建设或改造过程中密码产品和服务的部署和应用是否正确；商用密码应用有效性评估是指判定信息系统中实现的密码保障系统是否在信息系统运行过程中发挥了实际效用，是否满足了信息系统的安全需求，是否切实解决了信息系统面临的安全问题。

（4）密码硬件设计制造。密码硬件设计与制造涵盖密码芯片、密码卡和密码机。密码芯片集成了多种密码算法，提供高速、高效、可靠的密码能力，是密码应用的重要组成部分。其设计和制造要求掌握电路设计、芯片设计流程、物理设计、器件选型等技能。密码卡是一种支持多种密码算法的计算机外围设备，提供数据加解密、数字签名和验证等安全服务，确保信息传输安全。其设计和制造需掌握计算机体系结构、PCI-E 总线规范、硬件设计、软件开发、安全设计与测试等技术。密码机则具备加解密、数字签名、身份认证和随机数生成等功能，其设计和制造要求掌握密码学、计算机科学、电子电路设计、嵌入式系统、硬件和软件开发、安全设计与测试等方面的综合技能。

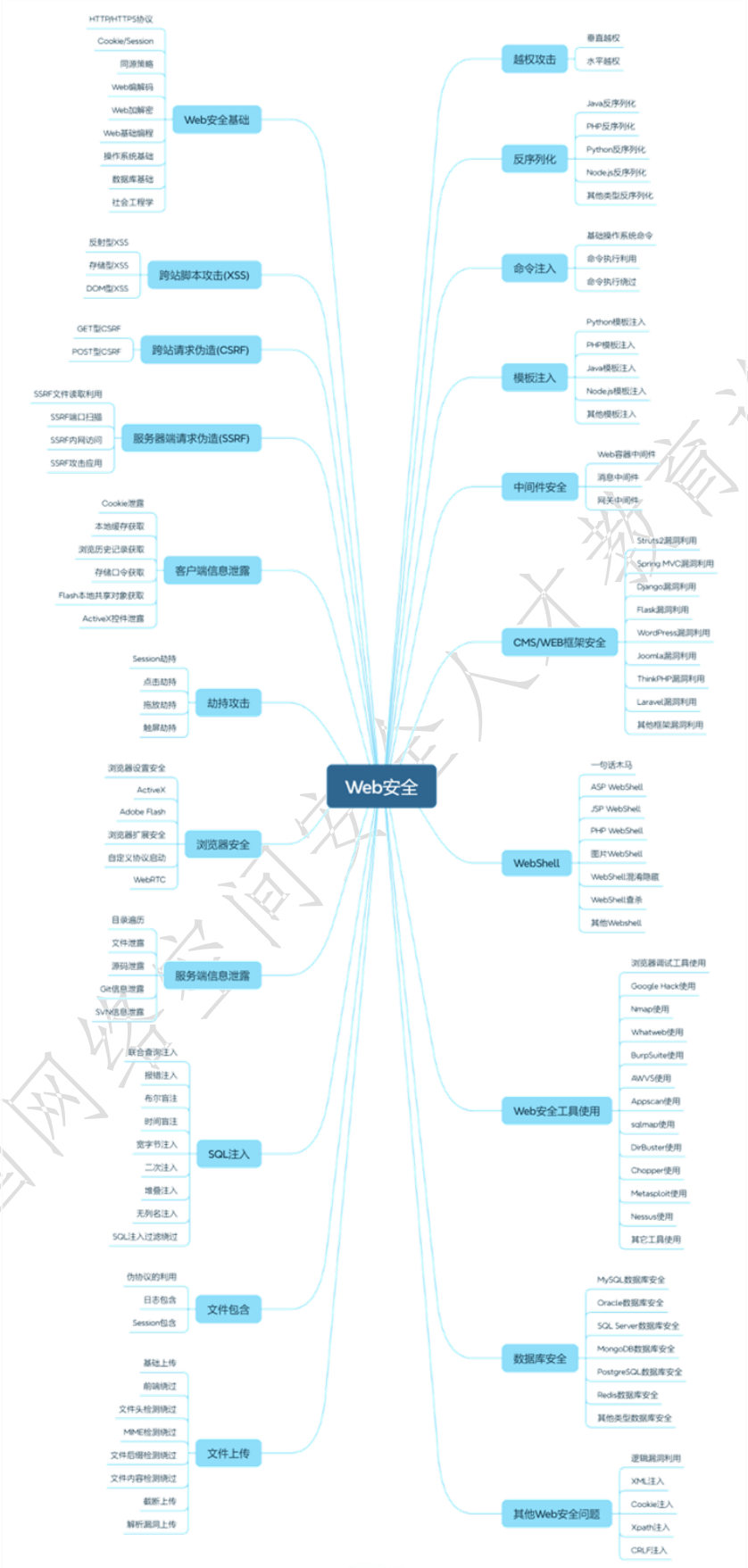
（5）密码技术典型应用。密码技术主要应用在物理安全场景、网络和通信安全场景、设备和计算安全场景、应用和数据安全场景。物理安全场景典型密码产品包括国密门禁系统、国密音视频监控系统；网络和通信安全场景典型密码产品包括国密安全认证网关、协同签名系统、VPN 网关、服务器密码机、统一身份认证系统等；设备和计算安全场景典型密码产品包括数字证书认证系统、国密 USB-KEY、时间戳服务器、国密浏览器、云服务器密码机等；应用和数据安全场景典型密码产品包括密码服务平台、签名验签系统、密钥管理系统、数据库加密机、电子签章系统等。

2. Web 安全知识技能体系

随着互联网的普及和 Web 的广泛应用，Web 安全已成为网络安全领域的重要组成部分，涉及从个人隐私保护到企业数据安全的方方面面。Web 安全旨在保护 Web 应用程序及其相关服务免受各种网络攻击和威胁，确保其正常运行。本指南聚焦 Web 安全主要技术和防护措施，将 Web 安全技术体系划分为 Web 安全基础、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）、服务器端请求伪造（SSRF）、客户端信息泄露、劫持攻击、浏览器安全、服务端信息泄露、SQL 注入、文件包含、文件上传、越权、反序列化、命令注入、模板注入、中间件安全、CMS/WEB 框架安全、WebShell、Web 安全工具使用、数据库安全、其他 Web 安全问题等 21 个核心组成部分。

（1）Web 安全基础。Web 安全基础涵盖了在 Web 安全研究中研究者应掌握的理论知识和基础技术，涉及系统、数据库、协议、编码等理论知识，以及 Web 服务器的搭建、基础配置、简单运维等技术。因此，Web 安全基础主要包括 HTTP/HTTPS 协议、Cookie/Session、同源策略、Web 编解码、Web 加解密、Web 基础编程、操作系统基础、数据库基础、社会工程学以及其他安全相关的 Web 基础技术等。

（2）跨站脚本攻击。跨站脚本攻击（Cross Site Scripting，XSS）是一种常见的 Web 安全威胁，攻击者将恶意代码植入 Web 客户端，以影响其他浏览此页面的用户。攻击者能够利用 XSS 在受害者的浏览器中执行脚本，并劫持用户会话、破坏网站或将用户重定向到恶意站点。XSS 主要技术包括反射型 XSS、存储型 XSS 和 DOM 型 XSS。



（3）跨站请求伪造。跨站请求伪造（Cross Site Request Forgery，CSRF）是指伪造成合法用户发起请求，挟持用户在当前已登录的Web 应用程序上执行非本意操作的攻击方法。CSRF 允许攻击者劫持用户浏览器向存在漏洞的应用程序发送请求，而这些请求会被应用程序认为是用户的合法请求。CSRF 主要技术包括 GET 型 CSRF 和 POST 型 CSRF。

（4）服务器端请求伪造。服务器端请求伪造（Server Side Request Forgery，SSRF）是指攻击者通过伪造请求，使服务器在不知情的情况下向指定的目标发送请求。这种攻击通常利用服务器的权限和信任关系，访问内部资源或执行未授权的操作。其中攻击方法包括文件读取利用、端口扫描、内网访问、攻击应用等。服务器端请求伪造包括 SSRF 文件读取利用、SSRF 端口扫描、SSRF 内网访问、SSRF 共计应用等。

（5）客户端信息泄露。客户端信息指存在于客户端的用户数据，包括基本信息、设备信息、账户信息、隐私信息等，此信息若保护不当，一旦被攻击者获取，就会被利用进行网络诈骗、身份仿冒等恶意操作。客户端信息泄露主要技术包括 Cookie 泄露、本地缓存获取、浏览历史记录获取、存储口令获取、Flash 本地共享对象获取、Active X 控件泄露等。

（6）劫持攻击。劫持攻击指攻击者通过某些特定的手段，将本该正确返回给用户的数据进行拦截，呈现给用户虚假的信息，主要是通过欺骗的技术将数据转发给攻击者。劫持攻击主要技术包括 Session 劫持、点击劫持、拖放劫持、触屏劫持等。

（7）浏览器安全。浏览器是互联网最大的入口，是大多数网络用户使用互联网的工具，因此浏览器安全是一个极其重要的安全领域。浏览器安全主要技术包括浏览器设置安全、ActiveX、Adobe

Flash、浏览器扩展安全、自定义协议启动、WebRTC 等。

（8）服务器端信息泄露。服务器端信息泄露问题指因错误配置或 Web 组件漏洞导致服务器目录、文件等敏感信息遭泄露的问题。敏感信息可能被攻击者利用，进而对服务器发起针对性攻击。服务器端信息泄露主要技术包括目录遍历、文件泄露、源码泄露、Git 信息泄露、SVN 信息泄露等。

（9）SQL 注入。SQL 注入指通过将恶意的 SQL 语句注入正常的 GET 或 POST 类型的 HTTP 请求，以改变 Web 服务器后端代码处理请求参数的执行逻辑，从而间接对服务器数据库执行增、删、改、查等操作的行为。SQL 注入主要技术包括联合查询注入、报错注入、布尔盲注、时间盲注、宽字节注入、二次注入、堆叠注入、无列名注入、SQL 注入过滤绕过等。

（10）文件包含。文件包含的合法用途是在代码中引入其他项目中的包、库等，以实现代码的有效复用。文件包含漏洞指因编程缺陷，导致 Web 服务器在处理代码时未能对所引用文件严格限制，致使所引用的文件可被攻击者控制的问题。文件包含主要技术包括本地文件包含和远程文件包含。本地文件包含包括伪协议的利用、日志包含、Session 文件包含等；远程文件包含通常用于引用攻击者构造的恶意外部文件以在服务器上执行恶意操作。

（11）文件上传。文件上传指向 Web 服务器直接上传恶意脚本、WebShell 等恶意文件的安全问题。文件上传时，通常需要解决文件格式限制绕过、上传路径获取、上传文件正确解析等问题。文件上传主要技术包括基础上传、前端绕过、文件头检测绕过、MIME 检测绕过、文件后缀检测绕过、文件内容检测绕过、截断上传、解析漏洞上传等。

（12）越权攻击。越权攻击是 Web 应用程序中常见且严重的安

全威胁，攻击者通过绕过系统的访问控制机制，获取或修改未经授权的资源。越权攻击主要分为水平越权和垂直越权两种类型，常见的攻击手法包括直接对象引用、参数篡改、会话劫持和功能滥用等。

（13）反序列化。序列化指编程语言将变量、函数等对象转化为字节序列的过程；反之，将字节序列转化为对象的过程称为反序列化。反序列化漏洞指攻击者通过构造字节序列，转化生成恶意对象的安全问题。反序列化技术主要包括 Java 反序列化、PHP 反序列化、Python 反序列化、Node.js 反序列化等。

（14）命令注入。命令注入是一种严重的安全漏洞，攻击者通过向应用程序传递恶意输入，使其执行未预期的操作系统命令，从而控制服务器或获取敏感信息。命令注入攻击可以通过多种途径实现，包括 Web 表单注入、URL 参数注入、HTTP 头部注入和 Cookie 注入等。

（15）模板注入。模板注入是一种通过向模板引擎传递恶意输入，使引擎将恶意代码进行解析进而控制服务器的漏洞。其中包括 Java 模板注入、PHP 模板注入、Python 模板注入、Node.js 模板注入等。

（16）中间件安全。中间件是为应用提供常见服务与功能的软件和云服务，可以帮助开发和运维人员更高效地构建和部署应用。中间件安全主要技术包括 Web 容器中间件、消息中间件、网关中间件等。

（17）CMS/WEB 框架安全。CMS（内容管理系统）是一种位于 WEB 前端和后端办公系统或流程之间的软件系统，CMS/WEB 框架常用于快速的网站建设。CMS/WEB 框架安全问题涉及各类组件、Web 应用。CMS/WEB 框架安全主要技术包括 Struts2 漏洞利用、Spring MVC 漏洞利用、Django 漏洞利用、Flask 漏洞利用、

WordPress 漏洞利用、Joomla 漏洞利用、ThinkPHP 漏洞利用、Laravel 漏洞利用等。

（18）WebShell。WebShell 是网站后门的一种形式，通常是以 ASP、PHP、JSP 或者 CGI 等网页文件形式存在于代码执行环境中，以达到控制网站服务器的目录。WebShell 主要技术包括一句话木马、ASP WebShell、JSP WebShell、PHP WebShell、图片 WebShell、WebShell 混淆隐藏、WebShell 查杀等。

（19）Web 安全工具使用。Web 安全工具的使用能够有效提高工作效率、发现潜藏安全问题，使用 Web 安全工具可以进行信息收集、漏洞探测、漏洞利用等操作。Web 安全工具主要技术包括浏览器调试工具、Google Hack、Nmap、Whatweb、BurpSuite、AWVS、Appscan、sqlmap、DirBuster、Chopper、Metasploit、Nessus 等。

（20）数据库安全。数据库安全指数据库管理系统的安全问题，常见的数据库管理系统有 MySQL、Oracle、PostgreSQL 等，保证数据库安全对防止黑客入侵、防止数据被窃取以及破坏具有重要意义。数据库安全主要技术包括 MySQL 数据库安全、Oracle 数据库安全、SQL Server 数据库安全、MongoDB 数据库安全、PostgreSQL 数据库安全、Redis 数据库安全等。

（21）其它 Web 安全问题。指未包含在上述知识点的其他安全问题及未来新出现的问题或方法技术。主要技术包括逻辑漏洞利用、XML 注入、Cookie 注入、Xpath 注入、CRLF 注入等。

3. 网络渗透知识技能体系

在信息化和数字化的时代背景下，各类基础设施、应用系统等成为了企业和组织不可或缺的一部分，但其面临的威胁也日益复杂和多样化。网络渗透是模拟攻击者的攻击行为来发现系统潜在安全

风险的方法，通过全面的网络渗透测试，评估和提升网络和系统的安全性。本指南基于攻击者入侵的视角，聚焦网络渗透流程方法，将网络渗透方向划分为目标侦察、资源准备、边界突破、攻击执行、权限维持、权限提升、防御规避、凭据获取、环境探测、横向移动、敏感信息收集、远程控制、数据窃取等 13 个核心组成部分。

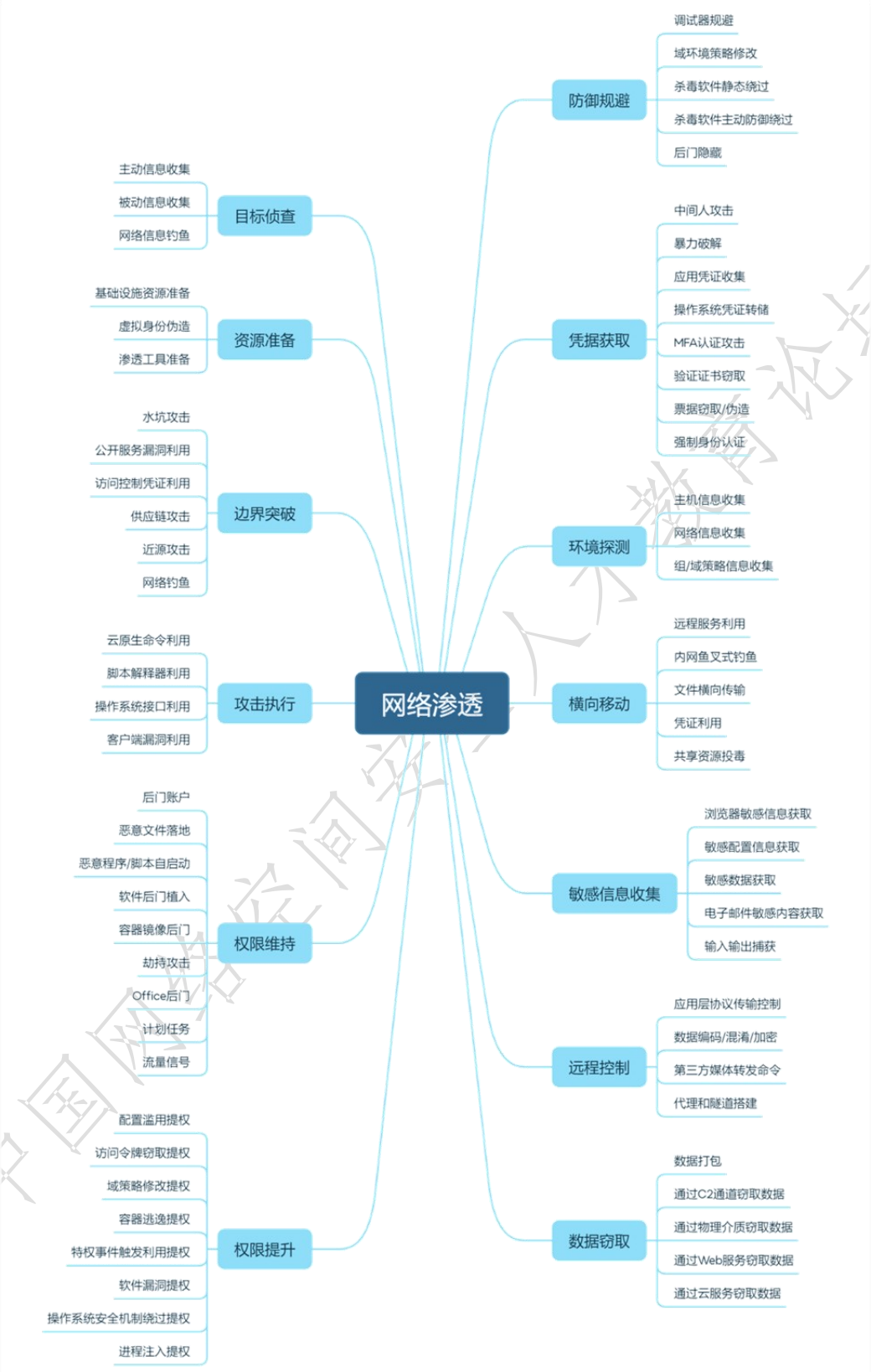
（1）目标侦察。目标侦察是指通过主动信息收集、被动信息收集和网络信息钓鱼等技术方法，尽可能全面地获取目标情报信息，以制定针对性的行动策略，提高渗透的效率和成功率。此类信息通常包括目标组织、基础设施或工作人员的详细信息等。

（2）资源准备。资源准备是指在对目标发起攻击动作之前，需要准备的基础设施资源、虚拟身份、渗透工具等。因此，资源准备包括基础设施资源准备、虚拟身份伪造、渗透工具准备等。

（3）边界突破。边界突破是指使用各种攻击技术手段获得目标网络或系统初始入口点权限，从而突破网络边界，以展开后续的网络渗透。边界突破常用技术包括水坑攻击、公开服务漏洞利用、访问控制凭证利用、供应链攻击、近源攻击、网络钓鱼等。

（4）攻击执行。攻击执行是指通过本地或远程的方式在受害服务器上执行命令和代码的技术，通过执行命令或代码，以达到恶意目的。攻击执行常用技术包括云原生命令利用、脚本解释器利用、操作系统接口利用、客户端漏洞利用等。

（5）权限维持。权限维持是指发生重新启动、凭据修改等其他可能切断与受害系统连接事件的情况下，保持对系统的持续访问的相关技术。权限维持常用技术包括后门账户、恶意文件落地、恶意程序/脚本自启动、软件后门植入、容器镜像后门、劫持攻击、Office 后门、计划任务和流量信号等。



（6）权限提升。权限提升是指攻击者为了能够在受害者主机或

网络中获得更多资源、扩大攻击影响范围采取的攻击技术，主要目的是获取管理员、系统级别的执行权限。权限提升常用技术包括配置滥用提权、访问令牌窃取提权、域策略修改提权、容器逃逸提权、特权事件触发利用提权、软件漏洞提权、操作系统安全机制绕过提权、进程注入提权等。

（7）防御规避。防御规避是指在整个入侵过程中避免被目标和防护设备发现所使用到的技术。防御规避的技术包括调试器规避、域环境策略修改、杀毒软件静态绕过、杀毒软件主动防御绕过和后门隐藏等。

（8）凭据获取。凭据获取是指通过技术手段获取账户凭证、票据、证书等身份认证信息，从而突破身份验证措施，以便后续渗透的工作开展。凭据获取的主要技术包括中间人攻击、暴力破解、应用凭证收集、操作系统凭证转储、MFA 认证攻击、验证证书窃取、票据窃取/伪造和强制身份认证等。

（9）环境探测。环境探测是指通过技术方法获取已失陷系统主机情况和内部网络架构、服务开放情况，从而确定下一步渗透方向。环境探测主要技术包括主机信息收集、网络信息收集、组/域策略信息收集等。

（10）横向移动。横向移动是在攻击者进入目标网络后，在目标内部横向扩散，以获得更高级别目标的执行权限或获取更多有价值数据的过程。横向移动主要技术包括远程服务利用、内网鱼叉式钓鱼、文件横向传输、凭证利用、共享资源投毒等。

（11）敏感信息收集。敏感信息收集是攻击者对账户凭证、敏感配置、敏感数据等敏感信息进行针对性收集的过程。敏感信息收集主要技术包括浏览器敏感信息获取、敏感配置信息获取、敏感数据获取、电子邮件敏感内容获取、输入输出捕获等。

（12）远程控制。远程控制是指攻击者在渗透过程中需要搭建稳定的用于远程访问失陷系统和主机的流量隧道，用于远程命令下发和系统控制，同时结合编码、加密等技术提升隧道隐蔽性。远程控制主要技术包括应用层协议传输控制、数据编码/混淆/加密、第三方媒体转发命令、代理和隧道搭建等。

（13）数据窃取。数据窃取是指在渗透过程中获取到敏感信息和重要数据时，使用各种方式将其传输到失陷系统外部，以实现数据的持久性利用。数据窃取主要技术包括数据打包、通过 C2 通道窃取数据、通过物理介质窃取数据、通过 Web 服务窃取数据、通过云服务窃取数据等。

4. 逆向分析知识技能体系

逆向分析是通过分析目标程序的结构、功能和行为来理解其工作原理的一种技术。它集技术性、挑战性、实用性于一体，通过深入剖析程序内部逻辑与实现细节，为安全防御体系构建和潜在脆弱环节发掘提供有力支撑，在软件安全、恶意代码分析、漏洞挖掘等领域有着广泛的应用。本指南聚焦于逆向分析技术体系，将逆向分析技术体系划分为基础知识、工具使用、低级语言分析、高级语言逆向分析、文件格式分析、静态分析对抗、动态调试对抗、脱壳分析和操作系统机制分析等 9 个核心组成部分。

（1）逆向分析基础。逆向分析基础涵盖了研究者应掌握的理论知识和基础实践能力。逆向分析基础主要包括寄存器基础、内存基础、堆栈基础、网络协议基础、密码学基础、函数调用约定等。

（2）逆向分析工具使用。逆向分析工具使用是指借助已有的逆向分析工具以及相关插件，或者自己实现相关的分析工具，可以有效减少重复劳动，甚至是极大的提高逆向分析的效率。逆向分析工具主要包括 Detect It Easy 使用、x64dbg 及相关插件使用、dnSpy 使

用、Ghidra 及相关插件使用、Resource Hacker 使用、Spy++使用、IDA 及相关插件使用、Windbg 及相关插件使用、Ollydbg 及相关插件使用、GDB 及相关插件使用、JEB Decompiler 使用、ILSpy 使用等。

（3）低级语言分析。低级语言通常指汇编语言。在没有编译器的情况下，其按照标准文档可以与机器指令互相转换，也正因为如此，二进制程序在没有源代码的情况下可以被反汇编成汇编语言并在此基础上进行安全分析。与二进制程序被反汇编成汇编代码类似，脚本语言代码编译后生成的字节码文件可以被反编译成对应的中间语言，并且中间语言通常可以被还原成类似原始脚本语言源代码的结果。低级语言分析主要技术包括 Intel 汇编语言分析、ARM 汇编语言分析、MIPS 汇编语言分析、Smali 语言分析、MSIL（Microsoft Intermediate Language）语言分析、Python 字节码分析等。

（4）高级语言逆向分析。高级语言逆向分析是一个广泛而复杂的领域，涵盖了多种编程语言和逆向分析技术，不同的编程语言具有不同的特点和逆向分析挑战。高级语言逆向分析主要包括 C/C++逆向分析、C#逆向分析、Python 逆向分析、Java 逆向分析、Go 逆向分析、Rust 逆向分析等。

（5）文件格式分析。文件格式指文件的内部构成方式。在计算机系统中，文件格式类型多种多样，对机器本身而言均为二进制数据格式，在逆向分析时，对可执行文件格式进行分析是一个重要环节，其主要相关技术包括 PE（Portable Executable）文件格式分析、ELF（Executable and Linkable Format）文件格式分析、APK（Android Package）文件格式分析及其他文件格式分析等。

（6）静态分析对抗。逆向对抗（即反逆向）与逆向分析是一场持久的对抗。逆向分析人员可以通过逆向分析来理解目标程序的内部实现逻辑，开发人员也可以通过相关技术来提高逆向分析人员的

分析成本，以降低程序在短时间内被其他人员成功逆向分析的风险。根据逆向分析方式的不同，逆向分析对抗技术可以划分为静态分析对抗与动态调试对抗。静态分析对抗主要技术包括花指令混淆、Android Guard 混淆、LLVM 混淆、字符串加密、API 动态调用、DLL 反射加载、VM 混淆、代码自解密等。

（7）动态调试对抗。动态调试对抗即检测当前程序是否正在被调试器调试，如果是则作出相应的对抗行为，例如进入不同的代码分支、退出进程，甚至是利用调试环境的漏洞发起攻击等。动态调试对抗主要技术包括 Being Debugged 检测反调试、NtGlobalFlag 检测反调试、HeapMagic 检测反调试、ProcessDebugPort 检测反调试、ThreadHideFromDebugger 反调试、DebugObject 检测反调试、0xCC 断点检测反调试、TLS（Thread Local Storage）反调试、DbgHelp 模块检测反调试、窗口标题检测反调试、父进程检测反调试、时间差检测反调试、基于异常的反调试等。

（8）脱壳分析。加壳程序可以在不改变原有程序功能的基础上为其提供一层“保护壳”，从而增加逆向分析的成本。对于经过加壳保护的程序，逆向分析人员的首要工作是对其进行脱壳，之后才能进行后续分析工作。脱壳分析主要技术包括 UPX 脱壳、UPX 变种脱壳、ASPack 脱壳、PECompact 脱壳、Yoda's Crypter 脱壳、ASProtect 脱壳、VMProtect 脱壳、Themida 脱壳、DLL 文件脱壳等。

（9）操作系统机制分析。操作系统是计算机系统的核心，它管理和协调计算机硬件和软件资源，为用户和应用程序提供了一个高效、可靠、安全的运行环境。深入理解操作系统的内部机制是进行系统级逆向分析的基础。操作系统机制分析涉及多个方面，主要包括保护模式分析、进程/线程管理分析、设备通信管理分析、异步调用机制分析、内存管理分析、中断处理分析、事件处理分析、异常

处理分析、内存管理分析、消息机制分析、调试机制分析、虚拟化技术分析等。

5. 漏洞挖掘与利用知识技能体系

漏洞挖掘与利用是信息安全领域中的重要方向，旨在发现、分析并利用软件或系统中的安全漏洞，从而评估和提高系统的安全性。通过系统化的漏洞挖掘与利用，可以提前发现潜在的安全隐患，并采取有效的防护措施，减少攻击带来的风险和损失。本指南聚焦于漏洞挖掘与利用技术体系，将漏洞挖掘与利用技术体系划分为基础技术、符号执行、模糊测试、漏洞利用、缓解机制绕过、代码审计等 6 个核心组成部分。

（1）基础技术。基础技术是指涵盖了研究者在漏洞挖掘与利用研究领域中应当掌握的基础理论知识和技术实践能力，涉及汇编语言、C/C++语言、脚本语言等常见编程语言的阅读、理解、编写，以及进程管理、内存管理等操作系统原理和机制。基础技术包括了函数调用过程、内存管理机制、Shellcode 编写、网络协议与通信等。

（2）符号执行。符号执行是指一种程序分析技术，用于系统地探索程序的所有可能执行路径，以发现潜在的错误或漏洞。使用符号执行分析特定程序时，该程序会使用符号值作为输入，而非一般执行程序时所使用的具体值；在到达目标代码时，分析器可以得到相应的路径约束，然后通过约束求解器来得到可以触发目标代码的具体值。符号执行主要技术包括 Angr 使用、Triton 使用、S2E 使用、Klee 使用等。

（3）模糊测试。模糊测试（Fuzzing）是指通过向程序输入大量随机或半随机数据，以发现程序中的漏洞和缺陷的一种自动化软件测试技术。其主要目标是通过异常输入触发程序的未定义行为，从而找到潜在的安全漏洞。模糊测试主要技术包括 Peach Fuzzer 使用、AFL 使用、libFuzzer 使用、honggfuzz 使用、WinAFL 使用、syzkaller 使用等。

（4）漏洞利用。漏洞利用是指通过触发特定缺陷或漏洞，从而执行未经授权的操作或取得对系统的控制。漏洞利用主要技术包括栈缓冲区溢出利用、堆缓冲区溢出利用、数组越界访问、释放后重引用利用、双重释放利用、符号溢出利用、内存未初始化利用、条件竞争利用、类型混淆利用、格式化字符串利用、空指针引用利用等。

（5）缓解机制绕过。缓解机制绕过是指一系列保护技术，旨在增强软件和系统的安全性，降低漏洞利用的成功率。绕过缓解机制

需要深入理解其工作原理和潜在弱点，涉及多种技术手段和工具。缓解机制绕过包括 DEP 绕过、ASLR 绕过、GS（Stack Cookie）绕过、SafeSEH 绕过、SEHOP 绕过、CFG 绕过、KASLR 绕过、SMAP 绕过、SMEP 绕过、CET 绕过等。

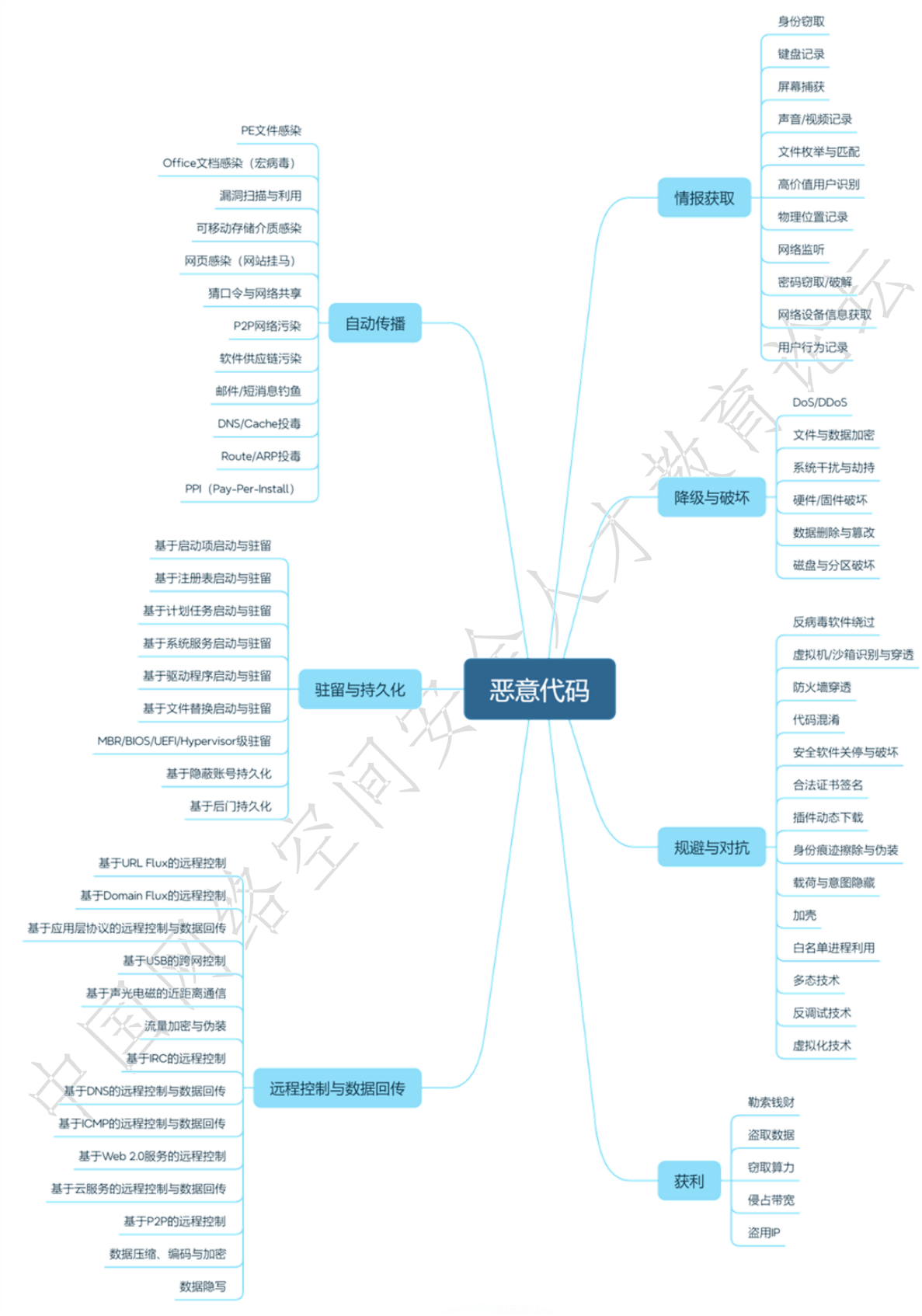
（6）代码审计。代码审计是指在不实际执行程序的情况下，对代码语义和行为进行分析，由此找出程序中由于错误的编码导致异常的程序语义或未定义的行为。它能在软件开发流程早期就发现代码中的各种问题，从而提高开发效率和软件质量。代码审计主要技术包括 Codeql 使用、ASAN 使用、Cppcheck 使用、Clang static analyzer 使用等。

6. 恶意代码知识技能体系

恶意代码是一种用来破坏、窃取或篡改计算机系统及其数据的代码。它包括病毒、蠕虫、特洛伊木马、勒索软件、间谍软件和广告软件等类型。这些代码可以通过电子邮件附件、恶意网站、感染的软件或其他载体传播。一旦被执行，恶意代码可能导致系统性能下降、数据丢失、隐私泄露或直接经济损失。本指南聚焦于恶意代码分析技术，从恶意代码的自动传播、驻留与持久化、远程控制与数据回传、情报获取、降级破坏、规避与对抗、获利等 7 个技术角度全面分析阐述恶意代码的运行机制和技术原理。

（1）自动传播。自动传播技术赋予恶意代码自我复制和持续再生的能力，堪称恶意代码区别于其他网络攻击形态的独有特性。自动传播技术包括 PE 文件感染、Office 宏病毒、漏洞扫描与利用、可移动存储介质感染、网页感染（网站挂马）、口令与网络共享、P2P 网络污染、软件供应链污染、邮件/短消息钓鱼、DNS/Cache 投毒、Route/ARP 投毒、PPI（Pay-Per-Install）等。

（2）驻留与持久化。驻留与持久化技术是帮助恶意代码在系统



重启后再次获得执行机会而又不引起明显异常，从而实现尽可能长时间的生存。驻留与持久化技术包括基于启动项启动与驻留、基于注册表启动与驻留、基于计划任务启动与驻留、基于系统服务启动与驻留、基于驱动程序启动与驻留、基于文件替换启动与驻留、MBR/BIOS/UEFI/Hypervisor 级驻留、基于隐蔽账号持久化、基于后门持久化等。

（3）远程控制与数据回传。远程控制主要是针对僵尸网络（Botnet）、远控木马（Remote Access Trojan，RAT）而言的，僵尸网络侧重建立健壮的命令与控制信道（Command and Control Channel）来管理大规模“瘦客户”，而远控木马侧重建立轻量级命令与控制信道管理小规模“胖客户”；数据回传，指的是将被控端上的感兴趣数据以良好的穿透性、隐蔽性回传给攻击者的过程。远程控制与数据回传技术包括基于 URL Flux 的远程控制、基于 Domain Flux 的远程控制、基于应用层协议的远程控制与数据回传、基于 USB 的跨网控制、基于声光电磁的近距离通信、流量加密与伪装、基于 IRC 的远程控制、基于 DNS 的远程控制与数据回传、基于 ICMP 的远程控制与数据回传、基于 Web 2.0 服务的远程控制、基于云服务的远程控制与数据回传、基于 P2P 的远程控制、数据压缩、编码与加密以及数据隐写等。

（4）情报获取。获取情报是恶意代码主要危害之一。远控木马和僵尸程序常常窃取用户身份信息以获取经济利益，而 APT 中的恶意代码更关注敏感文件、键盘与屏幕等可获取商业与军事机密的情报。情报获取技术包括身份窃取、键盘记录、屏幕捕获、声音/视频记录、文件枚举与匹配、高价值用户识别、物理位置记录、网络监听、密码窃取/破解、硬件设备信息获取、用户行为记录等。

（5）降级与破坏。降级与破坏是指通过干扰、篡改、攻击等方

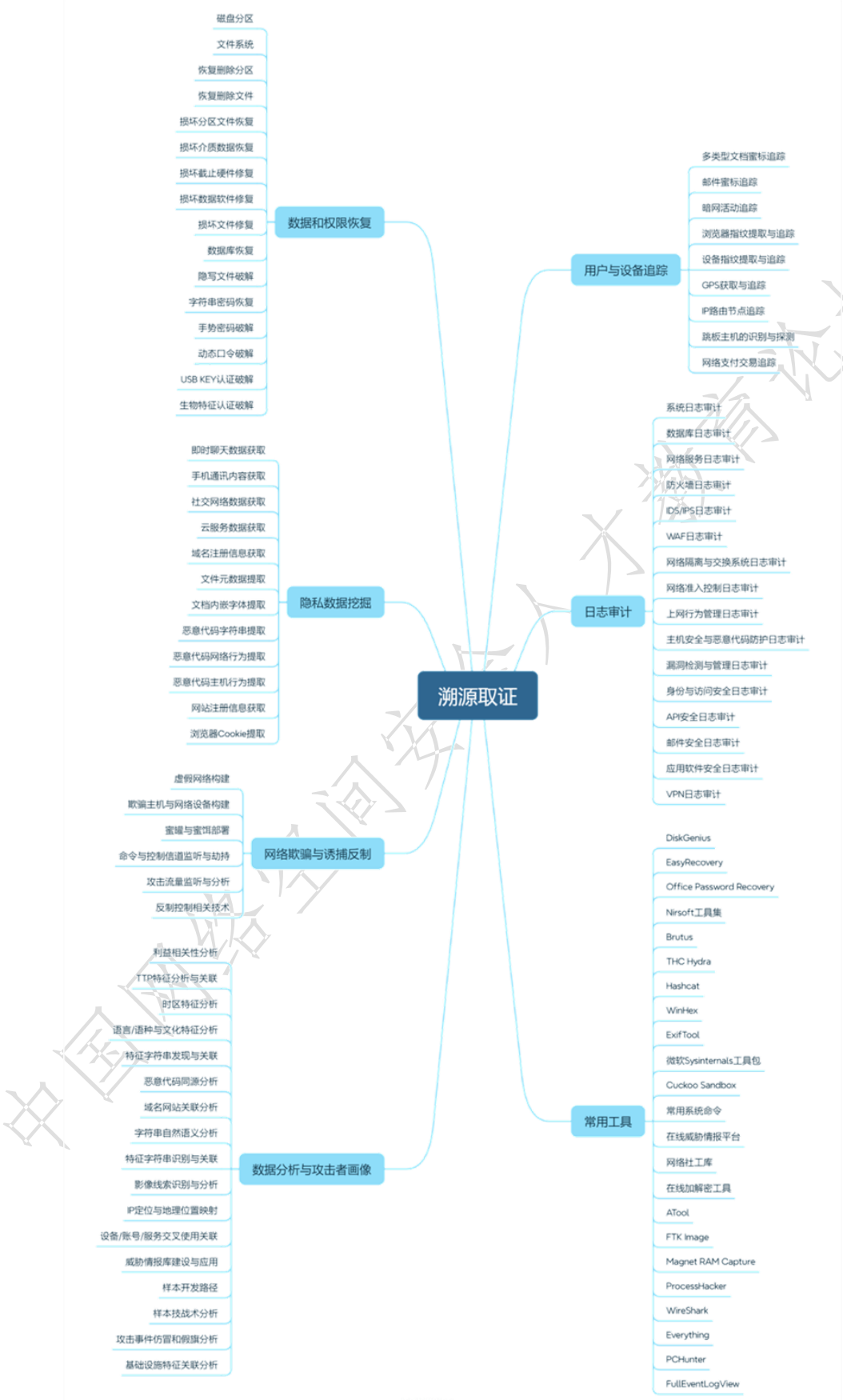
式，降低目标网络、系统、设备等的正常服务与运行能力，甚至彻底破坏目标的生存。对信息系统造成降级和破坏是恶意代码的主要危害之一。降级与破坏的技术有 DoS/DDoS、文件与数据加密、系统干扰与劫持、硬件/固件破坏、数据删除与篡改、磁盘与分区破坏等。

（6）规避与对抗。从 DOS 时代起，病毒与杀毒软件的对抗就已拉开帷幕并不断升级演进。今天的恶意代码采用的规避手段早已超越病毒时代的 EPO、多态、变形和加壳，而且已不限于纯技术手段，而杀毒软件也从单一化终端软件演化为端-网-云全覆盖、融入人工智能技术、具备态势感知能力的叠加演进防御体系。规避与对抗的技术包括反病毒软件绕过、虚拟机/沙箱识别与穿透、防火墙穿透、代码混淆、安全软件关停与破坏、合法证书签名、插件动态下载、身份痕迹擦除与伪装、载荷与意图隐藏、加壳、白名单进程利用、多态技术、反调试技术、虚拟化技术等。

（7）获利。恶意代码入侵成功后的获利方式。获利技术包括勒索钱财、盗取数据、窃取算力、侵占带宽和盗用 IP 等。

7. 溯源取证知识技能体系

在网络安全领域，溯源取证是指通过科学的方法和专业的工具收集、保留证据，对网络攻击或安全事件的来源、路径及相关证据进行深入追踪与分析的过程；旨在确定攻击者的身份、行为模式、攻击手段和攻击动机，并以收集到的充足证据有效支持后续的法律追责程序或防御措施制定。溯源取证知识技术重点关注 APT 攻击追踪溯源和网络犯罪取证，是维护网络安全、打击网络犯罪的关键环节。本指南聚焦于溯源取证知识技术体系建设及其实战应用，将溯源取证划分为数据和权限恢复、网络欺骗与诱捕反制、日志审计、用户与设备追踪、隐私数据挖掘、数据分析与攻击者画像、常用工具等 7 个核心组成部分。



（1）数据和权限恢复。数据和权限恢复是指一种在攻击者非配合甚至故意破坏的情况下，访问其存储介质、物理设备、网络服务的取证技术手段。数据和权限恢复知识技能包括磁盘分区、文件系统、恢复删除分区、恢复删除文件、损坏分区文件恢复、损坏介质数据恢复、损坏截止硬件修复、损坏数据软件修复、损坏文件修复、数据库恢复、隐写文件破解、字符串密码恢复、手势密码破解、动态口令破解、USB KEY 认证破解、生物特征认证破解等。

（2）网络欺骗与诱捕反制。网络欺骗是指为使用骗局或者假动作来误导攻击行为，诱捕网络攻击，从而更好地为溯源取证创造条件。诱捕反制是指一种高效的溯源取证手段，但是可能涉及司法有效性问题。网络欺骗主要技能包括虚假网络构建、欺骗主机与网络设备构建、蜜罐与蜜饵部署；诱捕反制主要技术包括命令与控制信道监听与劫持、攻击流量监听分析、反制控制相关技术等。

（3）日志审计。日记审计是指通过审计各类日志可以发现网络攻击留下的时间、活动、IP 地址、漏洞利用代码、账号等线索，从而分析出网络攻击大致的源头和过程。日记审计主要技能包括系统日志审计、数据库日志审计、网络服务日志审计、防火墙日志审计、IDS/IPS 日志审计、WAF 日志审计、网络隔离与交换系统日志审计、网络准入控制日志审计、上网行为管理日志审计、主机安全与恶意代码防护日志审计、漏洞检测与管理日志审计、身份与访问安全日志审计、API 安全日志审计、邮件安全日志审计、应用软件安全日志审计和 VPN 日志审计等。

（4）用户与设备追踪。用户与设备追踪主要解决两方面问题：第一，建立攻击者的网络身份、真实身份、设备和攻击事件间的交叉关联关系，并形成持续稳定追踪以刻画整个攻击过程甚至揭露攻击者的真实身份；第二，追踪攻击行为本身及附加行为所产生的网

络痕迹，以发现其与攻击者真实身份的关联线索。用户与设备追踪主要技术包括多类型文档蜜标追踪、邮件蜜标追踪、暗网活动追踪、浏览器指纹提取与追踪、设备指纹提取与追踪、GPS 获取与追踪、IP 路由节点追踪、跳板主机的识别与探测、网络支付交易追踪等。

（5）隐私数据挖掘。隐私数据挖掘是指在溯源取证过程中可对用户主动公开的个人数据、网络服务商安全措施保护范围之外的数据、执法机构依法获取的数据、攻击者在恶意代码中泄露的隐私数据进行主动提取和分析，合理合法地利用这些数据进行溯源取证。因此，隐私数据挖掘主要技术包括即时聊天数据获取、手机通讯内容获取、社交网络数据获取、云服务数据获取、域名注册信息（Whois）获取、文档元数据（Metadata）提取、文档内嵌字体提取、恶意代码字符串提取、恶意代码网络行为提取、恶意代码主机行为提取、网站注册信息获取和浏览器 cookie 提取等。

（6）数据分析与攻击者画像。数据分析与攻击画像是指溯源攻击者身份最为重要的环节，基于已获取的关键线索，以威胁情报等数据为信息储备，利用大数据、人工智能等技术手段，实现线索溯源与攻击者身份映射，最大程度刻画其身份特征。数据分析与攻击者画像主要技能包括利益相关性分析、TTP 特征分析与关联、时区特征分析、语言/语种与文化特征分析、特征字符串发现与关联、恶意代码同源分析、域名网站关联分析、字符串自然语义分析、特征字符串识别与关联、影像线索识别与分析、IP 定位与地理位置映射、设备/账号/服务交叉使用关联、威胁情报库建设与应用、样本开发路径、样本技战术分析、攻击事件仿冒和假旗分析、基础设施特征关联分析等。

（7）常用工具。常用工具主要包括 DiskGenius、EasyRecovery、Office Password Recovery、Nirsoft 工具集、Brutus、THC Hydra、

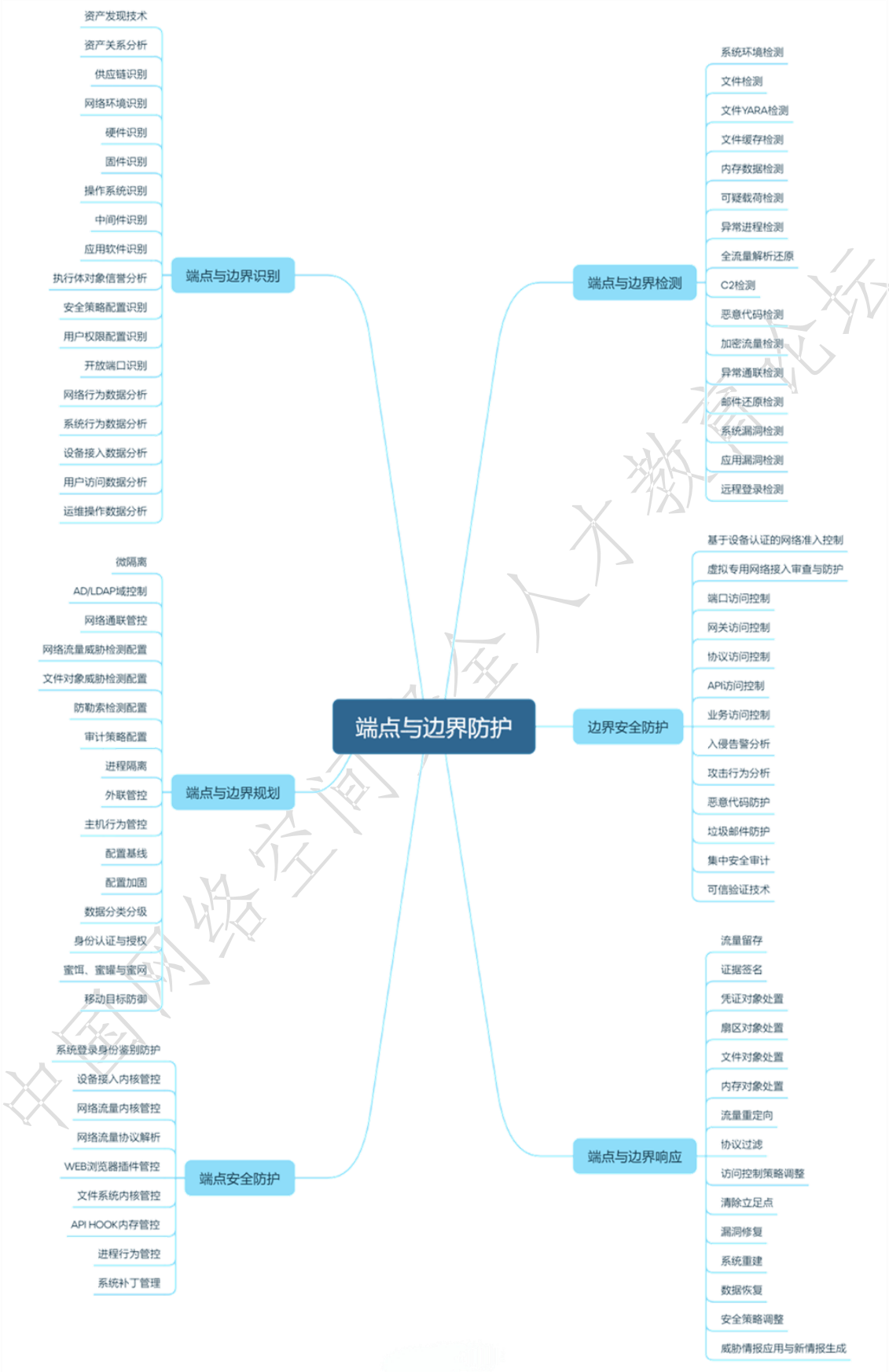
Hashcat、WinHex、ExifTool、微软 Sysinternals 工具包、Cuckoo Sandbox、常用系统命令、在线威胁情报平台、网络社工库、在线加解密工具、ATool、FTK Image、Magnet RAM Capture、ProcessHacker、WireShark、Everything、PCHunter、FullEventLogView 等。

8. 端点与边界防护知识技能体系

端点与边界防护是指通过一系列技术手段，保护网络中的终端设备和网络边界免受恶意入侵、数据窃取及其他安全威胁。它涵盖了对端点设备的监控、访问控制和数据防泄漏等技术，以及在网络边界通过防火墙、入侵检测与防御等技术过滤和阻止潜在威胁。本指南聚焦保障网络安全的关键防线，将端点与边界防护体系划分为端点与边界识别、端点与边界规划、端点安全防护、边界安全防护、端点与边界检测、端点与边界响应等 6 个核心组成部分。

（1）端点与边界识别。端点与边界识别是网络安全管理的基础。通过提升组织对网络安全风险的认识能力，加以对系统、人员、资产、数据以及功能等进行网络安全管理，旨在提升组织对自身的认知。端点与边界识别技术包括资产发现技术、资产关系分析、供应链识别、网络环境识别、硬件识别、固件识别、操作系统识别、中间件识别、应用软件识别、执行体对象信誉分析、安全策略配置识别、用户权限配置识别、开放端口识别、网络行为数据分析、系统行为数据分析、设备接入数据分析、用户访问数据分析、运维操作数据分析等。

（2）端点与边界规划。端点与边界规划是建立防御主动性的前提，是指对关键系统要素制定标准、定义系统控制原则或利用资产、拓扑、场景以及环境等的识别进行模拟的过程，旨在更好的与对手进行威胁对抗活动。端点与边界规划技术包括微隔离、AD/LDAP 域



控制、网络通联管控、网络流量威胁检测配置、文件对象威胁检测配置、防勒索检测配置、审计策略配置、进程隔离、外联管控、主机行为管控、配置基线、配置加固、数据分类分级、身份认证与授权、移动目标防御及蜜饵、蜜罐与蜜网等。

（3）端点安全防护。端点安全防护是对威胁做出的防御行为。是指通过制定并执行具有针对性的保障措施，使组织具备限制或控制潜在网络安全事件产生影响的能力，旨在确保关键服务的网络安全性。端点安全防护技术包括系统登录身份鉴别防护、设备接入内核管控、网络流量内核管控、网络流量协议解析、WEB 浏览器插件管控、文件系统内核管控、API HOOK 内存管控、进程行为管控、系统补丁管理等。

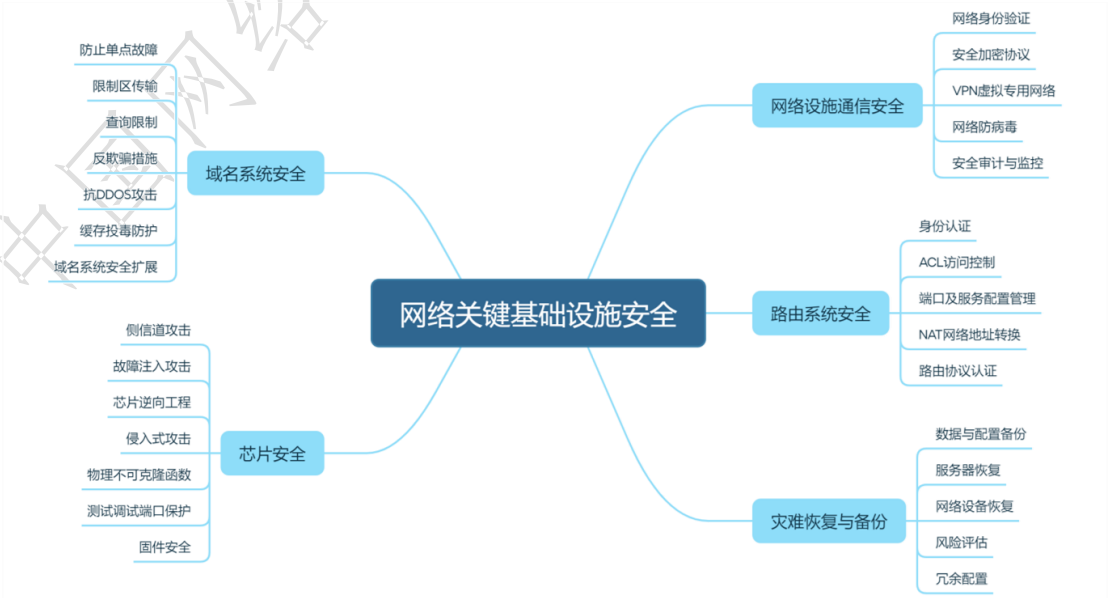
（4）边界安全防护。边界安全防护是对威胁做出的防御行为。是指通过制定并执行具有针对性的保障措施，使组织具备限制或控制潜在网络安全事件影响的能力，旨在确保关键服务的网络安全性。边界安全防护技术包括基于设备认证的网络准入控制、虚拟专用网络接入审查与防护、端口访问控制、网关访问控制、协议访问控制、API 访问控制、业务访问控制、入侵告警分析、攻击行为分析、恶意代码防护、垃圾邮件防护、集中安全审计、可信验证技术等。

（5）端点与边界检测。端点与边界检测是发现、定位和定性网络安全威胁方法的统称。是指制定并执行适当的行动对边界、端点、流量等进行检测，发现系统存在或潜在的漏洞、风险等，旨在避免网络安全事件的发生。端点与边界检测技术包括系统环境检测、文件检测、文件 YARA 检测、文件缓存检测、内存数据检测、可疑载荷检测、异常进程检测、全流量解析还原、C2 检测、恶意代码检测、加密流量检测、异常通联检测、邮件还原检测、系统漏洞检测、应用漏洞检测以及远程登录检测等。

（6）端点与边界响应。端点与边界响应是处理、管理风险和威胁事件的过程。指通过制定并执行适当的行动，利用组织所具备的控制潜在网络安全事件影响的能力，对检测到的网络安全事件采取处置措施，旨在清除网络安全事件影响。端点与边界响应技术包括流量留存、证据签名、凭证对象处置、扇区对象处置、文件对象处置、内存对象处置、流量重定向、协议过滤、访问控制策略调整、清除立足点、漏洞修复、系统重建、数据恢复、安全策略调整以及威胁情报应用与新情报生成等。

9. 网络关键基础设施安全知识技能体系

网络关键基础设施安全旨在保护国家和社会赖以运行的核心设施的安全性。这些设施一旦遭到破坏或数据泄露，将对国家安全、经济发展和公共利益造成严重威胁。网络关键基础设施安全关注保护这些设施的完整性、可用性和敏感数据的保密性，对于维护国家安全、社会稳定和经济发展至关重要。本指南聚焦于网络关键基础设施安全技术体系，将网络关键基础设施安全划分为域名系统安全、路由系统安全、网络设施通信安全、芯片安全、系统软件安全等5个核心组成部分。



（1）域名系统安全。域名系统实现了域名和IP等标识之间的映射转换，是支撑网络设备互联、网络资源访问、网络应用、网络服务等的网络关键基础设施。域名系统在支撑互联网持续高效平稳地运行的同时，也遭受着包括缓冲区溢出攻击、域名污染、域名欺骗、拒绝服务攻击在内的各类攻击。域名系统安全技术主要包含防止单点故障、限制区传输、查询限制、反欺骗措施、抗 DDOS 攻击、缓存投毒防护、域名系统安全扩展（DNSSEC)等。

（2）路由系统安全。路由系统安全是指作为网络互联的重要基础功能，以各类路由器为核心部件的路由系统成为关键基础设施中重要的安全防护目标。路由系统安全主要技术包括身份认证、ACL访问控制、端口及服务配置管理、NAT 网络地址转换、路由协议认证等。

（3）网络设施通信安全。通信网络安全是指保护通信网络（例如互联网、移动通信网络等）和其中的信息免受非法访问、攻击、破坏和窃取的一系列技术和管理措施。通信网络安全主要技术包括网络身份验证、安全加密协议、VPN 虚拟专用网络、网络防病毒、安全审计与监控。

（4）芯片安全。芯片处于整个系统最底层，它的安全问题会带来系统软件、应用软件、互联网络等一系列的安全问题，并且无法通过传统手段加以解决，软件和硬件联合起来是解决芯片安全问题的重要手段。芯片硬件安全问题有很多，包括未知的软硬件漏洞、预设的软硬件后门、智能持续病毒攻击等。芯片安全需要综合考虑设计、制造、封装过程中存在的漏洞，通过安全的芯片架构以及相关的检测防御技术来保证。芯片安全主要技术包括侧信道攻击、故障注入攻击、芯片逆向工程、侵入式攻击、物理不可克隆函数、测试调试端口保护、固件安全等。

（5）灾难恢复与备份。灾难恢复与业务连续性对于网络关键基础设施安全具有重要意义。它不仅可以帮助企业防止业务中断、保护企业声誉和符合法规要求，还可以降低财务损失、保障客户信任和提高组织弹性。灾难恢复与备份主要技能包含数据与配置备份、服务器恢复、网络设备恢复、风险评估、冗余配置等。

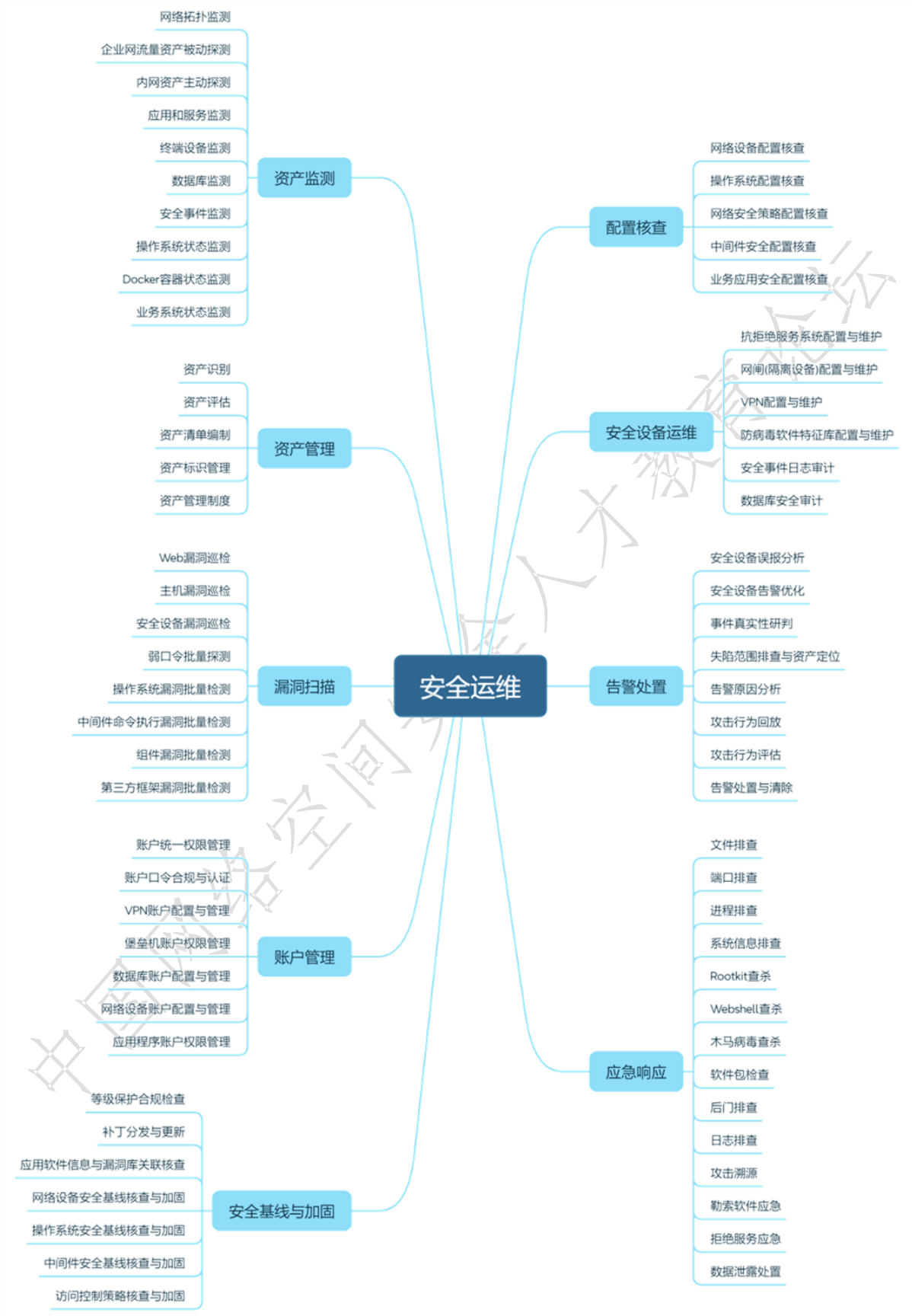
10. 安全运维知识技能体系

安全运维是维护信息系统安全稳定运行的核心环节。在信息化、网络化、数字化飞速发展的时代背景下，安全运维通过实时监测、风险预警、应急响应等措施，构筑起坚固的网络安全防线，确保数据资产不受侵害，以及网络系统能够稳定、安全、高效的运行。本指南聚焦于安全运维技术体系，将安全运维划分为资产监测、资产管理、配置核查、安全基线与加固、账户管理、漏洞扫描、安全设备运维、告警处置、应急响应等 9 个核心组成部分。

（1）资产监测。资产监测是安全运维的基础。通过IT资产监测，确保企业运维资产不被遗漏，IT 资产在可见、可控和可管条件下实施。资产监测主要包括网络拓扑监测、企业网络流量资产被动探测、内网资产主动探测、应用和服务监测、终端设备监测、数据库监测、安全事件监测、操作系统状态监测、Docker 容器状态监测、业务系统状态监测等。

（2）资产管理。资产管理是安全运维重要工作之一。资产管理能够帮助运维团队实时掌握 IT 资产的状态，包括硬件、软件、网络设备等，确保这些资产处于最佳运行状态。资产管理主要包括资产识别、资产评估、资产清单编制、资产标识管理、资产管理制度的完善等。

（3）配置核查。配置核查是安全运维日常工作之一。运维工作人员通过定期核查配置，查缺补漏，确保企业网络安全配置的有效



性以及合规性。配置核查主要包括网络设备配置核查、操作系统配置核查、网络安全策略配置核查、中间件安全配置核查、业务应用安全配置核查等。

（4）安全基线与加固。安全基线与加固是安全运维重要工作之一。通过建立安全基线，确保企业安全建设符合国家政策需求和企业自身安全建设的最低要求。安全基线与加固主要包括等级保护合规性检查、补丁分发与更新、应用软件信息与漏洞库关联核查、网络设备安全基线核查与加固、操作系统安全基线核查与加固、中间件安全基线核查与加固、访问控制策略核查与加固等。

（5）账户管理。账户管理是力图消除企业员工账户使用不规范、不合规带来的安全隐患，避免因员工账户、口令和权限的安全问题给整个企业网络环境带来更大的安全隐患。账户管理主要包括账户统一权限管理、账户口令合规与认证、VPN 账户配置与管理、堡垒机账户权限管理、数据库账户配置与管理、网络设备账户配置与管理、应用程序账户权限管理等。

（6）漏洞扫描。漏洞扫描是安全运维日常主要工作之一。通过漏洞扫描与漏洞巡检，能够全面了解企业网络安全风险状况，及时了解新增的高危漏洞和企业暴露的漏洞情况。漏洞扫描工作主要包括 Web 漏洞巡检、主机漏洞巡检、安全设备漏洞巡检、弱口令批量探测、操作系统漏洞批量检测、中间件命令执行漏洞批量检测、组件漏洞批量检测、第三方框架漏洞批量检测等。

（7）安全设备运维。安全设备运维是安全运维日常主要工作之一。通过安全设备运维来保障企业的安全防护体系不被随意打破。安全设备运维工作主要包括抗拒绝服务系统（Anti-DDoS 系统）配置与维护、网闸（网络安全隔离设备）配置与维护、VPN 配置与维护、防病毒软件特征库配置与维护、安全事件日志审计以及数据库安全

审计等。

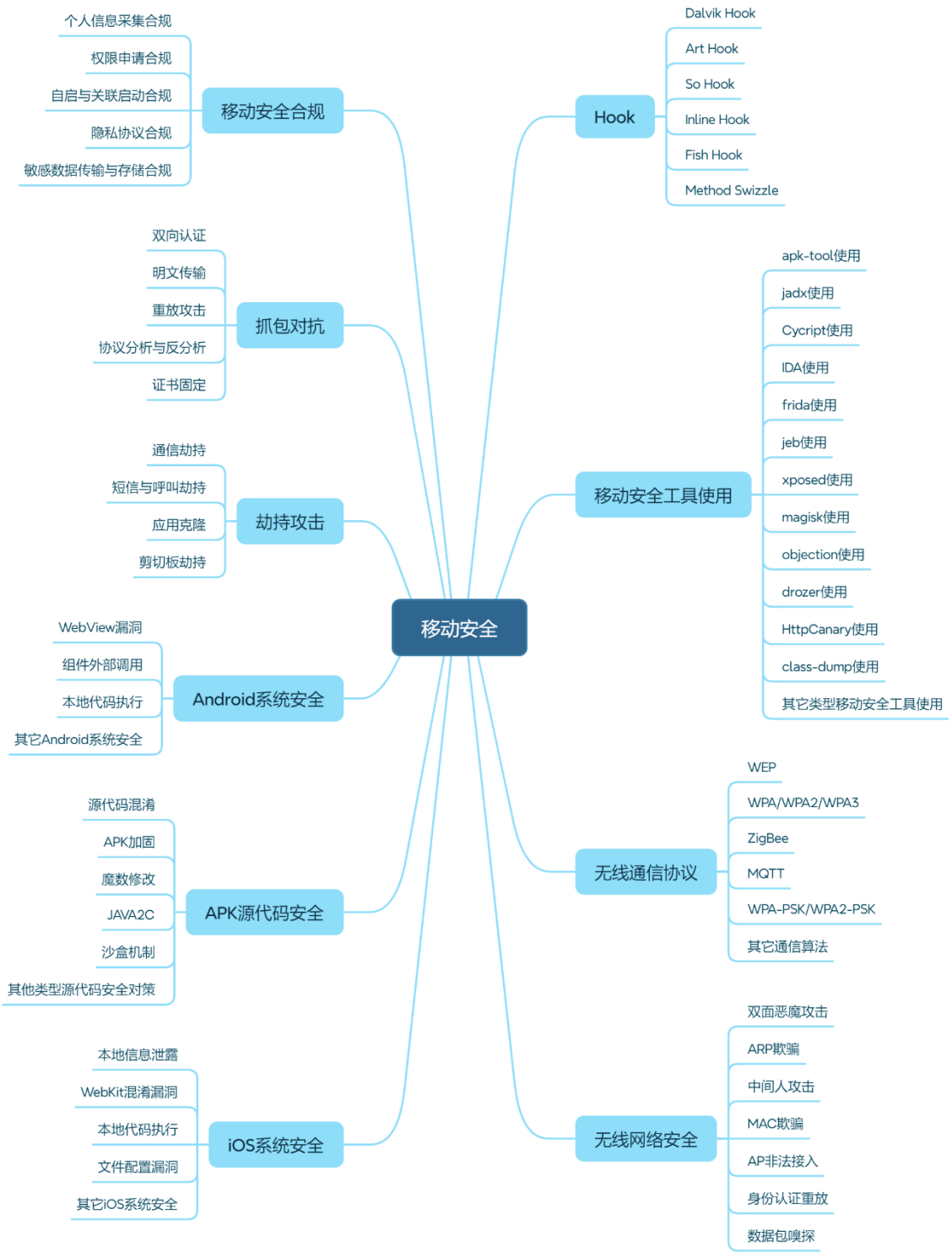
（8）告警处置。告警处置是安全运维重要工作之一。通过处置安全设备/系统的告警，保障企业能够有效地检测与防御外部攻击，并且能够及时发现与修复企业自身的安全缺陷。告警处置主要包括安全设备误报分析、安全设备告警优化、事件真实性研判、失陷范围排查与资产定位、告警原因分析、攻击行为回放、攻击行为评估、告警处置与清除等。

（9）应急响应。应急响应是安全运维重要工作之一。企业需要在各种意外的安全事件发生后采取有效的应对措施，力保将企业因安全事件造成的损失降低到最小。应急响应主要包括文件排查、端口排查、进程排查、系统信息排查、Rootkit 查杀、Webshell 查杀、木马病毒查杀、软件包检查、后门排查、日志排查、攻击溯源、勒索软件应急、拒绝服务应急、数据泄露处置等。

11. 移动安全知识技能体系

随着计算机技术的进步与移动互联网的迅速发展，智能手机、移动平板、各种各样的蓝牙产品等移动设备日益普及。近些年来，移动设备更是从日常消遣品和通讯工具逐步发展为兼具办公、金融、身份认证等功能的个人便携式终端。本指南聚焦于移动设备及与移动设备密切相关的移动无线网络的安全技术体系，将移动安全分为移动安全合规、抓包对抗、劫持攻击、Android 系统安全、APK 源代码安全、iOS 系统安全、Hook、移动安全工具使用、无线通信协议、无线网络安全等 10 部分。

考虑“指南”的整体性，部分与移动安全一级标签关系密切的如漏洞挖掘、社会工程学、沙盒逃逸等二级或三级标签已包含在其他一级标签内，此类内容不再本标签重复。



（1）移动安全合规。移动安全合规包括个人信息采集合规、权限申请合规、自启与关联启动合规、隐私协议合规、敏感数据传输与存储合规等。

（2）抓包对抗。抓包对抗是指目前移动端对于抓包的对抗几乎都基于中间人（MITM）攻击，而对抗也围绕着这一点展开。因此，抓包对抗主要技术包括双向认证、明文传输、重放攻击、协议分析与反分析、证书固定等。

（3）劫持攻击。劫持攻击是指攻击者通过某些特定的手段，将本该正确返回给用户的数据进行拦截篡改，或将数据转发给攻击者。劫持攻击主要技术包括通信劫持、短信与呼叫劫持、应用克隆、剪切板劫持等。

（4）Android 系统安全。Android 系统安全是指作为目前全球安装量第一的开源移动系统，Android 在保持代码透明的同时也会面对比闭源系统更多的漏洞风险。Android 系统安全主要包括 WebView 漏洞、组件外部调用、本地代码执行及其他 Android 系统安全等。

（5）APK 源代码安全。源代码安全是指 APK 安全的基石。攻击者通常会通过反编译的源代码对客户端进行代码审计并从中找寻漏洞和 API 路由。APK 源代码安全主要包括源代码混淆、APK 加固、魔数修改、Java2c、沙盒机制、其他类型源代码安全对策等。

（6）iOS 系统安全。作为目前移动端安装量最大的闭源操作系统之一，iOS 以高度封闭性和严格的安全措施著称。但在过去的十数年内 iOS 也被曝出过存在多种类型的漏洞。iOS 系统安全主要包括本地信息泄露、WebKit 混淆漏洞、本地代码执行、文件配置漏洞、其它 iOS 系统安全等。

（7）Hook。Hook 是指在移动端测试中一种非常重要的技术手段，也是开发者通常会检测和规避的一项内容。Hook 允许攻击者在不修改客户端内容的情况下跟踪运行时变量或修改返回值，以达到破解客户端加密算法或破坏客户端运行状态的效果。Hook 主要技能包括 Dalvik Hook、Art Hook、So Hook、Inline Hook、Fish Hook、

Method Swizzle 等。

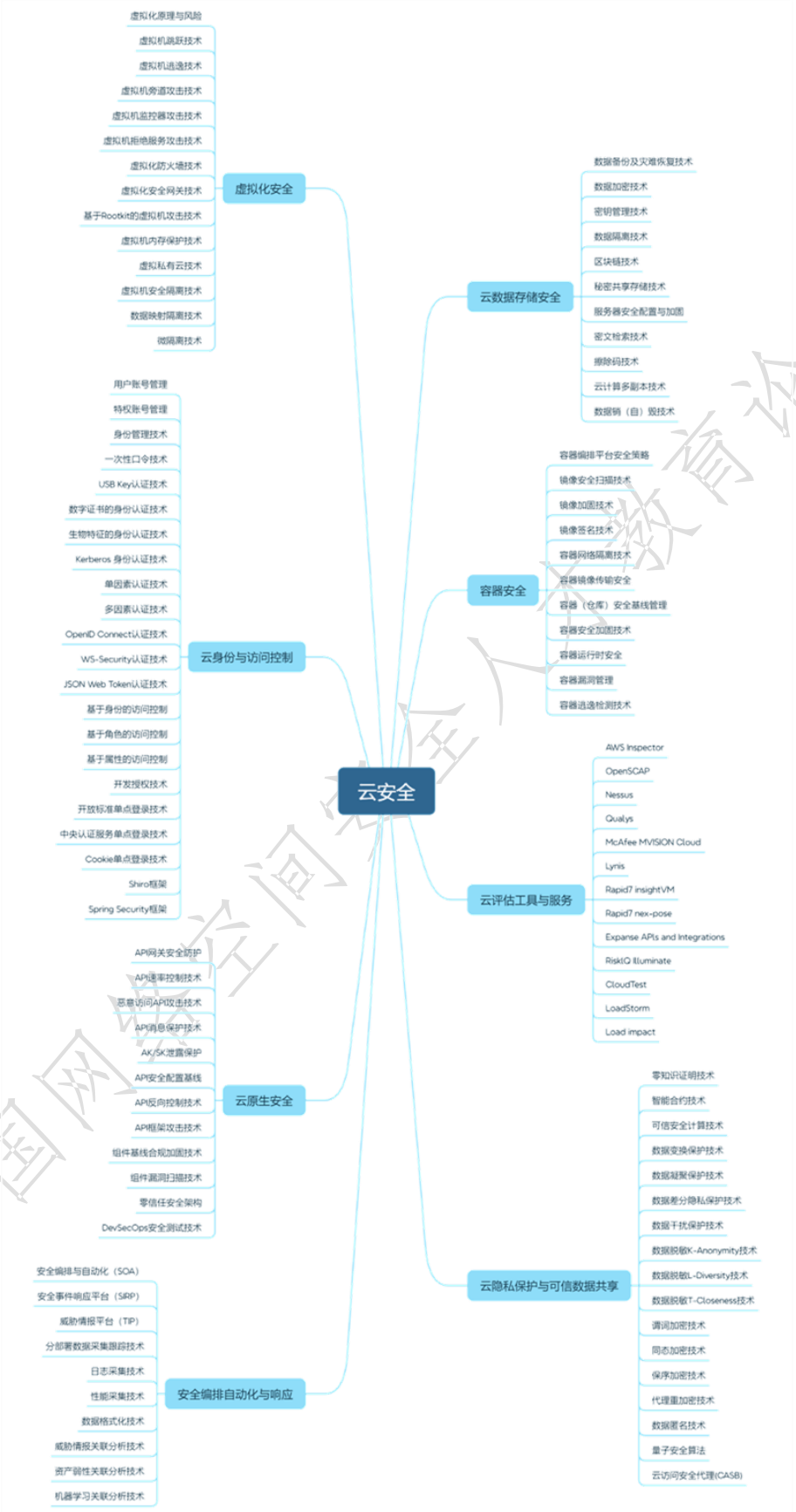
（8）移动安全工具使用。移动安全工具的使用能够有效提高工作效率、发现潜藏安全问题，使用移动安全工具可以进行信息收集、漏洞探测、漏洞利用等操作。移动安全工具主要技术包括 apk-tool 使用、jadx 使用、Cycript 使用、IDA 使用、frida 使用、jeb 使用、xposed 使用、magisk 使用、objection 使用、drozer 使用、HttpCanary 使用、class-dump 使用、其他类型移动安全工具使用等。

（9）无线通信协议。无线通信协议是指在无线网络中（如 WIFI、蓝牙）通常会使用 WEP/WPA/MQTT 等通信协议，也有很多自建的其它通信协议。无线通信协议主要包括 WEP、WPA/WPA2/WPA3、ZigBee、MQTT、WPA-PSK/WPA2-PSK、其它通信算法等。

（10）无线网络安全。无线网络安全包括三大类，一类是基于 ARP/MAC 的欺骗攻击；一类是基于数据包嗅探和重放的中间人攻击；一类是基于 AP 欺骗的钓鱼。无线安全网络主要技术包括双面恶魔攻击、ARP 欺骗、中间人攻击、MAC 欺骗、AP 非法接入、身份认证重放、数据包嗅探等。

12. 云安全知识技能体系

云安全是指在云计算环境中保护数据、应用和基础设施的技术和策略，旨在确保云服务的安全性、合规性和隐私保护。随着云计算的迅速普及，企业和个人越来越依赖云服务进行数据存储和处理，因此云安全的重要性愈发凸显。本指南聚焦于云安全技术体系，将云安全划分为虚拟化安全、云身份与访问控制、安全编排自动化与响应、云数据存储安全、容器安全、云原生安全、云评估工具与服务、云隐私保护与可信数据共享这 8 个核心组成部分。



（1）虚拟化安全。虚拟化技术已成为云计算的主要基础支撑技术，为云应用场景的高弹性、高可用性要求提供了可行的基础前提。在共享底层池化资源的基础上独立运行的虚拟设施也面临着自身脆弱性被利用的风险。虚拟化安全涉及的主要技术包括：虚拟化原理与风险、虚拟机跳跃技术、虚拟机逃逸技术、虚拟机旁道攻击技术、虚拟机监控器攻击技术、虚拟机拒绝服务攻击技术、虚拟化防火墙技术、虚拟化安全网关技术、基于 Rootkit 的虚拟机攻击技术、虚拟机内存保护技术、虚拟私有云（VPC）技术、虚拟机安全隔离技术、数据映射隔离技术以及微隔离技术等。

（2）云身份与访问控制。云身份与访问控制是由云服务提供商或租户对云环境中各类应用、场景资源访问的合法身份标识和授权管理的基础设施，应具有部署较快速、兼容性较强、维护成本低、自身安全性可靠、扩展性良好等特点。云身份与访问控制在云安全中，扮演着资源合法访问识别和授权的重要关卡的角色，是合法与非法访问的重要分水岭。云身份与访问控制的主要技术包括用户账号管理、特权账号管理、身份管理技术、一次性口令技术、USB Key 认证技术、数字证书的身份认证技术、生物特征的身份认证技术、Kerberos 身份认证技术、单因素认证技术、多因素认证技术、OpenID Connect 认证技术、WS-Security 认证技术、JSON Web Token 认证技术、基于身份的访问控制、基于角色的访问控制、基于属性的访问控制、开发授权技术（OAuth）、开放标准（SAML）单点登录技术、中央认证服务（CAS）单点登录技术、Cookie 单点登录技术、Shiro 框架、Spring Security 框架等。

（3）安全编排自动化与响应。安全编排自动化与响应是在边界融合、软件定义边界的云环境中，面对海量资产的场景中，集合资产动态信息、威胁情报、事件响应、安全编排等多维度融合的综合

性技术。安全编排自动化与响应可根据安全剧本设置，建立多方位、全流程、快决策的自动化响应处置机制。安全编排自动化与响应的主要技术包括安全编排与自动化（SOA）、安全事件响应平台（SIRP）、威胁情报平台（TIP）、分布式数据采集跟踪技术、日志采集技术、性能采集技术、数据格式化技术、威胁情报关联分析技术、资产弱性关联分析技术以及机器学习关联分析技术等。

（4）云数据存储安全。云数据存储安全以云端数据生命周期为主线，为数据提供安全的保护技术，兼顾数据存储安全、使用安全、数据销毁等功能需求，以及面对数据威胁（数据泄露、数据丢失、数据删除等）时，均能确保数据的机密性、完整性、可用性得以实现，由此共同构成云数据存储安全。云数据存储安全的主要技术包括数据备份及灾难恢复技术、数据加密技术、密钥管理技术、数据隔离技术、区块链技术、秘密共享存储技术、服务器安全配置与加固、密文检索技术、擦除码技术、云计算多副本技术、数据销（自）毁技术等。

（5）容器安全。容器安全聚焦于容器相关组件和应用的安全防护。容器在云原生时代，以其快速拉取、方便部署的优势特点，占据着重要地位，为应用的高弹性、高可用方案落地提供了支撑。容器安全涉及的主要技术包括容器编排平台的安全策略（如Kubernetes）、镜像安全扫描技术、镜像加固技术、镜像签名技术、容器网络隔离技术、容器镜像传输安全、容器（仓库）安全基线管理、容器安全加固技术、容器运行时安全、容器漏洞管理、容器逃逸检测技术等。

（6）云原生安全。云原生安全聚焦于云原生架构、组件和应用安全。近些年，借助于开源社区的力量，云原生脱颖而出，围绕着云原生架构和应用的最佳实践，相关技术也呈现出高速迭代的趋势。

云原生环境下的自有特性的安全问题、安全防护呈现安全左移趋势，可归纳为 API 防护、组件安全、动态的安全开发测试三个方面。云原生安全设计的主要技术包括 API 网关安全防护、API 速率控制技术、恶意访问API攻击技术、API消息保护技术、AK/SK泄露保护、API 安全配置基线、API 反向控制技术、API 框架攻击技术、组件基线合规加固技术、组件漏洞扫描技术、零信任安全架构（Zero Trust Security）、DevSecOps 安全测试技术等。

（7）云评估工具与服务。云评估工具和服务旨在快速发现云计算平台存在的风险。云服务提供方需对自身云的安全能力进行周期性评估，云用户也需对自身管理区域内的资产安全进行评估，以及监督管理机构执行监督职权时，均需要体系、高效的工具/服务。云评估工具和服务主要涉及（含商业软件）:AWS Inspector、OpenSCAP、Nessus、Qualys、McAfee MVISION Cloud、Lynis、Rapid7、insightVM、Rapid7 nex-pose、Expanse APIs and Integrations、RisklQ Illuminate、CloudTest、LoadStorm、Load impact。

（8）云隐私保护与可信数据共享。云隐私保护是一种用于防止云中敏感数据泄露的技术。大数据分析应用技术为社会的发展、政策的制定提供了可靠的数据基准，但同时应防止个体识别数据、敏感数据的恶意使用，以及带来的隐私泄露风险，因此需要对云隐私数据进行安全防护，主要涉及三个方面：隐私安全保护、限制发布、隐私加密脱敏。云隐私保护的主要技术包括零知识证明（Zero-Knowledge Proofs）技术、智能合约技术、可信安全计算技术、数据变换保护技术、数据凝聚保护技术、数据差分隐私保护技术、数据干扰保护技术、数据脱敏K-Anonymity技术、数据脱敏L-Diversity技术、数据脱敏 T-Closeness 技术、谓词加密技术、同态加密技术、保序加密技术、代理重加密技术、数据匿名技术、量子安全算法、云

访问安全代理（CASB）等。

13. 物联网安全知识技能体系

伴随新一代物联网信息技术的深入发展和广泛应用，智慧城市和数字化转型建设快速发展，正日益对交通、医疗、生产、消费活动以及经济运行机制、社会生活方式产生重要影响，物联网安全建设已成为新型基础设施规划、建设、管理领域关注的重点。本指南聚焦于物联网安全建设和体系化防护技术，将物联网安全划分为身份认证、访问控制、数据加密、流量行为分析、攻击检测、安全事件分析、数据安全处理、安全监管等8个组成部分。由于物联网的强应用场景，其相关三级标签知识技能已在其他已述标签下讲述，此处不再重复。

（1）物联网接入身份认证。物联网接入身份认证是物联网终端接入系统中的第一道安全防线，物联网实体在交互通信和传输数据之前，必须验证其身份的真实性、合法性后才可允许接入。当身份认证机制不健全时，感知节点易被替换、仿冒接入，造成网络攻击。物联网接入身份认证技术主要包括 IoT 设备身份标识、IoT 设备密钥认证、安全连接行为认证、数字证书认证、密钥管理等。

（2）物联网访问控制。物联网访问控制是根据感知节点身份和所属定义组限制其访问信息系统或资源请求的认证和控制，防止非法感知节点的非法访问或者合法节点的不正当使用，确保整个物联网系统资源能够被合理正当地使用。物联网访问控制技术是确保物联网安全性的关键组成部分，主要包括基于属性的访问控制（ABAC）、基于角色的访问控制（RBAC）、基于任务的访问控制（TBAC）、信任评估与动态服务授权等。

（3）物联网数据加密。物联网数据加密指的是通过使用密码技术来保护物联网中的数据，能够确保数据在传输和存储过程中不被未经授权的第三方访问和篡改，从而保证数据的机密性、完整性和可用性，有效地保护用户的隐私和安全。物联网数据加密技术主要包括对称加密算法、非对称加密算法、完整性校验、SSL/TLS 协议、数字签名技术、轻量级加密算法等。

（4）物联网流量监控分析。物联网流量监控分析技术在应对物联网场景下的威胁监测与溯源时，基于网络流量分析的方法实现对网络攻击的识别恶意节点并进行防御，确保能够在入侵或者非法攻击发生时，能够及时的隔离问题系统和恢复正常的功能。物联网流量监控分析技术主要包括流量特征挖掘、终端指纹分析、物联网场景建模、流量分类算法、策略库匹配模型、流量线性采集解包技术、异构数据统一处理、高维特征计算技术等。

（5）物联网异常行为检测。物联网异常行为检测技术是对物联网终端进行分析建模，以多种维度，对物联网终端的日常行为设定活动范围，通过深度分析建模形成行为基线，对物联网终端的行为进行偏离分析，及时发现物联网终端的异常行为并其进行策略性阻断。物联网异常行为检测技术主要包括行为分析、动态防御、功率分析、流量分析、基于机器学习的检测、基于运动模式分析的检测、基于设备识别的检测等。

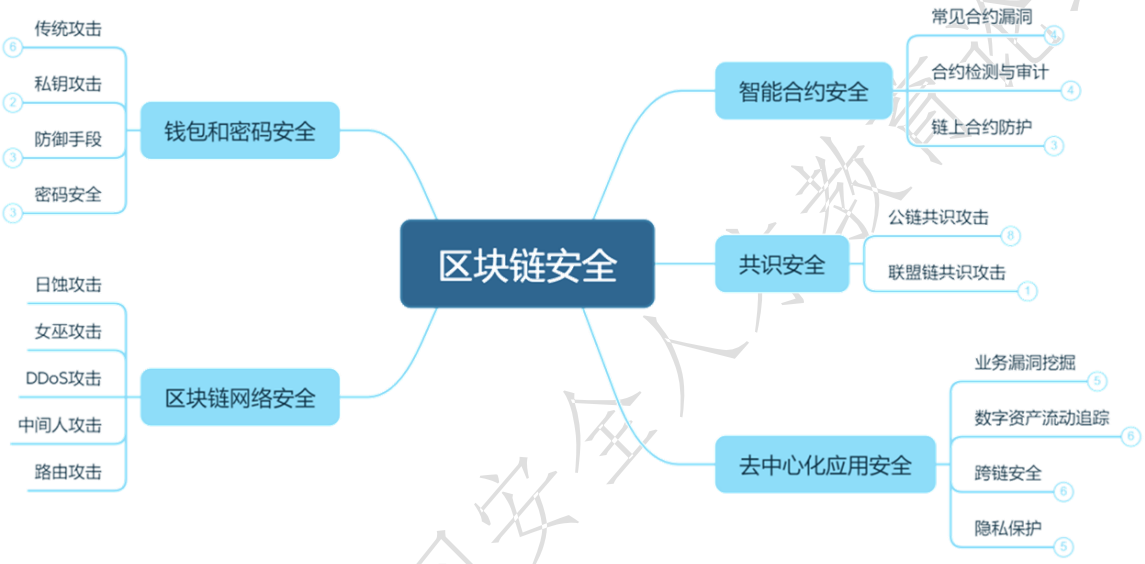
（7）物联网资产识别。物联网资产识别是对在网的物联网资产进行梳理并分析，对设备的厂商、类型进行识别和统计，对于进一步发现物联网设备的安全问题具有重要意义。物联网资产识别技术主要包括基于流量分析的识别、基于行为特征的识别、被动资产识别技术、传感定位技术、蜂窝通信定位与识别、短程无线通信定位与识别等。

（8）物联网漏洞扫描。物联网漏洞扫描是发现物联网设备安全隐患的重要手段，有效解决物联网终端由于软件漏洞、固件漏洞及安全缺陷所带来的威胁，识别物联网中的设备安全风险，采取防护手段。物联网漏洞扫描技术与计算机及计算机网络漏洞挖掘与利用中相关的漏洞挖掘、漏洞检测、漏洞缓解、漏洞分析等技术高度重合，但包含部分诸如固件提取、黑盒建模等物联网攻击技术。

（9）物联网安全监管。物联网安全监管是对海量物联网终端的实时可见、可管、可控，以及攻击的准确溯源定位，及时发现异常情况并采取措施来干预和防范未来的安全风险，同时为后续的安全分析提供数据支持。物联网安全监测技术与计算机网络安全监测相关技术具有一定的重叠，包括诸如情报分析、威胁分析、风险分析、攻击路径分析、态势预测等。

14. 区块链安全知识技能体系

本指南聚焦于区块链自身安全知识和技能，也即区块链内生安全。区块链系统体现层次化结构，可以划分为数据层、网络层、共识层、合约层、应用层，各层级安全问题和攻防模式差异显著。按照指南“从业人员工作内容”这一分类视角，将区块链安全划分为钱包和密码安全、区块链网络安全、共识安全、智能合约安全和去中心化（DApp，Decentralized Application）应用安全等 5 个核心部分。



（1）钱包和密码安全。钱包和密码安全包括传统攻击、私钥攻击、防御手段和密码安全 4 个方面。传统攻击方式包括钓鱼攻击、Web 攻击、钱包漏洞、浏览器漏洞、恶意插件、社工攻击等，攻击钱包所在 web 插件；私钥攻击包括私钥窃取、骗取交易签名，攻击区块链账户私钥；防御手段包括使用安全芯片、多重签名、加密通讯等方式；密码安全包括 SM2、SM3 和抗量子密码算法等算法。

（2）区块链网络安全。区块链网络安全主要指的面向区块链网络层 P2P 协议的攻击，包括日蚀攻击、女巫攻击、DDoS 攻击、中间人攻击、路由攻击等，其与常规计算机网络面临的网络层次安全具有较大的重叠性。

（3）共识安全。共识安全主要分为公链共识攻击、联盟链共识

攻击两部分，主要攻击交易排序过程，根据自身利益倾向对交易顺序进行调整（或者添加、阻止特定交易上链），进而获取非法利益。其中，公链共识攻击主要针对共识过程中的主链选择原则（例如最长链原则、最大分支原则）构建包含恶意交易的主链，并选择时机将其全网广播，用以替换原本的主链，包括 51%算力攻击、双花攻击、算力伪造、扣块攻击、自私挖矿、长程攻击、抢跑攻击、三明治攻击等；联盟链共识攻击主要指渗透排序节点，通过多节点共谋和投票操纵，促使攻击者控制的节点被选举为排序节点。

（4）智能合约安全。智能合约的安全问题、解决方案与传统软件基本一致。差异在于区块链账本不可篡改，因此智能合约一旦部署，其代码漏洞极难修复。智能合约安全一般包括常见合约漏洞、合约检测与审计、链上合约防护 3 个部分。其中，常见合约漏洞包括重入攻击、异常访问控制、整数溢出、短地址攻击等触发虚拟机指令异常执行的漏洞；合约检测与审计与传统软件测试方法类似，包括静态分析、动态分析、形式化验证、模糊测试等方法，目前工业界主要使用高度产品化的智能合约检测框架，并集成了多种面向智能合约开发的检测技术（例如静态分析、动态分析、形式化验证、模糊测试等），能够有效支撑智能合约在部署前的功能性与安全性检测；链上合约防护包括链上合约模糊测试、上链前攻击阻断、上链后交易回滚，链上合约模糊测试基于合约的世界状态在测试环境下进行模糊测试，上链前攻击阻断检测未上链合约和内存池交易是否为恶意交易以发起抢跑交易转移被攻击合约数字资产，上链后交易回滚将恶意交易的检测、拦截逻辑部署在被攻击合约内部以回滚攻击交易。

（5）去中心化应用安全。去中心化应用与传统应用的主要区别是其核心数据存储在区块链智能合约的状态数据中。去中心化应用

安全主要包括业务漏洞挖掘、数字资产流动追踪、跨链安全、隐私保护等4个部分。其中，业务漏洞通常并不触发虚拟机在执行指令时的非预期行为，而是基于常规业务的异常操作（或异常操作组合）触发违反正常业务逻辑的智能合约状态。对于此类智能合约漏洞，抛开合约业务语义，合约漏洞并不存在，而漏洞发现的关键在于对业务语义的理解（例如价格操控攻击，rug pull 等）。业务漏洞挖掘主要包括基于生成式大模型对业务漏洞的梳理，和基于标准化协议的业务流程总结，标准化协议的业务主要指去中心化应用、非同质代币、去中心化社交网络生态，主要业务漏洞包括，攻击结算机制、流通过程的授权和交易漏洞、链下数据的中心化管理风险、二层链单点故障等；数字资产流动追踪因承载大量非法交易、窃取数字资产并销赃、公共基础服务易追踪等恶性行为而备受关注，主要采用域名解析、交易时间、账户画像等方法；跨链协议的主要攻击方式是攻击可信中介的验证密钥（例如Ronin攻击、Harmony攻击等），或者攻击桥接合约的漏洞（例如Wormhole攻击、Nomad攻击等），主要攻击的对象是跨链交易的验证过程，其改进思路为使用更加鲁棒的去中心化验证网络替代可信中介，或使用主动式的跨链交易监控以对异常交易进行实时的拦截和处理。隐私保护主要采用零知识证明、同态加密、保密计算、链下执行等方式在智能合约中处理隐私数据。零知识证明允许一方（证明者）向另一方（验证者）证明其拥有某个特定信息（例如，数据的真实性）而不透露该信息的内容，典型应用有 zk-SNARKs、zk-STARKs。同态加密允许在合约中直接对密文进行等价算术计算，该技术使得在合约中聚合分布式联邦学习结果具有可行性。保密计算将合约执行验证环境放在了可信执行环境中，使得合约执行过程保密且可信，Oasis Network、Algorand、Secret Network 等区块链都使用可信执行环境增强合约数据的隐私保护。链下计算将主链计算任务迁移到侧链或者二层链中，

从而使得计算过程对主链不可见，典型技术如乐观汇总。

15. 人工智能安全知识技能体系

人工智能安全（Artificial Intelligence Security）是指保护人工智能系统免受威胁和攻击，确保其可靠、稳定和符合伦理道德标准。人工智能安全不仅涵盖了技术层面的安全，还包括了社会、法律、伦理等维度的安全，是一个多维度、跨学科且快速发展的领域。本指南聚焦于人工智能安全技术体系，将人工智能安全技术体系划分为业务安全、算法安全、数据安全、平台安全等4个核心组成部分。与其他具有领域应用特点的一级标签相似，人工智能安全相关二级及三级标签与已述标签下的知识技能具有一定的重叠，此处在内容上不再重复，但可随标签内容跟踪定位到前述标签。

（1）业务安全。业务安全包括安全攻击检测、业务安全防御、深度伪造检测、业务合规评估4部分。其中，安全攻击检测指识别和防御针对人工智能系统的各种安全威胁和攻击，主要技术包括对抗样本检测和算法后门检测；业务安全防御包括业务访问控制、业务安全隔离、业务安全冗余、业务安全熔断、业务安全监控；深度伪造检测指通过真实内容与伪造内容之间的特征差异进行真伪内容检

测，根据检测对象的不同，分为针对图像的深度伪造检测方法、针对视频的深度伪造检测方法，针对音频的深度伪造检测方法，针对文本的深度内容检测等；业务合规性评估是指确保 AI 业务操作符合相关的法律法规、行业标准和企业内部政策，主要包括自评估和第三方评估。

（2）算法安全。算法安全包括算法鲁棒性增强、算法公平性保障、算法可解释性提升、算法知识产权保护、算法安全评测。算法鲁棒性指算法在面对意外输入、噪声或恶意攻击时仍能保持正确性和稳定性的能力，算法鲁棒性增强主要技术包括数据增强、鲁棒特征学习、模型随机化、模型正则化、训练数据采样等；算法公平性是指算法在处理不同个体或群体时不会产生不公平的偏见或歧视，保障算法公平性的主要技术包括算法公平性约束、偏见歧视后处理；算法可解释性是指算法的决策过程和结果能够被人类理解和解释，提升算法可解释性主要技术包括模型自解释、算法全局解释、算法局部解释；算法知识产权保护是指保护算法版权、商业秘密等不受侵犯，主要技术包括加密和安全存储、模型水印；算法安全评测是指对算法的安全性进行全面评估，以确保其抵御攻击和错误的能力，算法安全评测主要技术包括鲁棒性评测、公平性评测、可解释性评测等。

（3）数据安全。数据安全包括数据隐私计算、数据追踪溯源、问题数据清洗、数据公平性增强、数据安全评测。数据隐私计算是指在不泄露个人隐私的前提下，对数据进行处理和分析的技术，主要技术包括安全多方计算、同态加密、零知识证明、差分隐私、可信执行环境、联邦学习等；数据追踪溯源是指能够追踪数据来源、使用历史和传播路径的技术，主要技术包括数据安全标签和区块链追踪溯源；问题数据清洗是指识别和纠正数据集中的错误、异常和

不一致性的过程，主要技术包括异常数据删除、问题数据重构、问题数据修复；数据公平性增强是指确保数据集在代表性、平衡性和无偏见方面的质量，以促进算法公平性，主要技术包括数据平衡、偏见检测、代表性增强；数据安全评测是指对数据的安全性进行全面评估，以确保数据不受未授权访问、泄露或其他安全威胁，主要包括数据合规性评测和数据泄露安全性评测。

（4）平台安全。平台安全包括模型文件校验、漏洞挖掘修复、框架平台安全部署。模型文件校验是指对人工智能模型文件的格式、大小、参数范围、网络拓扑、节点名称、数据维度等关键信息进行检测校验，在模型文件加载前发现存在的安全问题，防止恶意人工智能算法模型文件被加载；漏洞挖掘修复是指识别和修复人工智能平台中的安全漏洞，以防止潜在的攻击，主要技术包括代码审计、模糊测试、安全响应机制；框架平台安全部署是指确保人工智能框架和平台在部署时的安全性，主要技术包括环境安全、访问控制、数据保护、日志和监控、灾难恢复计划等。

第四章 网络安全工程技术人才培养路线

4.1 网安人才层次化培养必要性

从我国网络空间安全的现状和对网安人才需求特征来看，具有基本的网络空间安全认知和意识，了解基础的网络与安全保密方法，掌握常规加解密、防病毒等安全防护工具，是对庞大基数的网民、普通信息技术用户等的要求，对其只需要基础层次但却是最重要和广泛的认知意识培养。一线安全运营人员是网络空间安全人才队伍中规模最大、行业职责任务最关键的一类从业人员，对其的培养培训，需要兼顾理论知识、操作实践、沟通协作等，从而培养其“接近用户、靠近设备、触摸事件”的一线现场能力。工程技术开发人员肩负着网络信息系统、系统软件、安全工具等的设计、开发和解决方案的规划与实施，其培养成长的重点在问题分析能力、建模能力、方案设计与组织实施能力，以及程序设计、开发和系统的安全测试等。安全研究创新人员需要具备发现安全理论问题、提取并构建问题模型、创新理论和技术方法，从而推动网络空间安全理论发展与技术迭代进步，是网络空间安全领域科学问题的发现与解决者，是相关技术革命换代的推动者。对其培养应重在科学研究方法论的实践和科研实验方法的训练上。安全规划治理人员是组织、机构乃至区域或行业领域等的网络空间安全的管理者、规划者和监督人，不仅需要具备专业基础知识和丰富的工作经历，还需要管理能力、组织协调能力、前瞻与规划能力等，对其培养应不仅仅限于学校培训，还在于任职培训、任务培养，是一个长期的培养过程。

由此可见，不同类型网安人才，其工作内容、任职要求等存在较大区别，总体框架是从基础专业知识和基本工具运用，过渡到分析和构建，再到建模和研究，最后是监督和治理，具有明显的专业

化、层次化特点。对网安人才的培养，也应该构建层次化培养体系。

4.2 一线安全运营人员培养

在培养机制上，包括校内培养和任职集训两种。在培养形式上，包括以下几种。

（1）理论课程和实践结合。培训课程应该涵盖网络安全的理论知识，同时重视实际操作，如模拟演练、实际案例分析等，使学生/学员能够将学到的知识应用于实际工作中。

（2）导师制度。为学生配备实战经验丰富的老师，带领学生打牢实战实践技能基础，或为新入职的安全运营人员配备经验丰富的导师，帮助他们快速适应工作环境、提升技能。

（3）持续学习。网络安全领域发展迅速，培训计划应该是持续的，以保持安全人员的竞争力和对新技术的适应能力。

（4）团队合作。培训过程中加强团队合作，不仅有助于知识共享，还能锻炼团队协作能力。

在培养内容和路线上，包括以下几种。

（1）学习基础知识学习。从网络安全的基础知识开始，包括密码学、网络原理、操作系统安全等。

（2）培养专业技能。学习安全运营工具的使用，如入侵检测系统、防火墙配置等，同时了解常见的攻击手法和防范方法。

（3）安全实践。参与模拟演练和实际案例分析，锻炼应急响应能力和问题解决能力。

（4）参与认证考试。通过考试，推动或促进专业技术的提升，并加持个人专业和信誉。

（5）持续学习和成长。参加行业会议、研讨会，阅读最新安全

技术文献，保持对领域发展的关注，并不断提升自己的技能和知识。

通过以上形式和路线的培养，一线安全运营人员可以建立坚实的网络安全基础，提升自身的技能水平，更好地应对日益复杂的网络安全威胁。

4.3 工程技术开发人员培养

网络空间安全的工程技术开发人员在培养过程中需要掌握广泛的技术知识和实践经验。在培养机制上，以在校学习为主，以任职集训和自我学习为辅。在培养形式上，包括以下几种。

（1）项目实践。培养人员应该通过参与实际项目来学习，例如开发安全工具、参与漏洞挖掘、进行安全代码审计等。

（2）导师指导。为学生指派校内和企业双导师，尤其是企业导师，结合项目实践，帮助学生解决实际工程中遇到的问题，并传授行业经验。

（3）团队协作。学习和培训过程中加强团队协作，通过团队项目和合作来促进技术交流和共同进步。

（4）持续学习。网络安全技术日新月异，培训计划应该是持续的，鼓励持续学习和技术更新。

在培养内容和路线上，包括以下几种。

（1）学习基础知识。学生或受培养人员需要学习并掌握扎实的计算机科学基础知识，包括算法、数据结构、操作系统等。

（2）学习网络安全技术。学习网络安全领域的专业知识，包括攻击和防御技术、加密算法、安全协议等。

（3）培养编程技能。掌握至少一种编程语言，并深入了解安全编程实践，如安全代码审计、漏洞挖掘等。

（4）参与安全工具实践。通过项目实践的形式，参与开发网络安全工具和系统，如入侵检测系统、漏洞扫描工具、安全监控系统等，从工程项目实践中，认知并掌握软件工程、产品化等岗位化专业技能。

（5）参与开源社区。积极参与网络安全开源项目，学习开源社区开发模式和技术，提升开发能力和经验。

（6）参与考试认证。通过分析类、开发类、运营类等网络安全认证考试，推进并提升学生的技术水平和专业能力。

通过以上形式和路线的培养，工程技术开发人员可以建立扎实的网络安全技术基础，掌握实际开发经验，提升自身的技术水平和创新能力，更好适应网络空间安全领域岗位的需要。

4.4 安全研究创新人员培养

网络空间安全的安全研究创新人员在培养过程中需要具备深厚的研究能力和创新思维。从人才培养角度，其主要机制在于高校或科研机构研究生层次的培养。在培养形式上，包括以下几种。

（1）科研项目式培养。学生应该参与具有挑战性和创新性的科研项目，从事前沿的网络安全研究工作，提升研究能力。

（2）参与学术交流。鼓励参加国际性的学术会议、研讨会，与国内外同行交流思想、分享成果，拓展研究视野。

（3）配备高水平导师。为学生配备有丰富研究经验的导师，辅以科创型企业高级工程师或高级管理人员作为企业导师，给学生提供科研、工程两个层面的指导和支持，帮助其在科研领域取得突破。

（4）跨学科合作。鼓励与其他学科领域的专家合作，拓宽研究思路，促进跨学科研究和创新。

在培养内容和路线上，包括以下几种。

（1）打牢学术基础理论。扎实的计算机科学和网络安全领域的学术基础知识，包括算法、密码学、网络协议以及网络攻防、对抗博弈理论等。

（2）培养掌握研究方法论。学习科学研究方法和技巧，包括文献综述、实验设计、数据分析等，培养扎实的科研能力。

（3）前沿技术理论学习。深入研究当前网络安全领域的前沿技术和热点问题，如人工智能在安全领域的应用、物联网安全等。

（4）参与研究实践。积极参与安全研究项目，发表高水平的学术论文，参加安全比赛和挑战，锻炼独立思考和解决问题的能力。

（5）积极的学术交流和合作。与国内外优秀研究团队保持联系，参与国际性的合作项目和学术交流活动，拓展研究合作机会。

（6）打造个人科研声誉。参与安全领域的学术认证，如 IEEE、ACM 等国际学术组织的会员资格，提升个人学术声誉和影响力。

通过以上形式和路线的培养，安全研究创新人员可以形成出色的研究能力、思辨能力和创新思维。

4.5 安全规划治理人员培养

网络空间安全的安全规划治理人员在培养过程中需要具备良好的安全意识、规划能力和治理技能。在培养机制上，更多侧重通过工作实践和在岗任职培训。在培养形式上，包括以下几种。

（1）课程培训。提供系统化的培训课程，包括网络安全规划、风险管理、合规性要求等内容，帮助人员建立全面的安全治理知识体系。

（2）实践案例分析。通过案例分析和模拟演练，让培训人员了

解实际安全事件处理和规划治理的流程，培养应对危机的能力。

（3）合作导师辅导。为人员提供职业导师或合作导师，指导帮带其在实际工作中如何进行安全规划和治理，解决实际挑战。

（4）获取行业认证。鼓励参加相关的网络安全规划治理认证考试，提升规范制定、标准评判、风险评估等专业水平。

在培养内容和路线上，包括以下几种。

（1）学习安全治理基础理论。学习安全治理的基本概念、原则和方法，包括风险评估、合规性管理、安全政策制定等。

（2）学习相关法律法规。了解网络安全相关的法律法规，包括GDPR、HIPAA、CCPA 等，学习如何遵守法规并保护用户隐私。

（3）掌握风险管理方法。学习风险管理方法和工具，包括风险评估、风险处理策略的制定和实施，确保组织安全合规。

（4）安全规划实践。参与安全规划项目，制定组织的安全战略和规划，确保安全措施与业务目标的一致性。

（5）应急响应培训。学习应急响应流程和技巧，建立应急响应团队，增强对安全事件的快速响应能力。

（6）职业持续学习。定期参加安全治理领域的培训课程和研讨会，关注行业动态和趋势，不断提升自身的专业知识和技能。

通过以上形式和路线的培养，安全规划治理人员可以建立完善的安全治理知识体系，掌握有效的安全规划和治理技能，为组织的网络空间安全提供有力支持。

第五章 网络安全工程技术人才培养实例

5.1 实例背景

没有网络安全，就没有国家安全。网络空间安全是国家总体安全的核心之一。粤港澳大湾区作为国家战略布局的一部分，在信息技术行业、先进制造业等产业布局以及“一带一路”国家战略和港澳前沿方面，具有无可替代的核心作用。目前国内网安人才紧缺且缺口不断扩大，粤港澳大湾区作为经济发展、社会治理和对外开放的排头兵，表现尤其明显。培养有实战能力、适应新信息技术安全要求的网安人才，是行业亟需破解的难题。

当前，网安人才培养存在以下问题。一是课程适用性和系统性不足，课程内容与新的网络攻防技术不匹配，实践课内容分散独立，不利于培养整体安全观和综合实战能力；二是实训的时效性和综合性不足，围绕夺旗形式的行业比赛与真实网安场景差异较大，同时，教师独立部署的单机或小规模实践平台，在规模、完整性、真实性等方面存在不足，难以构建真实完整的实训环境；三是教师专业知识和实战技能存在局限性，由于专业背景和考评机制的影响，教师难以将最新的信息及安全技术带入课堂。设计有效的网安人才培养模式是行业当前的重中之重。

5.2 方班概况

针对网络空间安全领域所具有的伴生性、交叉性、对抗性等特点，以及投映到网安人才培养中所具有特殊性，为培养满足社会需求的网络空间安全相关专业人才，中国工程院方滨兴院士提出了“授之以渔”的网安人才培养教育理念，并于 2017 年创立了“方滨兴院士实验班”（简称方班），聚焦硕士研究生层次，培养网络空

间安全相关专业人才，探索和推广实践创新型高层次网安人才培养模式。

方班于 2018 年首期依托广州大学网络空间安全学院，建立了国内第一个实体“广州大学方班”，在硕士研究生层次，通过将科研成果转化为案例式教学资源、将科研和工程问题提炼为启发式教学案例、将最新安全产品纳入教学实训平台，逐步完善形成了“方班 654321 网安人才培养体系”。在这一模式体系下，广州大学方班与国内一批顶尖的网络安全企业合作建立了聚焦人才培养的联合实验室，开展校企合作模型下实战化教学，打造了“方班演武堂”创新课，将优秀开源项目、典型攻防场景作为教学资源纳入到实践教学课堂，培养学生攻防实战能力、工程实践能力，塑造工程思维和产品意识，同步为冬奥会、亚运会、最近的 7 届“广交会”和 2 届文博会提供网络安保服务，提升学生的分析工程技术问题、应对实际安全挑战能力；与国内包括港澳在内的 40 多所知名网安高校组建虚拟教研室，打造了“方班研讨厅”创新课，通过跨校联合教学、本地创新探索等形式，形成了“一讲多评群问式”课堂教学模式，培养学生发现问题、提出问题、创新思辨能力；开设“方班前沿秀”课程，邀请院士、国家级人才、企业专家等科学家和行业大咖为广州大学方班学生讲授前沿科学理论与工程方法，把“开阔眼界、触摸前沿”纳入到方班的日常教学。

截至目前，广州大学方班培养了 300 余名网络空间安全专业相关硕士研究生，当前在校生近 600 人；经历了广州大学方班模式培养的国内其他高校研究生近 2000 人。广州大学方班学生发表高水平学生论文 300 余篇，申请技术专利 200 余项，获得省部级及以上学科竞赛获二等以上奖励 200 余项。多次得到国内媒体报道，被凤凰卫视誉为“不落遗珠”。

5.3 模式举措

1. 育人理念

提出“授之以渔”的教育理念，变知识传递为能力培养，结合网络空间安全学科的特点，创新性提出网络空间安全人才培养的六个特殊性，以其为指导思想，提出方班技能体系、课程体系，覆盖用人单位岗位需求，课堂教授内容以及人才培养效果的认证评价的整个人才培养周期。

2. 培养机制

成立了“方滨兴院士实验班”（简称方班），推行研究生教学改革；建立“方班教学团队”，实践检验并迭代优化方班人才培养模式；提出方班技能体系、课程体系和认证体系，覆盖用人单位岗位需求，课程内容以及教学效果认证评价的整个人才培养周期。强化科研产教融合驱动，通过预科计划、名师计划、迭代计划、三创计划等四项计划，打通网安学生入口渠道，完善师资素质水平建设，以对接产业发展为先导，以系统培养技术技能为基础，强化实践教育，通过学校教育教学过程、科研项目研发过程以及企业生产过程的对接，融教育教学、素质养成、技能提升、科技研发和社会服务于一体。

3. 教学模式

开创性设计推出“一讲多评群问”的研讨厅课堂教学模式，培养学生思辨能力；“高校+企业，演练+点评”的双加实践教学模式，培养学生的工程实践能力。围绕教育教学目标，建成了方班研讨厅、方班前言秀和方班演武堂三门代表了“研讨点评式”教学模式的新课程，通过培养学生掌握“求源、熵减、思辨”的方法从而提升学术创新能力，掌握“分析、验证、工程”的方法从而提升工程实践

能力，学界和产届专家在前沿秀课程中将学术前沿思想和问题、产业技术动向和需求带入课堂开阔学生眼界和思维，培养实践创新型网安人才。

4. 实训平台

针对专业实践教学在人才培养过程中的作用和有效性落实不足、虚拟仿真教学资源缺乏特色这两方面的问题，探索实践教学新模式，实施情景教学、实践教学和能力认证。通过采用“虚、实”结合的解决路径，打造学习平台，基于网络靶场，构建方班教学实践平台，结合情景教学、互联网+模式教学、Gamification 教学和实践教学，并应用于实践教学中，取得了明显的成效。提高学生攻防实践能力。

致 谢

指南（综合版）是在前序版本（1.0、2.0、3.0、4.0）的基础上，结合网络空间安全工程技术现状、网络安全工程技术人才从业现状而修订和综合的，得到了历次版本参编单位和机构的专家、行业专家的支持和指导。在此表示衷心感谢!

指导专家：陈晓丰 廖鹏 刘宝旭 刘潮歌 刘建伟 刘奇旭 刘哲理 罗夏普 相里朋 薛继东 薛晓天 严波 杨珉 杨卿 杨霞 周亚金 邹德清。

历次版本牵头及参编单位/机构:

广州大学

360 企业安全集团

安天科技集团股份有限公司

北京神州绿盟科技有限公司

北京邮电大学

广东为辰信息科技有限公司

国家网络安全产业园区（长沙）

杭州安恒信息技术股份有限公司

湖南会览网安教育有限公司

湖南蚁景科技有限公司

华中科技大学

南开大学

任子行网络技术股份有限公司

软极网络技术（北京）有限公司

上海彼德研究院有限公司

深信服科技股份有限公司

腾讯安全联合实验室

天融信科技集团股份有限公司

中国科学院信息工程研究所

（牵头单位，参编单位按名称全拼字母序）

在参阅、使用过程中发现本指南的纰漏、不足或提出意见建议，请联系执行编委（邮箱：wangle@gzhu.edu.cn）。

附 中国网络空间安全人才教育论坛

中国网络空间安全人才教育论坛（即网教盟，原名中国网络空间安全人才教育联盟），是在中国产学研合作促进会的指导下，由从事网络空间安全相关教育、科研、产业、应用的高校、科研学术机构、地方政府、企业单位、社会团体、事业单位和政府机关直（隶）属单位以及热衷于网络空间安全人才教育的个人共同自愿结成的全国性、行业性、非营利性、创新性组织。

论坛旨在发挥桥梁纽带作用，组织和动员全国网安领域顶级高校、企业、事业单位和社会团体，针对人才教育、培养、培训、认证以及就业等环节，探索科学可行的网安人才培养新模式，努力缩小和补齐国家网安人才需求的缺口和短板，为国家网安事业发展提供有力的支撑。

论坛成立于 2018 年 9 月，设理事会、常务理事会和秘书处，共同受会员代表大会监督，在会员代表大会集体授权下，开展工作。论坛下不常设分支机构或分会，根据论坛主旨和当前工作重点，成立了网安人才供需协调工作组、网安人才挖掘发现工作组、网安人才培训培养工作组、网安人才标准认证工作组和网安意识培养提高工作组、创新与思辨能力培养工作组等主题性工作组。

欢迎有志于网络空间安全人才教育的企业、机构和个人加入！

中国网络空间安全人才教育论坛公众号

（此页无正文）