信息系统密码应用安全性评估与测评实践

杨倩文　张　曼
中国软件评测中心　北京　102206

摘　要：全文深入探讨信息系统密码应用安全性的评估与测评实践，通过案例分析展示企业内部与金融机构在密码应用安全性方面的实际操作与改进成效。文章强调加强标准建设、提升评估与测评能力、推动密码应用普及等对策建议，旨在为提升信息系统整体安全性提供有力支持。实践案例揭示评估与测评在发现安全漏洞、优化密码应用策略方面的重要作用，为行业内外提供了宝贵的参考与借鉴。

关键词：信息系统；密码应用；安全性评估；测评实践

在信息化时代，信息系统的安全性直接关系到组织机构的运营稳定与数据安全。密码应用作为信息安全的核心防线，其安全性评估与测评实践显得尤为重要。本文旨在深入探讨信息系统密码应用的安全性评估，通过分析当前密码应用面临的挑战与问题，提出有效的评估策略与改进措施。

1 信息系统密码应用安全性评估理论基础

1.1 密码学基础

密码学基本概念：密码学是研究如何保护信息在传输或存储过程中不被未授权者获取、篡改或滥用的科学。它主要包括两个分支：密码编码学（Cryptography），专注于信息的加密与解密技术；密码分析学（Cryptanalysis），则致力于破解密码或分析密码技术的安全性。第一原理及分类。密码学的核心原理在于利用数学函数（称为密码算法）对明文信息进行特定变换，使得只有拥有特定密钥的用户才能解密或认证原始信息。根据密钥的使用方式，密码算法可分为对称密码算法（如AES、DES，双方使用相同密钥）、非对称密码算法（如RSA，使用一对公钥和私钥）和密码杂凑算法（如SHA-256，用于生成信息的数字指纹，不可逆）。第二，商用密码产品的种类、特点及应用场景。商用密码产品种类繁多，包括但不限于密码卡、加密机、密码芯片、安全中间件等。这些产品通常具有高强度加密、易于集成、符合国家标准等特点。应用场景广泛，涵盖金融交易、电子政务、网络通信、云计算等多个领域，确保数据在传输和存储过程中的机密性、完整性、真实性和不可否认性。

1.2 密码应用安全性评估标准

随着信息技术的快速发展，密码应用的安全性评估变得尤为重要。国内外已制定一系列标准来规范密码应用的安全性评估，如中国的GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》、GB/T 43206-2023《信息安全技术信息系统密码应用测评要求》和GB/T 43206-2023《信息安全技术信息系统密码应用设计指南》等，以及国际上的FIPS 140-2（美国联邦信息处理标准）、Common Criteria（通用准则）等。这些标准通常规定不同级别的密码应用要求，如基础级、增强级等，每个级别对应不同的安全控制措施和评估指标。评估流程一般包括准备阶段、实施阶段、报告阶段和认证阶段，涉及对密码算法合规、技术合规、产品和服务合规、密钥管理安全等多个方面的评估。评估指标则具体量化了密码应用的安全性能，如加密算法强度、密钥生命周期管理、安全审计能力等。值得注意的是，国外标准通常采用Level 1、Level 2、Level 3、Level 4分类，而国内则采用第一级到第四级进行分类。根据GMT 0116-2021《信息系统密码应用测评过程指南》的指引，应该包括四个阶段来完成密码应用的安全性评估。

2 信息系统密码应用安全性评估与测评实践存在的问题

在信息系统密码应用安全性评估与测评实践中，存在几个显著的问题。密码应用不广泛是一个普遍现象，许多企业和组织在信息系统建设过程中，尚未充分认识到密码技术的重要性，导致大量数据和应用系统缺乏有效的密码保护。这不仅增加数据泄露和篡改的风险，也影响信息系统的整体安全性。密码应用不规范是另一个突出问题，尽管国家已经出台一系列法律法规和标准规范，要求使用经认可的商用密码产品，但在实际操作中，仍有部分单位和个人违规使用自研或境外生产的密码产品，或者在使用商用密码产品时未遵循相关标准和规范，导致密码应用的安全性大打折扣。密码应用不安全也是亟待解决的问题，一些信息系统仍在使用已被证明存在安全漏洞的加密算法，如MD5、SHA1、RSA1024

等，这些算法已无法有效抵御现代密码分析技术的攻击。部分系统在密码管理、密钥生成、存储和传输等方面也存在安全隐患，给信息系统的安全稳定运行带来了严重威胁。

3 信息系统密码应用安全性测评实践

3.1 安全性测评的流程和方法

在信息系统密码应用安全性测评实践中，一个清晰、系统的测评流程是确保评估结果准确、全面的关键。一般而言，安全性测评的流程可以概括为几个阶段；（1）准备阶段：此阶段主要任务是明确测评目标、范围和要求，组建专业的测评团队，并收集和分析被测信息系统的相关资料，包括系统架构、密码应用方案、安全策略等，需要制定详细的测评计划，明确测评的时间表、任务分配、资源需求等。（2）设计阶段：在准备阶段的基础上，设计阶段主要进行测评方案的设计。这包括确定测评的技术路线、选择适用的测评标准和方法、设计具体的测评场景和测试用例等。设计阶段还需要考虑如何模拟真实的攻击场景，以全面检验信息系统的密码应用安全性。（3）实施阶段：实施阶段是测评工作的核心，主要按照设计阶段的方案进行实际操作。测评人员通过执行预设的测试用例，对信息系统的密码应用进行全面的测试和分析。这包括加密算法的有效性验证、密钥管理的安全性评估、密码协议的实现正确性检查等。在实施过程中，需要详细记录测试过程和结果，为后续的分析和总结提供依据[2]。（4）报告阶段：在完成所有测试后，进入报告阶段。此阶段的主要任务是整理和分析测试数据，编写测评报告。报告应全面反映信息系统的密码应用安全性状况，包括存在的问题、潜在的风险以及改进建议等，报告还需要对测评过程进行回顾和总结，提炼经验教训，为未来的测评工作提供参考。

在密码应用安全性评估（密评）中，测评方法系统性地围绕DAK三要素——密码使用的有效性、密码算法/技术合规性和密钥管理安全性展开。这包括通过场景验证模拟实际业务场景，以评估密码技术在保护数据机密性、完整性等方面的有效性；功能测试则确保采用密码技术的功能模块按预期实现安全功能。同时，合规性审查核对密码算法是否符合国家密码管理局标准，如SM系列算法的合规使用，而算法强度评估则着眼于算法在当前技术环境中的安全状况，防范已知漏洞。密钥管理安全性评估则细致考察密钥的生成、分发、存储、保护与更新废止流程，确保其全过程的安全。此外，结合文档审查、访谈交流及专业工具的辅助，可进一步深化评估，全面了解系统安全架构和密码应用情况，有效识别和应对潜在安全问题。

3.2 安全性测评的实施步骤

安全性测评的实施步骤通常包括几个环节：第一，前置准备与调研：在开始密评之前，需深入了解被测信息系统的基本情况，包括系统的架构设计、密码技术的使用现状、业务逻辑等；获取等保定级备案的相关信息，明确评估的级别和安全要求。这一阶段还包括与信息系统的运维团队进行沟通协调，了解系统的运行状况，为后续的评估工作做好充分准备。第二，测评准备：在测试环境搭建完成后，进行测评前的准备工作。这包括制定详细的测试计划、准备测试数据和测试用例、培训测试人员等。还需要与被测信息系统的运维团队进行沟通协调，确保测试工作的顺利进行。第三，执行测试：按照测试计划和测试用例，执行具体的测试工作。测试人员应严格按照测试步骤进行操作，记录测试过程中的各种现象和数据。在测试过程中，应注意保护被测信息系统的安全和数据的完整性，避免对系统造成不必要的损害。第四，数据分析：测试完成后，对收集到的测试数据进行整理和分析。通过对比预期结果和实际结果，发现信息系统的密码应用安全问题。同时还需要对问题进行分类和排序，确定问题的严重性和优先级。第五，报告撰写：根据数据分析的结果，撰写详细的测评报告。报告应包含测试目的、测试范围、测试方法、测试结果、问题分析和改进建议等内容。报告应客观、准确地反映信息系统的密码应用安全性状况，为后续的改进工作提供依据。

4 信息系统密码应用安全性对策建议

4.1 提升技术能力与创新能力

随着信息技术的快速发展，密码技术和应用也在不断演进。作为测评人员，我们需要不断提升自身的技术能力和创新能力，紧跟技术发展潮流，掌握最新的密码技术和评估方法。通过参加专业培训、技术交流会议等方式，不断拓宽视野、更新知识，为密评评估工作提供更加专业、高效的支持。

4.2 提升评估与测评能力

评估与测评能力是确保密码应用安全性评估与测评工作有效进行的关键。为了提升这一能力，需要加大对评估与测评人员的培训力度。通过组织专业的培训课程、研讨会和实践活动等方式，提高评估与测评人员的专业素养和实践能力，使他们能够熟练掌握各种评估与测评方法和工具，准确识别和分析密码应用中的安全问题。还可以引入先进的密码测评工具如算法校验工具、协议分析工具、数字证书校验工具、电子签章校验工具

以及密码应用安全测评辅助工具、密评报告编制工具，提高评估与测评的智能化水平[3]。

4.3 推动密码应用普及

密码应用的普及是提升信息系统整体安全性的重要途径。为了推动密码应用的普及，可以采取以下措施：首先，加强宣传和教育，提高社会各界对密码应用重要性的认识。通过举办讲座、展览、宣传活动等方式，普及密码知识，让更多的人了解密码应用的必要性和好处。其次，制定优惠政策，鼓励企业和组织采用密码技术保护信息系统。例如，可以给予采用符合标准密码技术的企业一定的税收优惠或资金补贴等支持措施，还可以建立示范项目，展示密码应用的成功案例和效果，为其他企业和组织提供可借鉴的经验和模式。通过这些措施的综合运用，可以推动密码应用的普及，提升信息系统的整体安全性。

5 信息系统密码应用安全性评估与测评实践案例分析

5.1 案例一：企业内部信息系统密码应用安全性评估与测评实践

在企业内部信息系统密码应用安全性评估与测评实践中，某大型科技公司面临着因业务扩张而带来的信息系统安全挑战。该公司决定对核心业务系统进行全面的密码应用安全性评估与测评，以确保系统数据的机密性、完整性、真实性和不可否认性。评估团队首先制定详细的评估计划，明确评估范围、评估标准和评估方法。随后，采用静态代码分析、动态渗透测试等多种技术手段，对系统的密码算法实现、密钥管理、密码协议应用等方面进行了深入检查。通过评估，团队发现了系统中存在的几个关键密码应用安全问题，如加密算法使用不当、密钥存储缺乏防护措施等。针对这些问题，评估团队提出了具体的改进建议，并协助企业进行了整改。经过一系列修复和优化措施，该企业内部信息系统的密码应用安全性得到了显著提升，有效降低了潜在的安全风险。

5.2 案例二：金融机构信息系统密码应用安全性评估与测评实践

金融机构作为处理大量敏感信息的关键部门，其信息系统的密码应用安全性至关重要。在某金融机构的信息系统密码应用安全性评估与测评实践中，该机构聘请了专业的第三方评估机构进行全面的评估。评估工作围绕密码算法的合规性、密钥管理的安全性、密码协议的实施效果等多个方面展开[4]。评估团队采用了先进的评估工具和技术手段，对金融机构的信息系统进行了全面而深入的测试。通过评估，团队发现该机构在信息系统密码应用方面表现出较高的安全水平，但也存在一些潜在的薄弱环节，如部分系统间的密码协议互操作性不强、部分用户密码策略设置不够严格等。针对这些问题，评估团队提出具体的改进建议和实施方案，并协助金融机构进行相应的整改工作。

结束语

信息系统密码应用安全性的评估与测评实践是确保信息系统安全不可或缺的一环。通过科学严谨的评估流程和方法，能够及时发现并修复密码应用中的安全隐患，为信息系统的稳定运行保驾护航。未来，随着技术的不断进步和应用的不断深化，有理由相信，信息系统密码应用的安全性将会得到进一步提升，为构建更加安全可信的数字世界贡献力量。

参考文献

[1]邓福彪.信息系统密码应用安全性评估与测评实践[J].福建电脑,2020,36(1):27-29.DOI:10.16707/j.cnki.fjpc.2020.01.007.

[2]赵劼旭,常俊,程燕,等.陕西地震行业网优化的实践[J].地震科学进展.2024,54(3).DOI:10.19987/j.dzkxjz.2023-056.

[3]刘节威,王钢,颜培志,等.基于CNN的国产商用分组密码算法识别研究[J].网络安全与数据治理.2022,41(9).DOI:10.19358/j.issn.2097-1788.2022.03.006.

[4]傅承主,余张杰,李云霄.国产商用密码算法在全民健康信息平台的应用研究[J].现代医院.2022,22(12).DOI:10.3969/j.issn.1671-332X.2022.12.028.