论信息系统的安全风险

摘要

近年来，随着经济金融的良性互动，银行业务得到了快速发展。而快速发展的银行业务和社会化普遍金融服务，迫切要求人民银行牵头建立功能齐全、协调高效、信息共享、监控严密、安全稳定的跨行交易支撑平台。***人民银行领导经过研究，决定于 2005 年利用自身技术力量开发设计 E 户通电子转账系统，作为本地银行间的中间业务公共支撑平台，满足银行间跨行转账、资金清算、集中式代收付等业务需求，并支持银行利用此平台进行新中间业务创新。我作为项目工程实施组负责人，全面参与了系统的建设。在项目建设中项目组全面分析和评估了系统面临的信息安全风险，在网络、主机、数据加密等方面采取了针对性的措施和解决方案，较好地满足了系统建设需要。项目投产后，系统运行安全稳定，达到了建设要求，得到客户好评。

正文

近年来，各银行的信息化发展非常迅速，直接带动了银行中间业务的发展。银行随着多年的建设，已经在中间业务上建立了多个业务系统：如行内的通存通兑系统、定期借记系统、定期贷记系统等。由于这些系统都是由各银行的内部需求为主导建设的，只能支持单个银行系统内部的服务，难以实现银行间的服务。如以银行代收水电费为例，如工行能代收水费，农行能代收电费，老百姓如果需要同时交纳水电费，就必须同时在这两家银行开户，十分麻烦。与此同时，银行因开展业务的需要，不得不与不同的收款单位联网，如水厂，电厂等。数量一多，银行也很麻烦，安全控制越来越复杂。老百姓和银行都迫切要求进一步提升服务质量，实现银行中间业务联网，合理规划和利用银行的总体资源。为此，***人民银行领导经过研究决定于 2005 年利用自身技术力量开发设计 E 户通电子转账系统。该系统采用了 C/A/S 模式，以星型模式连接相关的银行和企业，作为公共的电子转账业务支撑平台，满足银行间的跨行转账业务、定期借、贷记业务，并支持各商业银行在此基础上建设新的中间业务。我作为工程实施组组长，组建了 12 人的开发队伍，全程参与

了项目建设。项目从05年7月启动，06年4月结束，历时9个月。

在项目建设中，有效地规避信息安全风险是项目组考虑的重点内容之一。在项目建设期间，正好公安部门和上级主管部门正在试点信息安全评估和等级保护工作。项目组在全面了解有关信息安全评估的政策要求、保障措施的基础上，结合项目建设实际，全面分析了E户通系统可能面临的信息安全风险。通过初步分析，项目组认为该系统建设和运行可能面临物理环境、网络、主机、数据和应用风险。

物理环境风险主要指今后系统投入运行后，其主机所在环境的风险，包括供电、门禁、防火、防水、防累、空调等方面物理环境的安全。网络风险主要包括网络中断、非授权访问、地址欺骗、攻击等风险。主机风险主要指主机硬件、操作系统、主机服务、日志审计等方面的风险。数据风险主要包括数据泄露、篡改和破坏的风险；应用风险主要指系统应用中的风险，在应用系统设计过程中应该充分考虑到应用系统的有关身份验证、权限控制、数据备份、故障恢复、操作审计等，需要制定良好的信息安全管理制度和组织。

根据以上的分析，结合金融系统网络安全事件、交易安全以及应用安全事件相对多发的实际情况，项目组和客户部门一起研究，对以上风险采取了PHA(初步风险分析)和FMECA（失效模式、影响与致命度分析）的定性分析方法。之所以采用这方法，主要是因为这些方法被广泛采用，易于理解和分析，也在公安部门推荐的范围中。该方法主要是通过初步的风险分析（PHA），找出风险资产，根据遭受风险后可能的严重程度，判断出系统风险的总体情况，并决定采取的相应措施。通过分析，我们确定应将信息安全风险防范的重点放在确保网络安全、主机安全和数据安全上，并决定以技术成熟、成本适中、方便管理为原则，制定了主动防御和被动防御相结合的信息安全风险防范策略。

在网络安全上，以ISS公司的P2DR模型为指导，以公安部门的安全风险评估检查表为参考，采用国外主流防火墙产品和国内主流厂商的网络安全产品相结合，采用防护和检测两重机制来保证安全。防护主要由防火墙和陷阱机实现，属于被动防御。银行网络和我们系统的网络各自采用网络防火墙。银行前置机系统、我们的应用服务器和数据库服务器各自防置在相关防火墙的停火区内，利用防火墙技术实现内外网的隔离和授权访问，防范对内及内对外的非法访问。陷阱机隐藏在防火墙后面，制造一个存在漏洞的诱导环境来诱导入侵，引开对应用服务器和数据库服务器的攻击，从而提高网络的防护能力。

检测是主动防御的核心，主要由IDS、漏洞扫描系统、陷阱机和取证系统共同实

现。IDS 对来自外界的流量进行检测，主要用于模式发现及告警。漏洞扫描系统对相关主机端口漏洞进行扫描，找出漏洞或没有打补丁的主机，以便做出相应的补救措施；陷阱机日志记录了网络入侵行为，引开了攻击行为。取证分析系统记录了网络数据和日志数据，通过事后分析可以检测并发现病毒、漏洞和攻击。

在主机安全上，项目组主要做了三项工作：一是采用正版的主机操作系统和数据库系统，并打上最新的补丁；二是将系统不需要的服务和端口进行关闭；三是打开了系统的审计功能，对产生的日志定期转储和分析；四是对系统用户采取强口令。

在保护数据安全上，项目组经过仔细研究，决定采用银行业目前通用的标准 3DES 算法和对称密钥体系做法，对交易数据产生数据摘要（MAC）。信息发送者在发送报文时，利用加密机计算出报文的 MAC，附在交易报文中。如果该数据报文在传送环节被篡改，则接受者根据篡改后的报文计算出的 MAC 会发生变化，这样，信息接受者就会发现数据被篡改了。采用该机制，密钥就是关键的环节。项目组采用不同机构不同密钥对的做法，使不同银行的密钥各不相同，并采取分段加解密做法。信息发起时，发起行使用自身密钥计算 MAC，E 户通服务器收到报文后，首先用发起行密钥核对 MAC，核对正确后利用接收行的密钥重新计算 MAC 并替换原 MAC 转发到目标行。在国内***研究所的大力支持下，项目组顺利找到了相应的硬件加密机实现以上设计（该加密机通过了国家保密委的认证）。

同时，根据通存通兑业务必须保护客户存折、银行卡的交易密码（PIN 码）隐私问题，我们还设计了多级密钥体系和动态密钥机制。多级密钥体系指系统中除了根密钥外，还根据应用的种类设计了不同的密钥，如工作密钥、保护密钥等。动态密钥体系指联网银行在每个工作日系统初始签到时，动态下载本工作日的工作密钥，用来加密客户的 PIN 码。所有 PIN 码的加密、解密和核密，都是在加密机内部进行，外力不可干预，确保了数据安全。

在应用安全上，项目组主要是帮助客户合理确定系统操作用户的权限和角色，对一线操作层次、决策支持层次、系统管理员层次等不同层次的用户进行不同的角色设置，分配不同的权限。同时，配合、培训用户制定相关的运行制度，落实安全运行组织。

通过以上措施和手段的施行，我们在项目建设过程中有效控制了风险，项目投产后，运行稳定，安全，达到了建设目的，得到了领导和银行的好评。

我们在项目建设过程中，切实感觉到信息安全问题是一项长期、复杂的系统工程，安全防范的机制、手段也在不断发展变化，需要在实践中不断检验和发展。如在项目中， 为了主机安全，我们打开了主机系统级的审计功能。但是根据用户反馈，该日志只是针对操作系统层面的，远没有防火墙系统和网络分析系统、数据库日志详细，而且该日志膨胀很快，浪费硬盘资源，用户后来关闭了该功能。这些缺陷和不足，有待于在今后的实践中予以改进。