

国内外金融业信息安全综述

李连朋¹, 罗宏²

(1. 中国人民银行总行, 北京 100800;
2. 中国人民银行成都分行, 四川 成都 610041)

摘要: 从金融信息化、金融信息安全概念着手, 就当前国内外金融业信息安全面临的包括网络安全、数据安全和业务连续性安全在内的主要风险展开综述, 对业界一些有效技术和控制措施进行介绍, 并给出相关启示和提出建议。

关键词: 金融信息安全; 金融信息化; 信息安全; 风险控制

中图分类号: F49

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00124

Review of domestic and international financial security

LI Lian-peng¹, LUO Hong²

(1. The People's Bank of China, Beijing 100800, China;
2. Chengdu Branch, The People's Bank of China, Chengdu 610041, China)

Abstract: Based on financial informatization, financial information security concept, current major risks to financial information security in domestic and international were overviewed and summarized, including network security, data security and business & services continuity, etc. Some effective techniques and control measures in this areas were introduced. Finally, relevant implications and recommendations were proposed.

Key words: financial information security, financial informatization, information security, risk control

1 引言

金融是一个国家国民经济的命脉, 金融业发展与变革牵动全球各行业的神经系统。自 20 世纪 60 年代以来, 计算机科学发展与应用颠覆了传统金融业的运营模式, 金融产品与服务不断推陈出新, 金融核心业务与信息技术呈现紧耦合。进入 21 世纪, 以互联化、数字化、智能化为标志的信息技术创新出现深度融合、广泛应用和快速变化的特征, 物联网、移动互联、大数据、云计算、区块链等新技术的研究应用, 深刻地影响着人们的生活形态和行为方式, 也同步引领和改变现代金融业发展的战略、理念和行动。

信息科技俨然已成为现代金融发展的基础和支柱, 全球各国金融行业的基础业务、核心流程、客户关系、行业间往来等事务和活动都运行在信息化基础设施之上, 关键、敏感数据都以电子化、数字化形式存储在信息系统和信息设备中, 海量信息和数据通过封闭或开放、专用或公用的电子网络完成传输和交换。金融业具有行业特殊性, 经营和管理巨额资金的同时, 高度运用信息技术开展业务, 存储重要和敏感数据信息, 对信息安全的需求极为苛刻, 信息安全已融入到金融信息化的全生命周期。随着移动互联网技术的广泛应用, 金融犯罪呈现网络化、高科技化和快速敏捷化特征, 金融信息安

全受到威胁和挑战。

2 金融信息化简介

2.1 金融信息化的概念

维基百科(Wikipedia)^[1]对金融信息化做出3个方面的释义。1) 金融信息化是指在金融领域全面发展和应用现代信息技术,以创新智能技术工具更新改造和装备金融业,使金融活动的范围和重心从物理空间向信息空间转变的过程。2) 金融信息化是信息技术(如计算机技术、通信技术、智能技术、控制技术)广泛应用于金融领域,引起金融理论与实务发生革命性、根本性变革的过程。3) 金融信息化是构建在由计算机、通信网络、信息资源和人力资源四要素组成的国家信息基础框架之上,由具有统一技术标准,通过不同速率传送数据、图形图像、音频视频的综合信息网络,将具备智能交换和增值服务的多种以计算机为主的金融信息系统互联在一起,创造金融经营、服务和管理新型模式的系统工程。

2.2 金融信息化的发展历程

全球金融行业信息化发展历经了3个重要阶段^[2]。1) 金融业内部信息化建设。其主要以银行业为代表,参考传统会计业务活动进行流程再造,运用计算机技术、网络技术和存储技术构建银行内部业务处理系统,即技术先进且相互协调的柜面业务服务网络以及以经营管理为目标的银行管理综合信息系统网络。2) 金融业之间横向信息系统建设。随着各项业务往来的频繁,银行间的票据和现金转账结算业务急剧上升,资金清算的及时、有效处理成为提高银行经营管理效率的重要措施。发达国家的大型银行之间以及全球性金融服务机构开始建立统一、标准化的资金清算体系,以实现快速高效、安全可靠的资金清算。例如,环球同业银行金融电讯协会的全球银行结算网络系统(SWIFT)、美联储电子资金转账系统(FEDWIRE)、美国纽约清算所银行同业支付系统(CHIPS)、日本汇票与支票清算系统(BCCS)、日本银行金融网络系统(BOJ-NET)、中国人民银行的现代化支付清算体系(大小额支付系统、网上支付跨行清算系统和人民币跨境支付系统)等,

这些金融信息化设施的建立在降低交易成本的同时,加快了金融交易速度,为客户提供多种新型金融服务。3) 金融业面向客户的信息系统。金融企业推出面向社会公众的各类智能化、自动化服务,建立全方位的客户服务网络系统,包括金融机构面向企业客户建立企业金融平台,以及金融机构面向社会大众建立的电话金融、网络金融、移动金融,通过各类电子服务终端为客户提供全面、多样化的金融服务。

从全球金融信息化发展看,呈现2个方面的转变^[3]。首先,金融信息的技术化很大程度改变了金融经营环境,金融体制、经营方式和运营模式发生根本性变革,先进信息技术已成为金融变革的主要驱动力和支撑力。其次,金融信息服务呈现产业化发展模式,运用金融电子化技术为客户提供更加优质的金融业务支持与金融信息服务。金融机构通过金融信息化产品为客户提供“5A”(anyone、anytime、anywhere、anyway、anyservice)服务,持续提升金融服务水平和质量。近几年,随着移动互联网普及应用,以大数据和云计算为主导的新兴技术再一次引领金融行业进入新的信息化时代——互联网金融(ITFIN)^[4]。互联网金融是传统金融机构与互联网企业利用互联网技术和信息通信技术实现资金融通、支付、投资和信息中介服务的新型金融业务模式,互联网金融是在实现安全、移动等网络技术水平上,从用户体验角度出发,设计、开发的金融新模式及新业务,是传统金融行业与互联网技术相结合的新兴领域。

3 金融业信息安全

3.1 信息安全的概念

信息安全的范围非常广泛,从国家层面讲,信息安全关系到国家利益和安全;从组织机构层面看,信息安全关系到组织的信息资产和商业机密,关系到机构的正常运作和持续发展;就个人而言,信息安全是个人隐私保护和个人财产安全的客观要求。无论是国家、组织机构还是个人,保证关键信息资产和重要数据的安全性都十分重要。信息安全的目标,就是采取有效措施(技术方法、管理行为和强制措施)使信息资产受到保

护，或者将威胁的后果和风险的可能性降到可容忍程度，以维护信息主体的权益。表 1 列举了业界对信息安全的定义^[5-8]。

本文认为国际标准化组织对信息安全的定义更具通用性。从微观角度看，信息安全主要是指信息生产、加工、传播、采集、处理直至提取利用等信息传输与使用全过程中的信息资源安全，信息安全的核心是信息处理过程的安全、信息存储环境的安全以及信息传输和数据交换过程的安全这 3 个方面。从宏观视角看，信息安全是国家的信息化产业能力，以及信息技术体系能够抵御外来威胁与侵害，强调的是全面信息化产生的信息安全问题：一方面泛指信息技术和信息系统发展的安全；另一方面特指国家重要信息化体系（如

国家金融信息系统、国家通信信息系统、国防信息系统等）的安全。随着网络技术的发展，信息安全的内涵已经发展为信息系统运行安全、数据信息安全和通信网络安全，包括物理环境安全，软件、硬件和网络系统安全，信息保密安全，组织和个人隐私安全，信息系统基础设施与国家信息安全。

3.2 金融信息安全的主要属性

金融信息安全是信息安全在金融行业中的应用，除了具备广义信息安全的通用定义和特性外，还具有一些关键属性。根据 ISO/IEC 27001:2013 信息安全管理体系，结合金融业对信息安全的主要需求，金融信息安全具有 9 个关键属性（如表 2 所示）。

表 1 信息安全的概念	
来源	定义内容
国际标准化组织(ISO)	为数据处理系统建立而采取的技术和管理的安全保护。保护计算机硬件、软件、数据不因偶然或恶意的原因而受到破坏、更改、泄露
美国国家安全电信和信息系统安全委员会(NSTISSC)	对信息系统以及使用、存储和传输信息的硬件的保护，是所采取的相关政策、认识、培训和教育以及技术等必要手段。确保存储或传送中的数据不被他人有意或无意地窃取与破坏，包括：信息设施及环境安全，如建筑物与周遭环境的安全；数据安全，确保数据不会被非法入侵者读取或破坏；程序安全，重视软件开发过程的品质及维护；系统安全，维护计算机系统正常运作
欧盟信息安全评价标准组织(ITSEC)	在既定的密级条件下，网络与信息系统抵御意外事件或恶意行为的能力。这些事件和行为将威胁所存储或传输的数据以及经由这些网络和系统所提供服务的可用性、真实性、完整性和机密性
信息安全资深专家	戴宗坤院士 确保以电磁信号为主要形式，在计算机网络系统中进行获取、处理、存储、传输和利用的信息内容，在各个物理位置、逻辑区域、存储和传输介质中，处于动态和静态过程中的机密性、完整性、可用性、可审查性和不可抵赖性，与人、网络、环境有关的技术和管理规程的有机集合
	沈昌祥院士 保护信息和信息系统不被未经授权的访问、使用、泄露、修改和破坏，为信息和信息系统提供保密性、完整性、可用性、可控性和不可否认性

表 2 金融信息安全的属性特征	
金融信息安全关键属性	属性描述
保密性	保障信息仅为那些被授权使用的人所获取。保证信息不被非授权访问，即使非授权用户得到信息也无法知晓信息内容或无法利用信息资源
完整性	保证数据从产生、传输到接收全过程的一致性，防止数据被非法篡改。涉及信息使用、传输、存储的过程中不发生篡改、丢失和错误；信息处理方法正确，不会对原始信息造成破坏
可用性	保障授权使用人在需要时可以获取和使用信息。保证合法用户对信息和资源的使用，而不会被不正当地拒绝
真实性	对信息的来源进行判断，能对伪造来源的信息予以鉴别
不可抵赖性	也称作不可否认性，通过建立有效的控制机制，防止相关方否认其行为，这一属性在金融信息安全中极其重要
可控制性	对信息的传播及内容具有控制能力。授权机构对信息的内容及传播具有控制能力，可以控制授权范围内的信息流向及其方法
可追溯性	对出现的安全问题提供调查的依据和手段。在信息交换过程结束后，相关方不能抵赖曾经做出的行为，也不能否认曾经发送/接受的信息
可靠性	信息系统在限定条件和限定时间内完成规定动作，可靠性是信息系统建设和运行的基本要求，也是金融信息安全的重要目标
连续性	具备应对风险进行自动调整和快速反应的能力，以保证关键业务的连续运转。金融业信息安全的连续性主要包括高可用性（high availability）、连续操作（continuous operation）和灾难恢复（disaster recovery）

总的来说,金融信息安全研究的领域和范畴与一般信息安全有较多相似性,但从行业应用来看,更加注重涉及保密性、完整性、可用性、真实性、可追溯性、可靠性保护和连续性等方面的技术和理论。

3.3 金融业信息安全事件和事故回顾

按照 ISO/IEC 27001:2013 标准解读及改版分析,信息安全事件是指识别出发生的系统、服务或网络事件,表明可能违反信息安全策略或防护措施失效,或以前未知的与安全相关的情况。信息安全事故是指一个或系列非期望的或非预期的信息安全事件,这些信息安全事件可能对业务运营造成严重影响或威胁信息安全。

对于金融信息安全事件,由于金融业多金的本质,长期以来,全球各类非法组织、不法分子不断研究和尝试运用各种先进技术手段,利用金融企业管理和金融信息系统的信息安全缺陷和脆弱性,策划和组织金融犯罪活动,资金损失、信息泄密事件层出不穷。此外,金融业一些内部从业人员,也因为利益的驱使,放下道德底线,从内部窃取数据或越权操纵,导致安全堡垒从内部被攻破,内外安全问题夹击,使金融业信息安全更加危机四伏。

对于金融信息安全事故,金融信息化建设促进金融业信息化程度高度发达,但由于核心业务和核心数据高度依赖信息系统,系统任一环节的运行故障或操作失误都可能会造成严重事故,关键数据的损失可能会对金融企业和金融行业造成致命打击。而信息系统运维失误、外部因素导致的系统运行连续性事故往往是产生金融信息安全事故的主要来源。表 3 收集了互联网上公布的近 3 年来全球范围发生的金融信息安全事件和事故。

3.4 金融信息安全主要风险及控制措施

3.4.1 网络安全风险

现代金融信息化已经高度依赖网络技术,网络是现代金融的基础,也是金融信息安全的关键环节,网络安全风险是目前金融业的头号信息安全风险。据普华永道国际会计事务所(PwC)2016 年发布的《关于全球金融犯罪活动的调查报告》^[9]显示:在金融犯罪活动中,利用网络实施犯罪已成为主要手段,出现的频率越来越高。近年来,网络犯罪分子找到了一些新的攻击方式,如网络钓鱼攻击、针对某个特定目标的鱼叉式钓鱼攻击、以及融合了社会工程学技术的攻击等。随着 IT 技术不断向前发展,这些网络攻击手段也变得更为

表 3 近 3 年来全球金融信息安全事件和事故	
年度	信息安全事件
2016 年	环球银行金融电信协会(SWIFT)信息系统发生多起网络入侵盗窃事件。2016 年 2 月,网络黑客入侵孟加拉国中央银行窃取 8 100 万美元;2016 年 6 月,黑客攻破乌克兰银行核心网络系统,盗取 1 000 万美元。几宗案件的作案手法十分雷同,均为黑客通过入侵银行账户系统,植入网络木马程序,盗取转账凭证,并篡改 SWIFT 文件,控制交易流程
2015 年	美国大型医疗保险商 CareFirst 遭遇专业黑客攻击,约有 110 万医疗保险客户的个人信息遭泄露,包括客户的个人姓名、生日、邮箱地址、医疗保险号码等信息,部分信息被发现遭到非法利用 美国证券服务商 Scottrade 发生了信息系统数据泄露事故,数百万用户的敏感数据受到影响,受影响的数据库中包含用户的社会安全号码和电子邮件地址 汇丰银行由于内部控制原因,大量秘密银行账户文件被非法盗取,涉及约 3 万个账户,总计 1 200 亿美元资产
2014 年	英格兰银行大额支付系统(CHAPS)故障导致系统宕机长达 10 h,事故当日积压大量交易数据,政府、商业和个人的支付业务受到严重干扰,对英国的经济造成重大影响 欧洲中央银行(ECB)遭到严重的网络攻击,网络黑客通过其外部网站的数据库,窃取了网站上 1.5 亿注册者的电子邮件件和用户的个人信息,包括电子邮件、家庭住址和电话号码在内的部分未加密数据被非法利用 美国第二大零售商家得宝(Home Depot)公司支付系统遭到网络攻击,近 5 600 万张银行卡的信息被盗,比 2013 年美国塔吉特(Target Group)发生的客户银行卡数据被盗事件更加严重 摩根大通银行 7 600 万家庭和 700 万小型企业的相关信息被位于南欧的网络黑客盗取,涉及银行客户的姓名、住址、电话号码和电邮地址等个人信息,与这些用户相关的内部银行信息也遭到泄露
2013 年	2013 年 6 月 23 日,中国工商银行上海数据中心主机运维失误,造成国内多地的网点柜面、ATM、网银业务出现故障,无法办理业务和提供资金服务,故障时间持续 1 h,故障波及北京、上海、广州、武汉、哈尔滨等多个大中型城市,造成较大影响

复杂,给金融行业的网络安全造成了严重的威胁。安永国际会计事务所2016年发布了《第18届全球信息安全调查报告》^[10],结果显示:随着数字化的快速发展,尽管全球金融行业在构建网络安全方面已取得积极进展,但由于网络攻击者不断寻找更新、更具侵入性的攻击方法,网络威胁的性质也随之发生变化,全球1775家被调查企业中近三成无法识别出复杂的网络攻击;其中,犯罪集团(59%)、内部员工(56%)和黑客组织(54%)是排名前三位的最有可能的网络攻击来源,同时,国家背景攻击者(35%)位于该榜单的第六位。

1) 网络应用漏洞与脆弱性

美国专业从事安全基准评估公司 Security Scorecard^[11]2016年调查发现:在全球7111家金融企业中,有1356家企业的网络至少存在一个 CVE (common vulnerabilities & exposures)漏洞,并且仍未得到修复,而其余企业至少受到2个 CVE 漏洞的影响。其中,有72%的企业主要是受到 CVE 2014-3566 (poodle)的影响;另有38%的企业受到 CVE 2016-0800 (drown)的影响,23%的企业受到 CVE 2015-0204 (freak)的影响。此外,金融信息系统常见的漏洞还有 CVE-2014-0160 (heartbleed)、CVE-2014-6271 (bash)等,这些漏洞能够对网络和主机系统的安全造成严重缺陷。Symantec^[12]最新数据显示:2015年内发现的零日漏洞是2014年的2倍,数量高达54个,高级别的网络犯罪组织通常最先利用零日漏洞实施网络攻击,或将漏洞出售给低级别攻击者以从中获利。

在国际网络安全组织 OWASP^[13] (open Web application security project)公布的金融业网络安全漏洞造成的入侵行为中,跨站脚本 (cross-site scripting)、注入漏洞 (injection flaw)、远程恶意软件执行 (malicious file execution)、跨站冒名请求 (cross-site request forgery)、身份验证功能缺失 (broken authentication and session management)、未加密的存储设备 (insecure cryptographic storage)、未加密的网络联机 (insecure communication) 以及无权限的控制 (failure to restrict URL access) 等是当前最容易遭到利用的网络漏洞类型,由于大量的金融应用和服务运行在内部

网络和公众网络,操作系统和应用系统本身的安全漏洞或脆弱性缺陷被同步放大到网络环境,这些漏洞容易造成大面积影响。

虽然大型金融机构对网络应用级漏洞造成的信息安全问题保持高度警惕,但全球仍有大量中、小型金融机构因为网络漏洞控制缺失导致信息安全控制受损,甚至影响到内部业务流程和资金安全。目前,针对网络应用漏洞,主要采取被动型系统级漏洞检测和主动型网络漏洞扫描的结合,系统级漏洞检测根据漏洞库配置策略执行基于应用、主机和目标的检测;网络漏洞扫描则通过编制脚本模拟攻击行为,检测目标网络和应用场景的安全性。系统管理员收集漏洞检测结果,研究分析是否采取进一步纠正措施。

2) 网络攻击检测与防御

直接或间接网络攻击是当前金融业信息安全面临的最严峻的网络安全威胁,也是对金融业信息安全基础设施造成损害的重大风险之一。从全球网络安全和管理解决方案顶级企业 Arbor Networks^[14]公布的2016年上半年全球分布式拒绝服务 (DDoS, distributed denial of service) 攻击数据来看,规模最大的DDoS攻击流量达到579 Gbit/s,较2015年提高73%,平均大小为986 Mbit/s,较2015年增长30%;全球平均每周会发生124000起DDoS攻击事件,流量超过100 Gbit/s的DDoS攻击274起,流量超过200 Gbit/s的DDoS攻击46起,美国、法国和英国成为大部分流量超过10 Gbit/s DDoS攻击的目标。从DDoS攻击目标中分析,针对金融业服务和互联网商务的攻击比例分别高达42%和37%,对金融机构、互联网服务提供商 (ISP) 和政府机构发动的流量超过400 Gbit/s。在如此暴力的攻击下,全球任何一家金融机构的网络系统和主机系统都难以承受压力,系统及业务连续性受到严重威胁。图1是来自Arbor的DDoS应用层攻击分类统计数据。

根据Arbor预测,当前DDoS攻击的趋势变化为:①攻击动机发生变化,黑客行为、蓄意破坏已不再是引发DDoS攻击的最主要原因,而转变成不法分子展示其攻击实力的重要手段,并且这些攻击也常常与企图进行的金融犯罪有关;②攻击规模不断增长,规模最大的攻击规模已经超

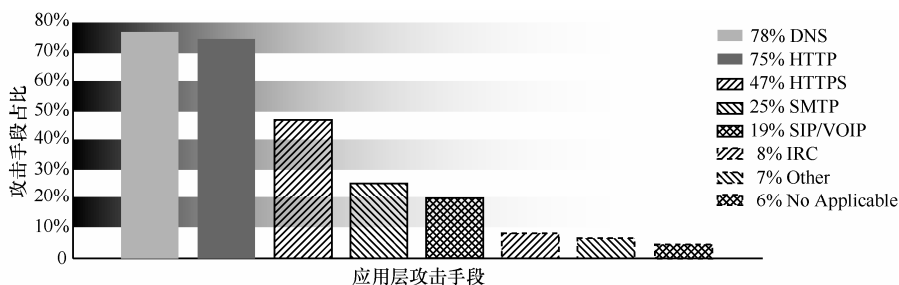


图 1 DDoS 应用层攻击目标分类

过 10 年前的 60 倍；③ 复杂攻击逐步兴起，56% 的机构同时遭到针对基础设施、应用及服务的多矢量攻击，更有 93% 的机构受到了针对应用层的攻击；④ 反射放大攻击平均规模增长迅速，一些大型 DDoS 攻击所使用的 DNS 服务器，运用反射放大技术允许攻击者增大流量；⑤ 防火墙在抵御 DDoS 中持续失败，面对大规模 DDoS 攻击，许多防火墙不是运行中断就是发生故障，无法起到防御作用。

金融信息安全针对 DDoS 攻击风险采取的措施通常在网络边界和核心网络外围部署攻击检测和防御网络硬件设备，同时结合多层次网络拓扑结构设计，实现对网络攻击的预防和控制。具体的安全技术体现 2 个层面^[15]：网络层攻击检测和控制、应用层攻击检测和控制。具体如下。

网络层攻击检测和控制。DDoS 在网络层攻击首先会引起不同协议类型数据分组的数量分布发生变化，也会导致相同协议不同类型数据分组在数据分组头信息、访问源地址数量及分布、数量比例等多个方面发生变化，同时会导致链路严重拥塞，数据传输时延迅速增加。根据防御控制设备在网络结构中部署的位置，DDoS 网络层攻击控制可分为源端迁移控制（source）、中间层限流控制（intermediate）、末端阻断控制（victim or end）以及采用专门设计的网络体系结构和网络安全协议实施控制。

应用层攻击检测和控制。与 DDoS 网络层攻击不同，DDoS 应用层攻击在网络层没有明显异常特征，上述 DDoS 网络层攻击的检测方法不适用于 DDoS 应用层攻击，必须通过应用层协议开展检测和分析。DDoS 应用层攻击比较突出的特点是导致应用服务的访问量大幅增加，同时伴随出现一些明显特征。例如，不同于正常访问，单

个用户发起的访问请求数变大，出现大量地址聚簇（cluster），访问地址分布及访问量相对均匀，访问请求也集中在少数消耗较多主机处理能力的服务文件。DDoS 应用层攻击控制的研究主要侧重于如何区分正常数据流和异常数据流，一般分为基于行为模型的方法（根据网络分层模型理论按照速率、时间和请求对象序列建立行为观测模型）以及基于流量测试的方法（根据活跃流量的自相似性和统计分析方法建立的测试模型）。这些模型是根据金融业务服务的主体和业务类型来设计和定制的。

3) 网络访问控制

网络访问控制是网络安全控制最基本的技术和手段，一般通过网络硬件设备（如路由器、交换机）、硬件软件一体化设备（防火墙）以及应用软件（网络管理服务）等途径实现，但由于金融系统网络体系结构复杂，网络上的各类设备、应用、人员都需要配置不同的访问控制范围和权限，网络内外部访问关系错综复杂，因此访问控制也是容易出现漏洞和缺陷的环节。此外，金融信息网络在一定程度上具有开放性，即便是金融内部网络，局域网络范围内也具有相对开放性。网络的开放性，致使网络中的身份识别、攻击源查找困难，病毒、木马、入侵、IP 欺骗、DNS 欺骗、虚假身份和有害信息等层出不穷，严重威胁着网络运行的稳定性和连续性。

金融系统网络需要构建一个安全可信的网络环境，可信网络连接^[16]（TNC, trusted network connect）是确保网络访问者的完整性。TNC 的结构分为 3 层：① 网络访问层，从属于 ISO/OSI 网络体系结构的网络互联和安全层，支持虚拟专用网（VPN, virtual private network）和 IEEE 802.1X 等技术，该层包括网络访问请求（NAR,

network access requests)、策略执行点(PEP, policy enforcement point)和网络访问管理(NAA, network access authority) 3个组件;②完整性评估层,该层依据一定的安全策略评估访问请求者(AR, access requests)的完整性状况;③完整性测量层,这一层负责搜集和验证AR的完整性信息。目前,国外金融企业的最佳实践核心框架采用安全准入控制技术实现TNC可信网络连接框架中的用户身份识别和用户安全检查,保证合法和符合安全条件的终端接入网络。目前,可用于终端身份验证的技术包括终端准入域控制(EDA, end user admission domination)、网络扩展认证协议(EAP, extensible authentication protocol)、Portal协议,其中,EAP包括EAP-TLS、EAP-PEAP、EAP-MSCHAPV2等,Portal协议包括认证(authentication)、授权(authorization)、记账(accounting)等。此外,TNC可信网络连接框架中定义了网络行为检测和管控要求,通过分级授权限定用户接入网络后的行为,准予不同的用户终端和角色访问不同网络资源,赋予运行不同网络应用的权限,并且采取服务质量保证(QoS)为用户终端分配差异化的网络带宽资源等。目前,金融机构还普遍采用了网络审计技术,目的是监控用户接入网络的行为、接入网络后的网络访问行为,以及用户终端操作行为,及时发现非法接入和非法操作行为,提高网络运行安全性。

3.4.2 数据信息安全风险

美国“棱镜”事件发生后,全球对数据信息安全的意识空前提高。金融信息化环境下,数据是金融业的核心和生命,金融业数据除了金融机构自身的行业运营和组织管理数据外,更多是各类客户的海量数据,包括账户数据、交易数据、投资融通数据、客户基本信息等,这些数据信息的重要性和机密性不言而喻,这些数据信息同时具有潜在的商业价值,也是金融犯罪活动瞄准和关注的目标。因此,金融行业自身以及监管机构对金融数据信息安全的要求非常苛刻,数据在产生、传输、处理、交换、存储和处置的全过程必须保证数据的完整性、一致性、真实性和保密性。同时,数据在访问和使用过程中需要进行严格的权限控制,避免越权和非法获取数据。

1) 数据加密

数据加密是信息安全的核心,也是金融数据信息安全的属性之一,通过应用加密技术,重要信息数据的保密性、完整性、可用性以及抗抵赖性能够得到有效保证。目前,国内外金融信息安全主要采用的加密技术是对称加密(私钥)、非对称加密(公钥)。

如果加密和解密数据所使用的密钥相同,或者尽管不完全相同,但可以通过较简单的方式由其中任意一个推导出另一个,这种密码体系属于单密钥的对称密码,又称私钥密码。分组密码将明文消息编码分组后,在密钥控制下变换成等长的输出数字序列,是一种典型的私钥密码,如美国数据加密标准DES、IDEA算法、Skipjack算法、Rijndael算法等。分组密码技术的研究和应用目前已经比较成熟,如美国国家标准技术研究所于2001年公布的AES加密标准。DES、AES标准是当前金融业在支付报文交换、银行卡数据加密中普遍采用的对称密码技术。

如果加密和解密数据使用的相互密钥完全独立,即加密和解密分别使用不同的密钥实现,且加密密钥(公钥)和对应的解密密钥(私钥)是完全不可逆的,这种密码体系属于非对称密码。国内外金融业应用最广泛的是1978年Rivest等提出的RSA公钥体制。非对称加密算法比对称加密算法慢数千倍,但在保护数据安全方面,非对称加密算法十分可靠。

2) 数据完整性和抗抵赖性

保障交易信息在网络传输中的完整性和合法性是金融交易信息安全的属性。数字证书机制普遍被金融信息安全用来保护数据相关方的机密信息和交易不被未经授权的人截获和窃取。数字证书基于公钥/私钥对(DES/RSA),每一个密钥都是独一无二的,每个用户的身份与一份证书绑定,具有唯一性。数字签名使用散列算法(散列函数),如MD5、SHA-1等从数据报文中提取一个摘要,但这个摘要也是不可逆的,不能通过相同的散列算法恢复原始信息,因此摘要非常安全,不会留下任何最初明文的痕迹;但如果原始信息受到任何改动,则接收方计算出的摘要与发送方生产的摘要完全不同,数据的完整性因此得到保证。

数字证书经合法的、权威的第三方证书授权中心 CA (certificate authority) 签发, 确保数字证书的有效性和真实性。目前, 全球最大的 PKI/CA 运营商 VeriSign 为全球 90% 的大型金融机构提供数字信任服务, 在我国, 中国金融认证中心 (CFCA, China Financial Certificate Authority) 为国内金融机构、支付机构提供安全身份认证服务。

3) 反欺诈

中国猎网平台^[17]发布的《2015 年网络诈骗趋势研究报告》显示, 2015 年国内发生网络诈骗举报 24 886 例, 涉及金额 1.27 亿元。面对当今金融欺诈行为高居不下的态势, 近年来, 国际先进金融机构把金融理论、统计分析技术和信息技术等结合起来, 不断完善反欺诈的定量管理技术。比如, 发达国家的大型银行, 企业级反欺诈监控体系已经初步形成, 核心目标是防止欺诈风险在银行内部业务、人员和产品间进行转移。目前, 国际金融反欺诈研究^[18]主要基于 3 个方面。一是交易行为特征分析。主要内容是构建实体行为档案库, 要素包括使用的设备、关联账户、交易类型、用户偏好等行为特征数据, 这些行为数据记录和总结了这些实体在一定时间段内的交易行为特征, 如平均交易金额、常用的交易方式等。在交易过程中, 实时将当前交易的特征值与历史档案库资料进行比对, 计算出偏离值, 分析判断该笔交易发生欺诈的概率。二是智能模式识别。智能模式是一种量化模型, 主要用于测算欺诈风险, 将获取的交易行为特征变量加载到模型中, 得出评价结果并与模型指标控制值进行比较, 衡量交易的欺诈风险, 并将欺诈风险按等级分类。智能模式的起点是用户交易的第一个行为, 每次经过评估计算后, 将相应的风险评估值赋予交易行为, 为选择哪种合理的智能模式, 采取怎样的反交易欺诈策略提供科学依据, 对欺诈风险较高的交易进行阻断和进一步展开调查。三是关联分析。通过收集形成的历史欺诈事件库以及相关实体 (如欺诈者、欺诈目标、欺诈方式等)、通过一系列数据变量 (如交易时间、交易地点、交易账号、交易对象等) 把这些实体之间相似的信息进行关联分析, 必要时可以运用社会网络关系分析, 最终确定所采取的反欺诈策略和手段。

3.4.3 业务连续性风险

2006 年, 巴塞尔银行监管委员会发布《业务连续性高级原则》^[19] (high-level principles for business continuity), 同时针对监管机构和银行企业进行了责任定位和规范, 并提出了原则性需求, 突出了对业务连续性管理的相关重点。《巴塞尔协议 III》(2012) 强调^[20], 由于信息系统软件、硬件、网络、机房环境、通信电力等不确定性因素发生故障, 导致业务中断或者出现差错, 将对银行金融机构的服务、资金和名誉等造成损失, 应予以重视和做好相应的业务连续性计划并加强管理。德意志银行从 1993 年开始对业务连续性风险进行分析, 并建立了一整套完整的业务连续性计划 BCP (business continuity plan), 以应对突发事件或灾难。2001 年 “911” 事件发生后, 德意志银行调动全球资源, 短时间内在距离纽约不远的地方恢复了业务运行。而当时的美国纽约银行, 虽然在纽约建设了同城灾备数据中心, 但由于距离灾难区域较近, 通信线路全部中断, 导致灾难连锁反应, 当时纽约银行发布声明, 恐怖袭击导致部分重要信息系统瘫痪, 一些分支机构被迫关闭, 部分业务无期限中断。

国际标准化组织制定 ISO 22301:2012^[21] 指导企业对潜在的灾难加以辨别分析, 帮助其确定可能发生的冲击对企业运作造成的威胁, 并提供一个有效的管理机制来阻止或抵消这些威胁, 减少灾难事件给企业带来的损失。金融业信息安全对业务连续性的要求是指金融企业面对信息安全灾害, 有快速响应、风险应对和自我修复的能力, 以保证核心金融业务的连续运转。金融业信息安全为重要应用和流程提供业务连续性应包括信息系统基础设施和核心业务的高可用性、连续运行和灾难恢复这 3 个方面。

1) 高可用性。信息系统的个别或某些 (重要) 部件出现故障时, 能无间断继续运行的能力, 无论故障的原因是物理设施、业务流程, 还是 IT 软硬件故障。按照信息安全的一般度量方法, 金融业对信息系统的可靠性采用平均无故障时间 (MTTF, mean time to failure) 来度量, 即计算机系统发生故障时平均能够正常运行的时长, 平均无故障时间长度与系统的可靠性成正比。可维护

性用平均修复时间 (MTTR, mean time to repair) 来度量, 即系统失效发生所必需的时间, 以及维护恢复所需要的时间, 系统的可维护能力与平均维修时间成反比。信息系统的可用性为:

$$\frac{MTTF}{MTTF + MTTR} \times 100\%$$
。国际性大型金融业机构对信息系统的可用性要求近乎 100%, 不允许出现计划外的系统性中断。

对于主机系统, 由于大多数大型金融机构仍然采用主机平台运行核心业务和处理数据, 通常运用高可用 (HA, high availability) 技术或集群 (cluster) 技术构建可靠的主机运行环境, 确保主机单点故障能够被零延迟处置。对于网络系统, 金融机构一般采用硬件冗余保护措施实现, 即通过网络节点和网络线路形成网络拓扑冗余结构, 并采用多路径自动选择机制, 确保网络设备单点故障或通信线路局部失效时不影响网络上其他节点的正常通信。对于数据存储系统, 国内外金融机构运用的主流技术是采用存储阵列、存储光网络 (SAN)、虚拟化存储 (NAS) 以及卷管理技术构建的全冗余架构高可用存储系统 (storage HA), 任一存储设备出现故障时, 存储体系能够以透明方式调度存储资源, 确保主机的数据服务不受影响, 实现数据零丢失, 维护业务连续性。

2) 连续运行。当设备未发生异常故障时, 不会因为正常的系统运维 (如检修、备份等) 工作而暂停业务运行的能力。金融机构由于信息系统复杂、数据信息量大, 信息安全对系统的运行维护管理提出较高要求。因此, 需要建立完善的内部管理制度并有效落实执行, 包括一般性的日常运维检查, 周期性的系统脆弱性测试, 关键技术/性能指标监测, 内外部信息安全评估, 科学的配置管理、变更控制和问题故障处置。这些基于管理和技术的内部控制体系, 对金融机构业务连续性产生直接或间接影响。

3) 灾难恢复。当灾难破坏生产中心和数据中心时, 使系统和数据恢复正常的能力。近年来, 受严重自然灾害和恐怖主义破坏的影响, 全球金融机构对灾难应对能力非常重视, 灾备建设远远领先于其他行业。目前, 国内外大型金融机构通常采用 IBM 提出的“两地三中心”灾备技术架构,

即生产数据中心、同城灾备中心和异地灾备中心。这种方式最核心的 3 个要素是: 数据库、存储和网络。优点是基于数据库和存储的复制技术有较强的兼容性和通用性, 对应用的影响程度较小; 缺点是备份停留在数据级别, 其能容忍的最大数据丢失量 (RPO, recovery point objective) 和能容忍的恢复时间 (RTO, recovery time objective) 都不能达到最优化, 更加强调数据的物理安全, 且通常灾备环境处于非实时同步状态, 也叫单活, 在需要时通过手工切换。当前, 随着网络技术和存储技术的发展, 更先进的信息技术逐步被应用到互联网金融机构, 包括同城多数据中心、数据库分库分表、应用层面同城多活、异地远程数据备份, 在保证金融数据安全 (RPO 接近 0) 的基础上, 对 RTO 按用户需求分类, 在单节点 (单数据中心) 故障场景下, RTO 也接近 0, 相比传统灾备方案有更大的实用前景。

4 几点启示

2012 年, 国务院发布了《关于大力推进信息化发展和切实保障信息安全的若干意见》, 2014 年, 我国成立中央网络安全和信息化领导小组, 信息安全上升至国家战略高度。中国人民银行现任副行长强调, 各金融机构要更加注重网络和系统安全, 建设高可用性体系和高标准高要求灾备体系, 保证业务连续性目标; 同时, 各机构应主动探索系统架构转型, 积极研究、建立灵活、可延展性强、安全可控的分布式系统架构。因此, 我国金融业信息安全应得到国家层面和企业层面的更多重视, 从全球性、战略性和科学性的角度推动金融信息安全持续健康发展。

1) 注重金融安全与信息安全的融合, 提升金融信息安全的战略地位。金融是现代经济的核心, 金融安全关系着资金融通的安全和整个金融体系的稳定, 金融信息安全是国家发展战略的重要基石, 与国家安全、经济安全和社会稳定密切相关。在全球化、网络化发展背景下, 金融安全面临的威胁和挑战越来越复杂, 金融业的大量业务不但要满足监管要求, 在实际运营过程中对信息技术也有较高的依赖度。金融企业自身在构建金融安全防控体系架构时, 应充分考虑业务安全与信息

安全的有机融合,把信息安全纳入企业的战略发展规划,与组织管理、业务创新、风险控制同步发展,加强源头重视,完善过程控制,瞄准先进技术,使信息安全在金融信息化建设中具有重要地位。国家层面则创造积极良好的环境,严厉打击金融信息犯罪,并在金融监管和金融安全体系建设中将信息安全纳入监控范围,并积极推动,促进国家金融信息安全持续健康发展。

2) 加强产业合作,共建自主可控信息安全体系。当前,我国大多数金融机构的信息化技术架构、核心设备部署、行业应用服务仍然高度依赖于国外主要的技术寡头,特别是主机系统、核心网络系统和数据存储系统,长期以来受外部约束非常严重。近年来,随着移动互联网技术的突飞猛进,我国许多互联网企业在信息技术发展和应用方面取得了卓越的进步,甚至达到世界领先水平,经过实践和市场考验,去 IOE(IBM, ORACLE, EMC) 是可行和必行的。透过这些全球领先的互联网金融公司的技术发展路线,分布式计算机架构、国产网络体系结构、基于网络的数据存储技术能够很好地支持互联网环境中的大数据、高吞吐、快运算,并且能够实现信息安全的自我控制和自我修复。因此,国内大型金融机构的管理团队和技术团队应该积极加强与互联网先进企业的合作,以可持续和发展的视角,逐步构建具有自主知识产权,能够实现自我管控,具备时代领先的金融信息安全体系。

3) 持续完善金融信息安全管理体制和标准化体系。制度建设是金融信息化、信息安全体系建设的重要基础,2012年,中国人民银行编制了《金融行业信息系统信息安全等级保护系列标准》,发布了《网上银行系统信息安全通用规范》;2014年,银监会联合国家工信部发布了《银行业应用安全可控信息技术推进指南》,证监会、保监会制定了相应的行业信息安全保障制度和信息安全等级保护基本要求。但从当前我国金融业信息安全的需求和监管要求来看,法律制度建设还存在一定的滞后性,细化并完善金融行业相关信息安全标准十分必要迫切。例如,针对金融领域大数据,建立包括数据收集、数据使用、数据开放、数据管理和数据利用在内的应用规范,为合理保护和利

用大数据提供指导。针对服务外包,制定第三方安全服务机构服务质量基本评价指标体系,包括第三方安全服务机构的制度体系评价指标、服务内容合规性评价指标、人员管理水平及稳定性评价指标等。针对灾备系统,建立并完善相应的运行、维护、测评和应急处置的相关标准规范体系。

5 结束语

风险管理和风险控制是金融安全的基础,先进的信息技术手段在良好的风险控制体系配合下,可以大幅度提高金融企业管理水平和经济效益,结合有效的信息安全控制措施,可以使高度信息化带来的风险得到容忍和接受。金融业作为国民经济支柱之一,必须具备高度安全的经营环境,从而有力地保障整个国家经济的平稳健康发展。金融信息安全防护水平的提高,对国家的长治久安、经济的平稳发展和社会的和谐进步有重要的意义。本文首先简要介绍了金融信息化和信息安全的有关概念;然后列举了近几年国内外金融业信息安全事件,重点对当前金融信息安全的风险和风险控制措施进行介绍,具体包括网络安全风险、数据安全风险以及业务连续性风险,并结合国外网金融业信息安全实际分析了风险原因,提出了相关控制措施;最后针对我国金融业信息安全发展给出了几点启示和提出建议。

参考文献:

- [1] Financial informatization[EB/OL].<http://wiki.mbalib.com/wiki/>, 2006.
- [2] 孙天琦, 焦琦斌. 信息化与金融安全: 开放视角下的分析[J]. 工程研究, 2013, 5(2): 166-167.
SUN T Q, JIAO Q B. Information and financial security: open analysis perspective[J]. Journal of Engineering Studies, 2013, 5(2): 166-167.
- [3] 贾风军. 关于金融信息化热点问题的深度思考[J]. 中国金融电脑, 2009(6): 24-26.
JIA F J. Deep thinking on the hot issue about financial information[J]. Financial Computer of China, 2009(6): 24-26.
- [4] 姚文平. 互联网金融: 即将到来的新金融时代[M]. 北京: 中信出版社, 2014.
YAO W P. Internet financial: upcoming financial times[M]. Beijing: China CITIC Press, 2014.
- [5] 谢宗晓, 孔庆志. ISO/IEC 27001:2013 标准解读及改版分析[M]. 北京: 中国标准出版社, 2014.
XIE Z X, KONG Q Z. ISO/IEC 27001:2013 revision of the standard interpretation and analysis[M]. Beijing: China Standards Press, 2014.
- [6] 魏军, 谢宗晓. 信息安全管理体系审核指南[M]. 北京: 中国标准

- 出版社, 2012.
- WEI J, XIE Z X. Guidelines for information security management systems auditing[M]. Beijing: China Standards Press, 2012.
- [7] 戴宗坤. 信息安全管理指南[M]. 重庆: 重庆大学出版社, 2008.
- DAI Z K. Guidelines for information security management[M]. Chongqing: Chongqing University Press, 2008.
- [8] 沈昌祥. 信息安全导论[M]. 北京: 电子工业出版社, 2009.
- SHEN C X. Introduction to information security[M]. Beijing: Publishing House of Electronics Industry, 2009.
- [9] PWC. Global economic crime survey[EB/OL]. <http://www.pwc.com/crimesurvey>.
- [10] EY. The 18 th global information security survey[EB/OL]. <http://www.ey.com/gl>.
- [11] Security Scorecard. 2016 financial industry cybersecurity report[EB/OL]. <https://securityscorecard.com/featured>.
- [12] Symantec. Internet security threat report 2016[EB/OL]. <https://www.symantec.com/security-center/threat-report>.
- [13] OWASP. Top security risks and state of security with financial networks[EB/OL]. <https://www.owasp.org/>.
- [14] Arbor. Annual worldwide DDoS and security reports Q2 2016[EB/OL]. <https://www.arbornetworks.com>.
- [15] 张永停, 肖军. DDoS 攻击检测和控制方法[J]. 软件学报, 2012,23(8): 2058-2072.
- ZHANG Y T, XIAO J. Attack detection and control methods to DDoS[J]. Journal of Software, 2012, 23(8): 2058-2072.
- [16] 黎泽良, 余健. 可信网络访问控制技术及其系统[J]. 电信科学, 2010,15(12): 115-116.
- LI Z L, SHE J. Trusted network access control technology and system [J]. Telecommunications Science, 2010,15(12):115-116.
- [17] 360 猎网平台. 2015 年网络诈骗趋势研究[EB/OL]. <https://110.360.cn/>.2015.
- 360 game network. 2015 online fraud trends[EB/OL]. <https://110.360.cn/>. 2015.
- [18] Peter goldmann. Financial services anti-fraud risk and control workbook[M]. Wiley, 2009.
- [19] Basel committee on banking supervision. High-level principles for business continuity[M]. Switzerland: Bank for International Settlements Press & Communications, 2006.
- [20] 肖祖珽. 巴塞尔资本协议与商业银行全面风险管理[M]. 北京: 中国人民大学出版社, 2014.
- XIAO Z T. Basel capital accord and the commercial bank's comprehensive risk management[M]. Beijing: China Renmin University Press, 2014
- [21] TONY D. Manager's guide to ISO 22301[M]. ITGP Press, 2013.

作者简介:



李连朋 (1978-), 男, 河北衡水人, 硕士, 中国人民银行总行工程师, 主要研究方向为信息技术审计、金融网络安全、金融信息安全。



罗宏 (1978-), 男, 重庆涪陵人, 硕士, 中国人民银行成都分行工程师, 主要研究方向为中央银行信息技术审计、金融网络安全、金融信息安全。