Software Engineering and Applications 软件工程与应用, 2016, 5(6), 327-335
Published Online December 2016 in Hans. http://www.hanspub.org/journal/sea
http://dx.doi.org/10.12677/sea.2016.56038

Hans汉斯

Design of the Credit Reporting Information Data Exchange System Based on Multi-Level Security Internet Platform

Qian Yao, Huamei Xie

Credit Reference Center, The People's Bank of China, Beijing
Email: tekkman_blade@126.com

Received: Dec. 2nd, 2016; accepted: Dec. 24th, 2016; published: Dec. 27th, 2016

Abstract

This paper describes a multi-level security internet platform technique, which has been applied for the credit information data exchange system to achieve the communication among different internet systems. By using this technique, both regulatory requirements for isolation among networks and need for real-time response to internet business have been satisfied. Excellent performance has been achieved.

Keywords

Credit Information System, Data Exchange of Two Networks, Multi-Level Security Internet Platform

基于多级安全互联平台的征信数据交换系统的设计

姚　前，谢华美

中国人民银行征信中心，北京
Email: tekkman_blade@126.com

收稿日期：2016年12月2日；录用日期：2016年12月24日；发布日期：2016年12月27日

文章引用: 姚前，谢华美. 基于多级安全互联平台的征信数据交换系统的设计[J]. 软件工程与应用，2016，5(6)：327-335. http://dx.doi.org/10.12677/sea.2016.56038

摘　要

本文介绍多级安全互联平台技术，并应用于征信数据交换系统，实现不同定级系统之间的数据互联互通。该数据交换系统既符合两网隔离的监管要求，又满足实时响应互联网业务的需要，已取得良好成效。

关键词

征信系统，两网数据交换，多级安全互联平台

1. 研究背景

1.1. 征信系统现状

根据国务院部署，人民银行从信贷征信起步，组织商业银行集中力量于 2006 年先后建成了全国联网、集中统一的个人和企业征信系统。该系统以采集信贷信息为主，广泛整合其他非银行信息，并利用覆盖全国的服务网络，为金融机构、金融监管机构、政府部门以及企业和个人提供征信服务。征信系统基本覆盖所有放贷机构、覆盖了每一个有信用活动的企业和个人，征信数据质量不断提高。征信系统作为金融基础设施的信贷支持作用得到有效发挥，应用广泛。一是为金融机构提高审贷效率、防范信贷风险、促进信贷市场发展提供了重要支持；二是为加强金融监管和宏观调控提供服务，为促进行业信用建设和执法管理创造了条件；三是提高了社会信用意识，有助于社会形成“守信激励、失信惩戒”的激励约束机制[1]。

1.2. 人民银行征信业务现状

近几年，随着业务量不断增长，征信业务由人民银行内联网逐渐向互联网拓展。根据国家和金融行业标准[2]，征信系统为安全等级保护三级系统，依托人民银行相对独立的内联网对外提供征信服务，商业银行总行通过专线一口接入人民银行内联网，信息主体只有通过人民银行各分支机构临柜查询本人版个人信用报告。随着信用意识的增强，查询需求快速增长，造成临柜查询网点面临巨大压力，例如：2013 年 7 月份，广西北海爆发了群体聚集查询个人信用报告事件[3]。为保障信息主体的知情权，提供更便捷的信用信息服务，征信中心自 2014 年在全国推广互联网征信查询服务。该服务让信息主体可足不出户查询自己的信用报告。这项便民服务进一步刺激查询需求，两年内互联网本人查询量赶超过去十年内联网的本人查询量。

随着业务量的不断增长，当前互联网征信服务能力遇到瓶颈，迫切需要提高两网数据交换效率。而根据央行网络的总体规划和部署，要求内联网与互联网隔离，只能采取安全 U 盘以摆渡的方式实现内外网数据交换。这种数据交换方式效率低，无法满足业务需要。

2. 多级安全互联平台

2.1. 多级安全互联平台的研究意义

由于人民银行的内联网与互联网是相互隔离的网络，而主要业务数据都存储在内联网中。随着每天交换的数据量不断增长，安全 U 盘逐步突显出性能低、人工干预多、安全风险大等缺点，每次交换平均时间超过 5.5 小时，最长达 10.6 小时。受数据交换效率低的限制，每天交换频率不足 2 次，每次查询要

在 24 小时后才能获得结果，无法满足业务需要，客户满意度低。

同时，随着征信业务的不断发展，社会公众对互联网征信服务也提出了实时响应的要求，所以迫切需要安全高效的数据交换技术来满足业务需要。

而通过多级安全互联平台的研究可以解决人民银行征信系统中两个相互隔离网络中不同定级系统之间的互联互通，并保证其能安全、高效的进行数据交换。

2.2. 多级安全互联平台的总体架构

多级安全互联平台的总体架构[4] [5]如图 1 所示。平台包括：跨级互联安全管理中心、定级系统前置和多级安全互联部件。

1) 跨级互联安全管理中心

跨级互联安全管理中心负责多级安全互联平台的系统管理、安全管理、安全审计。其中安全管理主要负责跨级互联安全策略的管理，可为跨级互联业务需求的定级系统安全管理中心提供策略接口，接收来自定级系统安全管理中心的策略信息，并生成跨级互联策略下发至多级安全互联部件及定级系统前置执行。

2) 定级系统前置

在未部署定级系统安全管理中心的定级系统中，可通过定级系统前置，对需要跨定级访问业务进行安全标记，同时负责提供跨定级访问互联服务接口并提供应用代理。

3) 多级安全互联部件

多级安全互联部件是定级系统间互联访问接口，并按照跨系统互联安全管理中心下发的互联策略对定级系统的跨级互联业务进行仲裁，同时提供应用信息流控制、身份认证、访问控制、日志审计等功能，确保只有策略允许的互联业务可以通过。

2.3. 多级安全互联平台的设计流程

跨级互联安全管理中心维护着一组跨定级系统互联访问控制策略，这些策略确定某一个定级系统内的某个客体允许被哪些系统外的主体访问。当某一个定级系统的安全区域边界收到外部访问请求时，请求的主体及客体标识通过本系统的安全管理中心提交给跨级互联安全管理中心，该中心通过搜索互联访

Figure 1. Multi-level security internet platform system architecture
图 1. 多级安全互联平台系统架构

问控制策略来确定是否允许该请求并将审批结果通过定级系统的安全管理中心下发给安全区域边界，安全区域边界根据下发策略对请求进行放行或拒绝操作。

各个定级系统的访问控制体系及主客体标识可能不一致，为了实现跨系统互联，安全区域边界需要进行访问控制规则和主客体标识的适配，甚至需要用代理主客体方式实现互联。

此外，在等级保护工作实践活动过程中，大量定级系统未建设安全管理中心，定级系统内也未对主客体进行安全标记。多级安全互联平台，可通过定级系统前置的安全标记功能，针对未进行安全标记的跨定级系统互联业务进行安全标记，为多级互联部件提供仲裁依据。

2.4. 多级安全互联平台的关键技术

1) 安全标记技术

目前，大量的定级系统内，未部署定级系统安全管理中心，同时，未对系统内进行主客体标记。因此，在跨定级系统互联业务中，难以对其身份或行为进行鉴别。多级安全互联平台，通过平台自带安全标记技术，针对未进行安全标记的跨定级系统互联业务进行安全标记，为多级互联部件提供仲裁依据。

2) 多维动态标记

不同于传统的标记，多级安全互联平台可以根据主客体信息、访问控制权限、应用协议等构建多维标记，从而实现对标记的立体化。此外，多维标记还可以根据时限要求进行自动更换，实现动态标记。多维动态标记技术可以有效地保护主客体对标记的使用安全，避免标记冒用的问题，提高标记的复杂性和安全性。

3) 应用协议模块解析技术

定级系统前置提供跨级访问应用的通用交换接口，支持基于例如：HTTP、FTP 等标准协议的数据格式转换。通过对协议中的数据进行过滤处理，评估数据的可信性。针对应用层协议，通过应用级攻击特征库，比对访问数据的安全验证规则，过滤源端数据包，从而避免目的端应用服务端遭受应用级访问攻击，实现防篡改、防伪造、防重放攻击。

4) 可信网络连接技术

多级安全互联平台可基于可信网络连接身份标识进行数据交换[6]，该系统中可信互联模块是对网内的安全终端，采用可信标识的管理方式，为其建立可信标识，确保终端的安全可信接入。允许可信终端与定级系统前置采用可信交换方式互相访问，禁止非授权用户接入互联前置，或通过 ARP 欺骗手段接入互联前置。确保那些有合法身份(即带有唯一可信标识)的终端，经过安全管理员批准并符合相关安全策略后，才能访问可信域。

5) 多机隔离技术

多级安全互联平台中的多级安全互联部件采用多系统隔离技术[7]，即通过多主机之间的专用通信硬件及专用通信协议交换方式，对跨定级系统互联业务进行协议剥离与转换，实现不同定级系统之间安全隔离前提下高效受控的数据交换。

2.5. 多级安全互联平台的功能

1) 应用接口

支持 HTTP、FTP、SMTP、数据库访问、文件交换、数据库交换等多种常见互联应用接口，为跨定级系统互联业务提供互联交换服务。

2) 安全标记

针对未采取安全标记措施的定级系统，在进行跨定级系统互联时，可根据标记策略，对交换业务数

据进行安全标记，为多级互联部件提供仲裁依据。

3) 信息流控制

支持基于安全策略的信息流向控制，可针对跨定级系统，控制互联业务的信息流向。

4) 身份认证

支持基于 IP/MAC、用户名口令、CA 数字证书等多种方式，认证数据源和目的合法性，禁止未认证用户、设备连接多级互联部件，保证非法的用户、设备无法进行跨系统互联。

5) 访问控制

支持对交换内容格式依据访问控制策略进行过滤，如数据库格式、文件格式、应用格式等进行格式检查，包括：交换数据的范围、服务的参数、类型、URL、关键字等。

6) 跨级应用审计

支持跨定级系统互联过程的审计，包括数据交换源、互联时间、互联行为、互联内容等。

7) 系统管理

支持系统管理员对安全互联部件与相同或不同等级定级系统的系统资源和运行进行配置、管理，包括用户身份管理、安全互联部件资源配置和管理等。

8) 安全管理

支持安全管理员对相同和不同等级的定级系统中与安全互联相关的主/客体进行标记管理，使其标记能准确反映主/客体在定级系统中的安全属性；对主体进行授权，配置统一的安全策略，并确保授权在相同和不同等级的定级系统中的合理性。

9) 安全审计

支持安全审计员对安全互联部件的安全审计机制、各定级系统的安全审计机制以及与跨定级系统互联有关的安全审计机制进行集中管理。包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行及时处理。

3. 多级安全互联平台安全性分析

在实际应用中，考虑到多级安全互联平台的安全性主要可能受到恶意攻击和数据安全性两方面的威胁，其中数据安全性是指外网用户通过多级安全互联部件非法入侵内网系统窃取敏感数据，内部人员通过多级安全互联部件非法向外散布敏感数据，而恶意攻击是指外网用户突破多级安全互联部件攻击内网应用系统，或者在掌握内网系统控制权后将内网主机作为跳板机继续攻击内网其他应用系统。

因此，多级安全互联平台对两大方面可能包含的不安全因素采取了下面四种防范措施[8]：

3.1. 保障数据安全的措施

1) 可信网络连接

平台系统中各组件系统之间通过可信网络连接来进行数据传输，通过可信网络连接的安全功能，可以避免交换源被仿冒的风险，从源端一直到目的端的整个交换都是置于可信机制上进行的，可以防止数据被恶意交换。

2) 标记权限访问控制

针对符合安全策略的数据进行安全标记，安全标记主要用于多级安全互联部件对数据的合法性进行验证以及访问级别权限的划分。安全互联部件通过对安全标记的解析，判断此数据是否可以通过部件到达另外一端，对没有安全标记的数据不予放行。此外，安全标记具有不同的级别权限，互联部件会对安

全标记的权限进行判别，从而避免越级访问的现象出现[9] [10]，保证数据在可控、可管的条件下进行交换。

3) 配置可传输文件类型的黑、白名单

多级安全互联平台通过配置可传输文件类型的黑、白名单，使得平台能够只允许传输内网应用系统生成的反馈文件，禁止传输可执行文件、脚本文件等。

4) 数据加密

平台中的内网数据文件的敏感信息都已使用不可逆算法进行了脱密，外网需要交换的文件由应用系统加密，防范数据被篡改。

3.2. 防范恶意攻击的措施

1) 可信增强平台

多级安全互联平台系统中的所有组件都具有操作系统增强模块，利用信任链传递，对操作系统内核装载的重要应用程序和服务进行完整性验证，支持对可执行程序型、恶意脚本、木马等病毒的主动防御。保证受控应用服务器所启动的应用程序都是可信的，并且应用程序运行过程中满足最小权限原则。

2) 统一配置

多级安全互联平台只能通过集中管理平台统一配置。

3) 部署策略

多级安全互联平台的部署策略降低了被攻击的可能性。外网用户只有攻破外网防火墙，且又未被入侵监测系统发现的情况下，才有可能进一步对多级安全互联平台实施攻击。

4) 严格服务端口管理

在平台的定级系统网前置上，仅内网前置提供管理服务端口，关闭其他所有无关的服务端口，防范外部用户对文件服务器的攻击。

3.3. 日志审计

多级安全互联平台自动记录文件传输、用户登录、数据传输等信息的详细日志，包括源地址，目标地址，数据传输量等，审计日志被保存至集中管理平台中。通过日志分析可发现多级安全互联平台运行异常及外部用户的攻击。

3.4. 多级安全互联平台的日常运行维护

1) 严格按照三级防护标准防护和管理互联网应用系统

多级安全互联平台将每年进行等保测评和深度强化测评，防止由于应用软件开发不善出现应用层的安全问题。

2) 制订多级安全互联平台运行管理制度

多级安全互联平台上线之后，征信中心将在坚持 24 小时值班制度的基础上，将多级安全互联平台安全纳入每日巡检工作内容。每天备份和比对多级安全互联平台配置文件，确保多级安全互联平台的安全运行。

3) 定期分析多级安全互联平台运行日志

在平台内网终端安装日志审计系统，设置多级安全互联平台运行异常监控指标，密切跟踪外网攻击行为，监控多级安全互联平台运行风险。

4) 加强业务监控

征信中心正在研发征信系统实时检测子系统，已将互联网用户行为纳入到检测范围，以便及时发现互联网系统的运行异常。

4. 征信数据交换系统的应用成效

考虑到两网数据安全交换方案在人民银行尚属首例，通过充分调研商业银行的数据交换方式，结合征信业务的自身特点[11] [12]，并组织专家进行论证，征信中心建议采用多级安全互联平台搭建征信数据交换系统。网络拓扑见图 2。

在具体的业务应用场景中，内联网和互联网之间采用双机热备的方式部署多级安全互联平台。交互方式有两种，分别是文件级或应用级，文件级交互常用于异步大批量数据传输，应用级交互常用于时效性要求高的查询请求。

文件级交互流程如下：互联网定级系统前置负责获取查询文件，并将其通过多级安全互联部件传送至内联网定级系统前置，多级安全互联部件通过标记匹配来检查所传输的文件是否合法，随后再由内联网定级系统前置将合法文件发送给内联网应用服务器，以此完成由外向内的跨级访问请求。待内联网应用服务器获取查询结果后，再以同样的方法，经内联网定级系统前置、多级安全互联部件、互联网定级系统前置，最后传送至互联网应用服务器，完成内到外的跨级访问请求。

应用级交互流程与文件级交互类似，互联网定级系统前置先对外部请求进行协议解析，再把合法的应用数据流进行标签定义，并发送给多级安全互联部件，互联部件在进行标签判定后，将应用数据直接发送给内联网的业务系统进行处理，并按逆向反馈结果。应用级交互效率高，可实现准实时服务。

两种交互方式在征信系统内均已通过测试验收，文件级交互速度峰值达 100 MB/S，应用级交互也可满足手机信用报告查询业务需求。

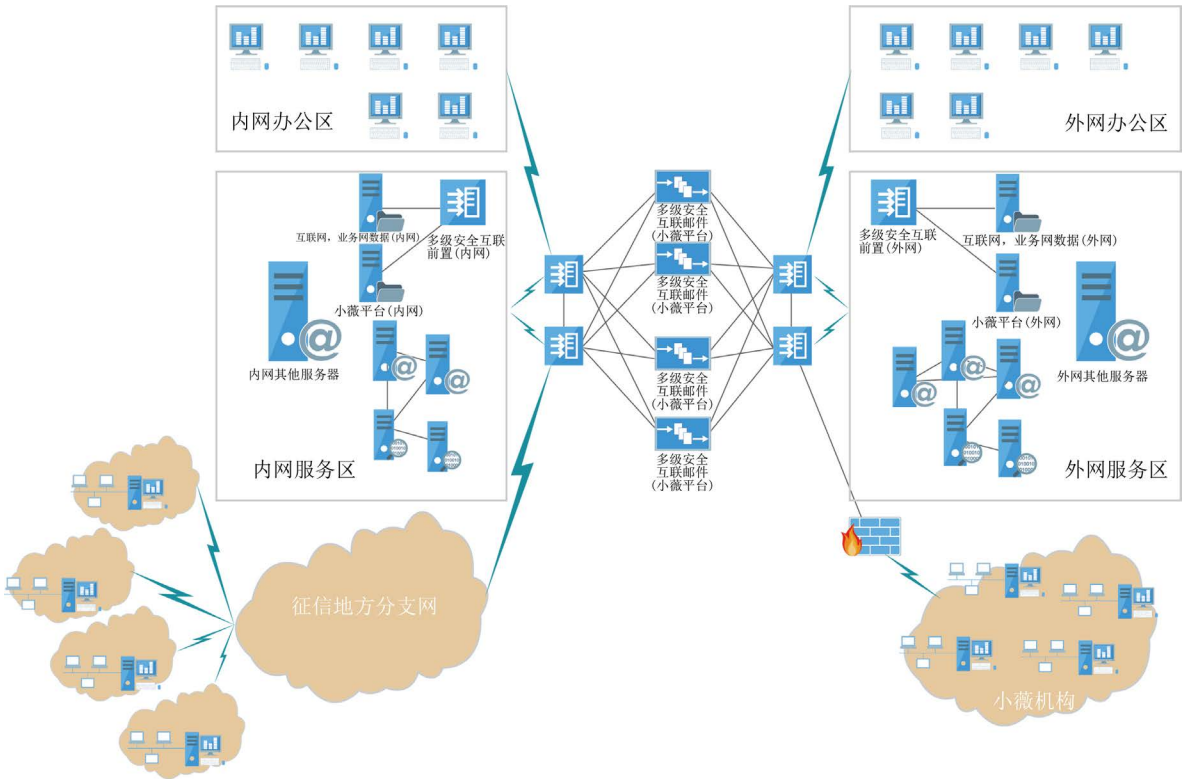

Figure 2. The physical topology in practical application of multi-level security internet platform
图 2. 多级安全互联平台的实际应用物理拓扑

5. 多级安全互联平台的创新之处

5.1.专为等级保护量身定制

在多级安全互联平台的设计中，参考 GB/T25070，综合了安全隔离、身份认证、访问控制等多种成熟技术应用的优点，解决了等级保护整改过程中，跨定级系统安全互联问题，为国家信息安全等级保护制度的落地提供了有力的技术支持。

5.2. 跨级主客体访问控制

在多个不同定级系统中，存在多个需要访问的主体和被访问的客体，而多级安全互联平台能够实现集中的主客体访问控制。通过“跨级互联安全管理中心”，可以对多级安全互联平台中所有的组件和主客体的访问控制策略进行集中管控配置，通过“多级安全互联部件和前置”，对既定的跨级主客体访问进行标记控制。

5.3. 定级系统安全标记

目前，大量的定级系统内，未部署定级系统安全管理中心，同时，未对系统内进行主客体标记。因此，在跨定级系统互联业务中，难以对其身份或行为进行鉴别。多级安全互联平台，通过平台自带安全标记技术，针对未进行安全标记的跨定级系统互联业务进行安全标记，为多级互联部件提供仲裁依据。此外，多维动态安全标记技术的使用，也使得标记的应用更加安全可靠。

5.4. 跨定级应用实时监控

通过多级安全互联平台可以实现对跨定级系统的应用进行实时监控，一旦业务出现中断，可以采用多种方式及时通知到管理人员，从而保证跨定级访问的有效性。

6. 结语

本文提出了安全高效的数据交换方案，是央行信息系统的首次尝试，具有良好的示范效应，值得推广。人民银行的多个系统都存在内联网与互联网之间的信息交互，因监管要求，按照两网隔离的安全策略进行数据摆渡。随着业务发展的需要，数据摆渡已经极大的影响了信息系统的交互效率和服务质量。一旦利用多级安全互联平台，实现访问控制，标记控制，定级系统主客体跨定级访问，应用协议细粒度检查等一系列技术和手段解决不同定级系统之间的数据互通互联的问题，势必可以增强央行的经济宏观调控能力。

征信系统采用安全高效的数据交换技术，对征信业务发展模式具有深远影响。征信中心是在保证系统安全和数据安全的基础上，对系统服务效率的一次质的飞跃。征信系统互联网能够提供准实时查询服务，可以进一步丰富互联网查询的业务种类，扩大互联网查询的业务范围，提高客户满意度，实现普惠金融都有重要影响。

参考文献 (References)

[1] 陈斌辉. 信息技术为征信系统保驾护航[J]. 金融科技, 2013(14): 60-61.

[2] 中国人民银行. 金融行业信息系统信息安全等级保护实施指引(JR/T 0071-2012) [M]. 北京: 中国金融出版社, 2012: 6-10.

[3] 周元元, 梁薇薇, 江东阳. 信息技术为征信系统保驾护航[J]. 征信, 2014(2): 29-30.

[4] 中国国家标准化管理委员会. 信息安全技术信息系统等级保护安全设计技术要求(GBT25070) [M]. 北京: 商务印刷馆, 2010.

[5] 乐春峡, 王勉华, 周奇勋. 一种新型隔离网络数据安全交换系统的设计[J]. 计算机工程与设计, 2004, 25(3): 444-446.

[6] 刘小杰, 韦卫. 网络可信接入认证方法及在 VPN 客户端上的实现[J]. 计算机工程, 2006, 32(9): 154-156.

[7] 孙学军. 隔离网络数据安全交换系统的设计与实现[J]. 网络与信息, 2011(4): 60-61.

[8] 佟鹏. 多级安全的网络安全通信模式以及关键技术分析[J]. 电脑开发与应用, 2014(11): 80-82.

[9] 张少中, 孙莹光, 郭玢, 陈红. 分布式数据库多级安全访问控制机制[J]. 辽宁工学院学报, 2003(2): 23-26.

[10] 孙松, 孙淑玲, 邵佩英. 多级安全数据库中标记生成规则的一致性[J]. 计算机工程与应用, 2001, 37(16): 123, 124, 127.

[11] 卢小龙, 朱建强, 朱杰, 林鸿, 宁翔. 个人征信系统总体框架的设计[J]. 金融电子化, 2005(3): 53-55.

[12] 朱杰, 杜海雷. 个人征信系统的架构设计[J]. 金融电子化, 2013(3): 64-66.