doi: 10.3969/j.issn.1006-1576.2010.12.016

# 跨域信息交换技术

李洪敏[1]，邓轲[2]，莫军[1]，韦力凡[1]
（1. 中国工程物理研究院 总体工程研究所，四川 绵阳 621900；2. 中国工程物理研究院 计划部，四川 绵阳 621900）

**摘要**：针对现有涉密信息系统数据无法分离和无密标的情况，通过对国内现有网络隔离与交换技术进行分析，并针对非密域与涉密域间的信息交换的需求，设计了基于系统安全加固、单向导入和电子密标的信息交换解决方案，在不改变现有涉密应用的基础上，采用定制应用模式实现信息交换。该方案实现了跨域信息交换，并符合标准要求。

**关键词**：安全域；信息交换；电子密标；应用交换
**中图分类号**：TP391 **文献标识码**：A

# Cross Domain Information Exchanging Technology

Li Hongmin[1], Deng Ke[2], Mo Jun[1], Wei Lifan[1]
(1. Institute of System Engineering, China Academy of Engineering Physics, Mianyang 621900, China;
2. Dept. of Planning, China Academy of Engineering Physics, Mianyang 621900, China)

Abstract: Aiming at the non data isolation and non label in MIS, new technologies and requirements of network isolation and information sharing are analyzed, then solution of information sharing based on security reinforced, one-way transfer and electronic label is designed. Then put forward the solution of application exchange using custom-suit application mode. This solution realize cross domain information sharing and accords with standards.

Keywords: security domain; information exchanging; electronic label; application exchange

## 0 引言

随着信息化的发展，跨机构的横向信息共享、机构内的纵向信息共享已成为军工集团信息化建设中不可逆转的趋势。而现有政策并未就以下情况提出明确的指导性方案：1) 高密级涉密网与低密级涉密网间的信息交换；2) 涉密网与非密网间的信息交换；3) 涉密信息的定密、标签及强制访问控制。为了既保证持续推进信息化建设，又规避安全域间信息交换的问题，现有军工涉密信息系统基本按照“系统高安全”进行处理，即系统密级按照系统内所处理信息的最高密级定密和防护，没有建立不同等级的安全域，无形中提高了整体防护代价和扩大知密范围的隐患。

新的军工保密资格认证标准中明确提出了非密人员不能使用和管理涉密计算机及涉密信息系统。为了保证非密人员在涉密计算机信息系统中使用和处理非密信息，就必须在涉密计算机信息系统中划分出非密安全域，同时要保证涉密信息不能流向非密安全域。为了规避该问题，目前普遍采用提升计算机、人员密级的方法，但这样会扩大知密范围，给保密带来更大的隐患。因此，制约信息化发展的巨大瓶颈是安全域间信息流向的控制问题。

现有军工网络是一个没有强制访问控制和分类标签的网络，在现有条件下难以实现涉密网间的跨域信息交换。故从理论和应用上对不同密级网络间的跨域信息交换（Cross Domain System，CDS）进行分析，提出符合政策要求的跨域信息交换解决方案。

## 1 国外跨域信息交换技术跟踪

在不同时期，国外针对安全域之间信息交换分别采用如表 1 所示的方法，从完全的物理隔离、人工交换，到采取可靠的硬件单向传输系统[1]，实现不同安全域的逻辑隔离。目前，国外采用的跨域信息交换的关键技术就是单向硬件传输和电子密标。

单向硬件传输系统采用类似数据二极管的技术原理，在发送与接收方分别部署该硬件，确保数据传输的单向性。战争同盟协作演示（Coalition Warrior Interoperability Demonstration，CWID）利用数据二极管作为单向传输系统基础，对跨洲季的 IIMS 系统进行互联和不同安全域的信息交换进行测试[2]，得出如下结论：

1) 数据二极管可提供实时网络连接并保证网络的高安全性；

2) 数据二极管具备了支持企业级互联跨域信息交换的能力。

收稿日期：2010-07-14；修回日期：2010-09-08
作者简介：李洪敏（1968-），女，辽宁人，硕士，高级工程师，从事网络信息安全研究。

表 1 国外不同时期信息交换的方法

| 方法 | 示例 |
|---|---|
| Sneaker Net | 通过 CD、磁盘等手工方式实现信息交换 |
| One-way cable assembly | 通过 RS-232、变换的 Ethernet 实现信息交换 |
| Complex software programs | 通过可信操作系统安全策略、加密实现信息交换 |
| Firewall enabled policy | 通过中间件、UDP 路由设置防火墙规则来实现信息交换 |
| One-way system hardware | 在发送与接收点采用双二极管的单向硬件系统来实现信息交换 |

## 2 国内现有网络隔离与交换技术分析

### 2.1 现有双向安全隔离与信息交换系统的技术

现有通过国家保密检测的安全隔离系统主要是双向的安全隔离与信息交换系统。由内端机、外端机和安全隔离交换硬件组成。内端机和外端机上运行有经过裁减的操作系统或安全操作系统，内端机通过内网口与内网相连，外端机通过外网口与外网相连。安全隔离交换系统内部由 2 个分别安装在内端机和外端机上的安全隔离交换硬件构成专用交换通道，完成内端机和外端机间的信息交换。通常的安全隔离与信息交换系统支持多种信息交换方式，如 HTTP、FTP、SMTP、POP3 等协议交换方式，或直接文件读写的同步交换方式。当内外网间的程序对（Application Pair）需要交换数据时，由发起端通过安全隔离交换系统的认证后使用该端代理，代理将收到的信息进行处理后通过交换通道交换到另一端，由另一端的代理进行数据重组并取回信息，在重复交换过程将结果返回发起端。由于目前的安全隔离与信息交换系统普遍没有对通过的数据进行标签检查且多为协议穿过方式，因此可能具有以下安全隐患：

1) 无法完全剥离协议进行内容检查；

2) 内外网间可以通过安全隔离交换系统的协议构建隐通道。

### 2.2 基于强制访问控制、单向传输系统的技术

为实现跨域信息交换，需要使用支持 Windows 等涉密网中主流操作系统的安全加固组件，对现有军工网络中涉及跨域信息交换的计算机进行安全加固，其主要功能包括：

1) 对信息进行分类标签；

2) 对主体进行授权；

3) 通过访问控制矩阵对主体操作文件、网络及其他 I/O 设备的行为进行访问控制；

4) 访问控制引擎和策略应独立于系统用户，强制执行。

以此为跨域信息交换提供授权主体、分级客体和可控的系统内工作流。

为实现跨域信息交换，还需要使用新型的单向传输设备，其中，单向传输设备可以完成由高到低（High to Low）或由低到高（Low to High）的系统间工作流。单向传输系统应实现以下安全策略：

1) 支持数据分级处理；

2) 使用基于光纤的单向传输模块，消除隐通道；

3) 使用冗余算法保证数据传输的完整性；

4) 安全策略在系统失效时也可执行；

5) 通过强制访问控制手段确保仅能与经过授权的计算机或进程通信。

因此，综合使用强制访问控制技术与单向传输技术，构建满足数据隔离、信息流控制、无隐通道，且支持失效隔离和强制审计的跨域信息交换技术方案，可以同时支持由低到高和由高到低的信息流。

在国内，该技术还处于实验室研发和测试阶段，在不同安全域针对数据库、基础管理和服务信息还无法实现有效交换。

## 3 基于典型工作流的跨域信息交换需求

### 3.1 典型工作流分析

目前，基于流程的协同应用系统主要采用 B/S 架构，但工作机与应用系统存储/管理的文件信息交换与传递又可以分为 2 种机制。

1) 工作机通过应用服务获取应用系统中存储的文件，文件传递发起者与系统中实际的文件读写者通过系统服务的隔离，没有直接通道；

2) 文件交换发生时，工作机与系统的文件存储服务之间通过 ftp、http 等多种方式建立了数据传输通道。这种方式为在数据传输通道上建立基于数据传输两端的数据传输主体安全等级的控制方式提供了基础。

### 3.2 工作流对跨域信息交换的基本需求

客户工作机具有不同的密级，分属不同的安全域。应用系统后台服务区存储了大量不同密级的业务信息，其密级总是不低于各工作机，是系统中密级最高的安全域。工作机与应用系统之间存在大量的跨域信息交换，其基本的控制要求是：所有的信

息交换渠道受控，信息只在受控的信息渠道内交换；工作机只能向应用系统提交不超过自身安全等级的信息；控制应用系统存储区高密级信息向低等级工作机传递，避免工作机获取超密级信息。

1) 涉密安全域与非密安全域之间信息交换的要求

(1) 2 个安全域之间只有标注“非密”的信息能进行交换，并要确保密级标签和信息的完整性。

(2) 数据隔离（Data Isolation）：对不同密级的数据增加标签，并控制所有非该密级的主体对其进行读写访问，以继续保持不同安全域间的数据隔离。

(3) 无隐通道（Prevent Convert Channel）：在主体进行跨域间信息交换时使用物理手段过滤网络间 I/O 方向，进而控制计算机间跨域信息交换的数据流。

(4) 工作流控制（Control of Information Flow）：对主、客体进行可靠识别，在自主访问控制系统中强制对进程间操作进行授权。确保非密安全域与涉密安全域之间只能传递非密文件。

2) 机密安全域与秘密安全域之间信息交换的要求

现有涉密应用系统都是不密级信息混存的，在涉密应用不改造的前提下，很难将不同密级的信息物理上分离，因此现阶段也很难将不同密级的涉密应用系统分别部署。

(1) 整个涉密安全域内共享一套基础服务和所有应用系统，实现统一认证、统一安全策略，整体按照机密级防护。

(2) 在保证机密级数据与秘密安全域有效隔离的前提下，保证所有基础服务和应用的正常使用。

(3) 工作流控制（Control of Information Flow）：对主、客体的可靠识别，在自主访问控制系统中强制对进程间操作进行授权。确保机密安全域与秘密安全域之间只能传递秘密级以下的信息。

(4) 涉密应用系统应支持人员定密、信息标密，并对信息流转过程进行控制。

## 4　跨域信息交换解决方案

### 4.1　总体设计思路

强化非密安全域与涉密安全域的隔离措施，建立基于电子密标和单向信息隔离的跨域信息交换体系，确保数据有效隔离和无隐通道。涉密安全域内部，在不改变现有应用系统的前提下，定制需要跨域交换的应用，建立基于应用交换的解决方案。

### 4.2　基于密标的跨域信息交换解决方案

#### 4.2.1　电子密标的设计体系（如图 1）

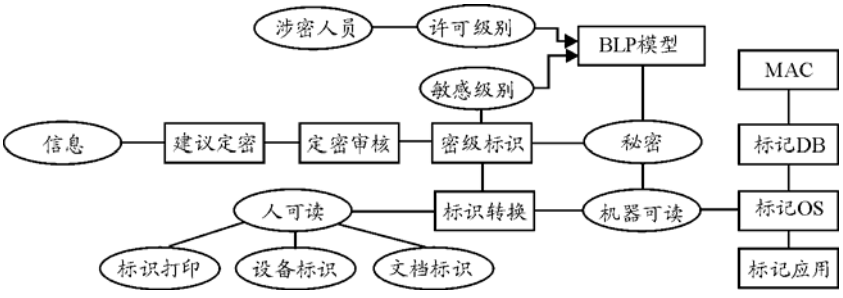


图 1　电子密标的设计体系

分析符合单位定密流程，建立包括初定、审核、定密的专用定密系统，实现信息、人员和设备所有要素的电子密标。

#### 4.2.2　非密域与涉密域之间信息交换解决方案

综合使用强制访问控制技术与单向传输技术，构建满足数据隔离、信息流控制、无隐通道，且支持失效隔离和强制审计的跨域信息交换技术方案（如图 2），可以同时支持由低到高和由高到底的 CDS 信息流。

该方案特点如下：

1) 创建一条由非密安全域向涉密安全域的单向数据通道，将数据单向导入到涉密域，同时确保在该通道上涉密域数据不会以任何形式（包括隐信道）传输到低安全域；二是创建一条具有人工检查功能和可追溯功能的由高安全域向低安全域的单向数据通道，将具有源发验证的并经过管理员检查的非密数据传输到外网。

2) 其中，导入方向负责完成低安全域向高安全域的单向数据导入，该导入实现数据库的全表导入、文件导入等，在该方向上不存在任何由高安全域向低安全域的数据流。

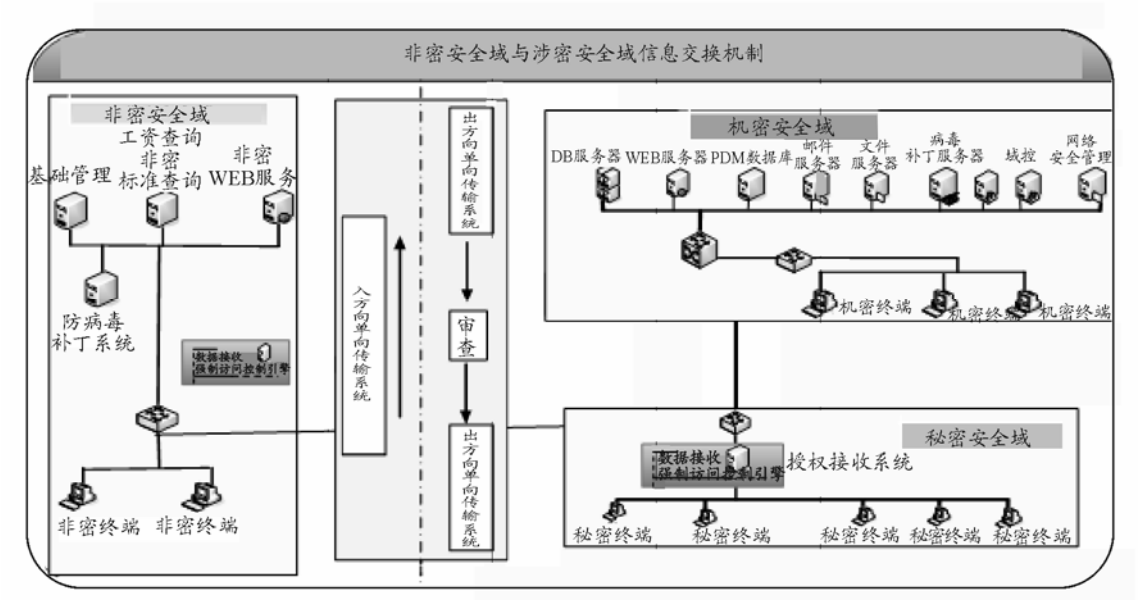


图 2　非密域与涉密域间信息交换机制

3) 对于需要导出的非涉密数据，发送者通过高安全域发布终端（通过 SEWindows 对信息进行非密标记并签名），通过出方向传输到标记检查主机，标记检查主机上的验证签名信息及内容后传输到非密接收终端。

4) 应用系统需要进行密标和信息流转控制功能的改造。

4.2.3　机密域与秘密域之间信息交换解决方案

整个涉密安全域内共享一套基础服务和所有应用系统，实现统一认证、统一安全策略，整体按照机密级防护。在现有涉密应用系统数据无法分离和无密标的情况下，数据的划分标准难以统一、原有数据加标记难、数据标记的保持和复制难、标记的粒度确定难，完全重新开发系统进行数据剥离是不现实的，因此考虑不改变现有涉密应用的基础上采用定制应用模式，完成数据筛选与流向控制，实现可控的数据交换方式[3]，如图 3。

该方案特点如下：

1) 接收方根据权限使用应用系统的部分功能和部分数据；

2) 接收方不能修改应用和数据，也不能反向上传数据；

3) 所有方通过管理应用权限进行数据控制；

4) 交换过程可以根据交换双方的需要进行灵活设计。

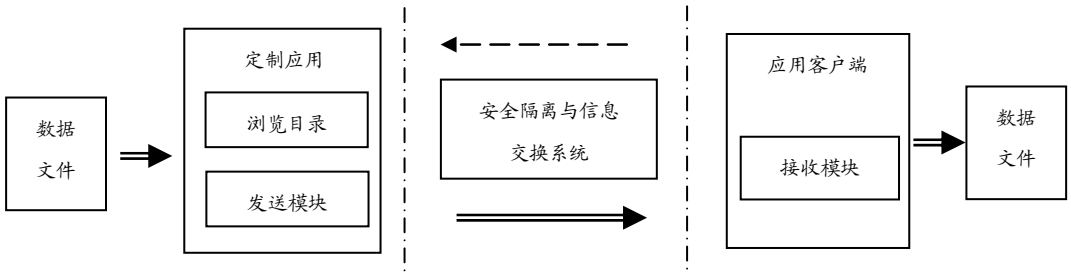


图 3　应用交换方式模型

## 5　结束语

跨域信息交换技术是在涉密信息系统中实施分级防护要求的关键，也是大力推进信息化的难点。下一步，还需要继续深入开展该研究，以适应不同的应用场景和保密需求。

## 参考文献：

[1] Information Assurance via OMG/TOG standard: A Necessary step for Affordable, Secure Cross Domain Interoperability

[2] CWID2007 Data Diode Case Study. www.owlcti.com

[3] 李洪敏. 内外网信息交换模式设计与实现[J]. 通信技术, 2009(4): 120-122.