网络隔离与信息交换理论基础的研究*

Research on Theoretical Foundation of Network Isolation and Information Exchange

石文昌
SHI Wen-chang

(中国科学院软件研究所，北京　100080)
(Institute of Software，Chinese Academy of Sciences，Beijing，100080，China)

摘要：为网络隔离与信息交换系统(ISOX)定义一个具有通用意义的抽象结构，并以此为基础从理论上研究网络隔离与信息交换系统的工作原理、安全作用和实用价值。用 ISOX 连接内网和外网，或者可以实现内网与外网的有效隔离，或者可以实现内网与外网间的实时信息交换，但难以在实现有效隔离的同时实现实时信息交换。

关键词：网络隔离　信息交换　安全

中图法分类号：TP316　　**文献标识码**：A　　**文章编号**：1005-9164(2007)01-0066-04

Abstract：A general-purpose abstract architecture is defined for Network Isolation and Information Exchange systems(ISOX). The working principles, security functionality and practical values of these systems are investigated theoretically based on that architecture. When the inner net and the outer net are connected with ISOX, the effective isolation or the information exchange in real time between the inner net and the outer net maybe work, but it is hard to conduct the real time information exchange when the effective isolation is on.

Key words：network isolation，information exchange，security

在多网环境中，两个网络之间的隔离与信息交换是两种不同的现实需求，这是一对矛盾，近年来兴起的网络隔离与信息交换技术就是为了试图解决这一矛盾而提出来的[1～3]。网络隔离与信息交换技术习惯上称为 GAP 技术，因而，很多网络隔离与信息交换产品(或称为网闸产品)，喜欢以 GAP 来命名，如：e-GAP、NetGAP、SGAP、ViGAP、PEGAP、Topwalk-GAP，等等。

迄今为止，网络隔离与信息交换技术仍缺乏足够的理论支持。本文为网络隔离与信息交换系统定义一个具有通用意义的抽象结构，并以此为基础从理论上研究网络隔离与信息交换系统的工作原理、安全作用与实用价值。

出于一般性的考虑，在本文的讨论中，我们把网络隔离与信息交换系统简称为 ISOX(取自 ISOlation 和 eXchange)，同时，在不影响讨论的情况下，我们不对“系统”和“产品”加以严格区分。

1　结构模型与类型

我们把网络隔离与信息交换系统(即 ISOX)定义为如图 1 所示的通用抽象结构。从图 1 可见，一个 ISOX 由 3 个节点(N_0、N_1、N_2)、3 个接口(I_0、I_1、I_2)和 1 个桥(B)构成，其中，I_0、I_1、I_2 分别是节点 N_0、N_1、N_2 的接口，桥 B 的作用是建立节点 N_0 与 N_1 之间的连接，或者，建立节点 N_0 与 N_2 之间的连接。不妨把 I_0、I_1、I_2 分别称为中间接口、内接口、外接口，相应地，N_0、N_1、N_2 分别称为中间节点、内节点、外节点。

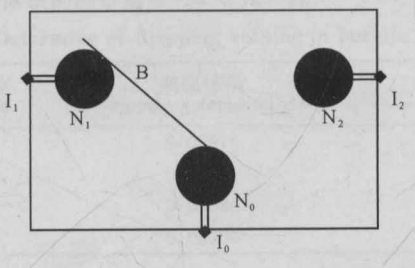

图 1　网络隔离与信息交换系统的通用抽象结构

Fig. 1　General-purpose abstract architecture of ISOX

根据不同发展阶段出现的不同形态，典型地，

收稿日期：2006-06-20
修回日期：2006-09-19

作者简介：石文昌(1964-)，男，博士，中国科学院软件所研究员，中国科学院研究生院教授，CCF 高级会员，IEEE 会员，主要研究方向为信息安全、可信计算、系统软件与虚拟机技术。

* 国家自然科学基金项目(60373054)资助。

ISOX 主要具有隔离卡、隔离主机、双机隔离设备、三机隔离设备等不同类型。

1.1 隔离卡类型

隔离卡类型的 ISOX 方案(ISOX-c)是在一台个人计算机(PC)中插上一块隔离卡,把该 PC 机虚拟成两台 PC 机,这两台虚拟的 PC 机除了硬盘存储空间和网线连接口不同以外,其他部分都是公共的。其中,两个不同的硬盘存储空间可以是一个硬盘中的两个不同区域,也可以是两个不同的硬盘。

两个不同的硬盘存储空间各自安装独立的操作系统,因而,两台虚拟 PC 机各自运行独立的操作系统。两台虚拟 PC 机通过各自不同的网线连接口连接不同的网络。在任一时刻,只能有一台虚拟 PC 机在工作。通过在两台虚拟 PC 机之间进行切换,用户可以访问不同的网络。

ISOX-c 的节点 N_0 可以定义为两台虚拟 PC 机的公共部分,节点 N_1 和 N_2 可以定义为两个不同的硬盘存储空间,接口 I_1 和 I_2 可以定义为两个不同的网线连接口,而接口 I_0 可以定义为 PC 机的人机交互接口。若桥 B 接通节点 N_0 和 N_1,则虚拟 PC 机 1 可以工作,若桥 B 接通节点 N_0 和 N_2,则虚拟 PC 机 2 可以工作。

1.2 隔离主机类型

隔离主机类型的 ISOX 方案(ISOX-h)是把两台独立的 PC 机装配在一个机箱中,这两台 PC 机除了共用一套显示器、键盘、鼠标等人机交互设备外,其他部分都是各自独立的,即独立的主板、CPU、硬盘、网卡,等等。

隔离主机外表看似一台 PC 机,内部实际上是两台独立的 PC 机,自然可以连接两个不同的网络。两台独立的 PC 机运行独立的操作系统,可以同时工作。由于两台 PC 机共用同一套显示器、键盘、鼠标等人机交互设备,所以,在任一时刻,用户只能在一台 PC 机的环境中工作,只能访问一个网络。当然,用户可以从一台 PC 机环境切换到另一台 PC 机环境,从而访问另一个网络。

ISOX-h 的节点 N_0 可以定义为两台 PC 机共用的显示器、键盘、鼠标等人机交互设备,接口 I_0 可以定义为两台 PC 机共用的人机交互接口,节点 N_1 和 N_2 可以分别定义为 PC 机 1 和 PC 机 2,接口 I_1 和 I_2 可以分别定义为网卡 1 的接口和网卡 2 的接口。若桥 B 接通节点 N_0 和 N_1,则用户可以在 PC 机 1 的环境中工作,若桥 B 接通节点 N_0 和 N_2,则用户可以在 PC 机 2 的环境中工作。

1.3 双机隔离设备类型

双机隔离设备类型的 ISOX 提供的是独立的专用设备(ISOX-2)。一台 ISOX-2 设备中集成了两台微型计算机(MC)和一个数据缓冲与控制单元(DBC)。每台 MC(可分别标记为 MC_1 和 MC_2)拥有独立的 CPU、硬盘、网卡,等,MC_1 和 MC_2 可通过它们对应的网卡 1 和网卡 2 连接 2 个不同的网络。DBC 通常称为专用隔离硬件,提供数据缓冲、隔离与交换等功能。

ISOX-2 设备中的两台 MC 之间没有直接的连接通道,它们只通过 DBC 进行连接,DBC 硬件确保在任一时刻最多只与其中一台 MC 连通,进而,在任一时刻,两台 MC 之间总是处于不连通状态,即两者处于隔离状态。每台 ISOX-2 通过两台 MC 对应的网卡连接 2 个不同的网络,因而,由 ISOX-2 连接的两个网络在任一时刻总是处于隔离状态。

ISOX-2 的节点 N_1 和 N_2 可以分别定义为其中的 MC_1 和 MC_2,接口 I_1 和 I_2 可以分别定义为网卡 1 的接口和网卡 2 的接口,节点 N_0 可以定义为 DBC,而接口 I_0 可以定义为 DBC 的控制接口。若桥 B 接通节点 N_0 和 N_1,则 MC1 与 DBC 连通,MC_1 可与 DBC 交换信息,若桥 B 接通节点 N_0 和 N_2,则 MC_2 与 DBC 连通,MC_2 可与 DBC 交换信息。

1.4 三机隔离设备类型

三机隔离设备类型的 ISOX 提供的也是独立的专用设备(ISOX-3)。ISOX-3 可以看作是在 ISOX-2 的基础上演变而来的,它把 ISOX-2 中的 DBC 替换为一台 MC(可标记为 MC_0),也就是说,一台 ISOX-3 设备中集成了 3 台微型计算机(MC)。每台 MC(可分别标记为 MC_1、MC_2 和 MC_0)拥有独立的 CPU、硬盘、网卡,等,MC_1 和 MC_2 可通过它们对应的网卡 1 和网卡 2 连接 2 个不同的网络,MC_0 用作内部中央控制机,不用于连接网络。

ISOX-3 的 MC_1 与 MC_0 之间以及 MC_2 与 MC_0 之间,通过专用的硬件线路进行连接,除此之外,不存在 MC 之间的任何其他连接。专用硬件逻辑确保 MC 之间的 2 个硬件线路中最多只有 1 个是连通的。因此,在 MC_1 与 MC_2 之间,在任一时刻,不存在连通的通道,进而,由网卡 1 和网卡 2 连接的 2 个网络,在任一时刻,都处于隔离状态。

ISOX-3 的节点 N_1、N_2 和 N_0 可以分别定义为其中的 MC_1、MC_2 和 MC_0,接口 I_1 和 I_2 可以分别定义为网卡 1 的接口和网卡 2 的接口,接口 I_0 可以定义为 MC_0 的控制接口。若桥 B 接通节点 N_0 和 N_1,则 MC_1 与 MC_0 连通,MC_1 可与 MC_0 交换信息,若桥 B 接通节点 N_0 和 N_2,则 MC_2 与 MC_0 连通,MC_2 可与 MC_0

交换信息。

2 工作原理

对 ISOX 的结构模型的讨论结果表明，各种类型的 ISOX 都是通过接口 I_1 和 I_2 来连接 2 个不同网络的。不妨把 I_1 称为内接口，把 I_2 称为外接口。可以通过内接口连接内网，通过外接口连接外网。在 ISOX 中只有一个桥 B，B 的一端总是连接到节点 N_0，另一端要么连接到节点 N_1，要么连接到节点 N_2，但不可能同时连接到节点 N_1 和 N_2，而在 ISOX 中，除了 B 之外，节点间没有其他任何的连接途径。所以，我们得到以下结论。

结论 1：用 ISOX 连接内网和外网，在任一时刻，内网与外网之间均处于隔离状态。

2.1 两态 PC 机

ISOX-c 和 ISOX-h 这两种方案定位的是用户上网用的终端 PC 机，目标是为用户提供“一台”具有两态特性的 PC 机。所谓两态是指内网态或外网态，内网态的 PC 机呈现为连接在内网中的 PC 机，外网态的 PC 机呈现为连接在外网中的 PC 机。两态之间可以切换。根据实际需要，用户可以通过态的选择，利用两态 PC 机访问内网或外网。

在这两种方案中，ISOX 可以看作是两态 PC 机，I_0 是它的人机交互接口，态间的切换通过桥 B 在节点 N_1 与 N_2 之间的切换实现。每个 ISOX 解决的是“一台”两态 PC 机在不同的时段独立地访问内网或外网的问题，独立的目标是使对两网的访问能做到互不影响，互不干涉。所以，我们得到以下结论 2。

结论 2：ISOX-c 型和 ISOX-h 型 ISOX 适合于以隔离的方式对内网或外网进行访问，能较好地实现内外与外网的隔离，不能实现两网间的实时信息交换。

2.2 网络边界设备

与 ISOX-c 型和 ISOX-h 型 ISOX 不同，ISOX-2 型和 ISOX-3 型 ISOX 属于网络边界设备，与用户使用的终端 PC 机没有直接的关系。ISOX-2 型和 ISOX-3 型 ISOX 接入网络环境的方式及位置与防火墙比较类似。

用 ISOX-2 或 ISOX-3 把内网与外网连接起来时，在一定的条件下，内网中的计算机可以与外网中的计算机进行通信和交换信息，信息流通途径如下：

途径 1：内网→I_1→N_1→N_0→N_2→I_2→外网；

途径 2：外网→I_2→N_2→N_0→N_1→I_1→内外。

根据实际应用中的不同需求，有的 ISOX 提供双向信息交换功能，即既可通过途径 1 也可通过途径 2 进行信息交换；有的 ISOX 只提供单向信息交换功能，即只可通过途径 1 或者途径 2 进行信息交换。

内网中和外网中的网络通信是通过 TCP/IP 协议[4]实现的，但在 ISOX 内部，即在 N_1—N_0—N_2 之间，不通过 TCP/IP 协议进行通信，而通过专用的内部通信协议进行通信。每个 ISOX 厂商设计实现各自的内部通信协议。

在途径 1 中，当来自内网的 TCP/IP 数据包到达 N_1 时，N_1 对数据包进行协议剥离，提取出其中的应用层信息，在 ISOX 内部只传递来自网络的应用层信息，信息到达 N_2 时，N_2 把信息重组成 TCP/IP 数据包，再传送给外网。在途径 2 中，情况正好相反，N_2 进行 TCP/IP 协议剥离，N_1 进行 TCP/IP 协议重组。

为了实现 TCP/IP 协议的剥离、重组与传送，N_1 中设有代理服务器 P_1，N_2 中设有代理服务器 P_2。代理服务器 P_1、P_2 负责协议的剥离、重组与信息的传送，同时，也实施对应用层信息的安全检查与过滤等职能。

借助 ISOX-2 或 ISOX-3 把内网与外网连接起来后，在一定条件下，内网中的计算机和外网中的计算机可以随时发出通信与信息交换请求，并实现通信与信息交换，ISOX-2 或 ISOX-3 的存在对于它们来说是透明的。因此，我们有以下结论 3。

结论 3：ISOX-2 型和 ISOX-3 型 ISOX 可以实现内网中的计算机与外网中的计算机之间的实时信息交换。

3 安全性与信息交换能力

根据结论 2 我们知道，ISOX-c 型和 ISOX-h 型 ISOX 的使用，基本上不会导致源自一个网络的安全威胁危及另一个网络，但同时，用户无法借助 ISOX-c 型和 ISOX-h 型 ISOX 实现两个网络间的实时信息交换。

根据结论 3 我们知道，用户可以借助 ISOX-2 型和 ISOX-3 型 ISOX 实现两个网络间的实时信息交换。下面分析使用 ISOX-2 型和 ISOX-3 型 ISOX 的安全性问题。

ISOX 实施协议剥离措施的主要目的是为了防止基于网络协议的攻击威胁，特别地，防止源自外网的基于网络协议的对内网的攻击。对基于协议的攻击的讨论已超出了本文的范围，这里仅以典型的 SYN 洪水攻击[5]为例分析 ISOX 防止攻击的能力。

在 TCP/IP 协议中，TCP 连接的建立是一个由 3 个步骤组成的过程[4]：

第 1 步：客户机向服务器发出 SYN 数据包；

第 2 步：服务器向客户机发回 SYN/ACK 数据

包；

第3步：客户机向服务器发出ACK数据包。

根据这个原理，发动SYN洪水攻击的攻击机A向被攻击机S发出SYN数据包，并把发送方的源地址伪装成根本不存在的X机的地址，S向X发回SYN/ACK数据包，但因X不存在，S不会收到ACK数据包。这样，S为了处理欺骗性的TCP连接请求将消耗系统资源。如果攻击机在一定时段向S发送多个SYN数据包，最终将导致拒绝服务攻击。

由于TCP数据包不可能利用途径1或途径2穿越ISOX，所以，外网的攻击机A不可能向内网的服务器S发动SYN洪水攻击。ISOX可以比较有效地防止外网攻击者向内网计算机发动基于网络协议的攻击。

在途径1中，内网信息由I_1进入ISOX，由I_2离开ISOX，进入外网。到达N_1的信息，当桥B接通N_1—N_0时，传送到N_0。到达N_0的信息，当桥B接通N_2—N_0时，传送到N_2。设一组信息X从N_1传送到N_0所用时间为T_1，从N_0传送到N_2所用时间为T_2，等待B进行必要的切换所用的时间为T_d，则信息X从N_1传送到N_2所消耗的时间为：

$T=T_1+T_2+T_d$。

显然，根据结论1，在任一时刻，途径1是处于断开状态的。但是，从信息流通的角度来看，在时段T内，信息X可以从内网传送到外网（忽略接口处的时间），也就是说，对于信息X的传送而言，从本质上说，在时段T内，途径1是连通的，“途径1在任一时刻处于断开状态”的效果只是给信息X的传送施加了一个延迟T_d。

途径2的情况与途径1类似，只是信息传输方向相反，其他原理是相同的。因此，我们得到结论4。

结论4：用ISOX-2型或ISOX-3型ISOX连接内网和外网，对于任意一组信息X，存在一个时间值T，使得在时段T内，信息X可以从内网传送到外网，或者，从外网传送到内网；换言之，对于信息X的传输而言，在时段T内，ISOX本质上处于连通状态（非隔离状态），这种本质上的连通与实际上的连通的差别，只是给信息X的传送增加了一个时间延迟T_d。

综上所述，ISOX-2型和ISOX-3型ISOX可实现两个网络间的实时信息交换，但是，对于任意信息的传输而言，在一定的时段内，由ISOX-2型或ISOX-3型ISOX连接的内网和外网本质上处于非隔离状态。ISOX-2型和ISOX-3型ISOX可以比较有效地防止基于网络协议的攻击，但是，网络中还存在很多其他类型的安全威胁，这不是ISOX-2型和ISOX-3型ISOX能够容易地防止的。所以，结论5和结论6成立。

结论5：用ISOX-2型或ISOX-3型ISOX连接内网和外网，源自外网的安全威胁很有可能危及内网及其信息的安全。

结论6：用ISOX连接内网和外网，或者可以实现内网与外网的有效隔离，或者可以实现内网与外网间的实时信息交换，但难以在实现有效隔离的同时实现实时信息交换。

4 结束语

本文为网络隔离与信息交换系统定义了一个具有通用意义的抽象结构，并以此为基础从理论上对网络隔离与信息交换系统的工作原理、安全作用、实用价值进行了研究。研究结果表明，用网络隔离与信息交换系统连接内网和外网，或者可以实现内网与外网的有效隔离，或者可以实现内网与外网间的实时信息交换，但难以在实现有效隔离的同时实现实时信息交换。网络隔离与信息交换系统难以实现网络隔离与信息交换这对矛盾的有效统一。

参考文献：

[1] 屈波，熊前兴，吴业福，等. 基于物理隔离的安全网闸研究与系统设计[J]. 计算机科学，2004，31(9)：222-225.

[2] 张少波. 用网闸隔离确保安全——GAP技术及应用发展[J]. 中国计算机用户，2003(28)：44-45.

[3] 李建华，潘理. 安全隔离与信息交换系统及其在电子政务中的应用研究[J]. 计算机安全，2003，9(31)：56-58.

[4] RICHARD STEVEN W. TCP/IP详解：卷1：协议（英文版）[M]. 北京：机械工业出版社，2004.

[5] STUART MCCLURE，JOEL SCAMBRAY，GEORGE KURTZ. 黑客大曝光：网络安全机密与解决方案[M]. 王吉军，张玉亭，周维续，译. 第5版. 北京：清华大学出版社，2006.

（责任编辑：邓大玉）