第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·安全技术· 文章编号：1000—3428(2007)12—0137—02 文献标识码：A 中图分类号：TP393.08

一种新的入侵检测系统远程管理安全技术

赖 滇
(信号盲处理国防科技重点实验室，成都 610041)

摘 要：提出了一种新的入侵检测系统远程管理技术，使IDS远程管理端口无需IP地址和TCP/IP协议栈，工作于单向发送方式，有效解决了当前管理技术存在的安全问题。实验证明了这种技术的可行性。
关键词：入侵检测系统；远程管理；单向通信；安全

A New Remote Management Secure Method of IDS

LAI Dian
(National Defence Key Laboratory of Blind Processing of Signals, Chengdu 610041)

【Abstract】This paper proposes a new remote management method of IDS. Using it, the remote management port of the IDS has no IP address and TCP/IP suite, and transmitted data one way. It solves the secure problems of the present method effectively. The test result proves that the method is feasible.
【Key words】IDS; Remote management; One way communication; Security

1 概述

1997年，美国国家安全通信委员会(NSTA)下属的入侵检测小组(IDSG)给出了“入侵”以及“入侵检测”的定义。入侵是指对信息系统的非授权访问以及(或者)未经许可在信息系统中进行的操作。入侵检测是指对企图入侵、正在进行的入侵或者已经发生的入侵进行识别的过程。

入侵检测系统(IDS)是应用入侵检测技术形成的一种网络安全设施，可以是软件或者硬件。通常情况下，IDS具有两种类型的端口：管理端口和监听端口。这两种端口是相互独立的。监听端口工作于旁路监听模式，被动接收被监听的网络中的数据，是单向通信。管理端口提供管理终端与IDS交互的通道，是双向通信。图1给出了IDS监听端口与配置端口的一般工作方式[1~4]。

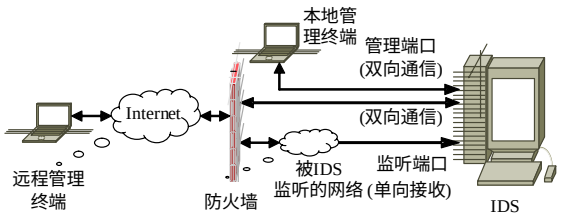


图1 IDS监听端口与配置端口的一般工作模式

2 当前远程管理的安全问题

对IDS的管理有两种方式：本地管理和远程管理。

本地管理是在本地直接将管理终端连接在管理端口上或直接操作IDS对其进行管理，本地管理端口的通信方式是双向通信，如图1所示。由于在本地操作，这种管理方式是安全的。

大多数网络入侵手段都需要事先知道目标的IP地址或需要接收目标的反馈信息[5]。IDS监听端口的单向接收安全性和本地管理的安全性使得网络入侵在本地管理端口和监听端口上对IDS是无效的。

远程管理是在远程终端上通过公共互联网或VPN对IDS进行管理，数据的发送和接收在管理端口上完成，管理端口的通信方式是双向通信，如图1所示。一般来讲，在实际的网络部署中很少采用VPN，而将远程管理的安全性依赖于管理员用户名和密码。这种管理方式存在两个安全隐患：(1)IDS存在一个与公共互联网连接的双向通信接口；(2)IDS存在一个与公共互联网通信的IP地址和TCP/IP协议栈。

大多数情况下，IDS远程管理往往是必需的，而当前远程管理技术带来的两个安全隐患给大多数网络入侵提供了条件。因此，需要一种新的远程管理技术来解决上述问题。

3 单向通信的远程管理技术

3.1 通信模型

从以上分析可以得出，要保证远程管理的安全性，新的IDS远程管理技术必须使IDS的远程管理端口和监听端口一样：工作于单向通信方式、无需IP地址和TCP/IP协议栈。因此，本文提出了单向通信的远程管理技术。通信模型如图2所示。

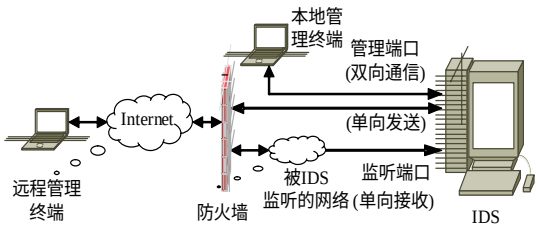


图2 单向通信的IDS远程管理技术通信模型

图2和图1的区别在于：图2的IDS远程管理端口工作方式是单向发送。单向通信可以使IDS远程管理端口无需IP地址和TCP/IP协议栈。

作者简介：赖 滇(1977－)，男，工程师、博士生，主研方向：信息安全
收稿日期：2006-06-29 **E-mail：**laidian@126.com

图 2 的远程管理过程由远程管理终端、IDS 监听端口、IDS 远程管理端口共同完成，即三者组成闭合的通信环路。IDS 通过监听端口接收远程管理终端发送的数据，通过远程管理端口将反馈数据发送到远程管理终端。

3.2 传输可靠性

单向通信存在一个问题：传输可靠性。简单文件传输协议(trivial file transfer protocol, TFTP)和 TCP 事务协议(transaction/TCP, T/TCP)提供了在无连接情况下，保障传输可靠性的方法[6]。基于停/等的传输机制，本文提出了一种新的传输协议。

3.2.1 传输过程

远程管理终端(remote management terminal, RMT)对 IDS 进行一次管理的过程如下：

(1)RMT－>IDS

1)RMT 向 IDS 发送管理数据(数据量较大时，则分片发送并对分片编号)，数据发送完后，发送结束信息。RMT 若等待时间 T 后，没有收到反馈信息，则重发所有数据。

2)IDS 在监听端口接收并缓存数据，收到结束信息后，检查数据正确性。若正确，则执行，并通过远程管理端口返回相应数据。若错误，则将错误的分片编号通过远程管理端口反馈到 RMT。RMT 重发相应数据分片。此过程可能重复执行，直到接收正确。

(2)IDS－>RMT

1)IDS 通过远程管理端口向 RMT 发送数据(数据量较大时，则分片发送并对分片编号)，数据发送完后，发送结束信息。IDS 若等待时间 T 后，没有收到反馈信息，则重发所有数据。

2)RMT 接收并缓存数据，收到结束信息后，检查数据正确性。若正确，则执行。若错误，则将错误的数据分片编号通过监听端口反馈到 IDS。IDS 重发相应分片。此过程可能重复执行，直到接收正确。

3.2.2 停/等机制的可靠性

本文提出的传输过程采取停/等机制以代替双方建立连接的过程，即等待时间 T 后，若对方无反馈信息则重发所有数据。图 3 给出停/等机制可靠性分析模型。

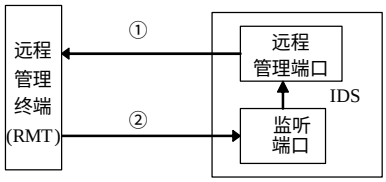


图 3 停/等机制可靠性分析模型

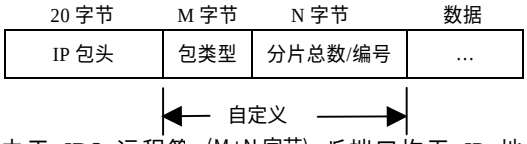
由于 RMT 与 IDS 之间通信是无连接的，因此图 3 中的过程①、②不可靠。本文采用的停/等机制能够确保过程①、②的可靠性，分析如下：

(1)若过程①发送失败，则过程②中 RMT 不会向 IDS 发送反馈信息。此时，IDS 将重复过程①，直到成功。

(2)若过程②发送失败，则过程①中 IDS 不会向 RMT 发送反馈信息。此时，RMT 将重复过程②，直到成功。

3.2.3 数据构造的一种方式

从路由协议可以知道，正确的 IP 包头即可保证数据包在网络上正确传输。基于此，本文提出了 RMT 与 IDS 之间传输数据的一种构造方式，如下所示：



由于 IDS 远程管理端口均无 IP 地址和 TCP/IP 协议栈，IP 头部对应的 IDS 地址设置为 IDS 监听的任意 IP 地址。

M=1、N=2 时，自定义字段和数据字段可按以下方式构造：

名称	长度	取值	描述
包类型	1B	0x00 或 0xFF	区分包的类型。0x00 表示该包为指令包，0xFF 表示该包为数据包
分片总数/编号	2B	0x0000 ~ 0xFFFF	表示分片总数或编号。如果包类型字段为 0x00，则表示数据的分片总数。例如，0x0001 表示该回传数据有 1 个分片，0x000F 代表该回传数据有 15 个分片。如果包类型字段为 0xFF，则表示数据的分片编号，以 0x0000~0xFFFF 范围的数字表示，如 0x0001 表示该回传数据的第 1 个分片，0x000F 代表该回传数据的第 15 个分片
数据			如果包类型字段为 0x00，表示包内容是需要重传的数据分片，如 03 0F，表示需要重传第 3、15 个分片。当包类型为 0xFF 时，表示包内容是数据；若数据部分为全 0，则为结束标志

3.3 传输有效性

同 UDP、TCP 相比，本文提出的数据构造方式具有更高的传输效率，主要体现在以下 3 个方面：

(1)数据传输的包头的开销为 3 个字节(M=1、N=2 时)，小于 UDP(8 字节)、TCP(20 字节)的包头开销。

(2)同 TCP 相比，本技术数据传输的过程省去了建立连接的三次握手和撤消连接的四次握手的时间。

(3)本文采取错误重传机制保证数据传输可靠性。实际上，面向连接的服务(TCP)也是采用错误重传机制来保证数据传输可靠性。不同的是，本文的技术是由应用程序发起错误重传，而 TCP 是在传输层发起错误重传。

4 仿真实验

在实际网络环境对本文的技术进行了仿真实验，结果如下所示：

(1)实验数据

数据量/B	数据分片大小/(B/包)	一次正确率/%	二次正确率/%	传输时间/s	
				本文技术	当前技术
500K	512	99.4	100	4.5	4.3
2.5M	512	99.8	100	20.6	20.7
5M	512	99.2	100	41.9	41.6
15M	512	99.9	100	125.8	124.5

说明：

1)一次正确率＝(一次正确接收数据分片总数)/(发送数据分片总数)×100%；

2)二次正确率＝(错误重传后正确接收数据分片总数＋一次正确接收数据分片总数)/(发送数据分片总数)×100%；

3)传输时间：一次传输过程完成时间。

(2)实验结论

从传输时间上看，本文提出的远程管理技术在效率上和当前技术是相当的。 (下转第 141 页)