网络入侵检测协同信息的安全传输

樊隽 龚俭

（东南大学 计算机系，210096 南京）

【摘要】本文介绍了一个面向网络入侵检测协同信息的安全传输系统的设计与实现，它能够支持检测协同底层的数据传输并保证各协同站点间的信道安全，是基于入侵网络检测系统中必不可少的一个组成部分。

【关键词】协同检测 IAP XML TLS IDS

中图分类号：TP393

The Secure Transfer of the Cooperative data in Network-Based Intrusion Detection System

Fan Jun, Gong Jian

(Southeast University, Computer Science Dept., 210096 Nanjing, P.R.China)

【Abstract】This paper discusses the design and implementation of a secure transfer of the cooperative data in a network-based intrusion detection system. It makes the data transfer of security cooperation available, ensurs the security of all the communicative channels between different cooperation spots and supply the base of ensuring NIDS accurately describe occurred security incidents to some extent.

【Key words】cooperative detection, IAP (Intrusion Alert Protocol), XML(Extensible Markup Language), TLS(Transport Layer Security), IDS(Intrusion Detection System)

1．引言

检测协同传输是实现检测协同的基础，一般将分为两层，下层实现数据传输并保证多个协同站点间的通信信道的安全，上层把从下层传输获得的安全事件作为参考事件用 XML 编码程序进行封装，供检测协同程序调用处理。

目前在网络安全监测方面比较著名的研究成果有由美国加州大学 Davis 分校的安全实验室提出的 CIDF（Common Intrusion Detection Framework）和由 IETF 安全领域的 IDWG（Intrusion Detection Work Group）负责建立的 IDEF（Intrusion Detection Exchange Format）标准，本文讨论的工作是根据 IDWG 完成的。

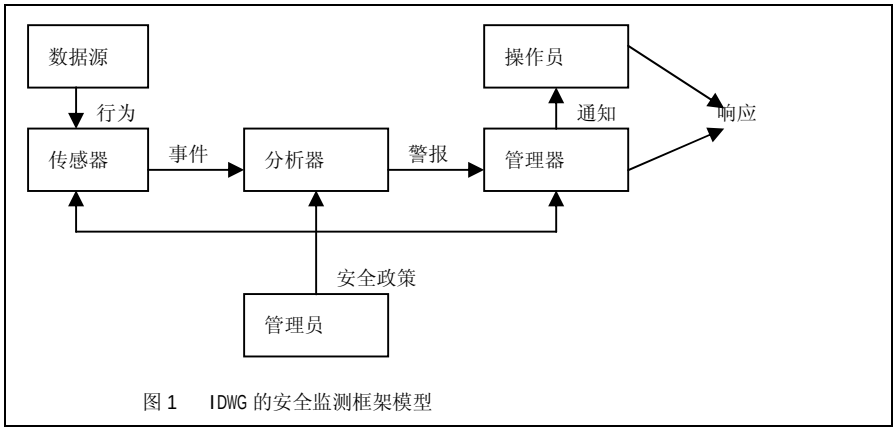

图 1　IDWG 的安全监测框架模型

IDWG 于 2000 年 1 月发表了“draft-ietf-idwg-iap-01”，对 IAP 进行了详细的描述。Intrusion Alert Protocol(IAP)是一个在入侵检测系统中各元素间，尤其是信道传感器（sensor）、分析器（analyzer）和管理器（manager）之间交换入侵警告数据的应用层协议，它独立于数据表达形式，并从设计角度保证了数据传输的完整性和安全性，使有关数据可在高速 IP 网中安全传输。IAP 应用 TCP 作为其底层传输机制，可用于多种 IP 服务中。在本系统的实现中，IAP 用于支持把警告信息从发现入侵的入侵信道传感器、分析器处传输到管理器上，而 IAP 的安全性是用 TLS 握手协议[1]实现的。 图 1 给出了 IDWG 的安全监测框架模型。

作者简介： 樊隽，硕士研究生，主要研究方向为网络安全。 龚俭，工学博士，东南大学计算机系教授、博导，主要研究方向包括网络管理、网络安全、网络体系结构、开放分布式处理等。

定稿日期：2001－05－28

另外，本系统用 XML 实现共享数据格式 IDMEF(Intrusion Detection Message Exchange Format)，一方面因为 XML 具有很大的灵活性，另一方面处理 XML 文档的软件工具很多，实现方便。此外 XML 支持 Unicode，用 XML 表示的消息格式满足 IDMEF 对国际化和本地化的要求，这也是实现中采用它的一个重要原因。

2．检测协同传输的总体设计

检测协同传输建立在 IP 层以上，应用层下，基于 TCP 进行面向连接的传输，分为服务器方和客户机方。协同服务器表现为一独立的进程，该进程能够对 TLS 和 IAP 进行支持，对请求信息进行验证，确定请求者拥有被信任的证书。在检测协同的请求方，即客户方，也能够对 TLS 和 IAP 进行支持，对协同服务器进行验证，确定其拥有被信任的证书。其总体结构如下图 2 所示：

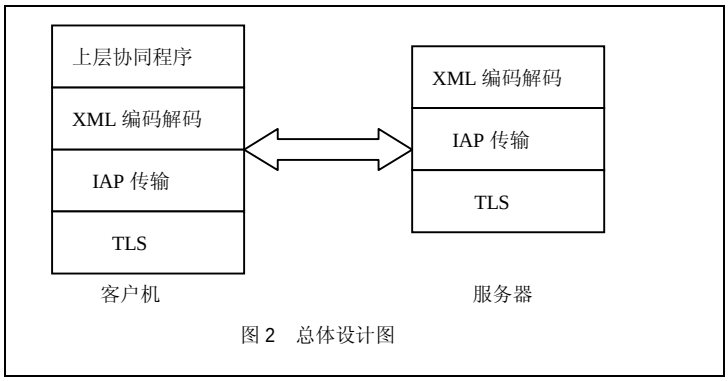

图 2　总体设计图

客户方首先对检测协同服务器进行身份认证，获得对方的可信证书，再对于协同决策要求协同的安全事件调用 XML 编码程序进行编码，通过 IAP 安全传输发送给需要协同的各个协同站点，从而获得肯定或否定性的证实。

服务器接受到客户方的检测协同请求后，先调用相应的 XML 解码程序获得请求验证的安全事件，再在安全事件库中进行查询，如有匹配则将获得的相关安全事件中的第一个作为参考事件用 XML 编码程序进行封装，并用 IAP 和 TLS 回答给请求方，否则给出否定性证实。具体流程如图 3 所示：

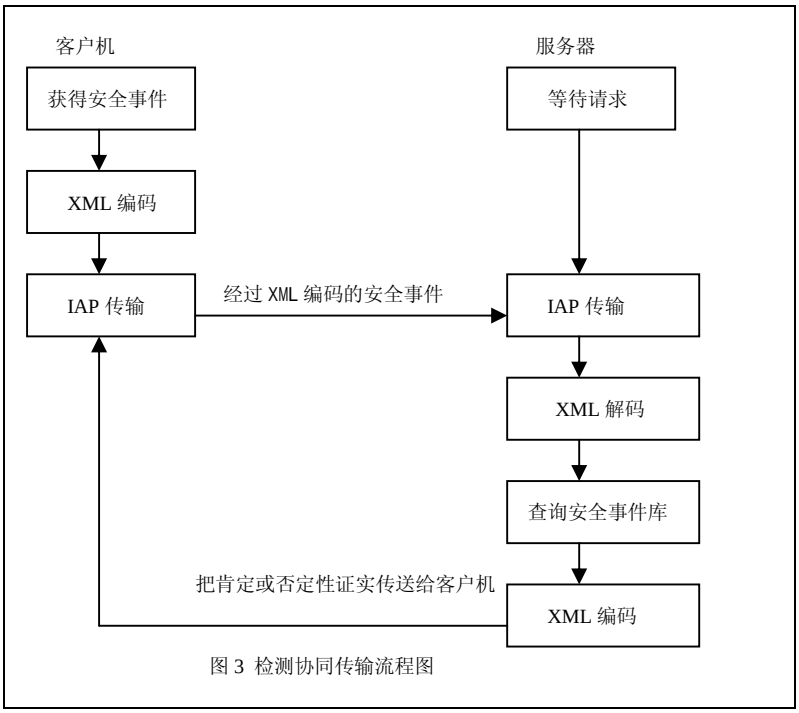

图 3 检测协同传输流程图

3、检测协同传输的实现

检测协同传输包括服务器方和客户端两个部分，服务器方实际就是管理器（Manager），而客户端有信道传感器

和分析器（SA）组成。在其实现中，应用的是 IAP 1.0 版本和 TLS 1.0 版本。整个检测协同传输可分为数据传输所依赖的底层环境和高层接口两个部分。而检测协同传输所依赖的底层环境就是 IAP 传输。

3.1 IAP 传输

检测协同底层传输模块部分用 C 语言实现。它提供了一个接口函数供上层调用。其设计思想主要依据 IAP 和 TLS。它在 TCP 以上，以 TLS1.0 作为其安全认证基础，其结构如图 4 所示：

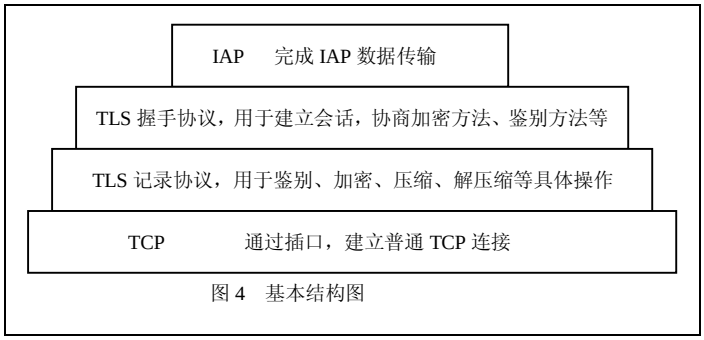

图 4 基本结构图

底层数据传输可分为四个部分：Protocol Setup、Security Setup、Secured data transport 和 Termination。

a. Protocol Setup

服务器和客户机双方首先通过套接字（Socket）建立普通的 TCP 连接。之后，双方采用 request-response 形式交换建立 IAP 连接的一些传输参数。客户方首先向服务器发送一个 iap-connect-request 的请求命令，相应的 IAP 服务器则发送一个 iap-response 响应，根据是否接受此连接，在 iap-response 中设置不同的状态参数。

b.Security Setup

在完成了协议的初始化建立之后，采用一对 request/reponse 对来完成传输连接的安全更新。客户机在接到 iap-response 命令后，发送一个 iap-upgrade-request 命令，而服务器在发送了 iap-response 命令后，等待 iap-upgrade-request 命令，若在有效期内没有接收到此命令或接收到其他的命令，就断开连接。接收到此命令后，服务器发送 iap-response 命令。若服务器接受了安全更新，双方就开始了 TLS 握手。本系统采用 Openssl0.9.6 中的 s-server 和 s-client 模块所提供的 API 接口函数来完成 TLS 握手，并定义采用的协议是 TLS 1.0，使用的 CA 是华东北网络中心 CA 服务器。双方进行 TLS 握手时，客户机首先查询服务器证书是否存在，若存在，则进行验证，从而决定是否可信。服务器也同样对客户机进行身份认证，如果成功，则协议的初始化及安全认证完成，服务器和客户机间的安全信道已可以用于警告信息的传输。

c. **安全数据的传输**

经过编码的警告信息根据特定的报文格式从客户机发送到服务器。其中所传输的数据是经过 XML 编码的数据。

d. **断链**

连接的两端都可以提出断链请求，以常规的 close-notify 请求和应答命令对实现。

3.2 高层接口

整个安全协同传输模块是安全协同的底层传输部分，它为安全协同提供了一个接口函数，适用于客户机。此函数格式为：int handle-request(int* length , struct sockaddr_in sa)，返回值为整型，失败返回 0，成功返回 1，同时 buffer 中返回服务器的应答，length 表示其长度。

在服务器方主要调用上层提供的一个相应函数为：int handle-request(int length)来处理从客户方传输来的入侵警告，并把相应的处理结果返回客户机。若此处理行为成功，函数返回 1；若失败，返回 0。

4、结束语

在今天的 Internet 中，对安全事件进行全局描述的重要性日益显著，对通信双方的身份认证的要求也会越来越高。本文的研究正是面向解决这些问题而做出的尝试。最终实现的系统采用标准的方式描述安全事件，并在安全可信任的通道上将信息在客户机和服务器间传递。进一步的工作将是为该系统完善其协同方面的功能，包括互纠、互补、调整检测等。