计算机科学1998 Vol. 25 №. 1

# Extranet 及其相关标准

Extranet and Its Relevant Standards

赵 慧 侯建荣 蔡希尧

(西安电子科技大学 西安710071)

**摘 要** Extranet是以最简单的形式扩展Intranet的更安全、更有价值的解决办法。本文介绍Extranet的概念和相关的主要标准。

**关键词** Extranet,标准

## 1. 引言

Internet 技术彻底地改变了企业计算的模式和扩大了企业计算的范围。愈来愈多的组织正在摒弃早期那种专有协议互相竞争的网络模式。取而代之的是,这些企业采用 Internet 作为通用网络体系结构,用于处理 Web 页面、收发 Email 和运行 Client-Server 应用软件等任何事务。Intranet 成为企业网络的发展趋势。正当人们开始认识到 Intranet 的诸多优点时,例如,改进企业内部信息流,通过公用的 TCP/IP 协议将各企业内各机构连在一起等,开发 Extranet(企业外部网)开始成为各公司的下一目标。

Extranet 是在 Intranet 的基础上发展的,充分考虑了企业的自身体系结构和运作行为,使计算机网络高层体系结构逐步与企业计算模式相协调。简单地说,一个 Extranet 是企业网络的一部分,用防火墙将它与 Intranet 上的重要资源和 Internet 上的不守规矩的用户隔离开来,使企业的贸易伙伴能够访问以前仅供内部职员使用的重要资源。"Extranet 是以最简单的形式扩展 Intranet 的更安全、更有价值的解决办法。"但建立一个 Extranet 所遇到的问题与建立 Intranet 所遇到的问题不同,Intranet 主要考虑企业内部部署,而 Extranet 则主要考虑在网络安全的前提下,如何扩大内部网的访问范围。

本文着重论述 Extranet 的概念和主要相关标准。

## 2. Extranet 的定义

### 2.1 Intranet 的含义

通常,Intranet 是 Internet 的内部版。它运行于开放的 TCP/IP 网络之上,使用 WWW 所用的同样类型的服务器和浏览器,例如 Web Server、Web Browser、Email、Ftp 等,完成分布于协作的 LAN 上的内部应用软件。由于 Intranet 基于相同的独立的标准 Internet 协议和技术,因此,对于组织内部的每一位成员,不管其硬件平台如何,均可访问 Intranet 上的信息。

Intranets 不仅解决了已有通讯模式遗留的问题,它还具有下述优点。

·选择自由:Web 技术基于开放的标准,在几乎所有的操作系统和硬件平台上都可用,并且能使原有数据库系统发挥更大的效用。

·安全:信息保护至关重要,甚至于一个小的协作网络。信息包加密传输确保信息安全,防火墙技术保证 Intranet 不受外界非法用户入侵。Netscape 公司的 SSL(Secure Sockets Layer)技术正作为 Web 相关产品的安全标准。

·使用简便:超文本联接使用户仅仅通过点击一个字或一幅图,很容易浏览和查找多种格式的信息。Intranet客户方软件,例如 Netscape Navigator、Microsoft Internet Explore 具有单一的前端界面,使用户不必学习新的软件就能访问内部和外部资源。

·花费合理:在购买、培训和部署方面,Intranet 应用软件不昂贵。而且,Intranet 的平台独立性减少了分配客户软件的需求以及为相同应用软件建立不同版本的需求。

Intranet 提供的服务如下:

Intranets 的用户服务有:信息共享和管理、通讯与协作、浏览、应用访问。

Intranets 的网络服务有:目录服务、复制、安全

服务、网络管理。

### 2.2 Extranet 的含义

通俗地讲，Extranet 就是用户象使用 Internet 那样访问 Extranet 的主页或 Web 站点。但是，仅仅为特定范围内的用户所使用，而不是整个世界范围。与 Intranet 区别，称作企业外部网。Extranet 的用户是一组为达到联合的目的，需要通讯、协作或交换文档的紧密相关的公司。因此，只有经认证或授权的用户方能访问 Extranet。

从企业角度看，Extranet 考虑了贸易伙伴的商业要求，使贸易伙伴能够获取以前只供内部网上的职员使用的重要信息。从技术角度，Extranet 是在保证核心数据安全平稳运行的同时扩大对网络访问范围。

由此，Extranet 是应用 Internet 技术将企业与其拥有共同目标的供货商、消费者或其他企业联接在一起的合作网络。

### 2.3 Extranet 与 Internet 和 Intranet 的比较

借助下面图表说明三者的区别：

| | Internet | Intranet | Extranet |
|---|---|---|---|
| 访问范围 | 公　共 | 私　有 | 半私有 |
| 用　户 | 所有用户 | 特定企业的用户 | 紧密相关的企业组 |
| 信　息 | 片段信息 | 专有信息 | 完全信任范围共享信息 |

## 3. Extranet 相关标准

### 3.1 Internet 标准

Internet 技术的广泛应用是由以下开放的应用标准支持的，它们适用于几乎所有的 Client 和 Server 平台。

HTML 和 HTTP 支持建立平台独立的内容以及发布和共享信息。应用 Java，JavaScript 和 CORBA(公共对象请求代理体系结构)，能够开发平台独立的软件，创建和使用分布式对象。SMTP(Simple Mail Transfer Protocol)，IMAP(Internet Message Access Protocol)、MIME(Multipurpose Internet Mail Extensions)、S/MIME(Secure MIME)、NNTP(Network News Transport Protocol)以及 RTP(Real-Time Protocol)等这些协议提供了 Email、研讨厅和会议等功能，允许各独立平台间消息传递和协作。LDAP(Lightweight Directory Access Protocol)提供目录服务、X.509提供安全服务、SNMP(Simple Network Management Protocol)提供网络管理能力。

### 3.2 Extranet 标准

上述标准适用于大范围的 Internet，而针对 Extranet 的特性，以下标准尤为重要。

3.2.1 轻目录访问协议 LDAP。目录服务已成为网络服务、应用和用户的基本指标。LDAP 是目录服务的 Internet 标准，它提供对 X.500目录的访问而不引起 DAP(目录访问协议)的资源需求，并对 DAP 本身作以补充。LDAP 在三个方面使用：作为匿名浏览的协议、对敏感信息的权限访问、Server 间通讯。LDAP 的核心部分有：

·协议元素直接在 TCP 上传输，绕过对话层/表示层的大部分。

·大多数元素编码为一般的字符串。

·轻型 BER(Basic Encoding Rules)编码用于对所有协议元素进行编码。

LDAP 采纳的协议模型是，Client 向 Server 发出将要执行的操作的协议请求，由 Server 负责在目录上执行必要的操作。一旦 Servers 完成了这些必要操作，便向发出请求的 Client 返回结果或错误应答。

LDAP 协议运行于面向联接的、可靠的传输，在数据流中一个八位字节的所有8位都有含义。LDAP 已与 TCP 和 COTS(Connection Oriented Transport Service)传输服务建立了映射。

为了协议交换的目的，所有协议操作均封装于一公共信包 LDAPMessage 中，LDAPMessage 定义如下：

```
LDAPMessage ::=
    SEQUENCE{
    messageID MessageID,
    protocolOp CHOICE{
                略
            }
        }
```

除了 LDAPMessage 的定义外，还有一些定义用于定义协议操作，这里不一一说明。

LDAP 的操作有：

·Bind：在 C 和 S 间启动协议会话，允许 C 向 S 的认证；

·Unbind：终止协议会话；

·Search：Client 请求 Server 执行 Search 操作；

·Modify：Client 请求 Server 执行 DIB 的修改操作；

·Add：Client 请求在目录中增加一项；

·Delete：Client 请求在目录中删除一项；

·Modify RDN：Client 改变目录中一项的名字的最后成份；

·Compare：Client 将一断言与目录中的项进行

比较；

·Abandon Operation：Client 发出 Server 作废未完成操作。

LDAP 在安全性方面支持认证(authentication)。版本2使用简单的认证(加密的信息在线路上传输)和 Kerberos(使用数据加密标准 DES 提供安全注册和认证服务的网络安全和认证系统)。版本3将使用 X.509的强认证技术，即采用公开密钥验证的技术。

3.2.2 IIOP 协议。Extranet 不仅仅提供的是分布式信息的共享，更重要的是分布式应用的互操作。CORBA 的 GIOP(General Inter-ORB Protocol)和 IIOP(Internet Inter-ORB Protocol)提供了互操作的支持。对象请求代理 ORB(Object Request Broker)使对象在分布式环境中透明地收发请求和响应，是构造分布式对象应用，使应用在不同层次的异构环境下互操作的基础。

ORB 互操作阐述了一种综合的、可伸缩的方法，这个方法支持分布的、多个遵从 CORBA 规范的异构 ORB 管理的对象网。互操作包括三个部分：ORB 互操作结构；ORB 间桥；GIOP 和 IIOP。

ORB 互操作结构定义了一种概念框架，说明了各种域的特定 ORB 信息的作用，包括对象引用域、类型域、安全域和事务域等。同一域中的 ORB 可直接通讯，而不同域中的 ORB 需借助桥进行通讯。桥的作用是确保将一 ORB 的内容和语法映射到另一个 ORB，使得任何给定 ORB 的用户仅看到自己的内容和语法。桥既可用于遵从 CORBA 规范的 ORB 互操作，也支持非 CORBA 系统。

GIOP 是 ORB 间传输语法标准和通讯的信息格式，是为 ORB 交互而建立的。基于面向联接的传输协议，不需要高级 RPC 机制。GIOP 消息传输在 TCP/IP 协议上的映射称作 IIOP。GIOP 由以下部分组成：

·CDR (Common Data Representation) 定义：CDR 是一传输语法，定义了 OMG IDL (Interface Definition Language) 数据类型与 ORB 和 Inter-ORB 桥(代理)间传输的低级表示的映射。

·GIOP 消息格式：GIOP 消息在代理与对象请求、本地对象实现和管理通讯通道间交换。

·GIOP 传输假设：GIOP 描述了广义的假设，即任何网络传输层可用于传输 GIOP 消息，也描述了如何管理联接以及 GIOP 消息指令的约束。

IIOP 在此基础上增加了一个成份——IIOP 消息传输：IIOP 描述了代理如何打开 TCP/IP 联接以及如何使用它们传输 GIOP 消息。

GIOP/IIOP 的主要特征：

·开放：OMG 的600多个成员支持 IIOP。由于 IIOP 是平台独立的，为大多数主流的硬件和软件平台开发的应用都是可行的。

·广泛适用：GIOP/IIOP 基于广泛应用的通讯传输机制(TCP/IP)，而且定义了 ORB 间传输 CORBA 请求的必要的最小协议层。

·简单：尽可能简单，以保证独立的可兼容的实现。

·可伸缩：GIOP/IIOP 支持 ORB、桥联接的 ORB 网络及至 Internet。

·花费少：在已有的或新的 ORB 中增加 GIOP/IIOP 支持，只需很少的投资。

·通用：IIOP 是针对 TCP/IP 定义的，GIOP 消息格式可用于任何满足最小假设集的传输层，而且 GIOP 也可在其他面向联接的传输协议上实现。

·体系结构独立：GIOP 关于代理(Agent)体系结构是在最小假设集上建立的，GIOP 将 ORB 看作是体系结构未知的透明的实体。

·可重用：因为基于 IIOP 的应用向网络提供标准接口，所以对于 Internet 或协作 Intranet 上其它基于 IIOP 的应用，它可作为一个构件。这种功能不仅使各应用间可以互操作，而且使开发人员建立可重用的、大粒度的、能被其他开发人员定制的服务，以构成新的应用或集成已有应用。

3.2.3 安全标准。在 Extranet 上，安全问题最重要。使用 PKCS(公开密钥标准)的安全标记、数字签名、验证授权使用户对信息资源进行安全的访问。加密技术使敏感信息的访问有了安全保证。DES(数据加密标准)用于网络传输和存储的文件加密和解密；Kerberos 对在分布式 LAN 客户和服务器应用之间进行的整个通讯对话进行加密；S/MIME 加密电子邮件的主体部分和附件。

**安全 MIME** 就是 PKCS 对电子邮件提供的安全服务。它是基于身份证明的加密和验证方式发送保密的 Email 消息的标准。PKCS #7 and #10定义了这部分标准，详细阐述了消息格式、消息处理、实现等细节。

**X.509 V3** 是用于加强验证和加密的电子凭证规范。数字验证提供一有效的、数字签名的信息的容器，在一个包括安全服务器、防火墙、Email 和付费系统的网络上，支持组织、目录户设备间的强验

计算机科学1998 Vol. 25 №. 1

# 建立 INTERNET 上的安全环境

Building a Security Environment on Internet

唐晓东　齐治昌

（国防科技大学计算机学院　长沙410073）

**摘　要**　In this paper, we analyse security risks of internet, then introduce a security architecture, finally analyse the security attributes of current Internet protocol sets.

**关键词**　Internet, Intranet, Kerberos, Security, Cipher, Security key, Firewall, TCP/IP

最近几年 INTERNET 飞速发展，为用户提供方便的远程计算、资源共享和电子数据传输等服务，促进了社会发展。然而，INTERNET 尚存在着一个致命缺点：缺乏安全性。在激烈竞争的社会中，用户面对着 INTERNET 拥有的巨大财富，既爱又怕，INTERNET 的安全已成为迫切需要解决的问题了。本文首先介绍一般性安全概念，然后讨论 INTERNET 存在的安全问题，并针对这些安全问题给出一个安全体系结构，最后分析现有 INTERNET 协议集的安全性。

证。它是 S/MIME、对象签名和 EDI 的安全基础。

在强安全方面，验证比密码有优越之处：鉴别身份、确保消息和内容的有效、保证隐私、授权访问、授权事务以及支持承认(non-repudiation)。

**vCard**　定义了个人之间电子化通讯的数据格式，即将电子、电讯手段加入 PDI(Personal Data Exchange)中，保证信息快速、准确地通讯、存储、组织和方便地定位。这种格式独立于特定的传输方法，可以是文件系统、点对点公共交换电话网、有线网或无线网。在 Internet 上，vCard 用于：

·转递电子邮件消息中的个人数据。通过使用 vCard，可自动操作 WWW 的用户在主页上填写的大量的表(form)。

·电子邮件的收件者自动记录发信者的个人信息，仅仅通过将电子邮件拖入他们的地址簿中，不需要信件头和信件尾消息。

·自动填写大量的主页表格。倘若 Web 服务器和浏览器支持 vCard，那么可加速这个应用。

**签名对象(Signed Object)**　是确保 Extranet、Intranet 和 Internet 上软件可靠分派，帮助用户和网络管理员决定软件资源是否可靠的一种技术。在 Extranet 上，可靠的跨平台鉴别、分派和访问控制，对于软件尤为重要。对象签名使用基于 X. 509 v3标准和一些 PKCS 规范，包括 PKCS #7签名和加密标准。数字签名可用于：

·鉴别签名者身份：确认个人、公司或其他实体的身份，他们的数字签名与一签名对象关联。

·检测变化：决定是否一签名对象未经授权而被改动。

·控制 Java/JavaScript 访问。

·自动更新软件。

Netscape 提出的 SSL 技术加密 Web 浏览器和服务器之间的通信对话。

**结束语**　Extranet 与其说是一种网络设计方案，不如说是一种概念。它是一个复杂的综合系统，涉及 ISP 的服务质量、通讯的可靠性以及信息的安全性。其中信息的安全性最为重要，授权和加密是两类主要的安全服务。建立 Extranet 需 Web 技术、分布式对象技术和安全认证技术的支持。在未来的二、三年里，Extranet 将成为企业的主选网络体系结构。

## 参考文献

[1] Georage Lawton, Extranets: Next Step for the Internet, IEEE Computer, 5, 1997

[2] The Common Object Request Broker: Architecture and Specification, OMG, July 1995

[3] Networke Working Group, RFC1777

[4] Overview of Extranet Standards Extending the Networked Enterprise, http://www.netscape.com/

[5] Security and Signed Objects, http://www.javasoft.com:80/