Internet 的网络安全

龚俭（东南大学）

摘要：本文介绍了 Internet 所涉及的网络安全技术的基本概念及其发展现状。

关键词：Internet、网络安全、鉴别技术、密钥管理、防火墙

1. 引言

Internet 的最大优势之一是它的自由性，没有严格的管理体制来约束网络中的应用；但是从安全的角度看，这同时又是 Internet 的最大缺点，过分自由的网络用户和网络应用给 Internet 带来严重的安全隐患。早期的 Internet 节点（site）主要是教育科研机构或政府部门，这些节点的主要安全考虑是防止计算机黑客的入侵，因此各自设置自己的安全政策和安全措施，不存在全局的安全体系结构。随着 Internet 的商业化，越来越多的企业进入网络并在网上开展业务，从而使得与交互有关的安全问题日益突出，例如用户的身份鉴别，敏感信息的传输保护，交互的无否认等。此外，日益开放的系统和网络结构也向潜在的黑客提供了更多的信息，因此对于在 Internet 中建立全局性的网络安全体系结构的需求日益迫切。

1994 年初，IAB 在美国南加州大学信息科学学院召开了关于 Internet 安全问题的战略研讨会，确认当前 Internet 发展的最大问题是规模和安全，且两者是相互关联的。进入九十年代以来，Internet 的安全问题集中在以下四个方面：

(1) 端－端的安全问题，主要指用户（包括代理）之间的加密、鉴
别、和数据完整性的维护；

(2) 端系统的安全问题，主要涉及防火墙技术；

(3) 安全服务质量问题，主要指如何保证合法用户的带宽，防止
用户非法占用带宽；

(4) 安全的网络基础设施，主要涉及路由器、DNS 服务器，以及
网络控制信息和管理信息的安全问题。

从中可以看出，防止用户非法侵入网络和非法访问资源是当前网络安全的主要问题。

2. Internet 的安全控制

Internet 的安全控制基于安全域的概念，它通常对应一个组织机构（如一个公司或学校），以及一个相

对独立的网络，各个安全域内的网络和信息系统使用自己的安全政策、安全机制、和安全系统。因此，Internet 的安全控制本质上是各自为战。

然而 1988 年底 Internet 蠕虫事件发生后，为了应付 Internet 出现的紧急安全问题，美国国家标准及技术学会（NIST）发起建立了 Internet 的计算机紧急响应工作组(Computer Emergency Response Team) 和相应的协调中心 CERT/CC（设在美国卡内基梅隆大学的软件工程学院），CERT 的系统秘书处设在 NIST。Internet 中的一些重要的网络也相应成立了类似的组织，以应付网络中出现的突发事件，维护网络的安全。CERT 在 Internet 中专门建立了一个新闻组，以通报网络中发现的安全问题及其解决方法。CERT 从 1988 年开始向外发布安全建议 (Advisories)；从 1994 年开始发布公告 (Bulletines)；从 1995 年开始发布摘要 (Summaries)；并且给出较为完整的测试表以及对安全信息、信息服务配置、安全概念、安全工具的总结。

目前 IETF 在网络安全领域设立了 12 个工作小组，组织研究当前 Interent 中的安全热点问题，并制定相应的标准；它们分别是

(1) 防火墙鉴别技术工作组（aft）；
(2) 通用鉴别技术工作组(cat)；
(3) DNS 安全工作组(dnssec)；
(4) IP 安全协议工作组(ipsec)；
(5) 一次性口令鉴别工作组(otp)；
(6) 公开密钥基础结构（X.509）工作组 (pkix)；
(7) 安全 Shell 工作组(secsh)；
(8) 简单公开密钥基础结构工作组(spki)；
(9) 运输层安全工作组(tls)；
(10) Web 的事务安全工作组(wts)；
(11) PGP 开放规范工作组(openpgp)；
(12) S/MIME 邮件安全工作组(smime)。

3. 端一端的安全问题

它包含了数据加密、鉴别、完整性维护等方面，这里的端可以指直接参与通信活动的主机或是它的代理（如防火墙）。数据加密可防止网络中存储和传输的数据内容被泄露，采用的方法包括通信双方使用相同密钥的对称密钥体制（如 DES、IDEA 等方法），也可以是通信双方使用不同密钥的公开密钥体制（如 RSA、离散对数方法等）。PGP 已成为 Internet 使用最广泛的端系统安全工具，因此 OPENPGP 工作组正在为各种版本的 PGP 实现制定统一的内部信息格式，以增强它们的互操作性。然而，数据安全是一个敏感问题，在绝大多数国家都存在控制和应用上的矛盾。例如，大部分数据加密技术涉及

知识产权问题，因此推广使用有一定的难度；另外，大多数Internet成员国对数据加密的使用有限制，这也为构造整个Internet的安全体系结构带来人为的障碍。Internet的最大成员美国的政策矛盾就很典型，一方面要求大力推行国际化的电子商贸，要求免除这方面的关税；另一方面又禁止数据加密技术出口，从而又束缚了美国企业在开展国际化电子商贸方面的手脚。

鉴别技术用以验证用户的身份，传统的方法是使用用户标识和口令，还可使用基于各种信息摘录（message digest）算法，如MD5，的数字签名技术，以提高可靠性。数据完整性技术用以保护网络中的数据不被非法修改，通常使用数字签名技术来实现。IAB建议端—端的安全问题应把加密与鉴别分开，以适应不同应用的需要和出口限制的约束。鉴别功能可在整个Internet范围内使用，而加密则根据需要进行。IETF有好几个工作组在同时从事这方面的工作。CAT工作组研究开发了一组可支持各种Internet协议开发的分布式通用安全服务和程序库（GSS—APIv2，RFC 2078），包括鉴别、加密、和完整性保护等多方面的功能，以方便新协议的开发和增强互操作性，同时可以使这些协议不受安全技术变化的影响。OTP工作组基于Bellcore的S/KEY™技术开发一个一次性口令鉴别系统（RFC 1938），可用于防止窃听口令的被动式攻击。SECSH工作组正在改进SSH协议（计划于1997年底完成），使其为传输的数据提供自动的加密、鉴别、和压缩功能，从而增加远程登录、文件传输、以及TCP/IP和X11转发的安全性。TLS工作组也在进行类似的工作，开发主机之间运输层之上的安全传输通道。WTS工作组研究WWW应用的安全性问题，并已提交了两个Internet标准草案：HTTP安全需求规范，和HTTP安全协议规范（SHTTPv1.1）。另外Netscape公司也提出了一个有关WWW安全的技术方案SSL，并已得到包括微软和IBM在内的诸多大公司的支持。

对于群通信，现有的加密、鉴别和完整性技术对支持其整体是合适的，但对于群中个别成员的安全性来说，目前的性能不满足要求。另外为了满足移动通信的要求，端—端的安全控制应基于端系统或用户标识符，而不是低层的标识符或定位符（即网络地址或物理地址）。与Internet上密钥管理有关的全局标识体系尚未完成。X.500具有良好的技术特性，这对于在Internet内建立全局标识体系较为理想，例如作为标识的属性提供对象的公开密钥。但是由于它进入Internet的速度太慢，至今尚未形成全局的管理体系，如对DN的定义和分配，因此无法进入实用阶段。PKIX工作组正在为之奋斗，他们研究使用X.509支持Internet全局的公开密钥管理，并

已提出了一系列的标准草案。SPKI 工作组 97 年初开始正在进行一项类似的工作，开发一个称为简单公开密钥基础结构的新标准。

4. 防火墙技术

(1) 概述

防火墙是对在 Internet 中传输的数据的过滤功能，分为安全通道（通常为加密的 TCP 连接）、IP 级防火墙、和应用级防火墙三类，用于对 Internet 的某一部分进行安全隔离。如果这一部分网络存在多个与外部网络的通路，则需要多个相互协调的防火墙。

目前 Internet 中对防火墙有两种看法。一类意见认为防火墙是一个强有力的概念，它将安全的管理、配置和实施集中到了一点；另一类意见认为防火墙提供了一种虚假的安全感，使内部人员放松了警惕，而大部分计算机犯罪是由内部人员所为。

对于大型企业网络而言，一些主机有较好的安全管理，如中央主机，安全水平可能高于防火墙；一些主机的安全水平则低于防火墙；因此设立防火墙对于前者是效率的损失，而对于后者是有益的，因此是否要设立防火墙取决于这两类机器的比例。

对于单机上网，防火墙是无意义的，因为防火墙的安全就是主机本身的安全。另外对于一个网络内的用户之间没有什么共同利益（如一个 ISP 所接入的各个用户）的情形，这时每个用户都可看成是一个单机，因此防火墙也无意义。概括地说，是否要设立防火墙取决于他所保护的那个组织的性质。防火墙适合于保护大型组织机构，且内部主机的安全管理并不严格的情形。

(2) 应用级防火墙

典型的应用级防火墙是位于网络边界的应用代理，如 WWW 服务器的 Proxy，使网络内部的用户与网络外部的服务之间不会有直接的 IP 报文交换，所有这个应用的数据均由防火墙进行转发和过滤。由于这改变了应用原有的工作方式，因此往往需要对用户端软件进行修改，这不仅限制了新应用的引入，并影响效率，而且使得当防火墙不能工作时，对应的网络服务也就不能使用了。

(3) IP 级防火墙

IP 级防火墙通常存在于多端口的路由器中，它对每一个到来的报文根据其报头进行过滤，按一组预定义的规则来判定该报文是否可以继续转发。对报文可采取的动作有继续转发、丢弃、返回一个失败响应、或记入日志以便事后追查等。

IP 级防火墙增加了网络的安全性，但也增加了网络的开销。性能的影响取决于报文过滤的程度（报头参与的数量和位置）。若报文过滤并丢弃的速度与防火墙接口的速率相当，则实际上防火墙就不能工作了，这就是服务失效攻击。另外，IP 级防火墙无法阻止内部用户使用合法的程序和手段向外泄漏信息，或外部用户向内传送有害信息，这属于管理问题和政策问题。

IP 级防火墙目前的问题包括

- 多路由器问题，如何协调它们之间的政策；
- 非对称路由问题；
- 群通信问题；
- 性能问题。

IETF 的 AFT 工作组为防火墙环境下的网络应用服务开发了一个安全鉴别协议，使报文在穿越各个 IP 防火墙时能不断地得到鉴别，所采用的技术方案基于著名的 SOCKS 系统（RFC 1928）。

5. 安全的网络基础设施

网络基础设施的重点是路由信息和 DNS 信息的控制，这包括

- 相邻的路由器之间交换的路由信息的鉴别；
- 所有路由信息源点的鉴别；
- 对路由信息操作的鉴别（待进一步研究）；
- DNS 的安全问题等。

DNSSEC 工作组过去几年的工作集中在增强 DNS 协议的安全性，以保护 DNS 的动态修改操作（防止恶意地重用、错序、和在传送过程中被篡改），已提出了两个 RFC（2065 和 2137）；目前正在研究如何将 DNS 用作为密钥分配的辅助工具。由于 DNS 被认为是公众信息，因此该工作组不考虑在 DNS 中使用任何数据加密机制和访问控制机制。

IPSEC 工作组通过在 IP 协议中增加鉴别报头（AH，RFC 1826）和安全负载封装（ESP，RFC 1827）功能来保护它所支撑的高层协议。这些安全功能的核心是加密安全服务（具体算法是可更换的），它可支持鉴别、完整性、访问控制、和数据安全等多种安全服务的组合。加密安全服务所需的密钥管理协议称为 IKMP（Internet Key Management Protocol），于 97 年 7 月成为标准草案。下一步将考虑将 Sun 公司提出的密钥管理协议 SKIP 的有关机制结合进 IKMP，最终目标是使 IP 协议支持密钥分配中心（KDC，源于 Kerberos 系统）的概念。

安全的 QOS 是一组访问控制机制，以保证用户应有的带宽，防止非法使用带宽，通常基于状态控制和类别控制（通过鉴别服务支持）。

6. 结论

良好的网络安全是需要付出高代价的，这不仅在增加物理设备或软件系统方面，更重要的是它增加了网络管理的复杂程度，并增加了对网络管理人员的知识和技能的要求。专家认为，Internet 的最大安全挑战是如何保持比黑客领先一步，因为目前发现系统安全漏洞的速度几乎与网络安全设施的开发一样快。据一些美国商业咨询公司估计，未来三年中 Internet 上的电子贸易营业额将超过 60 亿美元，但是若不能较好地解决网络安全问题（包括在技术和立法两方面），这个巨大的商业机会很可能会夭折。然而，就象飞机与火车的安全性比较一样有趣，据“Telecommunication”1996 年的统计研究，蜂窝移动电话系统因欺诈而产生的损失与营业收入的比例是 29.74 美元对 1500 美元；而 Internet 上这个比例为 1.5 美元对 1500 美元。这似乎也一个侧面说明目前的 Internet 网比电话网更安全。

参考文献

[1] Guy Robb，Internet Security: The Business Challenge，Telecommunication Vol.30 No.10，1996.10；

[2] RFC 1636，Report of IAB Workshop on Security in the Internet Architecture，1994.2；

[3] William R. Cheswick，Steven M. Bellovin，Firewalls and Internet Security，Addison Wesley Publishing Company，1994；

注：龚俭，计算机系教授，工学博士，中国电子学会高级会员，中国教育和科研计算机网专家委员会委员，江苏省“计算机网络技术”重点实验室主任；主要研究方向包括网络管理、网络安全、开放分布式处理。