第 33 卷 第 5 期 计 算 机 工 程 2007 年 3 月
Vol.33 No.5 Computer Engineering March 2007
·安全技术· 文章编号：1000—3428(2007)05—0114—03 文献标识码：A 中图分类号：TP309

基于 SSL 的安全邮件解决方案

费巧玲，徐向阳，蒋国清，潘 勇
(湖南大学计算机与通信学院，长沙 410082)

摘 要：分析了现存的安全电子邮件解决方案，发现它们一般只对邮件体进行加密和签名，而没有考虑邮件头的安全性。在某些环境下，邮件头也需要安全保密。研究了安全套接字层协议(SSL)，提出了一种基于 SSL 协议的安全邮件解决方案，既增强了邮件体的安全性，也保证了邮件头的安全性。

关键词：电子邮件；安全套接字层协议；简单邮件传输协议；邮局协议

Solution of Security E-mail Based on SSL

FEI Qiaoling, XU Xiangyang, JIANG Guoqing, PAN Yong
(School of Computer and Communication, Hunan University, Changsha 410082)

【Abstract】 After some security E-mail protocols being analyzed, the security of E-mail body is only researched, but not E-mail header. E-mail header also needs to keep secret sometimes. The secure socket layer is studied, and a solution is put forward to, which is based on the SSL protocol. For the solution, the security of E-mail body is enhanced, and the E-mail header is protected.

【Key words】 E-mail; Secure socket layer (SSL); Simple mail transfer protocol; Post office protocol

随着 Internet 的迅速发展，电子邮件系统以其方便、快捷的优势而成为人们进行信息交流的理想工具，也是 Internet 上应用最为广泛的服务之一。因 Internet 是一个开放的网络，故 E-mail 的安全性随着其应用的扩展变得越来越重要。目前人们使用的绝大多数电子邮件系统没有采取任何措施来保证电子邮件在网络中安全传送。比如，电子邮件的内容以明文的形式在网络中传递，其内容将暴露无遗；邮件发送人可以假冒他人发送电子邮件来进行邮件欺骗；邮件接收人无法确认邮件在传送的过程中是否被篡改或破坏。不仅电子邮件系统的安全得不到保证，甚至电子邮件系统还成为破坏者入侵系统的门户。

电子邮件的安全问题已经得到了人们的广泛关注，各种各样的安全方案也在特定领域中发挥作用，如 S/MIME、PGP、PEM、MOSS 等，这为人们提供了多种选择。

1 现有安全邮件解决方案的研究

目前 Internet 上有两套成型的安全邮件协议或标准：PGP 和 S/MIME。

1.1 PGP

PGP(Pretty Good Privacy)是 Phillip Zimmerman 在 1991 年提出的，它既是一种规范也是一种应用，已经成为全球范围内流行的安全电子邮件系统之一。

PGP 的特点是通过单向散列算法对邮件内容进行签名，以保证邮件内容无法修改，使用对称和非对称密码相结合的技术保证邮件内容保密且不可否认。通信双方的公钥发布在公开的地方，如 FTP 站点，而公钥本身的权威性则可由第三方（特别是收信方信任的第三方）进行签名认证。在 PGP 系统中，信任是双方之间的直接关系，或通过第三者、第四者的间接关系，但任意双方之间都是对等的，整个信任模型构成网状结构，这就是所谓的 Web of Trust。每个用户之间的信任关系都是通过网络传播的，也就是说在 PGP 中，一旦相信了网络中的一个用户，就意味着相信了网络上的所有用户，这就导致 PGP 不能在较大范围的网络中使用，也不能用于传输一些机密的敏感信息，而且 PGP 对密钥的废除管理也有缺陷，如果私钥丢失或损坏，几乎不可能通知通信各方相关的证书已经不可信。由于这种标准的可伸缩性差，也就是说，对素不相识的客户，这种模型无法建立可靠的信任关系，因此 PGP 标准只适用于较小的组织或团体中的保密 E-mail。

1.2 S/MIME

S/MIME(Secure/Multipurpose Internet Mail Extension)同 PGP 一样，也是利用单向散列算法和公钥与私钥相结合的技术，保证邮件内容保密且不可否认。与 PGP 不同的主要有两点：S/MIME 的认证机制依赖于层次结构的证书认证机构，所有下一级组织和个人证书均由上级组织负责认证，根证书相互认证，整个信任关系是树状的，这就是所谓的 Tree of Trust；S/MIME 将信件内容加密签名后作为特殊的附件传输。

S/MIME 基于 PKI/CA 机制，使电子邮件的安全服务更有保障，特别是采用了 CA，使电子邮件具有了不可否认性，增强了电子邮件的法律效力。但在现行的基于 S/MIME 的安全电子邮件系统中，CA 具有很高的权限，能“偷窥”用户的邮件，这就要求所有的用户都必须绝对相信 CA，给电子邮件的安全带来隐患，在这一点上，PGP 更具保密性。

2 SSL 协议

安全套接字层(Secure Socket Layer, SSL)协议起源于 Netscape，现在被广泛用于 Internet 上的身份认证和 Web 服务器与客户端浏览器之间的数据安全通信。SSL 建立在可靠的传输层协议(TCP)之上，与应用层协议(如 HTTP、FTP、

作者简介：费巧玲(1979－)，女，硕士生，主研方向：信息安全，密码学；徐向阳，副教授、博士；蒋国清、潘 勇，硕士生
收稿日期：2006-04-29 **E-mail：**feiqiaoling@163.com

TELNET、SMTP、POP 等) 独立无关，它可以有效地避免网上信息的偷听、窜改，以及信息的伪造。主要由以下两个协议组成：

(1)SSL 记录协议：负责应用程序提供的信息的分段、压缩、数据认证和加密，SSL V3 提供对数据认证用的 MD5 和 SHA 以及数据加密用的 DES，IDEA 等算法的支持，用来对数据进行认证和加密的密钥可以通过 SSL 握手协议来协商。

(2)SSL 握手协议：用来交换版本号，加密算法，身份认证并交换密钥。SSLV3 提供对 Deffie-Hellman 密钥交换算法、基于 RSA 的密钥交换机制和另一种实现在 Fortezza chip 上的密钥交换机制的支持。

SSL 协议在应用层协议通信之前完成加密算法、通信密钥的协商以及服务器认证工作，应用层协议传送加密数据，从而保证通信的私密性。

通过以上叙述，SSL 协议提供的安全信道有以下 3 个特性：

(1)数据保密。连接是保密安全的。在初始化握手协议协商加密密钥之后传输的消息均为加密的消息。加密的算法为单钥加密算法，如 DES、RC4、IDEA 等。

(2)身份认证。通信双方的身份可以通过公钥加密算法，如 RSA、DSS 等签名来验证，杜绝假冒。

(3)数据完整性。HASH 函数（如 SHA）被用来产生消息摘要 MAC。所传输的消息均包含数字签名，以保证消息的完整性。这样保证连接是可靠的。

3 基于 SSL 的安全解决方案

3.1 方案的提出

传统的邮件包括信封和信本身，电子邮件则包括邮件头和邮件体。通过对现存的安全邮件解决方案的研究发现，现在的安全电子邮件一般只对邮件体部分进行安全处理，而邮件头则由于邮件传输中寻址和路由的需要，以明文的形式在不安全的网络上传输。

邮件头一般包含有邮件主题、寄信人地址和收信人地址等。邮件主题是邮件的标题，通常是邮件正文的主要内容。这些信息以明文的形式传输也会带来一定的安全隐患。比如黑客可以截取、篡改邮件头的任何信息；可以获得邮件主题，进而很可能知晓邮件的大概内容；可以用寄信人和收信人的邮件地址发信进行假冒；可以给寄信人和收信人发送大量的垃圾邮件甚至是病毒邮件等。

可见邮件头的安全性在某些应用环境下也很重要。通过对安全套接字层协议的研究可知，在 SSL 握手协议之后传输的所有消息都是加密的，因此在 SSL 所建立的安全传输通道上运行 SMTP 和 POP 协议，并对这两种协议作一定的扩展，可以解决邮件头的安全传输问题。本文提出了基于 SSL 协议的安全邮件解决方案，该解决方案要求邮件客户端和服务器端都支持，而且都必须安装 SSL 证书。

3.2 系统总体框架

安全电子邮件解决方案系统总体框图如图 1。

(1)证书服务器：1)根据具体的证书策略审核申请人员身份，决定给用户发证书或拒绝申请；2)处理由于各种特殊原因而导致证书失效的证书撤消请求；3)发布证书和 CRL 列表(证书撤消列表)；4)提供用户身份信息和证书查询、下载。

(2)发送者：1)编辑、发送安全电子邮件；2)申请、下载用户证书。

(3) SMTP 服务器：1)传送安全电子邮件；2)申请、下载用户证书。

(4) POP 服务器：1)接收安全电子邮件；2)申请、下载用户证书。

(5)接收者：1)接收并解密安全电子邮件；2)申请、下载用户证书。

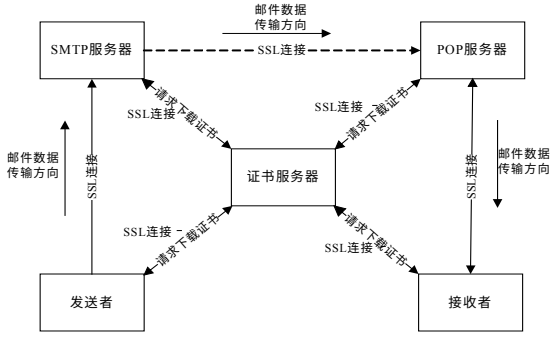

图 1 总体框架

3.3 发送邮件前邮件数据的处理

发送者在发送邮件前须对邮件数据进行安全处理，处理过程如图 2 所示。

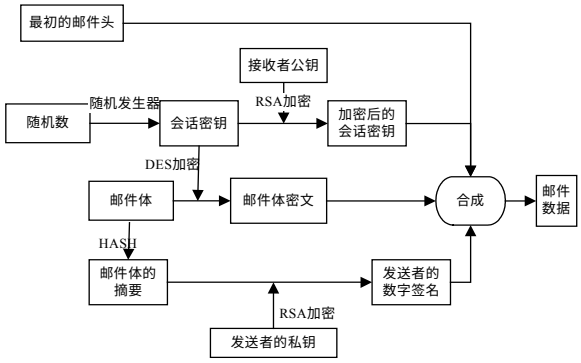

图 2 发送者对邮件数据的处理

3.4 邮件传输过程中的处理

SSL 协议的实现采用公开的 OpenSSL0.9.7。邮件数据的传输过程为：(1)SSL 发送端程序把邮件数据提交给本地的 SSL；(2)SSL 发送端先用对应连接的散列算法对邮件数据进行散列，得到邮件数据的散列值；(3)散列值和邮件数据一起用加密算法加密；(4)密文通过网络传给对方；(5)接收方的 SSL 用相同的算法对密文解密；(6)接收方的 SSL 用相同的散列算法对解密的邮件数据散列；(7)计算得到的散列值与接收的散列值比较；(8)如果一致，接收邮件数据有效，SSL 把数据上交给接收方的应用层；否则就丢弃数据，并向对方发出报警信息。严重的错误有可能引起再次的协商或连接中断。

3.5 接收到邮件后邮件数据的处理

接收者在接收到安全邮件后须对邮件数据进行解密、验证签名等处理，才能阅读该安全邮件。处理过程如图 3 所示。

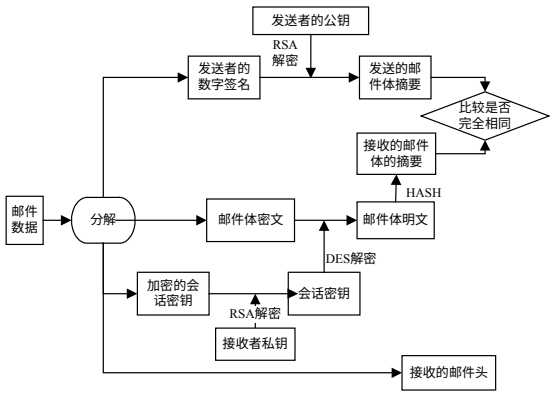

图 3 接收者对密文邮件的处理

3.6 安全评估

该安全电子邮件解决方案不仅提高了邮件体的安全性，还保证了邮件头的传输安全性。本节将从以下几个方面进行安全性能评估：

(1)抗窃听和泄密的能力

发送者对邮件体进行加密和签名（一般邮件安全解决方案）之后，将经过加密和签名的邮件体与邮件头一起打包，并通过 SSL 安全通道进行传输。保证邮件体只有希望的接收者才能阅读。由于邮件头也是在 SSL 的保护下传输的，因此避免了邮件头信息暴露的可能。

(2)防篡改的能力

“邮件体摘要”可以实现对信件完整性的鉴别。任何对信息的篡改都能被发现。

(3)抗击冒充他人发信的能力

发送的邮件带有发送者的数字签名，可用于接收者判断发送者的身份。保证信息的发送者不是冒名顶替的，它同信息完整性一起可防止伪造。

(4)抗抵赖的能力

由于发出的邮件带有发送者的数字签名，因此发送者不能抵赖自己发信的事实。此外，如果有必要还可以设置读信收条，保证接收者否认阅读信件的事实。

4 结束语

电子邮件作为 Internet 网络的重要应用，它的安全性越来越受到重视。本文针对目前电子邮件安全解决方案对邮件头处理不足的情况，提出了一种基于 SSL 协议的安全解决方案，融合安全套接字层协议、简单邮件传输协议和邮局协议，在开放的不安全的网络上建立安全的邮件传输通道，然后在该安全传输通道上运行 SMTP 和 POP 协议，实现电子邮件的机密性、完整性、不可否认性。该方案既增强了邮件体安全性，也保证了邮件头的安全性。

参考文献

1 Postel J B. Simple Mail Transfer Protocol[S]. RFC 821, 1982-08.

2 Crocker D H. Standard for the Format of ARPA Internet Text Messages[S]. RFC 822, 1982-08.

3 Myers J, Rose M. Post Office Protocol(Version 3)[S]. RFC 1939, 1996-05.

4 Dierks T, Allen C. The TLS Protocol(Version 1.0)[S]. RFC 2246, 1999-01.

5 Housley R, Ford W. Internet X.509 Public Key Infrastructure Certificate and CRL Profile[S]. RFC 2633, 1999-01.

6 Schneier B. E-mail Security[M]. New York: John Wily, 1995.

7 Johnson K. Internet Email 协议开发指南[M]. 科欣翻译组, 译. 北京：机械工业出版社, 2000.

8 樊　丰, 林　东. 网络信息安全&PGP 加密[M]. 北京：清华大学出版社, 1998.

9 许晓东, 荆继武, 杨　炜. 安全电子邮件的系统分析与密钥管理[J]. 计算机应用研究, 1999, 16(11): 59-61.

10 陈建奇, 张玉清, 李学农, 等. 安全电子邮件的研究与实现[J]. 计算机工程, 2002, 28(6): 121-134.

11 吴韶波, 于　珏. 安全电子邮件解决方案[J]. 信息技术, 2003, 27(3): 63-74.

12 Adams C, Lloyd S. 公开密钥基础设施: 概念、标准和实施[M]. 冯登国, 译. 北京: 人民邮电出版社, 2001-01.

（上接第 113 页）

```
    if hostY = hostA then
        event endBparam(hostB)
        event endBfull(NY, hostY, hostB, pkA, Nb)
        out(c, sencrypt(secretB, k)
process (定义协议 Sys)
    new skA; let pkA = pk(skA) in
    out(c, pkA)
    new skB; let pkB = pk(skB) in
    let hostA = host(pkA) in
    out(c, hostA)
    let hostB = host(pkB) in
    out(c, hostB)
    ((!processA) | (!processB))
```

通过分析，发现了 EKE 协议一个新的攻击——并行会话攻击，据我们所知这个攻击在已有的文献中没有被注明，攻击过程如下：

消息 1.1 A→Z(B)：$\{K_A\}_P$

消息 2.1 Z(B)→A：$\{K_A\}_P$

消息 2.2 A→Z(B)：$\{\{|K|\}_{K_A}\}_P$

消息 1.2 Z(B)→A：$\{\{|K|\}_{K_A}\}_P$

消息 1.3 A→Z(B)：$\{N_A\}_K$

消息 2.3 Z(B)→A：$\{N_A\}_K$

消息 2.4 A→Z(B)：$\{N_A, N_B\}_K$

消息 1.4 Z(B)→A：$\{N_A, N_B\}_K$

消息 1.5 A→B：　$\{N_B\}_K$

消息 2.5 Z(B)→A：$\{N_B\}_K$

其中，Z 为攻击者。攻击结果：A 认为是在和 B 进行通信，而实际上 B 根本就没有参与协议的运行。

4 结束语

本文基于 Spi 演算和逻辑编程规则，提出了一个密码协议新的验证方法，并利用该验证方法对 EKE 协议进行了分析，不仅证实了 EKE 协议已知的漏洞，还证明了 EKE 协议在并行会话攻击下是不安全的。同时还对许多密码协议的安全性质进行了验证，这些研究工作进一步证明了新验证方法的可行性和有效性。

参考文献

1 Lowe G. Breaking and Fixing the Needham-schroeder Public-key Protocol Using CSP and FDR[C]//Proceedings of TACAS. Springer-Verlag, 1996: 147-166.

2 Abadi M, Gordon A D. A Calculus for Cryptography Protocols: the Spi Calculus[J]. Information and Computation, 1999, 148(1): 1-70.

3 Bellovno S, Merritt M. Encrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks[C]//Proceedings of the IEEE Computer Society Conference on Research and Privacy. 1998: 72-84.

4 Diffie W, Hellman M. New Directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.