DOI:10.16208/j.issn1000-7024.2000.05.001
第21卷 第5期 计算机工程与设计 2000年10月
Vol.21 No.5 COMPUTER ENGINEERING AND DESIGN Oct. 2000

文章编号：1000-7024 (2000) 05-0001-05 中图分类号：TN918.4; TN911.22 文献标识码：A

SMTP、POP3协议及PEM标准安全性分析

谢冬青
(湖南大学计算机科学系，长沙 410082)

摘 要：分析了电子邮件中广泛使用的PGP系统，SMPT、POP3协议及PEM标准中的安全问题。PGP存在信任度递减、假冒攻击问题，SMTP、POP3没有采取安全措施，PEM建立了基于证书中心的安全机制。

关键词：电子邮件；协议；安全

1 电子邮件产品及其安全问题

现有电子邮件基本上都是基于TCP/IP协议的。在TCP/IP（IPV4）协议簇中，TCP协议对电子邮件通信双方的身份认证依赖于IP包中的源地址和目的地址。电子邮件在Internet上是以明文形式传递的，窃听者可以截获IP包，从中分析出源地址、目的地址以及邮件的内容。一旦窃听者掌握了通信双方的地址信息就可以假冒任意一方，重新启动与另一方的通信，邮件内容也会以明文的形式泄露。

当用户从当地的邮件服务器上收取电子邮件时，服务器会要求用户输入帐号及口令，以确认用户的合法身份。但用户输入的帐号和口令是以明文形式通过网络传递给服务器的，窃听者只要监听到客户和服务器在这一次应答过程中交换的数据包，就可以获得客户的帐号和口令，从而可以完全获得用户邮箱内的邮件及其内容，用户则毫无秘密可言。现在已出现很多的电子邮件产品，在安全性方面各有其缺点。PGP（Pretty Good Privacy）是近几年应用于保密电子邮件的一个性能很好的软件[1]。他能实现对邮件发送者身份的认证，对E-mail消息加密以及对E-mail明文消息的完整性进行校验。它的密钥管理采用了RSA公开密钥算法传送密钥。（模长512bits或1024bits），但没有采用证书管理体制；数据加密采用了IDEA（国际数据加密标准），加解密速度比较快；MD5用作单向Hash函数[2]，通过使用RSA加密算法，用邮件发送者的秘密密钥，对E-mail消息的MD5消息摘要进行加密实现数据完整性校验。尽管PGP应用公开密钥、单钥、Hash等算法实现了二级密钥管理，但它的密钥管理依旧存在缺陷——缺少第3方对通信双方身份的认证。下面分析PGP密钥管理的缺陷。

由于PGP没有采用第3方认证机制，且公开密钥是公开的，这就给PGP的安全性造成了极大的威胁。公开钥的鉴别模仿现实生活中人们的相互信任关系，划分成5级信任度，信任度存在递减问题。其次，假设用户A和B第1次使用PGP进行通信，此时双方均不知道对方的公钥，所以A在发送电子邮件给B之前，必须获得B的公钥，而B要将其公钥发送给A，如果也通过电子邮件传送，也只能以明文形式传递。如果攻击者T截获B的公钥，然后将自己的公钥取代B的公钥发送给A，于是T就假冒了B，从而导致A发给B的信息被攻击者T收取阅读，而A却无法察觉。另外，PGP在运行过程中使用了一些存储块，但是在使用PGP的清除功能时，并没有真正的将数据从存储块上清除掉，这给密码分析者留下了寻找密钥的可能途径；PGP重新运行时，可能会重复使用存储块上的数据。再者，PGP的随机数产生方式也不是太理想，它是通过测试用户击键的时间间隔来产生随机数，随机数的产生完全由软件实现，如果程序被修改，很可能产生的随机数不具有随机性；随机数种子以文件形式存

收稿日期：1999-03-22
作者简介：谢冬青 (1965-)，男，博士，副教授，主要研究方向：网络信息安全。

放在用户的存储空间中，文件的安全问题会导致整个系统安全性能的削弱。

保密电子邮件，涉及 SMTP、POP3 协议和 PEM 标准。

2 SMTP 协议分析

SMTP 协议，即简单邮件传输协议，RFC821 讲述了 SMTP 传输邮件的过程和规范[3]，RFC822 讲述了邮件消息的格式[4]。

2.1 SMTP 模型 (如图 1 所示) SMTP 模型在工作时，首先由用户发送请求给发送端 SMTP，然后，发送端 SMTP 与接收端 SMTP 建立双向传输通道。此处接收端 SMTP 可能是最终接收端，也可能是中间转发接收端。双向通道建立起来之后，接收端和发送端 SMTP 就按协议规定的命令进行应答。

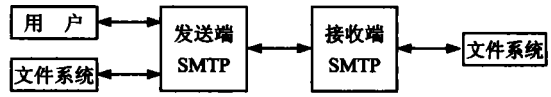

图 1 SMTP 模型

2.2 SMTP 命令及其规范 SMTP 协议中规定的命令有：MAIL、RCPT、DATA、VRFY、EXPN、SEND、SOML、SAML、HELO、QUIT、RSET、HELP、NOOP，共 14 条命令。其中 HELP、MAIL、RCPT、DATA、RSET、NOOP、QUIT 等 7 条命令组成了 SMTP 协议的最小命令集。

2.3 SMTP 安全性分析 SMTP 协议没有采用任何安全机制，全部信息采用明文形式传送，并且采用固定的端口号 25 进行邮件的发送，攻击者只要监听端口 25 的数据流，就能分析出 SMTP 命令及其参数内容，进而达到分析出所有邮件内容的目的。具体说来：① 在发送邮件的过程中，MAIL 和 RCPT 命令都可能被监听，分析其参数获知邮件的来源和去向；攻击者一旦掌握了这些信息，就可能采取假冒攻击。② VRFY 和 EXPN 命令也可能被监听，攻击者可以掌握用户名和邮箱地址，进而进行假冒攻击。③ DATA 命令很可能成为主动攻击的介入点。攻击者截获 DATA 命令，然后用自己伪造的邮件内容代替原邮件内容发送给接收者，即进行假冒攻击。④ TURN 命令可以使收发双方角色互换，攻击者利用这一命令可以逃避邮件过滤防火墙的检查，使得不允许外出的邮件出去，不允许进来的邮件进来了，从而使过滤防火墙失去其应有功能。⑤ 通过对 reverse-path 的修改，可以直接导致邮件误投，邮件被错误的导入攻击者的邮箱。

3 POP3 协议分析

POP3 协议，即邮件协议第 3 版，RFC1939 详细描述了其规范和命令[5]。与 SMTP 协议相对应，POP3 协议用于收取电子邮件。

3.1 POP3 协议的基本操作 与 SMTP 不同，POP3 使用固定的端口号 110 进行邮件的收取。POP3 服务器一直监听 110 端口，等待用户连接。如果用户需要接收电子邮件，他就与 POP3 服务器连接，然后，会话进入验证状态，这时用户输入自己的身份口令传给 POP3 服务器进行验证，验证通过后，会话进入传输状态，这时用户与 POP3 服务器交互，获取想要获取的邮件，直至关闭本次连接；最后，服务器进入更新状态，释放本次会话占用的资源。

3.2 POP3 协议命令及规范 POP3 协议规定的命令有：USER、PASS、STAT、LIST、RETR、DELE、NOOP、RSET、QUIT、TOP、UIDL、APOP 共 12 条。依据 POP3 会话的不同状态，这 12 条命令可分为 3 组，表 1 列出了不同状态下可用的不同命令。

4 POP3 协议安全性分析

与 SMTP 协议一样，POP3 协议也具有明文传送数据的不安全性因素。例如，user/pass 命令就是一个严重的漏洞，攻击者很容易窃听到用户名和口令，一旦口令暴露，用户的一切邮件就完全展现在攻击者面前。尽管 POP3 协议提供了一个 APOP 命令，用于对用户身份的认证，具有一定的安全性，但其提供的安全性能却是有限的和不完善的。第 1，该命令仅对用户名和口令加密，可以对用户身份的认证起到一定的保护作用，而对邮件的内容则毫无保护作用，无法抵御被动攻击，即使攻击者不知道

用户口令，他也能监听到以明文形式传递的邮件内容。第2，对用户名和口令的安全性而言，这条命令的作用也有限。因为根据APOP命令的安全机制，要保证用户名和口令的安全性，就必须保证POP3客户端和服务器端共知的一个秘密字符串的安全性，一旦这一字符串泄露，则APOP命令毫无安全性可言了。RETR和TOP命令都可以查看邮件内容，在邮件内容传递过程中，攻击者可以采取被动攻击，窃听邮件的内容；甚至可以采取主动攻击，修改邮件内容，欺骗接收端用户，或者根据邮件的内容，假冒接收端用户欺骗发送端用户。

表1 POP3状态—命令对照表

状 态	可 用 命 令 集
验证态	USER、PASS、APOP、QUIT
传输态	STAT、LIST、RETR、DELE、NOOP、RSET、QUIT、TOP、UIDL
更新态	QUIT

5 PEM标准分析

通过以上分析，SMTP和POP3两项协议都存在着严重的安全漏洞。由RFC1421，RFC1422，RFC1423和RFC1424规定的Internet保密增强邮件标准PEM在邮件的保密安全性方面大大的强于SMTP和POP3协议。RFC1421介绍了消息加密和验证过程[6]，RFC1422给出了基于证书的密钥管理[7]，RFC1423讲述了算法，模式和身份认证[8]，RFC1424讲述了密钥证书和相关服务[9]。PEM的最大特点是采用了公开密钥管理体制及基于这种体制的公开密钥证书机制。

表2 ENCRYPTED消息格式

域	含义、内容
Pre-EB	"-----BEGIN PRIVATE-ENHANCED MESSAGE -----"
Proc-Type	定义消息处理类型，此种格式只能为"4，ENCRYPTED"
Content-Domain	指明消息内容的表示方式，目前只有"RFC822"一种
DEK-Info	指明消息文本加密算法和参数，目前算法标志只规定了"DES-CBC"
Orgin-Cert	PEM消息发方证书
Key-Info	定义密钥管理参数，包括IK算法标志，IK加密的DEK，在此处的Key-Info是可选的
Issuer-Cert	发方证书签发者证书
MIC-Info	消息集成校验信息
Recpnt-ID-Asym	收方身份，包括收方证书管理机构和版本/有效期
Key-Info	定义密钥管理参数，包括IK算法标志，IK加密的DEK
PEM-Text	PEM消息正文
Post-EB	"------END PRIVACY-ENHAWCED MESSAGE ------"

5.1 PEM消息的格式

PEM定义了4种格式的消息：ENCRYPTED、MIC-ONLY、MIC-CLEAR和CRL。①ENCRYPTED消息具有可信性、真实性，提供MIC检查。②MIC-ONLY比ENCRYPTED消息缺少可信性，但仍然提供MIC检查和重编码。③MIC-CLEAR消息比MIC-ONLY消息缺少重编码这一步，可用非PEM软件查看邮件内容。④CRL消息用于传输注销证书列表之用，需要签名和重编码。

在设计和实现增强型保密电子邮件时，为了尽可能地提高电子邮件的安全性能，考虑到信息的保密性、真实性、完整性的实现，详细讨论了第1、第2种PEM格式，因为第1、第2种格式提供的安全性能较第3、第4种强得多。

ENCRYPTED消息格式如表2所示；IC-ONLY消息格式如表3所示。

表3 MIC-ONLY消息格式

域	含义、内容
Pre-EB	"-----BEGIN PRIVATE-ENHANCED MESSAGE -----"
Proc-Type	定义消息处理类型，此种格式只能为"4，MIC-ONLY"
Content-Domain	指明消息内容的表示方式，目前只有"RFC822"一种
Orgin-Cert	PEM消息发方证书
Issuer-Cert	发方证书签发者证书
MIC-Info	消息集成校验信息
PEM-Text	PEM消息正文
Post-EB	"-----END PRIVACY-ENHAWCED MESSAGE -----"

5.2 PEM消息加密和验证过程

PEM使用两级密钥：数据加密密钥（DEK）和交换密钥（IK）。PGP采用了单钥公开密钥管理体制，DEK用来加密消息正文和计算消息集成校验（MIC），同时用

来加密 MIC 的签名表示，DEK 一般每次会话生成一个，以达到“一次一密”的效果。而 IK 用来加密 DEK，以便在每次会话的初始段对 DEK 进行加密交换。加密 DEK 的 IK 就是收方的公开钥，加密 MIC 的 IK 就是发方私有钥，即实现对 MIC 的签名。依据 PEM 的机制，加密和签名过程为：Transmit-Form=Encode (Encrypt (Canonscalize (Local-Form))) 解密和验证过程为：Local-Form=DeCanonicalize ((Decrypt (Decode (Transmit-Form)))具体流程如图 2 和图 3 所示。

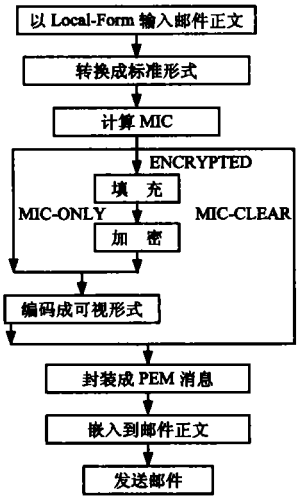

图 2 PEM 邮件加密签名生成过程

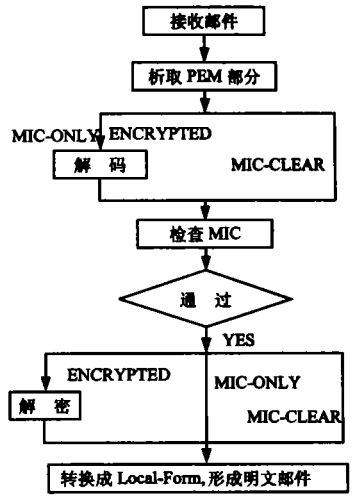

图 3 PEM 邮件接收和验证过程

5.3 PEM 密钥管理方式

PEM 与 PGP 的最大差别在于 PEM 采用了基于证书的密钥管理体制。证书是数字签名、身份认证、密钥管理等各种保密措施的综合运用，它提供的安全性明显高于 PGP 等非证书密钥管理体制。

在密钥交换过程中存在着一个通讯双方身份相互认证的过程，为了保护对对方身份的认证过程的正确性，应从可信的第 3 方获得对方的公开钥等信息。这个可信的第 3 方就被称为证书中心（CA：Certification Authority）。证书中心应用公开钥算法产生用户证书以保证用户身份的合法性。

证书中心通过对用户信息进行签名产生证书，证书内容包括用户名，用户公开钥和一些附加信息。X. 509 标准对证书格式有详细的说明。一般说来，具体的用户证书信息由签发此证书的 CA 确定。在证书中心签发出用户证书后，证书就具有两个特性：①任何用户都可恢复出证书中隐藏的公开钥，只要用户能得到证书中心的公开钥。②证书是不可伪造的，只有证书中心可以更改证书。

一个简单的证书如下：假设用户名为 A，用户身份号为 UA，证书中心名为 CA，证书中心身份号为 UCA，则 CA 签发的证书如下：CA<<A>>=CA {V, SN, AI, CA, UCA, A, UA, A_P, T^}。其中 V：证书的版本号；SN：证书的系列号；AI：签发证书所用的加密算法；UCA：证书中心的身份号，可选；UA：用户的身份号，可选；T^：证书的有效期，包括一个证书有效起始时间和失效时间；A_P：用户的公开密钥。PEM 使用的证书格式如表 4 所示。

证书中心签发证书时，将涉及到证书的申请、证书的分发、证书的存放以及证书注销、失效等一系列过程。这些过程，除了证书的申请，都可以通过网络自动进行。证书的存放需要维护证书库，所有未到期但又因怀疑有问题而注销的证书以及未到期而更换的旧证书须放入“黑名单库”，黑名单库对网络中的所有用户公开，以便于用户在解密邮件之前核对对方证书的有效性。

由于地域的广阔性和用户的复杂性，使用单个 CA 管理所有用户是不可能的，因此就必须对 CA 分级，实现密钥的分级管理。在 RFC1422 中规定证书的管理分 4 级，IPRA、PCA、CA 和用户或团体。IPRA 是 Internet 注册管理局，是在 Internet 内所有的证书唯一的根。IPRA 的下一级是策略证书管理局（PCA），每个管理局负责为 CA、用户或机构注册。每个 PCA 由 IPRA 签发证书，在 PCA 的下一级设立证书管理局（CA），以签证用户和下属机构，大多数用户都会在这些机构中注册。但也有一些用户希望独立注册，这就需要另外的一些 PCA 为其签发证书。这样，这 4 级模式就形成了基

表 4 PEM 证书格式

域	内 容
Version	证书版本号，以便于证书格式的更新
Serial Number	证书序列号，具有唯一性
Signature	证书签发者的签名，包括签名算法和参数
Issuer Name	证书签发者的名称
Validate Period	证书有效期
Subject Name	证书持有者名称
Subject Publickey	证书持有者公开钥

于证书的密钥管理的分层结构。即使分为4层的证书管理在一些情况下对CA来说也是太过庞大，所以在实际应用中CA下面又可分出几层，以实现证书链的管理方式，图4所示即为一简单证书链。

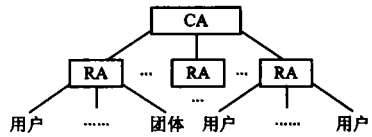

图4 证书链

5.4 PEM工作过程

①A、B分别向某个CA申请各自的证书；②A要向B发送邮件，必须先获得B的证书；③A获得为B签发证书的CA的证书，以验证B的证书的有效性；④验证通过后，A利用证书中B的公开钥，生成PEM邮件发送给B；⑤B收到邮件后，要检查邮件的真实性，必须获得A的证书；⑥B为了验证A的证书的合法性，要获得A端CA的证书；⑦B验证A的证书合法后，解密PEM邮件。

5.5 PEM安全性分析

PEM标准将各种安全技术综合于一体，其安全性几乎是无懈可击的。但是在密钥管理方面，虽然应用了基于证书的密钥管理，其中仍有一些小小的不足之处。在证书申请时，用户须将自己的公开钥置于申请书中，形成申请证书报盘。但这时公开钥不能加密，否则别的用户包括CA就会将加密的公开钥当作公开钥本身使用，使申请的证书无效或别的用户根本无法使用此证书。既然证书申请不能加密，那么如果在申请报盘时被第3方截获，用自己的公开钥替代申请书中的公开钥，而CA签发的证书由于CA无法察觉公开钥的正确与否而被认为有效，那么以后所有发给证书申请者的邮件都可能被第3者截获并解密，PEM就毫无安全性可言了。因此，在实际解决这个问题时，证书申请报盘不能通过网络自动进行，必须由用户按规定填写证书文件，生成公开密钥对，产生申请报盘，由人工送至CA处进行证书申请。

参 考 文 献:

[1] 樊成丰，林东. 网络信息安全&PGP加密 [M]. 清华大学出版社，1998.

[2] Philip Zimmermann. PGP User's Guide. 1994.

[3] John B. Postal. RFC821: Simple Mail Transfer Protocol [R]. 1982.

[4] David H. Crocker. RFC822: Standard for the format of ARPA internet text messages [R]. 1982.

[5] J. Myers and M. Rose. RFC1939: Post Office Protocol-Version 3 [R]. 1996.

[6] J. Linn. RFC1421: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures [R]. 1993.

[7] S. Kent. RFC1422: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Ke Management [R]. 1993.

[8] D. Balenson. RFC1423: Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes and Identifiers [R]. 1993.

[9] B. Kaliski. RFC1424: Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certificate and Related Services [R]. 1993.

The security analysis of SMTP, POP3 protocols and PEM standard

XIE Dong-qing

(Department of Computer Science, Hunan Univ. Changsha 410082)

Abstract: The security problems of Electronic Mail Systems widely used nowadays is researched into, SMTP and POP3 protocols and PEM standard is analyzed. PGP is the existing of pseudonym attacking, credit abasing. SMTP, POP3 don't take any security mechanism, and PEM set up security proposal based on certification authority.

Key words: electronic mail; protocol; security