一种安全电子邮件保证协议的研究

The Research of a Certified E-Mail Protocol

刘 祎[1] 徐 曼[2] 谢俊元[3]

(南京大学计算机科学与技术系 南京210093)[1]

(南京理工大学计算机科学与技术系 南京210094)[2]

(南京大学软件新技术国家重点实验室 南京210093)[3]

Abstract Protocols to facilitate secure electronic delivery are necessary if the Internet is to achieve its true protential as a communication tool of some important fields such as government, business. We present a protocol for secure e-mail that protects both sender and receiver, and can be implemented using current e-mail products and existing Internet infrastruture.

Keywords Certified E-mail, Trusted third party, Security analysis

电子邮件由于快捷、方便已逐步取代纸质邮件成为人们进行交流通讯的工具。但是在一些涉密的应用中，如政府、商业等重要部门还需具备加密/解密、完整性鉴别、身份认证以及抗否认等功能。其中最主要也是实现比较困难的是抗否认的实现，即：一方面，如何对抗发送方对已经发送邮件的否认；另一方面，如何对抗接收方对已经接收邮件的否认。在这个问题上已经有许多实现的协议，本文将在分析以前实现协议的基础上，提出一种安全的电子邮件保证协议，该协议可以很好地实现抗否认问题，而且易于在已有的网络设施上实现。

1. 已有实现协议的分析

在已有的实现抗否认电子邮件保证协议中主要可以归结为以下三类方法：

(1)采用"可信软件"(Trusted Software)来实现

这种方法主要原理是发送者向接收者发送一个经过"可信软件"加密后的邮件，只有当接收者发回"接收证明"后，才被授权阅读邮件的内容，这种方法主要依赖"可信软件"对邮件的加密来保证安全，但是易于被破解，并不能真正地保证安全。

(2)采用密码学中"同时签约的不经意传输协议"来实现

这种方法的核心思想是通信双方逐位交换各自的密钥，直至双方都已获得完整的对方密钥，从而达到双方同时公平交换信息的目的。但是这种方法在实现上是困难的：它要求邮件通信双方能够建立一个可靠的同步传输通道，而标准的电子邮件系统的重要特性是信息传递的不同步和存储-转发。因此，邮件收发双方不可能建立可靠的同步传输通道来完成密钥的逐位交换。这种方法不适合邮件的传输特性。

(3)采用"可信第三方"的机制来实现

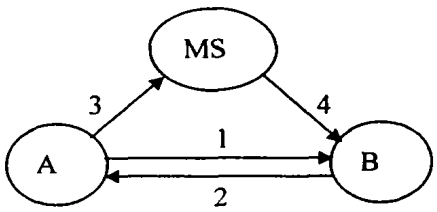
这种方法是现在协议中使用最多的方法，它主要是通过引入一个可信第三方来仲裁通信双方的通信，为双方提供证明。这种方法能够很好地解决抗否认问题，但是这种协议最终是以"可信第三方"发送接收方的回执信给发送方同时发送一个能够阅读信件内容的密钥给接收方而结束，而没有考虑由于网络传输错误所产生的问题。同时，对"可信第三方"的过分依赖以及实现的复杂性，使得该协议难于普及应用。

本文提出的电子邮件保证协议，能够利用现有的网络设施和邮件系统，有效地实现信息交换的抗否认性，而且易于实现、使用灵活。

2. 协议的模型与描述

2.1 协议的模型

设 A 和 B 进行通信，A 将向 B 发送消息 M，MS 为一个任意的公开服务器。



1：A-> B：[$E_B(EP_k(M), S_A(H(EP_k(M))))$]

2：B-> A：[$E_A(S_B(H(EP_k(M))), T, MS)$]

3：A---->MS：[$B, E_B(S_A(H(EP_k(M)), K))$]

4：MS---->B：[$B, E_B(S_A(H(EP_k(M)), K))$]

其中：

$EP_k(M)$：密钥 K 对 M 进行对称加密变换

$DP_k(M)$：密钥 K 对 M 进行对称解密变换

$E_i(M)$：用 i 的公开密钥对 M 进行公开加密变换

$D_i(M)$：用 i 的私人密钥对 M 进行公开解密变换

H(M)：对消息 M 进行 HASH 运算

$S_i(H)$：用 i 的私人密钥对 M 的 HASH 值 H 利用公开密钥算法进行数字签名

$V_i(H)$：用 i 的公开密钥对 M 的 HASH 值 H 利用公开密钥算法进行验证签名

2.2 协议的流程说明

A 发送一封内容为 M 的保证邮件给 B，则：

Step1

A 利用一个随机对称密钥 K 对邮件加密 $EP_k(M)$，并生成签名后的邮件摘要 $S_A(H(EP_k(M)))$，将[$E_B(EP_k(M), S_A(H$

刘 祎 硕士生，研究方向为计算机网络与信息安全。徐 曼 硕士生，研究方向为多媒体数据库，图像检索技术。谢俊元 教授，博导，主要研究方向为网络信息安全。

$(EP_k(M))))]=M'$ 发送给 B。

Step2

B 利用 $D_B(M')$ 得到 $EP'_k(M)$、$S'_A(H(EP_k(M)))$，通过比较 $V_A(S'_A(H(EP_k(M))))$ 与 $H(EP'_k(M))$[解释：这是 B 对 $EP_k(M)$ 利用与 A 同样 HASH 运算得出的结果]是否相等来验证邮件内容是否完整。如果通过验证，则 B 提出一个响应时间要求 T 和公布的位置 MS，将 $[E_A(S_B(H(EP'_k(M))),T,MS)]=M''$ 发送给 A。

Step3

A 利用 $D_B(M'')$ 得到 $S'_B(H(EP'_k(M)))$、T、MS。通过比较 $V_B(S'_B(H(EP'_k(M))))$ 与 $H(EP_k(M))$[解释：这是 A 原来对 $EP_k(M)$ 利用 HASH 运算得出的结果]是否相同来确定是否为发送邮件的摘要。如果验证通过，则 A 留下 $S_B(H(EP'_k(M)))$ 的记录，并在响应时间 T 内在 MS 服务器(可以是 Web 服务器，当然这个服务器是 B 容易接入的)上发布这样一个数据 $(B,E_B(S_A(H(EP'_k(M)),K)))$，向 B 公布随机对称密钥 K。显然消息只有 B 能看到，且经过了 A 的签名。

Step4

B 在响应时间 T 内在 MS 服务器上得到 A 公布的消息后，利用私钥解密得到 $H(EP_k(M))$ 和 K，可以用 K 进行 $DP_k(EP_k(M))$，得到消息 M。

3. 协议的安全性分析

该协议中，A、B 双方所承认的是 B 收到了发自 A 的一个以密钥 K 加密的密文，同时在指定的时间内收到了用于解密的密钥。经过上述四步可以有效地实现抗否认，同时保证双方的公平性。

3.1 A、B 双方完成上述四步的情况下，抗否认的证明

如果 A 想证明 B 已经收到他所发送邮件时，A 只需要提供 M，K，$EP_k(M)$，B 签名的 $S_B(H(EP_k(M)))$，A 发布在服务器上的信息 $(B,E_B(S_A(H(EP_k(M)),K)))$；如果这些都符合，则 B 无法抵赖。同样，如果 A 不能提供这些信息，或信息不正确，则 B 可以证明 A 没有发出这些信件；

如果 B 想证明 A 发送该邮件，只需要出示 M，K，$EP_k(M)$，$S_A(H(EP_k(M)))$ 和 A 发布在服务器上的消息 $(B,E_B(S_A(H(EP_k(M)),K)))$，则 A 不能抵赖他发出过信件，因为别人没有他的私人密钥，不能生成这些信息。

3.2 B 没有正确执行第二步情况下的分析

这种情况有三种可能：B 没有执行第二步；B 没有提供合理的日期；B 没有提供合理的 MS 服务器。这样 A 将协议终止，B 由于没有得到解密的对称密钥 K，等于没有得到消息 M，这是一次失败的通信，双方都没有损失。

3.3 A 没有执行第三步情况下的分析

如果第三步 A 没有把密钥发送到公开服务器上，却声明 B 已经收到并解密了邮件，则 B 可以通过要求 A 提供在 MS 服务器上的记录来证明他的声明。这种情况从概念上等价于 A 没有发送邮件却声明他发送了。

3.4 B 没有执行第四步情况下的分析

如果第四步 B 拒绝执行，不从服务器上取密钥，则这是 B 由于自身原因造成此次通信对他的不公平性。因为 B 执行了第二步。这种情况从概念上等价于 B 已经签名接收了这封信，但又拒绝打开。

4. 协议的安全特性分析及实例

4.1 协议的安全特性分析

协议的安全分析及优化

(1)通信的过程中，采用密文传输，同时采用公开密码体制，攻击者无法窃听邮件的内容以及发布的公共信息，保证了通信内容的保密性。

(2)如果 A 和 B 在通信过程中，任何一方不遵守协议的规定，否认在通信中的行为，则可以通过上述“安全性分析”可知，协议可有效地抗击否认。

(3)如果 A 和 B 双方在通信过程中，都遵照协议去执行，这样他们的通信对第三方是保密的，也就是说双方通过一个“匿名的第三方”进行了一次秘密的通信，增大了通信过程的保密性。

(4)分析协议中实现过程，可以很容易看出该协议同时还满足：身份鉴别、邮件的完整性鉴别等功能。

(5)如果 A 与 B 有可靠连接的话，我们可以将协议进行优化，在第二步和第三步之间加入：

·A 将 K 直接交给 B

·B 将 K 的接收证明交给 A

如果 B 将 K 的接收证明交给 A，则 A 就不需要将第三步要求的信息发布，(这样减少了网络流量，增加协议的可靠性)，如果 B 没有将接收证明交给 A，则 A 可以继续执行第三步，同样可以实现相同的目的。

实现过程中应该注意的问题

(1)在协议中的第二步，必须指明如何以及何时获得解密密钥，同时指出如何进行解密，这样可以防止 B 声明 A 没有按时发布解密密钥，也可以防止 A 延迟或不在预定的地方发布密钥。

(2)A 必须保留 T、K 以及 B 签名的回执信息用来证明 B 的接受，这从概念上等价于 A 必须保留 B 收到 A 发送邮件的证明。

4.2 协议的应用前景与实例模型

与其他电子邮件协议不一样的是，本文所提出的协议能够利用现有的 Internet 基础设施来实现。任何的安全电子邮件程序都能够利用这种方法提供可认证的电子邮件传输。

这种协议还可以应用于其他类似的需要认证的传输服务中，如：商业实体之间。商业上可认证传输服务一般需要将传输协议与某种支付协议(payment protocol)集成在一起。本文所提出的协议可以很容易地增加支付机制：一个商业实体如果想接收 A 的支付，只需要向 A 提供一个公共论坛来使 A 完成第三步。这种商业认证传输服务的公共“场所”可以任意选择；这与其他的涉及需要可信第三方机制的协议有着鲜明的优越性。同时，协议本身并不要求任何商业保证提供者的参与，仅仅是简单地使用已有的“公共场所”如：BBS、新闻组等。

对于普通 Internet 用户之间的私人信息往来，也可以使用该协议来保证双方信息的公平交换，而不需要第三者来参与。

下面是该协议在实际应用中的实例模型，实线所指出的数据流程是邮件传输的过程，也是协议实现的流程。

总结 本文提出一种安全的电子邮件保证协议，该协议除了能够实现抗否认、身份认证、完整性鉴别等功能外，对于通信双方以外的第三方具有更少的依赖性、更小的复杂度等特点。更少的依赖性意味着更大的安全性和扩充性，更小的复杂度意味着易于配置、易于实现。因此，该协议对需认证信息交换应用的实现有着很高的参考价值。 (下转第20页)

家信息安全测评认证中心也称是代表国家对信息技术、信息系统、信息安全产品以及信息安全服务的安全性实施公正评价的技术职能机构，而且宣称，“中华人民共和国国家信息安全认证”是国家对信息安全技术、产品或系统安全质量的最高认可。

第三，通过分析上述安全评价准则的制定和执行情况，我们认为可以从中吸取如下的经验和教训：

1. 政府应该保证获得评价的产品可以在市场上得到使用。英国就是强制政府部门购买使用经过 ITSEC 或 CC 评价的产品。相反因为美国政府并不强制使用安全评价产品，使得最初开发的一些安全系统（如 KSOS、SCOMP、MULTICS 等）没能得到应用，最终变成了历史的见证人。产品如果在市场上都不能立足，那么就谈不上进一步的发展了。

2. 要制定或采纳统一的评价准则，并由专门的权威机构进行管理。否则会使产品开发者陷入迷茫，或者需要付出较高的代价（如需要接受多次评价认证）。

3. “他山之石，可以攻玉”，充分吸取国外或国际准则中的众多安全工作者的智慧。制定准则时应该考虑不同的安全政策、威胁和目的，区分功能需求和保证需求，尤其是要保证准则的可操作性和开放性。

4. 为了保证评价质量和方便厂商产品的评价，应建立统一的评价认证方案和多个评价实施机构。事实上，在 2000 年，世界上所有的 CC 评价认证机构总共评价了 12 个产品，而我国在同年评价的产品数为 219。

4. 展望

我们认为，以后信息安全评价的研究方向可能会集中在如下几点：

1. 针对各种安全产品和系统的面向不同可信等级的保护轮廓书的制定。对于大多数安全产品开发商来说，他们或许能够编写产品的安全对象书，但是很少有能力制定该类产品或系统的保护轮廓书。因此，针对某类安全产品或系统，制定面向特定可信等级的保护轮廓书，既可以促进信息安全技术的进一步发展，又可以对信息安全市场起一定的规范作用。

2. 目前信息安全保护的主要目的是保证保密性和完整性，以后对可用性、可靠性及可生存能力的保护的评价研究将会得到重视。一方面是因为安全需求正在逐渐从军方和政府扩大到商业和生活领域，另一方面，随着信息网络的迅速发展，出现了各色各样崭新的威胁和攻击。

3. 各种辅助评测技术和评估工具的研究和开发。对于一个安全产品或系统，既要按照开发商提供的各类文档（和代码）进行审查，又要测试其是否实现了宣称的安全功能。研制各种辅助评估工具，将对提高测试的质量和加快测试的周期起到非常重要的作用。

结论 随着计算机技术的广泛应用和国际互联网络的不断发展，信息安全问题也愈趋复杂和多样。信息安全产品和系统的评价也日益得到人们的重视。为了对我国安全评价领域提供指导和参考，本文首次考察了近二十年的信息技术安全评价准则的发展历史和评价情况，并对它们的贡献和不足之处进行了详尽的分析，对几个得到广泛使用的标准进行了相关性比较。然后对安全评价相关的几个重要问题进行了探讨，并结合我国信息安全评价的情况，指出了我们可以从中吸取的经验和教训。最后给出了安全评价技术未来可能的研究方向。随着信息技术的发展和人们开发和评价经验的不断积累，我们有理由对我国未来信息安全的评价持乐观态度。

参 考 文 献

1 Anderson J P. Computer Security Technology Planning Study Volume II, ESD-TR-73-51, Vol. II, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01730, Oct. 1972

2 Bell D E, LaPadula L J. Secure Computer Systems: Mathematical Foundations. : [ESD-TR-73-278]. Vol. I, AD 770 768, Electronic Systems Division, Air Force Systems Command, Hanscom AFB, Bedford, Massachusetts, Nov. 1973

3 Department of Defense. Department of Defense Trusted Computer System Evaluation Criteria. DoD 5200. 28-STD, Washington, DC, Dec. 1985

4 Federal republic of Germany. Criteria for the evaluation of trustworthiness of information technology systems, ISBN 3-88784-200-6, Jan. 1989

5 Communication-electronics security group. UK systems security confidence levels. United Kingdom, Feb. 1989

6 Office for Official Publications of the European Communities. Information Technology Security Evaluation Criteria, Version 1.2. Jun. 1991

7 Pfleeger C P. Security in Computing, Second Edition. Prentice Hall PTR, 1997

8 National security agency. Combined Federal Criteria. 1992

9 Common Criteria Project Sponsoring Organizations. Common Criteria for Information Security Evaluation, Version 2.1. ISO/IEC 15408, Aug. 1999

10 中国. 计算机信息系统安全保护等级划分准则. GB17859-1999, 1999

11 http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/index.asp

12 http://niap.nist.gov/cc-scheme/ValidatedProducts.html

13 http://www.radium.ncsc.mil/tpep/epl/historical.html

14 http://www.infosec.org.cn/gonggao/

15 http://www.mctc.gov.cn/cpjs.htm

（上接第 100 页）

参 考 文 献

1 Bahreman A, Tygar J D. Certified Electronic Mail. In: Proc. of the Internet Society Symposium On Network and Distributed System Security, Internet Society, 1994. 3～19

2 Micali S. Simultaneous electronic transactions with visible trusted parties. U.S. Patent 5,629,982,13 13 May 1997

3 Asokan N, Schunter M M. Optimistic protocol for fair exchange. ACM Computer and communications security, 1997. 7

4 崔国华，等. 安全的电子保证邮件. 计算机工程

5 Bruce Schneier 著，吴世忠等译. 应用密码学. 机械工业出版社