阻止邮件内容“裸奔”

(2021 年 4 月 1 日)

如果有人告诉你-“今天在街上看到有人裸奔!”，请别相信，因为今天是西方的愚人节！但是，笔者今天告诉你-“我们天天都在使用的电子邮件已经“裸奔”了 50 年!“，这是真的。

笔者早在 **2006 年 1 月 23 日**就在当时非常有名计算机专业报刊《计算机世界》发表了技术文章《**阻止邮件内容“裸奔”**》，当时是以“沃通”的笔名发表的。15 年过去了，电子邮件内容安全还是不容乐观，当然也是有进步的，当时情况是国内没有一家邮件服务系统部署了 SSL 证书，而现在的主流电子邮件服务系统基本上都部署了 SSL 证书，能有效保障用户 Web 登录时用户名和口令安全，也能保障用户的 IMAP/SMTP 通信安全。也就是说，已经有一部分邮件内容不再“裸奔”。

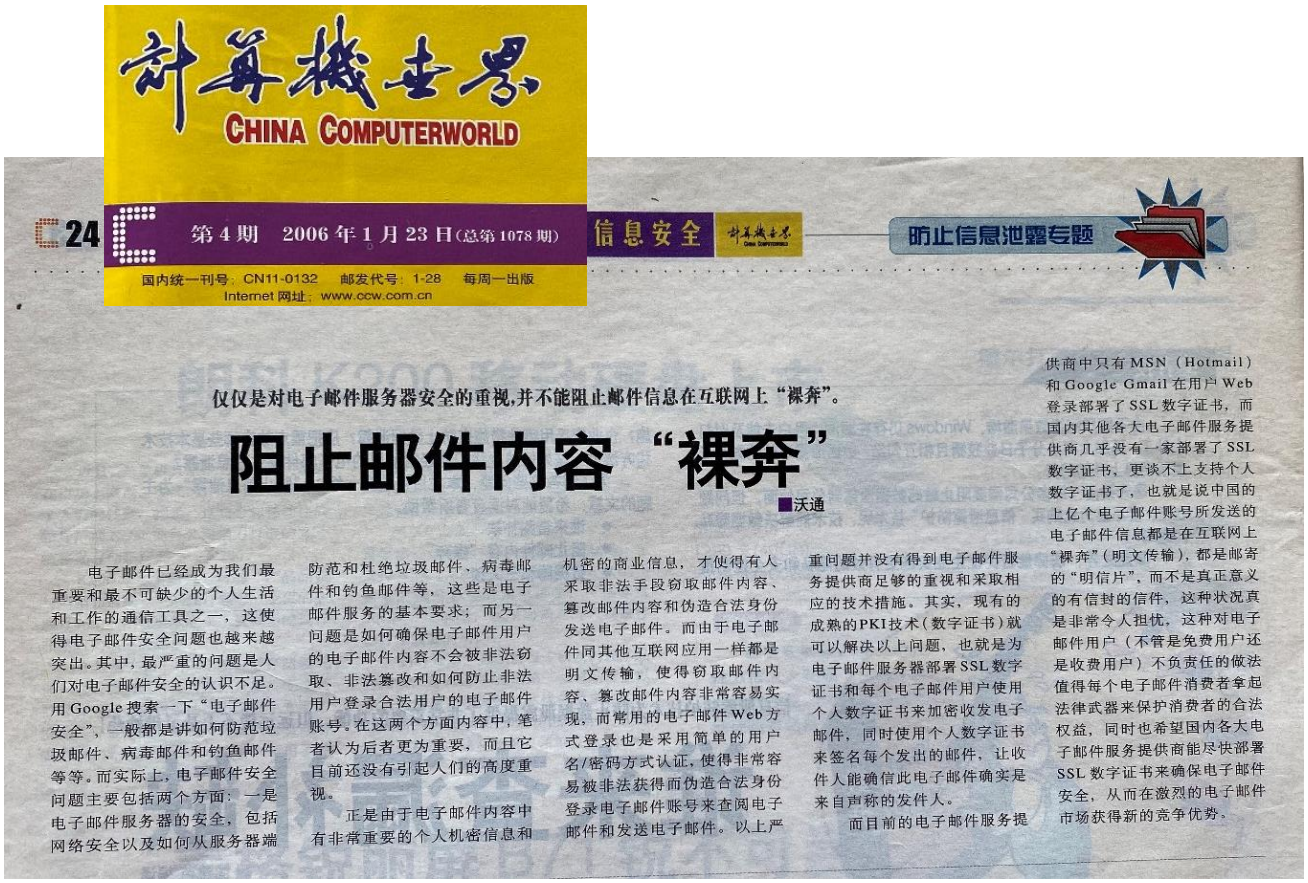
但是，由于还有许多邮件系统并没有部署 SSL 证书(包括不少政务邮件系统)，而即使是发件人邮件服务器部署了 SSL 证书，而由于收件人邮件服务器并没有部署 SSL 证书，则邮件从发件人邮件服务器发送到收件人邮件服务器的传输过程还是明文传输的，同时收件人从其邮件服务器收取邮件也是明文传输的。也就是说：仅仅在自家的邮件服务器部署 SSL 证书并不能保证邮件的全程加密传输，仍然是不安全的。

所以，要想实现可靠的电子邮件全程加密，而不用关心收件人的邮件服务器是否部署了 SSL 证书，则必须是邮件内容本身采用邮件证书加密。这个端到端加密解决方案在 15 年后的今天还没有实现普及应用，不仅仅是我国没有实现，全球也都没有实现，这是由于 S/MIME 邮件加密的确非常繁琐，需要用户花钱向 CA 购买和申请邮件证书，再费力地配置到邮件客户端中使用，还需要同收件人交换公钥才能实现邮件加密，这些即使 IT 人员也未必能搞定，难度可想而知了。

15 年过去了，所幸的是，现在的云计算和云服务已经非常成熟，密信技术建立了云密码基础设施，并研发了密信 App(加密邮件客户端)，“云”“地”一体相互配合，采用 S/MIME 技术全球率先独家实现了全自动邮件加密和数字签名加时间戳，使得发送加密邮件同发送普通明文一样简单，用户根本不用关心什么是邮件证书，也无需向 CA 申请邮件证书，也无需事先同收件人交换公钥，一键轻松发送加密邮件，保障邮件内容不再“裸奔”，这个邮件加密创新解决方案得到了全球 171 个国家/地区的用户的喜爱和热捧。

也就是说，有了密信技术提供的全自动邮件加密解决方案，有望真正实现笔者 15 年前的”

阻止邮件内容“裸奔”的梦想。“**不忘初心，方得始终**”，笔者坚信，通过密信人的继续努力奋斗，同全球互联网用户一道共同加油，一定能早日实现“邮件全加密”“阻止邮件内容“裸奔””的伟大梦想，让加密电子邮件真正造福全人类。



计算机世界
CHINA COMPUTERWORLD

C24 第4期 2006年1月23日(总第1078期) 信息安全 阻止信息泄露专题

国内统一刊号：CN11-0132 邮发代号：1-28 每周一出版
Internet网址：www.ccw.com.cn

仅仅是对电子邮件服务器安全的重视，并不能阻止邮件信息在互联网上“裸奔”。

阻止邮件内容“裸奔”

■沃通

电子邮件已经成为我们最重要和最不可缺少的个人生活和工作的通信工具之一，这使得电子邮件安全问题也越来越突出。其中，最严重的问题是人们对电子邮件安全的认识不足。用Google搜索一下“电子邮件安全”，一般都是讲如何防范垃圾邮件、病毒邮件和钓鱼邮件等等。而实际上，电子邮件安全问题主要包括两个方面：一是电子邮件服务器的安全，包括网络安全以及如何从服务器端防范和杜绝垃圾邮件、病毒邮件和钓鱼邮件等，这些是电子邮件服务的基本要求；而另一问题是如何确保电子邮件用户的电子邮件内容不会被非法窃取、非法篡改和如何防止非法用户登录合法用户的电子邮件账号。在这两个方面内容中，笔者认为后者更为重要，而且它目前还没有引起人们的高度重视。

正是由于电子邮件内容中有非常重要的个人机密信息和机密的商业信息，才使得有人采取非法手段窃取邮件内容、篡改邮件内容和伪造合法身份发送电子邮件。而由于电子邮件同其他互联网应用一样都是明文传输，使得窃取邮件内容、篡改邮件内容非常容易实现，而常用的电子邮件Web方式登录也是采用简单的用户名/密码方式认证，使得非常容易被非法获得而伪造合法身份登录电子邮件账号来查阅电子邮件和发送电子邮件。以上严重问题并没有得到电子邮件服务提供商足够的重视和采取相应的技术措施。其实，现有的成熟的PKI技术（数字证书）就可以解决以上问题，也就是为电子邮件服务器部署SSL数字证书和每个电子邮件用户使用个人数字证书来加密收发电子邮件，同时使用个人数字证书来签名每个发出的邮件，让收件人能确信此电子邮件确实是来自声称的发件人。

而目前的电子邮件服务提供商中只有MSN（Hotmail）和Google Gmail在用户Web登录部署了SSL数字证书，而国内其他各大电子邮件服务提供商几乎没有一家部署了SSL数字证书，更谈不上支持个人数字证书了，也就是说中国的上亿个电子邮件账号所发送的电子邮件信息都是在互联网上“裸奔”（明文传输），都是邮寄的“明信片”，而不是真正意义的有信封的信件，这种状况真是非常令人担忧，这种对电子邮件用户（不管是免费用户还是收费用户）不负责任的做法值得每个电子邮件消费者拿起法律武器来保护消费者的合法权益，同时也希望国内各大电子邮件服务提供商能尽快部署SSL数字证书来确保电子邮件安全，从而在激烈的电子邮件市场获得新的竞争优势。

附：《计算机世界》2016年第4期(2006年1月23日)C24页笔者文章全文

仅仅是对电子邮件服务器安全的重视，并不能阻止邮件信息在互联网上“裸奔”

阻止邮件内容“裸奔”

电子邮件已经成为现代人最重要和最不可缺少的个人生活和工作的通信工具之一，这就使得电子邮件安全问题也越来越突出。其中，最严重的问题是人们对电子邮件安全的认识不足。Google搜索一下“电子邮件安全”，一般都是讲如何防范垃圾邮件、病毒邮件和钓鱼邮件等等。而实际上，电子邮件安全问题最重要的主要包括两个方面：一是电子邮件服务器的安全，包括网络安全以及如何从服务器端防范和杜绝垃圾邮件、病毒邮件和钓鱼邮件等，这些是电子邮件服务的基本要求；而另一个问题是如何确保电子邮件用户的电子邮件内容不会被非法窃取、非

法篡改和如何防止非法用户登录合法用户的电子邮件账号。在这两个方面的内容中，笔者认为后者更重要，而且它目前还没有引起人们的高度重视。

正是由于电子邮件内容中有非常重要的个人机密信息和机密的商业信息，才使得有人采取非法手段窃取邮件内容、篡改邮件内容和伪造合法身份发送电子邮件。而由于电子邮件同其他互联网应用一样都是明文传输的，使得窃取邮件内容、篡改邮件内容非常容易实现，而常用的电子邮件 Web 方式登录也是采用简单的用户名/密码方式认证，使得非常容易被非法获得而伪造合法身份登录电子邮件帐号来查阅电子邮件和发送电子邮件。以上严重问题并没有得到电子邮件服务提供商足够的重视和采取相应的技术措施，其实，现有的成熟的 PKI 技术(数字证书)就可以解决以上问题，也就是为电子邮件服务器部署 SSL 数字证书和每个电子邮件用户使用个人数字证书来加密收发电子邮件，同时使用个人数字证书来签名每个发出的邮件，让收件人能确信此电子邮件确实是来自声称的发件人。

而目前的电子邮件服务提供商中只有 MSN(Hotmail)和 Google Gmail 在用户 Web 登录部署了 SSL 数字证书，而国内其他各大电子邮件服务提供商几乎没有一家部署了 SSL 数字证书，更谈不上支持个人数字证书了，也就是说中国的上亿个电子邮件帐号所发送的电子邮件信息都是在互联网上“裸奔”(明文传输)，都是邮寄的“明信片”，而不是真正意义的有信封的信件，这种状况真是非常令人担忧，这种对电子邮件用户(不管是免费用户还是收费用户)不付责任的做法值得每个电子邮件消费者拿起法律武器来保护消费者的合法权益，同时也希望国内各大电子邮件服务提供商能尽快部署 SSL 数字证书来确保电子邮件安全，从而在激烈的电子邮件市场获得新的竞争优势。

----------END----------