计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(7):71−77 [doi: 10.15888/j.cnki.csa.006427]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 DANE 的电子邮件安全研究①

柏宗超[1,2,3], 姚健康[2], 孔　宁[2]

[1](中国科学院 计算机网络信息中心, 北京 100190)
[2](中国互联网络信息中心, 北京 100190)
[3](中国科学院大学, 北京 100049)
通讯作者: 姚健康, E-mail: yaojk@cnnic.cn

摘　要: 电子邮件是当今重要的通信工具, 也是网络攻击的主要途径之一. 由于近年来 CA 机构有意无意的证书误签发、邮件中间人降级攻击、基于 DNS 的域名实体认证协议 DANE 的提出, 当前邮件协议的改进及邮件隐私和安全有了新进展. 从邮件加密和验证角度梳理了当前广泛使用的邮件协议, 分析了其优缺点, 归纳了邮件协议的最新研究进展、DANE 对当前邮件协议的改进及其不足, 提出了基于 DANE 的安全邮件系统架构. 最后对基于 DANE 的邮件系统的发展方向进行了总结与展望.

关键词: 电子邮件; 安全; STARTTLS; SPF; DKIM; DMARC; DANE

引用格式: 柏宗超,姚健康,孔宁.基于 DANE 的电子邮件安全研究.计算机系统应用,2018,27(7):71–77. http://www.c-s-a.org.cn/1003-3254/6427.html

Email Security Research Based on DANE

BAI Zong-Chao[1,2,3], YAO Jian-Kang[2], KONG Ning[2]

[1](Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China)
[2](China Internet Network Information Center, Beijing 100190, China)
[3](University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: Email is today's important communication tool, but it is also one of the main ways of cyber attack. As a result of certificates mistakenly issued by CA agency, man-in-the-middle downgrade attack, and the proposal of DNS-based Authentication of Named Entities (DANE), new progress has been made on the improvement of the current email protocol and the security of email. This study combs the widely used email protocol from the point of view of email encryption and verification, analyzes its advantages and disadvantages, summarizes the latest research progress of email protocols and the improvement of current email protocol, and proposes a secure email system architecture based on DANE. Finally, the development direction of DANE-based email system is summarized and prospected.

Key words: email; security; STATTLS; SPF; DKIM; DMARC; DANE

电子邮件是当前网络办公中最重要的沟通工具之一, 其传输的数据通常是用户的私人通信信息、密码恢复确认信息以及公司内部和公司间的极具价值的数据. 电子邮件也是发起有针对性的网络攻击的首选渠道, 一半以上的电子邮件 (53%) 属于垃圾邮件, 越来越多的垃圾邮件包含恶意软件, 其比例在 2016 年显著上升, 电子邮件已经一跃成为恶意软件传播的主要媒介[1]. 当今, 伴随着垃圾邮件的泛滥以及社会工程手段的加强, 很难判断一封电子邮件是否具有欺诈性.

电子邮件系统的基础是简单邮件传输协议 (Simple

① 基金项目: 发改委 288 域名安全专项
Foundation item: Special Project of NDRC 288 Domain Name Security
收稿时间: 2017-11-07; 修改时间: 2017-12-04; 采用时间: 2017-12-07; csa 在线出版时间: 2018-06-27

Mail Transfer Protocol, SMTP), SMTP 是发送和中继电子邮件的互联网标准[2,3]. 但是, 正如 1981 年最初设想的, SMTP 不支持邮件加密、完整性校验和验证发件人身份. 由于这些缺陷, 发送方电子邮件信息可能会被网络传输中的监听者截取流量读取消息内容导致隐私泄漏, 也可能遭受中间人攻击 (Man-in-the-Middle attack, MitM) 导致邮件消息篡改, 带来网络钓鱼攻击. 为了解决这些安全问题应对日益复杂的网络环境, 邮件社区开发了诸多电子邮件的扩展协议, 例如 STARTTLS, S/MIME, SPF, DKIM 和 DMARC 等协议. 当前的邮件服务厂商大都也是采用以上扩展协议的一种或几种组合, 辅以应用防火墙、贝叶斯垃圾邮件过滤器等技术, 来弥补电子邮件存在的安全缺陷.

但是需要注意的是, 以上邮件协议本身仍存在安全及部署问题, 这有但不限于缺乏针对终端用户的全球可扩展的密钥分发和撤销机制、当前邮件安全解决方案过于复杂以及自动化部署执行方案缺失等原因. 比如, 互联网工程任务组 IETF 在 1999 年就已经发布了针对终端用户安全的 S/MIME 协议, 但是直到 2017 年, 该协议也未能在全球邮件服务器中大规模部署.

为了解决当前邮件系统中存在的安全及部署问题, IETF 在近年发布了基于域名系统的域名实体认证协议 (DNS-based Authentication of Named Entities, DANE) 及基于 DANE 的诸多扩展协议来提升电子邮件的机密性及安全性[4−6]. 简而言之, 这些通过 DANE 改进的协议基于域名系统 (Domain Name System, DNS) 和域名系统安全扩展 (DNS Security Extensions, DNSSEC) 的现有基础架构, 创建终端用户使用的 X.509 证书的安全全局存储库以及验证电子邮件服务器的加密凭据, 弥补了当前电子邮件系统中存在的诸多不足.

截至目前, 国内对电子邮件系统及其协议的研究较少, 本文创新性地从邮件加密和验证两个方面系统地梳理了当前电子邮件系统所使用的协议及其架构演进, 分析了 DANE 及基于 DANE 对当前普遍采用的邮件协议的改进, 最后展望了未来基于 DANE 的电子邮件系统发展, 以期为未来研究提供有益的启发和借鉴.

本文剩余部分的组织结构如下: 第 1 节和第 2 节分别从电子邮件加密和验证角度介绍当前电子邮件系统的加密和验证机制. 第 3 节阐述 IETF 近年提出的 DANE、其对当前邮件加密和验证协议的改进和不足以及基于 DANE 的安全邮件系统架构. 第 4 节总结和展望.

1 电子邮件的机密性

为了保证电子邮件的机密性防止数据监听后明文读取, 通常是从邮件传输通道和邮件消息两个角度考虑数据加密.

1.1 邮件在传输过程中的机密性

为了保证邮件在传输过程中的机密性, IETF 在 1999 年发布了通过传输层安全协议 (Transport Layer Security, TLS) 来提升 SMTP 安全性的互联网标准[7]. 但是, 原始的 SMTP 协议并不兼容 TLS 协议, 为了解决这个问题, 一个新的命令 (STARTTLS) 被添加到协议中, STARTTLS 通过 TLS/SSL 将 SMTP 明文通信连接升级为加密连接. 在一个经典的 STARTTLS 会话中, 客户端首先与邮件中继服务器协商进行 SMTP 连接; 然后客户端发送 STARTTLS 命令, 该命令启动标准 TLS 握手; 最后, 客户端通过此加密保护信道来发送邮件内容、附件和任何相关联的数据. 图 1 为添加 STARTTLS 命令后的邮件传输的简化场景图.

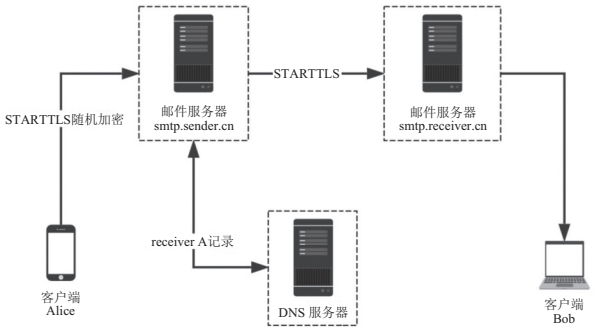

图 1 STARTTLS 随机加密简化场景图

STARTTLS 旨在保护与 SMTP 服务器之间邮件信息地发送, 主要是通过 TLS 加密的方式来防止电子邮件在传输过程中信息泄漏. 但是, STARTTLS 提供的是随机加密 (opportunistic encryption), 这与 HTTPS 客户端的行为不同, HTTPS 客户端严格要求通信双方都使用 TLS 协议. 而如果邮件中继服务器不支持或拒绝 STARTTLS 命令, 那么邮件将会以明文继续传输 (587 端口). 使用 STARTTLS 加密信道虽然防止了邮件在传输过程中被监听读取, 却不能阻止攻击者利用 STARTTLS 的这一特性发动降级的中间人攻击 (MitM Downgrade Attack)[8].

此外, 即使双方服务器协商使用 TLS 加密, 发送方也无法保证收件人邮件服务器的真实性. 在 RFC 3207 中并没有定义接收方如何验证接收到的加密证书, 而在几乎所有情况下, 接收方不会验证接收的证书, 这也是一个潜在的威胁.

针对以上问题, 当前 IETF 工作组提出了保护邮件通信安全的一个草案 SMTP-STS[9]. 该草案与 HSTS(RFC 6797) 标准类似, 在 HTTPS 协议中, 用户能够选择不允许通过不安全的信道, HSTS 则允许站点指示给用户之后的连接必须使用 HTTPS. SMTP-STS 的原理是让接收域在其 DNS 中发布资源纪录, 以明确的 URL 来发布其安全策略, 发件人则使用 HTTPS 进行访问. 该草案的优点在于它在解决 STARTTLS 以上两个问题的同时, 定义了规则、反馈机制及在 TLS 协商失败后采取对应的措施, 而且该草案并未规定使用 DNSSEC. 但是, 该草案也有其缺点, 它要求发送方邮件中继服务器 (Mail Transfer Agent, MTA) 必须使用 HTTPS 来确保安全信道存在, 还可能存在 DNS 欺骗或者分布式拒绝服务攻击, 阻止客户端查询这些策略.

SMTP-STS 虽然在一定程度上解决了 STARTTLS 中存在的问题, 但是该协议仍然是一个针对 MTA 之间通信的信任机制, 它对端到端的邮件加密和电子签名没有任何作用.

1.2 邮件端到端的加密

电子邮件协议在设计之初, 仅支持纯文本消息的数据传输 (RFC 822). 为了满足不同类型消息的发送, IETF 在 1996 年发布了多用途互联网邮件扩展协议 (Multipurpose Internet Mail Extensions, MIME)[10–12], MIME 协议的发布扩展了 SMTP 协议, 使得电子邮件可以支持格式化文本、附加文件、HTML 音视频、应用程序和图片等多种数据格式.

为了保证 MIME 数据的机密性、完整性以及来源验证, IETF 在 1996 年和 1999 年分别发布了基于 MIME 协议的扩展协议 OpenPGP[13]和 S/MIME[14], S/MIME 和 OpenPGP 都使用了公开密钥加密机制实现电子邮件的数字签名和加密. 由于信任链以及密钥管理等方式的不同, S/MIME 相对来说具有更广泛的应用场景.

公钥加密机制为电子邮件用户提供了一种产生公钥/私钥对的方式, 密钥通常需要被证书签发机构 (Certificate Authority, CA) 签名或者编码为自签名证书. 公钥数字证书旨在提供给全球的任何个人、组织和机构, 以便他们可以使用 S/MIME 来加密要发送的电子邮件. 在公钥密码体制中, 公钥加密的电子邮件只能被持有该公钥对应的私钥的接收者解密. 此外, 私钥还可用于电子邮件的数字签名, 因为只有发件人拥有某一公钥对应的私钥, 所以该机制能够确保电子邮件发件人的真实性及数据完整性.

然而, 一个不幸的事实是, 虽然 S/MIME 协议采用的信任机制很好, 但是, S/MIME 的部署过程过于复杂.

首先, 生成和安装 S/MIME 所使用的加密/签名密钥的手动操作步骤非常困难和耗时, 需要通信双方对公钥加密体制等密码学原理有所了解. 同时, 用户需要自行保管私钥. 考虑普通用户通常会有多个终端设备和多个电子邮件账号, 将私钥从一个终端设备传输到另一个设备, 这对大多数用户来说是不可能的. 因此, 大多数用户根本不会使用 S/MIME.

其次, 假设用户掌握了密钥安装和管理的技术, 下一步是关于分发和管理公钥数字证书. 到目前为止, 没有一个可以用于发布和检索个人公钥的全局密钥存储库. 相反, 通常是使用 S/MIME 加密的用户通过向收件人发送带有数字签名的电子邮件或者通过电话等方式手动分发密钥到收件人. OpenPGP 是通过“密钥交换方”和一组有限的密钥交换服务器使用信赖网络 (Web of Trust, WoT) 分发密钥. S/MIME 和 OpenPGP 都不具有很好的扩展性, 邮件服务器厂商无法向密钥未知的客户发送加密电子邮件, 这限制了用户对该加密协议的使用.

另一个操作问题是伪造数字证书. 某些可信任的权威 CA 可能会由于失误或者其它原因签发伪造的签名证书, 而通常情况下, 收件人又不会检查电子邮件证书的正确性, 只要证书存在, 通常会认为它是有效的. 与假冒证书相关的问题是类似域名中存在的“变体域名”问题, 也就是注册高度相似的极具欺骗性的域名, 比如域名“icbc.cn”和“1cbc.cn”. 在电子邮件系统的中, 当这些变体域名申请了伪造的数字签名后, 由于普通用户通常不具备足够的鉴别能力, 可能导致被欺骗. 比如来自“alice@examp1e.cn”(‘1’为数字 1) 的欺诈邮件可能会被误认为合法的“alice.example.cn”. 而此时如果能够有一个全局管理证书的存储库, 如 DNS, 通过向该存储库查询则可以鉴别真伪, 从而避免使用到恶意证书.

同时, S/MIME 协议本身是没有制定规则和反馈机

制的, 当由于一些未知原因导致拒绝接受 S/MIME 加密或签名的电子邮件时, 无法提供故障反馈.

2 邮件身份验证

虽然 STARTTLS 和 SMTP-STS 保证了邮件在传输过程中的加密, 防止遭受窃听读取, 但是其仍无法解决发件方身份伪造、消息篡改等问题. 当前的电子邮件系统主要是通过三种基于 DNS 来发布和检索资源记录的方式解决这些问题.

2.1 SPF 和 DKIM

发件人策略框架 (Sender Policy Framework, SPF) 是一种以 IP 地址认证电子邮件发件人身份的检测电子邮件欺诈的技术, 是非常高效的垃圾邮件解决方案[15,16]. SPF 允许组织授权一系列为其域发送邮件的主机, 而存储在 DNS 中的 SPF 记录则是一种 TXT 资源记录, 用以识别哪些邮件服务器获允代表本网域发送电子邮件. SPF 阻止垃圾邮件发件人发送假冒本网域中的“发件人”地址的电子邮件, 收件人通过检查域名的 SPF 记录来确定号称来自该网域的邮件是否来自授权的邮件服务器. 如果是, 就认为是一封正常的邮件, 否则会被认为是一封伪造的邮件而进行退回. SPF 还允许组织将其部分或全部 SPF 策略委托给另一个组织, 通常是将 SPF 设置委托给云提供商.

DKIM 域名密钥识别邮件标准 (Domain Keys Identified Mail) 是一种通过检查来自某域签名的邮件标头来判断消息是否存在欺骗或篡改的检测电子邮件欺诈技术[17]. DKIM 是利用加密签名和验证的原理, 在发件人发送邮件时候, 将与域名相关的私钥加密的签名字段插入到消息头, 收件人收到邮件后通过 DNS 检索发件人的公钥 (DNS TXT 记录), 就可以对签名进行验证, 判断发件人地址及消息的真实性. 需要注意的是, DKIM 只能验证发件人地址来源的真伪, 无法辨识邮件内容的真实性. 同时, 如果接收到无效或缺少加密签名的消息, DKIM 无法指定收件人采取什么措施. 此外, 私钥签名是对本域所有外发邮件进行普遍的签名, 是邮件中继服务器对邮件进行 DKIM 签名而不是真正的邮件发送人, 这意味着, DKIM 并不提供真正的端对端的电子签名认证.

SPF 和 DKIM 中共同存在的问题是缺少有效的策略和反馈机制, 这两个协议并未定义如何处理来自声称为某域的未经身份验证的电子邮件, 如何处理第三方声称托管的某域的未经身份验证的邮件, 如何反馈和统计声称是某域的身份认证成功或失败的电子邮件.

2.2 DMARC

DMARC 以域名为基础的邮件认证、报告和一致性标准 (Domain-based Message Authentication, Reporting, and Conformance) 就是用来解决 SPF 和 DKIM 中存在的这些问题[18], DMARC 的主要用途在于设置“策略”, 这个策略包含接收到来自某个域未通过身份验证的邮件时应执行什么操作、该域授权的第三方提供商发送了未经身份验证的邮件时该如何处理. DMARC 还会让 ISP 发送有关某个域身份验证成功或失败的报告, 这些报告将发送至“rua”(汇总报告) 和“ruf”(取证报告) 中定义的地址中. 同时, DMARC 依靠出站邮件流配置的 SPF 记录和 DKIM 密钥来确保邮件来源及签名的完整性, 当未通过 SPF 或 DKIM 检查的邮件时便会触发 DMARC 策略. 图 2 为基于 SPF、DKIM 和 DAMRC 的邮件验证简化场景图.

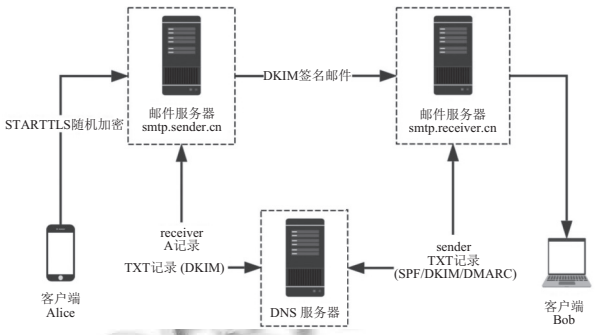

图 2 邮件验证简化场景图

3 基于 DNS 的域名实体认证协议 DANE

DANE 一种将 X.509 证书绑定到 DNS 中的机制, 可用于存储自签名证书或者从 CA 签发的特定 X.509 证书, 其中, 证书作为 DNS 资源记录通过 DNSSEC 来实现其来源验证和完整性保护[19–21]. 根据证书用途的不同, 基于 DANE 的 DNS 资源记录也有所不同: 资源记录 TLSA 用于发布使用 TLS 加密的证书, 资源记录 OPENPGPKEY 和 SMIMEA 分别用来发布 OpenPGP 和 S/MIME 协议中使用的证书.

保护公开密钥防止被篡改是实际公钥应用中一大难题, 公钥基础设施 PKI 的主要目的就是用来安全、便捷、高效地获得公钥, 而 IETF 发布 DANE 协议的动机之一是解决现有的基于 X.509 的 PKI 的问题. 例如, DANE 在应对欺诈证书、处理证书撤销、创建可

全球发布和检索证书的管理机制并允许自签名证书授权等方面提供了很好的解决方式.

DNS 的层级架构创建了授权机制, DANE 基于 DNS 的授权机制来实现以上目标. 在 DNS 中只有授权的域所有者才能够在其 DNS 域中放置相应的资源记录, 其他未授权的人都没有权限这样做. 例如, 只有拥有“example.com”域名的公司才可以在该域名的 DNS 名称空间中放置资源记录.

DANE 协议的第一个应用是针对 Web 服务器中使用的 TLS 证书的身份验证, 而目前其在邮箱中的应用主要针对以上 TLS、S/MIME、OpenPGP 和 DMARC 协议的改进.

3.1 基于 DANE 的 TLS

在 2.1 节中已经阐述了 SMTP 服务器在使用 STARTTL 命令开启 TLS 加密传输中存在降级的中间人攻击潜在风险, 而基于 DANE 的随机 TLS 加密则可以很好的解决这个问题[5]. 其大致流程图如图 3 所示.

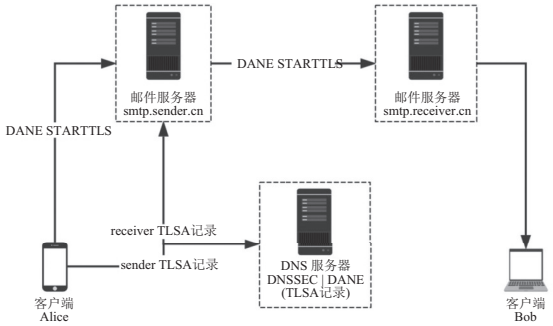

图 3 DANE STARTTLS

在发出 STARTTLS 命令之前, 邮件服务器先发出 DNS 查询请求, 查看接收方服务器是否存在相关的 DANE TLSA 记录. 如果记录存在, 那么使用加密传输的 STARTTLS 命令就一定会发出, 这时如果由于中间人等原因, 导致接收方服务器拒绝 STARTTLS 请求或者接收到的证书与 DANE TLSA 纪录不匹配, 邮件服务器就会中止通信, 并在稍后重新发送加密传输请求. 如果接收方 DNS 服务器中未部署 DANE TLSA, 则继续使用随机 TLS 加密.

因此, DANE 在保证邮件服务器加密传输的同时, 又能验证接收到的证书的真实性. 同时, 由于 TLSA 纪录存在与否并不影响当前邮件系统采用降级的 TLS 的加密传输策略, 所以可以增量部署 DANE 安全机制.

3.2 基于 DANE 的 S/MIME

尽管基于 DANE 的随机 TLS 加密提供了一种保证数据在邮件中继服务器之间加密传输的机制, 在邮件终端用户端到端的安全和验证方面却没有任何保障: 无法获取终端用户的数字签名, 无法对终端接收方身份验证以及无法保证电子邮件在到达接收方邮件服务器之后仍然加密存储. 在 1.2 小节中阐述了 S/MIME 协议可以用来解决这些问题及其自身存在的密钥管理和分发问题, 而基于 DNSSEC 的 DANE 则可以解决 S/MIME 的这些问题.

2017 年 5 月 31 日正式发布的 RFC 8162 通过定义 SMIMEA 资源记录来扩展 DANE 协议. SMIMEA 纪录与 TLSA 记录遵循相同的协议格式, 但是可以用来存储单个用户的证书数据. 该协议采用哈希算法将电子邮件地址存储在 SMIMEA 资源记录中, 保证发送方查询收件人证书的同时, 提供隐私保护. 该协议通过使用由 DNSSEC 保护的 DNS 系统, 利用 DNS 作为可信任的存储库, 实现终端用户电子邮件证书的身份验证.

3.3 DANE 对 DMARC 的补充

DMARC 为 SPF 和 DKIM 定义了一些策略, 提供反馈机制来报告所采取的行为, 旨在防止攻击者伪造电子邮件的发件域发送欺诈邮件, 防止重放攻击, 确保收件人收到的邮件确实来自声称域; 而 DANE 则可以确保双方通信信道安全, 能够让发件方确定确实是在与指定的收件人通信, 保证数据加密传输给特定收件人.

从两者功能考虑, DMARC 和 DANE 互为补充, 谁也不能取代谁. 为此, IETF 为 DANE 提出了 DMRAC 的扩展草案[22].

3.4 DANE 的不足

当然, DANE 也有其“先天不足”之处. 基于 DANE 的邮件系统最为外界所诟病的是其需要依靠 DNSSEC 来对接收到的 DNS 资源记录来源进行认证, 验证其存在性和数据完整性. 毕竟当前 DNSSEC 还未在全网广泛部署[23], 因此, 会阻碍 DANE 在全球范围内的部署.

同时, DNSSEC 本身也存在一些安全及部署问题[24]. 如果攻击者想要对基于 DANE 的邮件系统发动攻击, 此时, 可以针对 DNSSEC 的安全问题发送攻击, 一旦攻击导致 DNSSEC 无法正常运作, DANE 因此也会受到牵连, 从而导致基于 DANE 的邮件系统瘫痪.

最后, 由于域所有者需要对新添加的 SMIMEA 资

源记录进行管理, 因此可能存在一些管理上的问题, 这加大了管理者管理难度[25].

3.5 基于 DANE 的邮件系统架构

根据当前 IETF 提出的 DANE 及其对当前邮件协议的改进, 本文提出了基于 DANE 的邮件系统架构. 图 4 展示了基于 DANE 的邮件系统如何实现端到端的邮件加密、消息完整性鉴定和来源验证. 其具体流程如下文.

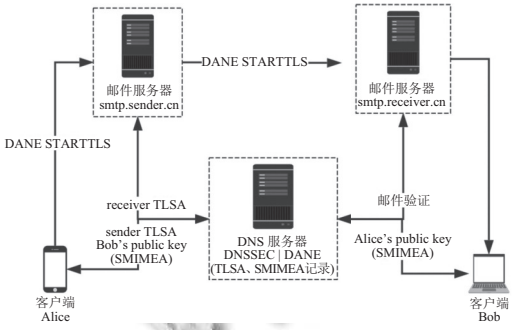

图 4 基于 DANE 的安全邮件系统架构

假设分别位于两个不同域的 Alice 和 Bob 需要使用加密和认证的电子邮件进行通信, 他们均已经获得了 X.509 证书. 此时, 如果没有针对电子邮件证书的全球公共存储库, Alice 和 Bob 如何获得对方所在域的证书? 如果针对电子邮件单独建立一个全球公共存储卡, 则无论是从管理还是花销上, 其代价都是巨大的. 而 DANE 通过在 DNS 中发布资源记录则可以相对“轻松”地提供这样的功能.

Alice 使用私钥对要发送给 Bob 的邮件消息进行数字签名, 这可以直接在其本地终端设备上使用 S/MIME 协议的电子邮件客户端中完成. 接下来, 为了加密消息, 本地客户的向 DNS 进行查询以检索收件人 Bob 的公钥证书, 使用公钥证书确保只有 Bob 可以解密邮件, 同时此证书由用户缓存以备将来再次使用. 签名和加密的消息之后发送给 Alice 所在域的邮件服务器, 邮件服务器在发出邮件之前, 继续使用基于 DANE 的 STARTTLS 进行协商加密, 保证邮件中继服务器之间的加密传输. 在最终 Bob 所在域的邮件服务器接收邮件之前, receiver 域还需要使用 DMARC 等协议来确保邮件来源的真实性以及邮件的完整性.

当 Bob 从邮件服务器接收消息后, 将通过他的私钥对邮件进行解密, 在 Bob 的终端设备中执行解密操作可确保数据在到达服务器之后的机密性. 之后 Bob 需要验证此消息, 确定该邮件真的是来自 sender 域的发件人 Alice 还是欺诈邮件. 为了确认真实性, 邮件客户端必须检查数字签名的真实性, 此时需要 Bob 通过执行发送 DNS 查询检索 Alice 的公钥证书, 用于解密数字签名并执行数据完整性检查. 如果签名验证正确, 则该消息是真实的, 同时确定该邮件在传输过程中没有改变.

4 总结与展望

当前业界采用的 STARTTLS 保证邮件传输过程中的机密性, SPF、DKIM 和 DMARC 保证邮件来源验证及完整性鉴别的方式, 在一定程度上解决了电子邮件中的诸多安全问题, 但是面对当下垃圾邮件肆虐、网络钓鱼横行的网络环境, 这些措施仍旧显得力不从心.

DANE 的出现为解决当前电子邮件中加密传输存在的降级攻击、邮件端到端加密等问题提供了一个可行的思路. DANE 基于 DNS 的特性保证了其可以建立一个全球范围的可扩展的电子邮件证书分发和管理机制, 为建立全球可信的电子邮件网络打下坚实的基础.

当前国内外基于 DANE 的研究及部署尚在初期阶段, 本文梳理了基于 DANE 的邮件扩展协议, 提出了一套以 DANE 为基础的邮箱系统架构, 以期为未来研究及建立一套全球范围更加安全的的邮件系统提供有益的启发和借鉴.

参考文献

1 Symantec. 2017 symantec internet security threat report. https://www.symantec.com/about/newsroom/press-kits/istr-22, 2017.
2 Postel JB. RFC 821 Simple mail transfer protocol. http://tools.ietf.org/html/rfc821. [1982-08].
3 Klensin J. RFC 5321 Simple mail transfer protocol. http://tools.ietf.org/html/rfc5321, 2008-10.
4 Hoffman P, Schlyter J. RFC 6698 The DNS-based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA. https://tools.ietf.org/html/rfc6698. [2012-08]
5 Dukhovni V, Hardaker W. RFC 7672 SMTP security via opportunistic DNS-based Authentication of Named Entities (DANE) Transport Layer Security (TLS). IETF, 2015.

6 Hoffman P, Schlyter J. RFC 8162 using secure DNS to associate certificates with domain names for S/MIME. IETF, 2015.
7 Hoffman P. RFC 2487 SMTP service extension for secure SMTP over TLS. https://tools.ietf.org/html/rfc2487. [1999-01].
8 Durumeric Z, Adrian D, Mirian A, *et al*. Neither snow nor rain Nor MITM...: An empirical analysis of email delivery security. Proceedings of the 2015 Internet Measurement Conference. Tokyo, Japan. 2015. 27–39.
9 Margolis D, Risher M, Ramakrishnan B, *et al*. SMTP MTA Strict Transport Security (MTA-STS) draft-ietf-uta-mta-sts-14. IETF, 2017. https://datatracker.ietf.org/doc/draft-ietf-uta-mta-sts/.
10 Freed N, Borenstein N. RFC 2045 Multipurpose Internet Mail Extensions (MIME) part one: Format of internet message bodies. https://tools.ietf.org/html/rfc2045. [1996-11].
11 Freed N, Borenstein N. RFC 2046 Borenstein. Multipurpose Internet Mail Extensions (MIME) part two: Media types. https://tools.ietf.org/html/rfc2046. [1996-11].
12 Moore K. RFC 2047 MIME (Multipurpose Internet Mail Extensions) part three: Message header extensions for non-ascii text. https://tools.ietf.org/html/rfc2047. [1996-11].
13 Atkins D, Stallings W, Zimmermann P. RFC 1991 PGP message exchange formats. Network Working Group, 1996.
14 Ramsdell B. RFC 2633 S/MIME version 3 message specification. Network Working Group, 1999.
15 Wong M, Schlitt W. RFC 4408 Sender Policy Framework (SPF) for authorizing use of domains in e-mail, version 1. https://tools.ietf.org/html/rfc4408. [2006-04].
16 Kucherawy M. RFC 6686 Resolution of the Sender Policy Framework (SPF) and sender ID experiments. https://tools.ietf.org/html/rfc6686. [2012-06].
17 Crocker D, Hansen T, Kucherawy M. RFC 6376 DomainKeys Identified Mail (DKIM) signatures. IETF, 2011.
18 Kucherawy M, Zwicky E. RFC 7489 Domain-based Message Authentication, Reporting, and Conformance (DMARC). https://tools.ietf.org/html/rfc7489. [2015-03].
19 Arends R, Austein R, Larson M, *et al*. RFC 4033 DNS security introduction and requirements. https://tools.ietf.org/html/rfc4033. [2005-03].
20 Arends R, Austein R, Larson M, *et al*. RFC 4034 resource records for the DNS security extensions. https://tools.ietf.org/html/rfc4034. [2005-03].
21 Arends R, Austein R, Larson M, *et al*. RFC 4035 protocol modifications for the DNS security extensions. https://tools.ietf.org/html/rfc4035. [2005-03].
22 Osterweil E, Wiley G. DMARC extensions for DANE. draft-osterweil-dmarc-dane-names-00. Internet-Draft, 2016.
23 Lian W, Rescorla E, Shacham H, *et al*. Measuring the practical impact of DNSSEC deployment. Proceedings of the 22nd Usenix Conference on Security. Washington, DC, USA. 2013. 573–588.
24 Herzberg A, Shulman H. DNSSEC: Security and availability challenges. 2013 IEEE Conference on Communications and Network Security. National Harbor, MD, USA. 2013. 365–366.
25 Gersch J, Massey D, Rose S. DANE trusted email for supply chain management. Proceedings of the 50th Hawaii International Conference on System Sciences. Waikoloa Village, HI, USA. 2017.