零信任能彻底解决邮件安全难题

(2021 年 5 月 17 日)

零信任是一个安全概念，就是不信任任何人和物，这虽然不是一项新技术，但这是一个创新的安全理念，为当今的数字化转型时代的网络安全发展指明了明确的方向。特别是目前的全球疫情时期，远程办公已经成为常态。据微软官网统计数据，在商业和教育行业的电子邮件使用量年同比增长 28%，而超过 90%的网络钓鱼攻击都是通过电子邮件进行的，每个月 Office 365 检测并阻止近 4000 万封网络钓鱼邮件。因此，每个组织都必须采取措施来防止和阻止钓鱼邮件安全威胁，这一点非常重要。

那么，如何才能根除这些恶意邮件攻击呢？还是先看看两类主要的邮件攻击方式：

其一：假冒公司总裁或者各政府部门的电子邮件地址给用户发送欺诈邮件，要求付款或提供个人重要账户信息等。这是由于电子邮件的设计“缺陷”造成的，因为发件人的电子邮件地址是很容易被假冒的。如果收件人邮件服务器设置了 SPF 发件人策略框架，则欺诈邮件往往就用类似域名来发送欺诈邮件，如 admin@micr0soft.com（用 0 来替代 o）来假冒微软公司邮件。

下图为假冒工商银行的邮件，发件人邮件地址看起来的确是工商银行域名，欺骗性非常强，只要用户点击了邮件的所谓的工行官网链接，实际上会链接到一个同工行官网一模一样的网站，让用户输入银行卡号和密码，许多用户就会纷纷中招。

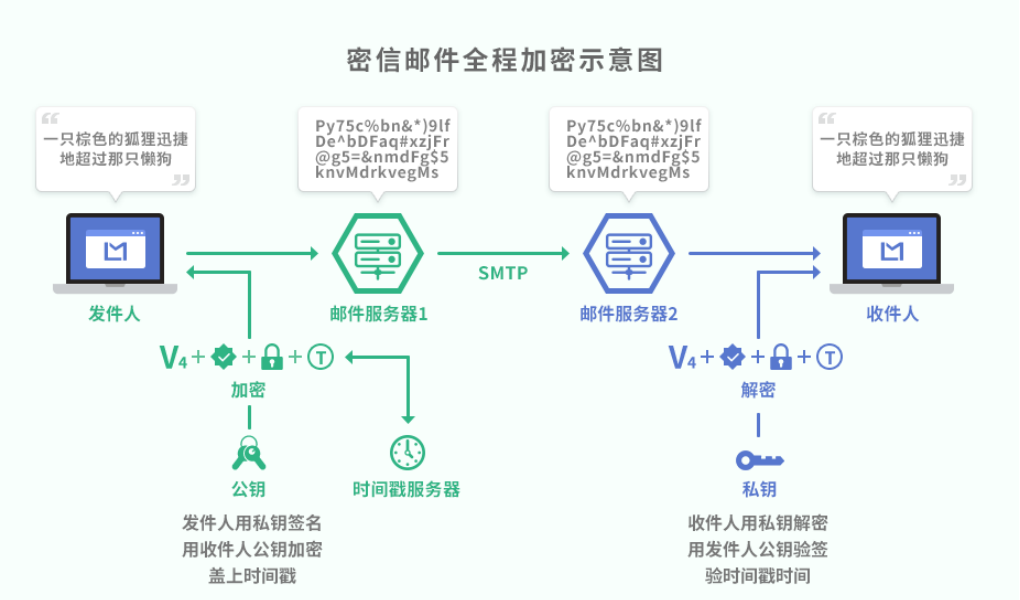
其二：不安全的 Web 邮件服务方式。Web 方式登录邮箱的确非常方便，使用任何浏览器都

能登录邮箱查看邮件，但是用户的用户名和口令往往非常简单，非常容易被枚举猜到，也非常容易被恶意键盘记录软件获得。用户登录后，由于所有邮件都是明文，所有邮件中的机密信息都可以轻松被窃取。这里有两个安全问题：一是用户名/口令认证非常不安全，二是邮件内容本身没有加密，明文存放。即使是邮件服务器启用了 TLS 传输加密也只能保证邮件在传输过程中的安全。

那么，零信任能否解决邮件安全难题？答案当然是可以！零信任的核心思想是不相信任何人，不相信声称是公司总裁的电子邮件，因为发件人的邮件地址是可以伪造的。只要坚守这一点，不相信任何有关付款或者提交任何机密信息的邮件，那就不会上当受骗！

当然，仅仅做到以上这一点还是不够的，并没有彻底解决邮件欺诈问题。密信邮件加密和数字签名解决方案实际上就是一个基于 PKI 技术的零信任邮件安全解决方案，具体主要有如下三点：

第一，不信任没有数字签名的邮件。每封邮件都必须有数字签名，有了数字签名，欺诈邮件是不可能使用银行域名邮件地址来发送电子邮件的，因为数字签名所用的签名证书是需要验证邮箱控制权的，假冒银行邮箱的发件人并没有真正的银行邮箱，所以无法拿到绑定银行邮箱的签名证书用于数字签名电子邮件。而如果用类似域名的真实邮箱则由于无法获得带有真实单位名称的签名证书也就无法使用假冒域名邮箱 admin@micr0soft.com 来假冒微软公司的邮件了，因为绑定单位名称的签名证书是需要通过严格的第三方 CA 验证身份后才能签发的。也就是说：不信任任何没有数字签名的邮件，才能保证不会上当受骗！常用的邮件客户端软件如 Outlook、密信 App 都会验证数字签名是否有效和是否可信，密信 App 会显示所有未签名邮件为“邮件未加密”。



第二，不采用不安全的用户名/口令认证方式。每个用户都必须有数字证书，邮件系统可

以禁用 Web 登录或者改造用户名/口令的登录方式为使用数字证书强身份认证登录，只有这样才能保证邮箱的 Web 登录安全。

第三，不相信明文邮件是安全，任何号称安全的邮件服务或邮件安全解决方案，如果邮件内容仍然是明文存放在邮件服务器中，都是不安全的，都不能相信其号称是安全的。怎么办？使用密信 App 自动加密每一封电子邮件，不仅能保证电子邮件在传输过程中的安全，也能保证电子邮件在邮件服务器中是以密文方式存放，使得即使邮箱口令被盗也无法获得电子邮件的机密信息，从而保证了邮件机密信息安全。

目前，之所以邮件安全问题还是非常严重，是因为传统安全厂商的方案只是防护邮件服务器不会被攻击，这是是不够的；而采用 VPN 登录位于内网的邮件服务器也不能解决所有邮件安全问题！而基于 PKI 技术的零信任邮件安全解决方案，不关心邮件服务器是在单位内网还是在公网云上，除了在邮件服务器上部署 SSL 证书来保护邮件传输链路安全外，还必须使用签名证书来实现强身份认证，替代不安全的用户名和口令认证。而对于邮件数据本身，还必须用加密证书来加密每一封邮件，而使用密信 App 作为邮件客户端软件来收发电子邮件能保证存放在邮件服务器上的邮件数据都是密文，即使被非法获得，由于无法解密而使得拿到的邮件数据是一堆废纸，使得各种邮件攻击失去了攻击的价值，邮件也就安全了。

常用的邮件客户端如 Outlook 和雷鸟等也支持 S/MIME 邮件加密和数字签名，为何大家都没有采用数字签名和加密来保障邮件安全呢？这是因为 S/MIME 加密太复杂，有申请证书、交换公钥和管理密钥这三道坎把用户拦在了 S/MIME 大门外。

只有密信邮件加密和数字签名解决方案才真正采用了 PKI 技术和零信任安全理念彻底解决了邮件安全难题。不信任明文邮件，数字签名和加密每一封邮件！密信零信任邮件安全解决方案，能真正解决邮件安全难题！欢迎下载密信 App 免费体验！

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

ceo@mesign.com