1.金笛电子邮件系统©

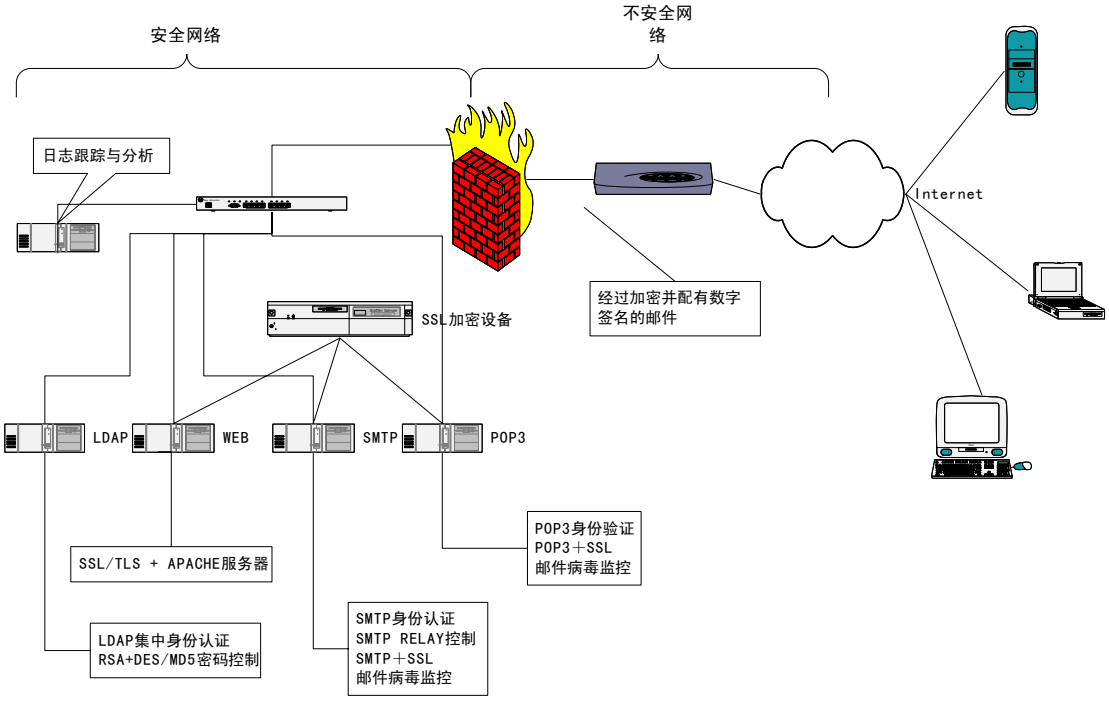
邮件系统安全性能说明

摘要

电子邮件是 INTERNET 上使用最广泛的服务，然而 SMTP/POP3/IMAP4 等电子邮件传输协议以及传统的电子邮件服务器软件在黑客面前显得非常脆弱，邮件用户很可能遭到密码被窃、邮件内容被截获甚至篡改、邮箱被炸毁等多种攻击，而邮件服务提供商也面临着邮件服务器被入侵的危险。在电子邮件得到迅速普及的今天，建立一个具有高度安全性的电子服务系统是开展该服务的重要因素，金笛系统是一个具有高性能、安全、稳定的电子邮件，从多个层次全面地阻止窃听、篡改等黑客行为，充分保护邮件服务提供商和用户的利益。

概述

电子邮件系统的安全，包括口令安全、传输安全、软件系统安全等多个方面，在整个系统上的任何一个漏洞，都足以使黑客截获用户收发的邮件甚至侵入服务器系统。当前广泛应用的免费电子邮件系统都提供用户 POP3 和 SMTP 服务，然而 POP3 和 SMTP 这两个邮件传输都是用明文来传输用户的密码和邮件的；同样的，用户通过浏览器访问 WEBMAIL 或用 IMAP4 协议下载邮件时，也是完全明文传输的。另外，SENDMAIL 等一些传统邮件系统都是直接采用系统用户帐号作为邮件帐号的，也就是说邮件用户能够访问到服务器上的系统资源，这是系统安全的一大隐患。建设一个高安全的邮件服务系统，应该在体系、硬件、软件上进行全面的改进，下图展示了金笛安全电子邮件系统的解决方案：



从图中可见，金笛电子邮件系统从十一个方面进行了安全性配置，有效地防止了黑客入侵系统、窃取邮件或传播病毒等攻击行为：

（1）采用具有 C2 级安全的 LINUX 操作系统，保证服务器安全；

（2）先进的邮件服务器软件体系；

（3）采用 DES/MD5/SHA/AES 等多种加密算法对用户密码进行加密，并采用 RSA 对密钥进行加密，保证密码安全，防止密码泄露；

（4）采用金笛虚拟邮件用户，与 LINUX 系统用户分开，降低服务器被入侵的风险；并采用 LDAP 集中式用户身份认证（选配），使全部邮件用户帐号得到安全可靠的管理；

（5）在 SMTP、POP3 和 IMAP4 协议之上应用 SSL，保证数据传输安全，防止内容被窃取；

（6）为 WEB 服务器配置 SSL 支持，保证 WEBMAIL 的使用安全，防止内容被窃取；

（7）采用 PGP 数字签名技术，防止邮件内容被篡改、伪造；

（8）设置 SMTP 转发限制，防止邮件服务器被恶意使用；

（9）兼容硬件加密设备（选配），降低服务器负担，提高数据加密效率；

（10）配置完善的日志跟踪与分析功能，提高对入侵的防范能力；

（11）邮件服务器配置反病毒模块，控制电子邮件病毒的传播。

2. 金笛安全邮件系统

2.1 操作系统安全

金笛电子邮件服务器金笛系统基于 Linux 操作系统平台，Linux 操作系统是吸取了 UNIX 系统长期实践的经验、并采用了现代操作系统的设计理念与设计方案。特别是其开放源代码的开发模式，保证了任何系统漏洞都能被及时发现和改正。因而 Linux 操作系统具有可靠稳定的性能以及相当高的安全性，这已经被众多的独立评测机构所证实。可以说，Linux 操作系统为邮件服务器提供了一个安全、可靠、稳定的运行平台，经过安全性配置之后，黑客利用 Linux 操作系统的漏洞侵入的可能性很小。

2.2 服务器软件安全

传统的电子邮件服务系统如 SENDMAIL 之所以不安全的重要原因是：邮件服务器软件是以管理员帐号（ROOT）运行的后台守护进程，一旦被攻破，黑客就有能够掌握全部服务器资源，所以这是一个非常重大的安全隐患。而金笛电子邮件服务器不用 ROOT 权限，而且也不是以守护进程运行，大大增强了系统的安全性。金笛邮件系统采用清晰的模块化体系结构，各部分均采用成熟安全的代码来实现，使整个系统的安全性得到很大的提高。

2.3 帐号与密码保护

在用户密码保护方面，本系统根据实际需要，为用户配置DES、IDEA、MD5、RMD160 或SHA等加

密模块。DES加密标准是由IBM为美国政府开发的数据加密标准，是使用 64 位密钥的 56 位算法，理论上解密DES需要作 $72*10^{15}$次运算，而改进型的DES算法将有更强的加密强度。国际数据加密算法（IDEA）是现在最安全的算法，由瑞士联邦技术研究所开发，使用 128 位的 64 位算法，但使用反馈算法使该算法强化，通过加密算法，使用户密码在网络传输过程中更加安全，如果没有密钥，即使黑客截获数据包也无法解密用户的密码。对于密钥，由于其重要性，本系统采用RSA算法进行加密。RSA是著名的公钥-私钥加密系统，可使用高达 1024 位的加密密钥，该算法通过使用不同的公钥和私钥，在发送方使用一个公开的密钥（公钥）完成加密过程，在接收方使用一个保密的密钥（私钥）完成解密，公钥和私钥是不同的，这样解密密钥完全不通过网络传输，根本不可能被黑客窃取取，而通过加密密钥来计算出解密密钥也是不可能的，因此RSA的保密程度是相当高的。通过这些加密算法的结合使用，使用户密码得到最可靠的保护。

在用户帐号管理方面，金笛系统采用虚拟邮件用户帐号的管理策略，邮件用户只有权限访问他自己的邮箱，而不可能进入系统访问任何资源，这样，黑客所探测到的用户帐号是毫无用处的。另外，由于采取了 LDAP 集中式认证方式，用户的密码只能由系统在处理登录时获得，而不象系统用户帐号可以随时用简单的方法就能看到。

2.4 邮件内容保密

SMTP、POP3 和 IMAP4 邮件传输协议都是采用明文传送邮件数据而没有加密手段，黑客只需使用一个网络监听设备就可以截取到用户所收发的任何邮件内容。为保证邮件传输安全，金笛邮件系统采用的是 SSL 加密策略。SSL（Secure Socket Layer）是目前获得广泛应用的一个工业标准，Netscape/Internet Explorer/Outlook 等软件产品均支持该标准，它在底层为上层协议提供数据加密服务，对用户是透明的，用户的邮件以加密的形式在网络中传输，即使被黑客窃听也不可能破译出邮件的真实内容。由于 HTTP 协议也是采用明文传送数据，因此用户使用 WEBMAIL 收发邮件也是不安全的，对这个问题，本系统采用 SSL 与安全 HTTP（HTTPS）相结合使用的方式，为 Apache 服务器配置 SSL 模块，负责对 WEB 数据的加密，系统生成的所有 WEB 页面都是经过加密之后才发送到用户的浏览器上，再经过浏览器解密，显示在用户面前。这样，就完全防止了邮件内容在传输过程中被窃取的可能。

2.5 邮件真实性保护

当邮件在网络中传输时，除了有被窃取的危险，还有篡改的可能，即使对于加密的邮件内容，黑客也可以先截取然后将其内容替换成伪造的再发出去。对这种入侵手段，应该采用数字签名技术来阻止。数字

签名技术是数据加密的一种应用形式，用来对发送方和接收方的身份进行认证，它采用公钥-私钥技术，发送方使用私钥进行加密，在接收方使用公钥来确认发送者的身份。现在的数字签名技术包括 DSS（数字签名标准）、SHS（安全 HASH 标准）、MD 系列等，这些数字签名算法根据邮件内容生成一个数字“指纹”，任何两个不同的邮件生成的数字签名都不同的。由于私钥由用户自己保存，因而其它任何人都不可能伪造出发信者本人的签名，这样切实地保证了邮件内容的真实性。金笛系统的数字签名服务为电子邮件提供了第二重保护，用户可根据需要选择 DSS/SHS/MD5 等成熟的数字签名模块。

2.6 SMTP 安全控制

除了 POP3 服务品上的用户帐号和邮件，SMTP 服务器本身也是黑客入侵的目标，一旦进入 SMTP 服务器，就可以将其作为跳板对其它的主机进行攻击。最常见的是利用 SMTP 服务器向外发送垃圾邮件或有毒邮件。对于这种情况，金笛系统可以配置 SMTP RELAY 限制，只有系统内的合法用户才可以使用 SMTP 服务向外发信，并且使用 SMTP 之前必须经过身份认证，否则就不能发信，这样有效地防止了系统外用户对 SMTP 的使用，而系统内部用户的使用情况则全部记录在案。

2.7 日志跟踪与分析

完善的日志跟踪与分析功能是金笛的一大特点，日志系统记录着系统内部的每一个动作，任何邮件用户的登录、收发信件、配置等操作都会被系统记录下来，因而，任何可疑的操作都能从日志中检查出来，例如失败的登录尝试、含有非法字符的操作参数等，金笛的日志系统将有助于管理员及时发现潜在的攻击者、找出可能存在的漏洞、跟踪攻击行为的来源等，是维护系统安全的最好的工具。

2.7.1 邮件监控功能

金笛系统独具有的邮件监控功能能最大化的满足管理者对于邮件使用者的控制，避免因为电子信息的快捷性而造成的企业重要信息损失，政府机关机密泄漏。适合对于信息传递和交流有特定要求控制的单位和行业。邮件监控功能将如实的记录系统内部每一个用户的收发邮件的时间、主题、正文，该功能将有效的提供企业生产效率，并且做到信息记录功能，在出现异常情况的时候有据可查。

2.8 病毒过滤模块

现在已经出现了很多随电子邮件传播的病毒，这些病毒轻的只是干扰用户的通信，重的则会破坏用户

计算机上的数据，最危险的是病毒中包含黑客程序的代码，会在安全的网络环境中制造出漏洞，使黑客能够入侵到用户网络中。因此防止病毒随电子邮件传播也成为邮件服务器一个重要的功能。金笛邮件服务器可以配置高性能的病毒过滤模块，它对每一封收到的邮件进行分析过滤，根据已有的病毒特征知识，判断该邮件是否感染了病毒，如果发现邮件感染了病毒，则会及时通知邮件用户、记录到日志并同时杀病毒。本系统内带有开放的病毒特征库，管理员可随时根据有关资料扩展病毒库，以保证系统能够发现并杀死新发现的病毒。

2.9 硬件加密支持

前面提到的数据加密算法尤其是 RSA、SSL 都非常复杂，为了提高保密程度，一般都采用 128bit 以上的密钥，随着加密强度的提高，服务器在进行加密运算时的负担也越大。不仅如此，由于每种加密算法的不同，服务器计算所需的时间也会不一样，而高明的黑客却能够利用这个时间差异猜测出服务器可能采用的加密算法，因此较长的加密时间也是一个潜在的安全漏洞，为了提高服务器运行效率并且消除潜在的安全漏洞，金笛安全邮件系统在服务器上可以配置硬件加密设备，由硬件直接进行加密运算，而不是通过软件进行运算。这样将大大提高加密效率，降低服务器的负担，并有效地防止了黑客的入侵。

3. 小结

建立一个安全的电子邮件服务系统应该从各个方面进行完善，因为黑客只需找到一个安全漏洞就很有可能控制整个系统。金笛电子邮件系统为用户提供了一个完整的安全邮件解决方案，能够安全、可靠地传送邮件，满足各种用户的需要。