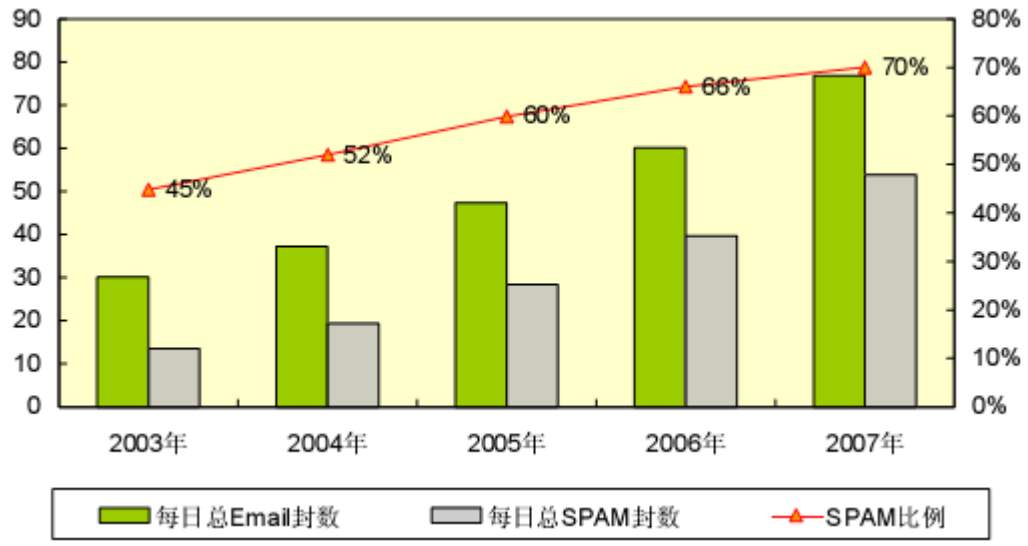
金笛邮件系统反垃圾邮件技术资料

垃圾邮件趋势图



一．金笛邮件网关反垃圾技术

1.关键字过滤
2.基于规则的评分系统
3.贝叶斯数据库
4.黑名单
5.实时黑名单
6.DNS MX 纪录查找
7.反向 DNS 查找
8.新反向查找系统
9.指纹识别技术
10.速率控制
11.意图分析
12.病毒扫描

二．金笛邮件网关反垃圾技术原理

从网路层（TCP/IP）、应用层、内容层拦截圾邮件。

网络层

首先在网络层控制 TCP 连接的数量、频率、合法性、连接时长，通过多重实时黑名单（RBL)拒绝垃圾邮件发送者的连接。管理员可以定义自己的 IP 黑名单，拒绝来自这些 IP 地址的连接。金笛提供了 IP 攻击的报表，以方便管理员决策是否将这些 IP 列入黑名单。管理员还可以定义 IP 地址白名单。对来自这些 IP 地址的邮件不进行垃圾检查，同时仍然执行病毒扫描以及附件的检查。

应用层

金笛在 SMTP 应用层进行五道检查，分别是转发控制、黑白名单、收件人核实、邮件协议与属性检查和邮件路由。

转发控制基于发信者的源 IP 地址和收件人的目的邮件域，金笛仅对指定的邮件域进行转发，可以有效的避免转发。避免用户的邮件服务器被不法机构利用转发垃圾邮件。应用层的黑白名单针对邮件地址的黑白名单，例如：管理员可以把本公司重要客户的发件人地址列入到白名单，这些邮件将不会进行垃圾检查尔快速的通过过滤网关到达用户的邮箱。金笛垃圾邮件网关还具有几项独特的功能，如发件人欺骗保护，这项功能阻止垃圾邮件仿冒用户的邮件域给用户发信。再比如收件人黑白名单功能。如果公司内部使用的一些邮件群不需要接收外部邮件，此时可以将之加入收件人黑名单中，拒绝外部垃圾的骚扰。

金笛网关支持通过 SMTP 或 LDAP 方式对收件人的地址进行核实，避免垃圾邮件者对服务器发动字典攻击、DHA 攻击，避免邮件服务器接收不存在的收件人邮件，从而较少了数据流，减轻了邮件服务器的负担。

邮件路由包括基于邮件域的路由、基于主机地址的路由、流量控制与延时投递，共同保证正常邮件从网关有控制、有保障的转发到后台邮件服务器。在邮件服务器发生故障时，系统将保留邮件 48 小时，从而保证邮件服务器发生故障时用户的重要信息不会丢失。

内容层

内容层是金笛反垃圾产品的核心竞争力，通过邮件指纹技术、意图分析技术、贝叶斯过滤技术、基于规则的评分系统等拦截垃圾邮件，并独创双层病毒扫描引擎对邮件病毒进行高效的扫描。还对附件进行垃圾和病毒扫描。

三．金笛邮件网关采用的技术详述

１．邮件指纹技术

垃圾邮件发送的商业模型是大规模的发出同样的邮件，通常几天或者几周内甚至几个月内发送数以百万计的邮件，这些邮件虽然可能在细微处有所变化，但是通过特定的算法，却可以将这些邮件的共同特征提取出来。这就是指纹技术。为此，依靠特定的算法，将这些邮件的共同特征－－邮件指纹提取出来，邮件指纹库。系统收到邮件后，发送相关的信息到远程的邮件指纹数据库中进行核对，从而迅速的确认这封邮件是否是垃圾邮件。

２．意图分析技术

垃圾邮件技术如今变得愈加复杂，许多垃圾邮件变得与正常的邮件几乎一样，在这些邮件中含有 URL 链接，这个链接往往指向一些不健康的网站，或某个商品促销的网站。金笛为此创建了意图分析技术，它检查邮件中的 URL 链接，确定邮件是否为垃圾邮件。

3．贝叶斯过滤技术

贝叶斯分析：命名于著名数学家托马斯贝叶斯（1702-1761)，他发展了一个数学领域全新的可能性推论理论。贝叶斯分析采用过去事件的知识预测未来事件。应用到反垃圾邮件领

域，贝叶斯过滤与以前收到的垃圾邮件与合法邮件的中相同词语与短语出现的频率对比此邮件中有问题的词语与短语的来确定垃圾邮件的可能性。他能自动适应垃圾邮件变化。是一种动态的智能过滤技术。

贝叶斯过滤器是非常强大的，也是阻断垃圾邮件最为精确的技术。大多数报告显示，当贝叶斯过滤器被“有效培训”以后，过滤器过滤垃圾邮件的准确率达到 90%。为了培训贝叶斯过滤器，需要该收件人大约 200 封有效邮件及 200 封垃圾邮件。在目标收件人中有越多的历史数据库，过滤器越准确。

采用了分用户贝叶斯后，使得不同邮件用户个性化的需求得以真正的实现。一般反垃圾邮件分用户个性化设置仅限于个人黑白名单。无法满足不同用户对邮件的不同偏好，然而用户通过调整培训自己的分用户贝叶斯数据库，就可以简单的实现这一功能。

4．基于规则的评分系统

垃圾邮件制造者清楚反垃圾邮件的原理，其中常用的一种办法经常将一些单词拼错，“Viagra”可能被有意地拼写为“V1agra”或者任何一种可能的变体，这样普通的词语过滤器就无法识别。基于规则的评分系统也被称为人工智能（AI）系统，金笛定义了近 6000 条垃圾邮件规则，每一条规则对应一定的评分，一封邮件与规则库进行比较，每符合一条规则加上该规则评分，获得的分数越高，该邮件是垃圾邮件的可能性就越高。如果一封邮件超过一定得分门槛（阈值），该邮件将被分类为垃圾邮件。在这些规则中，可以用来识别变化的词语或短语，例如垃圾邮件引擎侦测到变化型文字，垃圾邮件引擎会自动回复到原先字词，例如 V.I.A.G.R.A 回复为 VIAGRA。这些规则不仅包括语义分析，还包括对垃圾邮件发送工具的检测、对邮件中含有图片形态和比重的检测，对于 HTML 格式的各种特征的规则等。通过对一封邮件所有相关的信息都进行相关的智能分析，最终能够准确的判定一封邮件。由于垃圾邮件发送人及制造垃圾邮件的程序不是静态的，因此 jdmail 持续追踪互联网上的垃圾邮件的变化，及时更新规则库。采用这项技术，可以清除 90%的收到邮件中的垃圾邮件。金笛还专门定义了中文简体、繁体、日语等规则分库，以适应双字节邮件的过滤。

金笛网关还提供了丰富强大的自定义过滤策略：用户可以对邮件信头、主题、信体设立阻断、隔离、标记、关键字白名单等不同类型的关键字。再所有检查都进行完毕后，根据用户设立的评分策略，对邮件进行允许、标记、隔离、阻断等操作。金笛支持完全的正则表达式，为了方便用户使用，金笛公司提供了不同语种的关键字模版。

5．安全性与易用性

金笛垃圾邮件网关集成在金笛邮件系统平台下，去除了不安全的服务，系统运行稳定。管理员可以指定 IP 访问列表，只有列表中的 IP 才能对系统进行远程的管理。也可以设置 SNMP 和 API 的 IP 访问列表。并可以通过动态对称的加密的 HTTPs 通道进行。

金笛支持通过 LDAP 验证收件人地址的合法性，可以避免 DHA 攻击；若用户邮件系统不支持 LDAP，金笛还可以使用 SMTP 方式进行验证。金笛的速率控制机制能够有效的阻止某个 IP 发动的海量邮件攻击。