



LEON

Anti-Spam Server 2004

Whitepaper

Introduction	4
Where does the term “Spam” come from?.....	4
Why do people send spam?	5
How can I tell whom the spam is from?	5
How do spammers get my email address?	5
How Spammers work	5
How can spam be stopped?.....	7
The Uniwares Solution – Leon – The Anti Spam Server	7
Split-Server Architecture	7
Real-time black-lists.....	7
Internet Black Lists and White Lists.....	8
Trusts.....	8
Distrusts	9
Pass-through Lists.....	9
DNS Lookup	9
Anti-Spoofing	9
Header Analysis.....	9
Strict RFC compliance.....	10
Virtual Black Hole	10
Mail-bombing prevention	10
Directory Harvesting Attacks Prevention.....	10
Subject Analysis.....	11
Spam Profile Database	11
Content Analysis / Lexical Analysis.....	11
Bayesian spam filters	12
Heuristic Analysis	12
Web-beacons, Cookies & Scripts.....	13
TCP information headers	13
Chain verification	13
Sender Verification.....	13
Text Manipulation.....	13
Regular Expressions.....	13
Attachment Filtering	14
URL Classification.....	14

Custom Filters	14
Flexible Targets	14
Language Awareness	14
Multi-Language support	14
Custom Dictionaries.....	14
Restricted Mode	15
Anti-relay.....	15
Tar pitting.....	15
MMC Support.....	15
Windows Performance Counters	15
UNIWARES Service Profile	17
Leon Anti-Spam Server™	17
Spam Filtering.....	17
Policy Enforcement	18
Support & Protection Service Centre	18
About	18

Introduction

Email, being the most frequently used Internet application, is an essential tool for various types of businesses and personal communications. According to IDC in September 2000, email messages sent per year will increase from 9.7 billion in 2000 to 35 billion in 2005. Like any other technological development, the Internet has suffered some rather unpleasant side effects, like unsolicited bulk email (UBE) or unsolicited commercial email (UCE), commonly known as junk email or Spam.

Market Research Company Gartner estimates that a company of 10,000 employees suffers more than US\$ 13 million worth of lost productivity because of internally generated Spam. Add the mail traffic from the Internet and the problem gets a lot worse. "A year, year-and-a-half ago, Spam was an annoyance; now it's a productivity drain," says the Research Director for e-mail and messaging at Gartner. "A lot of the Spam has become quite distasteful, and it's a drain... not just on bandwidth, but on storage." Spam is a subject that affects a wide ambit of the Internet population. System administrators and Internet service providers (ISPs) are the main targets, fighting on a regular basis the defense of their assets and resources and try, many times in vein, to stay one step ahead of the Spammers, whose only interest is to hijack mail servers and computers. In a majority of the cases the efforts made to control such disruptions fail and recovery becomes a rather costly and time-consuming issue. From a Spammer's point of view, the most highly desired targets are those whose email accounts that are used regularly for work and personal reasons. Many of whom are forced into the mundane task of sorting and deleting spam from legitimate mail. The tools and techniques used by Spammers to aid in the delivery of spam are constantly improving, allowing them to update their arsenal with more efficient and productive tools. In addition, the concept of "Internet time", an expression used to describe the growth and rate of change of technology related to the Internet, increase the risks and with the expansion of processing speed and power and the bandwidth of the Internet, the amount of Spam multiplies, keeping pace with the growth creating bottlenecks on networks and mailing systems and taking up valuable storage space. If this situation remains unchecked, the cost will continue to slow down the development of email communication as a powerful tool.

Spam comes in many guises but the two most frequent types of spam received are characterized as "get rich schemes" and "adult or porn." The following breakdown gives an indication of how Spam is used: Get rich quick 37%, Adult 25%, Software offers 18%, Contests 2%, Vacation 1%, Health 2%, Web site promos 6%, Investment 5% and Other 4%.

Where does the term "Spam" come from?

The theory is that the term comes from a classic black comedy sketch by Monty Python's Flying Circus. It did not start with email and the term has its roots, in relation to the Internet, in the late 1980s or early 1990s in Multi-User Dungeons (MUD) and Multi-User Shared Hallucinations (MUSH), which are online, real-time, interactive, text-based virtual environments. It was said that a MUSH user programmed a macro key to type "spam spam spam..." in a MUSH until a SysAdmin terminated his connection. As a result other members referred to this incident as "the !*%@ who spammed us". From MUDs and MUSHes the expression Spam began to be used to describe "Excessive Multi-Posting" (EMP) on Usenet groups. Usenet "news" groups being forums where "authors" can "publish articles" to be read by other users and subsequently be discussed. Under normal circumstances a user would post a message to one or to a small number of newsgroups, asking questions or giving opinions.

By using a posting software to automate the process, it became possible to post the same message to thousands of newsgroups guaranteeing a readership of thousands or in some cases millions.

The very first Spam email was sent on 1st May, 1978 by a Digital Equipment Corp. salespersons advertising a demonstration for a new computer equipment. They attempted to send this email to all of the Arpanet users on the west coast of the US. The reaction from the recipients was very much like what we would expect today. Remember that Arpanet was a military project and commercial use was prohibited. At that time, there was no such thing as an email Spam filter to stop Spam mail because official Spam did not exist. In April 1994, a Phoenix law firm, Canter and Siegel, advertised their services by posting a message to several thousand newsgroups. This could be classed as the first automated large scale commercial use of Spam, and as a result the term became popularized, until then had been exclusively part of the cabalistic vocabulary of Multi-User Dungeons.

Why do people send spam?

People send Spam in hope of selling products and services or to promote an email scam. Some of the Spam is purely ideological presented by ideologists of thought. A large percentage of Spam is intended to draw traffic to web sites or to sell sex and money making schemes. Dissimilar to junk mail in your physical mailbox, Spam does not worry if it is successful or not. When marketing departments send out junk mail at considerable expense, without success, they usually stop, or change their sales pitch. Spam on the other hand can be entirely unsuccessful, but a large numbers of spammers are waiting to guarantee that we will continue to receive lots of it.

How can I tell whom the spam is from?

You cannot. Spam control can become very sophisticated. The more experienced users can look at email “headers” to find the origin of the message but in most cases the spammer will set up a one-time email account specifically to start the spam email shot. When the email shot is finished, the account is closed. Another method is that the spammer will forge headers making it difficult or impossible to trace the origin of the Spam, so finding the original sender will is very often pointless. Spam protection and junk email prevention require measures and policies rather than just finding the culprit.

How do spammers get my email address?

Some companies you may have had dealings with usually sell their mailing lists to third parties, including spammers. Spammers also use “robots” to search the Internet and harvest any email address that they find within their path. If you post to newsgroups you are also at risk of being picked up by spammers and as a result send you junk email.

How Spammers work

Spammers’ create and use a toolbox, which helps manipulate HTML, so that the result seen by the receiver appears to be the intended message from the spammer, while the complicated HTML code within the message is unintelligible to any simple spam filter. Spammers often use multiple tricks in a simultaneous fashion to hide or obscure the intended message. The most commonly used, independently and simultaneously, are as follows:

Black Hole Hides a message by using a size-zero font;

Numbers Game Hides letters by encoding them using “HTML entities,” or numeric

representations intended for sending special characters and non-English alphabets;

Invisible Ink Manipulates font and background colours to make text literally disappear on screen;

Slice and Dice Uses HTML tables to "shred" a message into thin strips.

Content Encoding Uses standard content encoding, often cascading, to further hide the real content. Base64, BinHex and Quoted Printable are the most commonly used.

Daily News Inserting parts of daily news into the text either using Invisible Ink or as separate MIME parts.

How can spam be stopped?

There are many techniques available in the fight against spam; individually none are able to completely eliminate spam without causing problems in the blocking of any legitimate email. However, combining of techniques together, spam can be reduced to at least 95% or even higher and still not block legitimate emails.

The following is a partial list of methods that can be applied to detect, filter or reject Spam:

- Real-Time Black-Hole List (RBL)
- Internal black lists
- Trusts
- Distrusts
- Pass through lists
- DNS Lookup
- Anti Spoofing
- Header Analysis
- Strict RFC compliance
- Virtual Black Hole
- Mail-bombing prevention
- Directory Harvesting Attack Prevention
- Subject Analysis
- SPAM Profile Database
- Content Analysis and Lexical Analysis
- Bayesian spam filters
- Heuristic Analysis
- Web-Beacons, Cookies and Scripts
- TCP Information
- Headers
- Chain Verification
- Sender Verification
- Text Manipulation
- Regular expressions
- Attachment filtering
- URL Classification
- Custom filters
- Flexible Targets
- Language Awareness

The Uniwares Solution – Leon – The Anti Spam Server

Leon incorporates a combination of these techniques mentioned above to combat SPAM and uses the concept of DPR – Detection, Prevention and Retaliation. Leon is built as a proxy mail server and it implements a full RFC 821/1869 compatible SMTP server.

Split-Server Architecture

The split server architecture separates the receiving mail server from the sending server. The receiving server can reside outside the firewalled network only sharing a writeable network drive with the sending server. Thus, the sending server is secure from outside attacks.

Real-time black-lists

RBL means Real-time Black hole list, which has become a generic term for DNS based systems designed to assist in the prevention of email abuse. The RBL consists of a DNS based system containing lists of IP addresses whose owners refuse to help in stopping in the proliferation of spam, this be done by running their mail servers as open relays, or by simply allowing their dialup users free outbound access to port 25. A lot of the anti-spam software programs use these lists to control Spam by refusing any of the emails that originates from one of these particular domains.

In order to discover if a domain is producing Spam, the offence must be reported. Reporting Spam without having any anti-abuse mechanism in place, however, leaves nothing to stop people from getting servers added to a these blacklists out of pure malice. The most obvious solution to the problem would be to require a minimum number of reported incidents to be submitted before blacklisting a server. This proves equally inadequate as a measure to stop Spam mail. Anyone who manages large mailing lists knows that a small percentage of people who subscribe subsequently accuse the sender of spamming them when they receive their email. Naturally, a company that sends out millions of legitimate commercial emails would be accused of Spamming rather than one that sends out a smaller amount of spam free bulk emails.

Black-lists are available on sites such as Spamhaus - <http://www.spamhaus.org>, MAPS - <http://www.mail-abuse.org> RBL (Real-Time Black-hole List), ORDB (Open Relay Database; - <http://www.ordb.org> and others, which contain dynamic IP addresses lists of mail servers that are known to send spam or are hijacked by spammers to relay spam. A complete list of the various Black Lists can be found at: <http://www.decluce.com/junkmail/support/ip4r.htm>. Leon comes with a default set of the most reliable free RBL 1 services. Leon can be configured to use several RBL's at any one time for higher accuracy. Leon users can also subscribe to the Uniwares Ltd to allow for full support of all the requirements.

Internet Black Lists and White Lists

Using blacklists as the only anti-spam tactic is entirely unsatisfactory to help curb the problem. Used as just one data point in a point system, however, blacklists can be helpful. An enterprise can also create a white list, which is the opposite of blacklists, of domains that are always allowed to receive e-mail, no matter what the content is. Simply blocking the sender email address is an inadequate technique due to the fact that spammers use random email addresses, which have existing valid domains names for 'each time they send out new multitudes of spam. However, blocking emails from certain domains that are known to be utilized by spammers can have good results.

Leon offers white list filtering for mail exchangers (MX), senders, mailing lists, single hosts, name servers, countries and recipients. This allows flexible pass-through configuration for any source or target. White listed items are never filtered out and administrators may manually add items to the black/white list filters. Items on these lists are always filtered out, even if they would pass all other filters. Leon provides an automatic update list of domains that are known to be utilized by spammers. Alternatively, Leon provides an email ONLY option to allow in the receipt of emails from assigned domains that a user communicates with on a regular basis.

Trusts

Leon also incorporates the concept of trusted peers. Often you communicate with partners, which are considered trusted. This might be either a single mail address, or a whole domain, or a mail exchanger (MX) or an IP address or address range.

¹ Blacklists are usually maintained by anti-spam organizations or by individuals with an intense dislike for Spam. The difficulty with these blacklists is the need for objectivity in deciding when to blacklist a domain.

Distrusts

Like Trusts, you can also configure certain peers as distrusted. Any mail or even TCP connection from these peers will be completely ignored or rejected.

Pass-through Lists

Mailboxes, domains and mail exchangers can be configured as pass-through items. An administrator can setup Leon to pass-through any mail coming from a certain MX; exclude some mail boxes from filtering; or, for ISP operation, exclude filtering for certain domains.

DNS Lookup

A DNS, which stands for domain name system, lookup is using an Internet domain name to find an IP address, where as a Reverse DNS lookup is using an Internet IP address to find a domain name. When you enter the address for a Web site in your browser the address is transmitted to a nearby router, which does a forward DNS lookup in a routing table to locate the IP address. Forward DNS lookup is the more common lookup since most users think in terms of domain names rather than IP addresses. This technique is able to identify if the sending mail server is legitimate and has a valid host name. This can help eliminate most of spam sent by mail servers connected through an Internet dial-up connection, as well as most ADSL and cable connections, due to the fact that they are not registered to any DNS as a qualified host meaning that they do not have their own static IP and a registered host name like mail.domain.com. There are specifically two methods can be used for DNS lookups:

HELO meaning host name lookup: The receiving server will get the host name of the sending mail server from the SMTP HELO command, perform a simple DNS query and verify that the IP address is indeed the IP address of the incoming connection.

Reverse DNS lookup, is a method that is not a very good as it is time-consuming. The receiving server performs a "reverse DNS lookup" on the IP address of the incoming connection and checks to see if there is a valid registered hostname associated to it. Leon uses HELO, considered to be the more efficient method as its DNS lookup option.

Anti-Spoofing

This security feature is designed to prevent unauthorized access to a network through the technique known as IP spoofing. IP spoofers insert a false sender IP address into an Internet transmission, in order to gain unauthorized access to a computer system and it is usually used to send email messages from outside sources masquerading as internal addresses within the organization. One example would be to send an email to jane@jungle.com masquerading as tarzan@jungle.com. Another example would be to send an email to tarzan@jungle.com masquerading as tarzan@jungle.com, so recipient thinks he is receiving an email from himself. Leon has a complete Anti-spoofing solution, blocking any emails masquerading from anyone within the organization.

Header Analysis

A good anti-spam agent will first analyze the header, looking for characteristics typical of spam messages. Header verification is the process of inspecting the email SMTP header for compliance with standards, making sure that spammers have not forge them. If the header alone gives a sufficient amount of evidence that the message is spam, the message can be "rejected" even before analyzing the body content. The header analysis look for items such as: Validity of the sender (using "reverse lookup").

Consistency between the “sender” and the “from” fields. Tactics used by known spammers that are highly unlikely to be found in normal messages. Leon blocks emails with deformed headers, as well as blocking spam emails according to a configurable identifier lists. Leon supplies an extensive identifiers list of all known spam mailers.

Strict RFC compliance

All communication between a mail server and a client is regulated by certain RFC’s which are the internet standards for various protocols. Leon follows all standards by the letter and thus does not allow for any exceptions. For the client it is not distinguishable which kind of mail server is answering the requests.

Leon also protects and limits the use of certain SMTP commands that are vulnerable or allow an attacker to gain information about the users or mailboxes.

Virtual Black Hole

By enabling the Black Hole functionality of Leon, the server acts as a virtual black hole which consumes all incoming requests but it does not reveal to the client or attacker if the request was successful or not, while still following the requirements of the standards. This helps block mail-digging attacks.

Mail-bombing prevention

Abusers repeatedly sending an email message to a particular address at a specific victim site characterizes the term email bombing. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact. Email bombing/spamming may be combined with email spoofing, which alters the identity of the account sending the email, making it more difficult to determine who actually sent the email.

Anti-bombing can regulate the flow of emails to help prevent an overload that may slow down email servers or cause DoS (Denial of Service). The anti-bombing feature monitors the number of email sessions that are open simultaneously, as well as the total number of email messages within the spool.

By increasing the ration of outgoing sessions to incoming sessions increases the throughput, and vice-versa. This feature enables the increase of tolerance of the mail server significantly to these types of attacks.

The most common bombing technique is the use of emails with a large number of recipients that leverages your SMTP server to multiply the volume that it handles by the number of recipients in each email. In limiting a maximum number of recipients per email allows for an effective blocking of spam and pyramid emails, which contain far more recipients than of any legitimate email.

Leon can be configured for a number of incoming and outgoing coexisting connections, and allows for email size and number of recipients.

Directory Harvesting Attacks Prevention

Leon provides full protection against the technique Directory Harvesting Attack (DHA), which allows spammers to collect valid email addresses from organizations that they wish to target. While a DHA is taking place, spammers will attempt to deliver emails to various addresses, such as janea@jungle.com, janeb@jungle.com, janez@jungle.com, etc, etc.

Those addresses that are not returned as none recognised addresses by the receiving mail server are considered to be valid and are then compiled and sold as part of spam mailing lists.

Subject Analysis

An analysis of the common text in the subject of the email found in most spam messages can be clearly identified and such examples are listed below:

Viagra at ...
Increase your ...
University diploma
Get rich quick
Credit repair
Save money
Make \$\$\$
Win a ...

Leon has a comprehensive updated list of keywords known to be used by spammers within the subject field and in the body text.

Spam Profile Database

Spam database technology extracts spam profiles from received emails and compares it against a database of known spam emails. This is a very powerful technology if implemented in a correct manner, because it has the potential of real-time spam blocking. Polymorphic spam, a spam that is able to modify from time to time, with all the batches sent, or even with every email sent. Spam Profiles are capable of handling these variations.

Spam Profiles are generated from the characteristics of an email and its contents. This means that every email is analyzed thoroughly, by disassembling and rebuilding before its contents are inspected. This is effective in the removal of all known tricks used by spammers who try to hide the content from computational analysis.

Leon implements local and global Spam Profiles. Local Spam Profiles are local to each email server installation and are updated automatically during the analysis and learning process. It is not necessary to maintain or administer the local Spam Profiles.

The global Spam Profiles are a subscription-based service provided by Uniwares Ltd., which updates the Spam Profiles on a permanent basis. As soon as a set of new Spam Profiles is made available at one of the SPS (Spam Profile Server), your server will receive automatically an electronic update.

Content Analysis / Lexical Analysis

This technique should be evaluated against the business goals of the enterprise customer. Content analysis includes one or more of the following capabilities:

A set of rules to search for known spammer tactics and known chain letters, hoaxes, and urban legends. The ability to look for words and phrases in a targeted "words list" (for example, porn, financial services) and the ability to "tune" the product for the environment. Leon is able to utilize predefined rules to analyze textual content in the email

body and classify the content as spam by its context or its content, which is otherwise unwanted.

Leon can also recognize the “Daily News” method, which hides the actual spam content within legitimate texts that are normally not seen by the recipient but usually confuse Spam filters.

Bayesian spam filters

Bayesian spam filters calculate the probability of a message being spam based in its contents. Unlike simple content-based filters, Bayesian spam filtering learns from spam as well as from the good email, resulting in a very robust, adapting and efficient anti-spam approach that returns hardly any false positives.

Heuristic Analysis

Heuristic analysis is employed to identify emails that look like spam based on certain common characteristics, such as mixed foreign character sets, image links which are server queries (with/without a unique recipient ID), mix of different obscure and/or non-printable characters, different encoding methods, etc.

The term heuristics is most often applied to viruses, where the algorithms try to find mutants of previously seen viruses, or new initiatives containing similar malicious behaviors. The term is less precise when applied to spam. The tactics used in these algorithms must be examined carefully.

The most common technique used by spammers to hinder the catching of spam is to automatically add a lot of random junk text or random junk HTML tags that are not visible to the receiver of the email and to confuse products that utilize the extract hash-signatures technique.

Here is an example portion of junk HTML tags embedded in spam email:

```
Ou<chessa>r US Lic<schoolteacherd>ensed Doct<castore>ors will<BR>
Pr<actsp>escribe Y<globulet>our Me<resta>dication F<abstaing>or
Fr<binuclearh>eePhen<convulsiong>termine, Ad<orlandoj>ipex, So<effiek>ma,
Fior<busboyb>icet, Ultr<infusiong>am,<BR> Celebr<geometerb>ex, Via<repeld>gra,
Val<buschv>trex, Zy<paramagneticv>ban, and man<grayishv>y, man<beckx>y
othe<libertarianb>rs.<BR> <B>Me<incredulousb>ds fo<redwoodc>r:
</B>We<deputyb>ight Lo<cavitatec>ss, Pa<anglophobiap>in Rel<floridav>ief,
Mus<shaveb>cle Pa<activationn>in Re<sapm>lief, wome<noneq>n's Hea<seymourw>lth,
Me<presbyteryz>n's<BR>
```

When the HTML comment tags are removed, the message is:

```
Our US Licensed Doctors will Prescribe Your Medication For Free Phentermine,
Adipex, Soma, Fioricet, Ultram, Celebrex, Viagra, Valtrex, Zyban, and many,
many others. Meds for: Weight Loss, Pain Relief, Muscle Pain Relief, women's
Health, Men's
```

Leon’s heuristic analysis identifies many common characteristics within spam, and then blocking such emails. As well as, identifying various spam characteristics.

Web-beacons, Cookies & Scripts

Web-beacons, also known as a *Web bug* or a *clear GIF*, used in combination with cookies, a *Web beacon* is an often-transparent graphic image, usually as small as 1 pixel x 1 pixel, which is placed on a Web site or in an e-mail that is used to monitor the behavior of a user visiting a Web site or sending a e-mail. When the HTML code for the Web beacon points to a site to retrieve the image, at the same time it can pass on information such as the IP address of the computer that retrieved the image, the time the Web beacon was viewed and for how long, the type of browser that retrieved the image and previously set cookie values.

Web beacons are used by third-parties to monitor the activity of a site. A Web beacon is detected by viewing the source code of a Web page and looking for any IMG tags that load from a different server. Turning off the browser's acceptance of cookies will prevent Web beacons from tracking the user's activity. The Web beacon will still account as an anonymous visit, but the user's unique information will not be copied.

Web beacons is a very powerful tool in the hands of the more sophisticated type of spammer that is able to identify "live" email addresses and intensify the sending of spam to these particular addresses.

Once an email arrives in the user's Inbox that contains a web-beacon, it is usually displayed in the preview panel on the screen. Leon is capable of blocking emails with web beacons as well as completely removing all scripts, cookies and other dangerous HTML commands from incoming emails.

TCP information headers

All incoming mail is extended with full connection information about the senders TCP connection. IP address, resolved host name, claimed host name, port and protocol are logged.

Chain verification

Leon checks Mail headers for RFC compliance and MX chain correctness. Non-compliant mails or MX chains, which fail verification, can be filtered.

Sender Verification

Verifies the identity of a TCP connection during initial communication. Connections from either blacklisted senders or senders with false or spoofed information can be blocked.

Text Manipulation

Most spam messages utilize tricks to difficult the use of anti-spam tools to textually analyze its content. The technique of Text manipulation is to replace certain characters within a spam text with characters that are similar in appearance, like `\/\` arez using Slash and backslash used to form the letter W, separating the characters making it difficult to analyze the whole word such as `V*I*A*G*R*A` , using symbols that are similar in sound, a letter or a number to replace words and parts of words, for example 4U instead of "for you", W1N the one substituting "i" and PoRN the zero replacing "O".

Regular Expressions

Leon allows the inclusion of additional Regular Expression filters allow filtering of other elements, which are configured by the administrator. This allows exclusion mails containing certain keywords, phrases or patterns.

Attachment Filtering

Leon allows Mail attachments to be filtered by type and/or size.

URL Classification

Literally all spam messages contain a URL link. Besides visible links such as “Click here for more information”, or an image link, many contain dynamically downloaded content like images text and advertisements, only visible on the opening of the email.

Checking against a database of known classified URLs all the URL links can achieve accurate results. Moreover, this technology can help deliver a nearly false positives zero rate.

In addition to the known spam URLs category, Leon users can select additional URL categories, which could be warranted as unacceptable, inappropriate, illegal, or unproductive like pornography, racism, hacking, criminal acts, hard drugs, etc, etc.

The Leon URL database is automatically updated 24 hours a day with an interval on average of 10 minutes.

Nameserver

Custom Filters

At almost any stage of filtering, Leon allows the administrator to add custom filters. These custom filters are generally RegEx (Regular Expressions) based.

Flexible Targets

Filtered mail may trigger customizable actions, can be forwarded to certain mailboxes, be dropped automatically or can be quarantined until administrative action is taken.

Language Awareness

During the analysis process, the language of a mail is determined. With this information, Leon is capable of applying the proper filters for each language. This also allows you to filter differently for every supported language or even completely block certain languages.

Multi-Language support

Leon contains full support for currently six languages (English, Portuguese, French, Italian, Spanish and German) through separate dictionaries and language specific Spam filters.

Custom Dictionaries

For even tighter integration with your organization, Leon uses support custom dictionaries for various business branches. Often Anti-Spam solutions fail for certain businesses because their every-day mail contains expressions and words also used in spam mail.

One good example is the banking branch where it is part of the daily correspondence to talk about loans, mortgage and interest rates but also 27% of the current spam contains the same words. Our custom dictionaries allow your daily mail to pass while blocking spam mail.

Restricted Mode

Leon can be configured into a restricted mode. It will then only answer requests from configured hosts. This is useful for gateway operation or in closed environments.

Anti-relay

An increasing number of "spammers" are exploiting open mail relays to disguise the true source of the junk mail they send. Anti-relay systems protect mail servers from possible hijackings, which would be used to broadcast unsolicited emails. Leon provides an anti-relay option that block all emails to recipients that are not part of the organization.

Tar pitting

Tar pitting enables delaying communication with sender who flood or otherwise misuse the SMTP service. A delayed connection will respond only closely within the timeout limits defined by the RFC's and thus slowing down the sender by a factor up to 50 times.

MMC Support

All configurations are performed through Microsoft Management Console (MMC) snap-ins. This reduces administration costs.

Windows Performance Counters

Using standard Windows mechanisms for performance measuring, Leon does allow easy integration into standard management tools. Performance counters reflect mail system activity and mail filtering performance.

Spam Catchers: The Leon Spam Analysis Resource

Spam Catchers, as the name suggests, are basically anonymous email boxes located on various mail servers that are utilized to attract spam, catch it and use it to increase the hash-signature database with real-time samples of spam email. Spam Catcher email addresses are exposed throughout the Internet where spammers are able to harvest the email addresses for their mailing lists.

About False Positives

There is a great fear that an anti-spam agent will falsely identify valuable business messages as spam and delay their delivery, creating situations with recipients that could be regarded as uncomfortable. Here is an example:

A reporter sent an announcement about a friend's wedding to about 100 of his friends who worked in various companies. The message was full of excitement and CAPITAL LETTERS and, to give emphasis, lots of exclamation marks, as well as an invitation to chip in with money as a contribution for the happy couple. This message was identified as being spam by tools installed at nearly half the companies that it was sent to.

This type of misunderstanding is a typical problem that is encountered when using a poor spam control tool. They usually stop only between 20 to 30 percent of the spam, and catch too many false positives.

UNIWARES Service Profile

Companies depend on the continuous flow of information within their organizations, with their clients and with the outside world. E-mail systems are now a critical part of this information flow, making businesses more and more dependent on e-mails as their main source of communication.

UNIWARES is a provider of email security and message management services. Our proprietary solution Leon Anti-Spam Server™ Management Service is built as a split architecture server that allows the service to be performed outside the firewall of a corporation, which is designed to meet the needs of enterprises of all sizes and not put at risk its existing security policy. Leon™ follows our proprietary methodology DPR™ – Detection, Prevention and Retaliation, which helps increase the level of security but adding the benefit of retaliating to any constant attack via specific servers located anywhere within the world.

UNIWARES services provide advantages and benefits:

- The control of Spam without losing legitimate business email;
- Economize on the consumption of the bandwidth;
- Reduction on administration costs of the corporate network;
- Gain with employee productivity;
- The reduction from the threat of DoS, viruses, malicious code and spy wares;
- Policy enforcement, policy adherence and regulatory compliance;
- Control of Content – monitoring the type of content that is appropriate;
- Retaliation against constant attacks from open servers;
- Enhance and improve the level of existing security system and policy.

UNIWARES provides an email security management service for enterprises, which uses its proprietary solution Leon Anti-Spam Server™ Management Service, to help companies manage the inbound flow of e-mail passing through their network gateways by providing a front line of defence. Leon Anti-Spam Server™ Management Service safeguards networks and corporate e-mail systems from the deluge of unsolicited commercial email (spam) and assaults on enterprise email servers via Denial of service attacks, viruses, malicious codes and spywares. In addition, Leon's split-server architecture ensures that in case of a successful attack of the receiving SMTP server, the corporate network is not compromised, hijacked or otherwise misused to send unsolicited bulk email (UBE), in return the service helps provide a higher level of security and protection that is robust and sustainable.

Leon Anti-Spam Server™

provides a comprehensive message management service for businesses of all sizes:

Spam Filtering

Our proprietary, anti-spam split-server architecture technology Leon™ ensures that unsolicited emails are automatically filtered before even passing through the firewall and entering the client's corporate network.

Policy Enforcement

Policy rules are easily enforced through customer-defined rules at the domain level for incoming email, ensuring that the flow of message communication complies with company rules. Clients have the ability to block messages and attachments by name/type; file size; number of recipients; domain; email address; and words and phrases.

Support & Protection Service Centre

All customers receive a set of standard support services with their Uniwares Annual subscription.

Support Incidents	Unlimited
24x7x365 Spam Profile and Rule Delivery	YES
Online Centre	
Maintenance updates and product upgrades	YES
Knowledge Base	YES
Product Documentation	YES
Product News and Updates	YES
Response Centre	
Named Contact(s) at Customer Site	5
24x7x365 Support access via phone and web	YES
Critical problem alerts, including security alerts	YES
Emergency Onsite Support Coverage Limits (Where trained VAR permits)	
Account Management Centre	
Support Usage Reports	YES
Support Account planning and quarterly reviews	YES
Migration assessment and patch management planning	YES
Semi-annual onsite audit and performance tuning	YES

UNIWARES service is designed to provide the best solution for enterprises. With our comprehensive policy management, spam filtering techniques and support & protection centre, we are able to ensure the integrity of your messaging infrastructure.

About

UNIWARES is an information technology company dedicated to the design, development and marketing of advanced core quality software products and added-value solution services in the area of Information, Internet and networks security. UNIWARES develops

and uses advanced cutting edge technology, offering superior quality services and advantages for organizations that strive to achieve a solution that is continuous and sustainable.