ciphertrust.com

JUNE 2004

Controlling Spam

The IronMail® Way

CipherTrust®
Peace of Mind in Messaging™

This document is PROPRIETARY and CONFIDENTIAL. Do not distribute without permission from CipherTrust.

Introduction

E-mail, the Internet's first killer application, is an essential element of business today, providing convenient, time-saving communication with co-workers, partners and customers. Anything that threatens the integrity, reliability and performance of e-mail has a profound impact on business operations. Spam is currently the biggest e-mail threat, and enterprises must take action to protect their e-mail systems.

Spam is defined as unsolicited commercial e-mail and is a powerful advertising channel for many companies.

This white paper examines the major components of CipherTrust's IronMail anti-spam solution. The reader will gain a better understanding of the spam epidemic, learn specific actions they can take to manage spam and its related threats, and understand the technologies IronMail employs to accurately detect and combat spam. This paper also introduces CipherTrust Threat Response Updates, an integrated service that provides real-time updates, signatures and policies to maintain the highest level of spam blocking effectiveness. Finally, the paper explains the importance of a comprehensive e-mail security and anti-spam solution implemented at the network boundary.

From Nuisance to Threat

Once considered only a minor nuisance, spam has emerged as one of the greatest Information Technology (IT) issues for enterprises today. From the minute users log onto their e-mail system, they encounter a deluge of unwanted e-mail that flows into their mailboxes all hours of the day and night. The exponential growth of spam, combined with increasingly sophisticated security attacks delivered via e-mail, makes deploying an anti-spam solution one of IT's top priorities.

"Fifty-seven million U.S. adults think they have received a phishing e-mail. More than 1.4 million users have suffered from identity theft fraud, costing banks and card issuers $1.2 billion in direct losses in the past year."

Gartner Research

A Growing Commercial Industry

Spam is commonly defined as unsolicited commercial e-mail and is a powerful advertising channel for many products and services. This has resulted in an overwhelming volume of unwanted messages into personal and enterprise e-mail boxes. Spamming is a profitable business, driven by the low cost of sending e-mail compared to other direct marketing techniques.

The Economics of Spam and Phishing

The cost to send a piece of spam is negligible:

	Cost per person	Breakeven for a $20 item
Direct mail:	$1.39	1 in 14
Spam:	$0.0004	1 in 50,000

- In 2003, the cost of spam exceeded $10 billion for corporate organizations (Source: Ferris Research).
- Phishing attacks have increased by 4000% during the six month period of November 2003 to May 2004 (Source: the Anti-Phishing Working Group).

Spam Threats

Spam presents three major threats:

- Overwhelming message volume
- Phishing
- Spoofing.

Spam has increased from under 20% of corporate e-mail in 2002 to over 80% in 2004.

CipherTrust Research

Overwhelming Message Volume

Most organizations experience extremely high volume of spam. According to CipherTrust Research, spam has increased from under 20% of corporate e-mail in 2002 to over 80% in 2004. This impacts e-mail and network availability, worker productivity and liability for offensive material.

The recent onset of fraudulent spam variants such as phishing and spoofing pose an even greater risk.

Phishing

Phishing is a specific type of spam message that solicits personal information from the recipient, such as social security, credit card and bank account numbers.

Spoofing

Spoofing is a deceptive form of spam that hides the domain of the spammer or the spam's origination point. Spammers often hijack the domains of well-known businesses or government entities to enhance the validity to their commercial message or scam.

An example of spoofing is an e-mail that appears to come from a known e-mail address that requests a credit card number to confirm the order of goods.

The combination of spoofing and phishing presents a major threat that can trick most anyone into providing personal information to a spammer.

Spam forces enterprises to spend an average of $49 per e-mail user per year to handle the load caused by overwhelming spam volume.

The Radicati Group

The Cost of Spam

With the volume and threat of spam on the rise, the business costs of spam have increased dramatically. The sheer volume of spam pouring into enterprise e-mail systems has required enterprises to increase the capacity of their e-mail systems with costly network and infrastructure investments to keep pace. An August 2003 study from the Radicati Group reported that spam forces enterprises to spend an average of $49 per e-mail user per year to handle the load.

Spam drains employee productivity as workers waste time reading, deleting or even responding to spam e-mails. Additionally, the sexually explicit nature of many spam messages poses potential liability for enterprises.

The IronMail Solution

CipherTrust's IronMail anti-spam solution protects the e-mail systems of the world's most respected organizations. Key features include:

- Effective and accurate spam blocking
- Continuous effectiveness over time against new spamming techniques and threats
- Enterprise scalability
- Integration within an overall e-mail security architecture.

"A 'cocktail' approach is best, whereby multiple techniques are used to combat spam."

Meta Group

Effective and Accurate

Although it takes a person only a moment to process a message and identify it as spam, it is difficult to automate that human process because no single message characteristic consistently identifies spam. In fact, there are hundreds of different message characteristics that may indicate an e-mail is spam, and an effective anti-spam solution must be capable of employing multiple spam detection techniques.

In addition to effectively identifying spam, enterprises must be assured legitimate mail is not blocked in error. Even one false positive, or incorrectly blocked e-mail, can have a significant impact on businesses today. Accurate spam blocking requires a combination of tools to examine various message criteria combined with real-time research and intelligence data.

By aggregating multiple spam detection technologies, IronMail combines the benefits of each individual technique while minimizing the drawbacks. The key to IronMail's effectives is the patent-pending Spam Profiler™.

By correlating the results of multiple detection techniques IronMail's industry-leading Spam Profiler leverages the strength of each spam detection method to provide the highest level of detection.

Genetic Optimization identifies the best possible combination of values for all characteristics examined by the Spam Profiler and automatically tunes the IronMail appliance.

The Spam Profiler

Working alone, each individual spam-blocking technique works with varying degrees of effectiveness and is susceptible to a certain number of false positives. IronMail provides a highly accurate solution by correlating the results of proven first-generation techniques with its industry-leading correlation engine, the Spam Profiler.

The core of IronMail's spam fighting capabilities, the Spam Profiler analyzes, inspects and scores e-mail on over one thousand different message characteristics. Each method is weighted based on historical accuracy rates and analysis by CipherTrust's experienced research team.

Genetic Optimization™

Optimizing the Spam Profiler requires precise calibration and testing thousands of combinations of values associated with various message characteristics. To automate this process, CipherTrust developed Genetic Optimization, an advanced analysis technique that replicates cutting-edge DNA matching models. Genetic Optimization identifies the best possible combination of values for all characteristics examined by the Spam Profiler and automatically tunes the IronMail appliance, reducing administrator intervention and assuring optimum protection against spam and spam-born threats.

Techniques for Identifying Spam

IronMail's anti-spam technologies are grouped into six categories:

- Connection analysis
- Lexical analysis
- Protocol analysis
- Authentication protocols
- Traffic pattern analysis
- Auto learning.

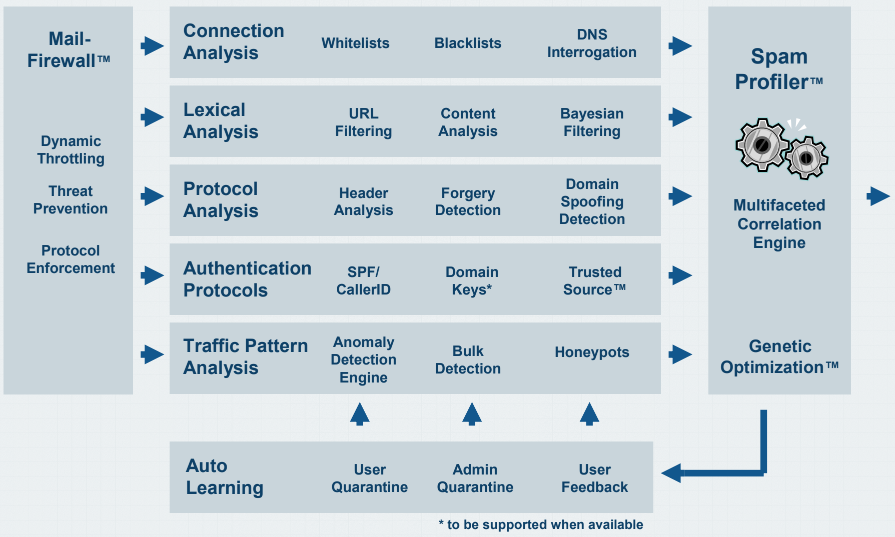
Connection Analysis

- Connection analysis identifies where the message is going and where it came from. IronMail's transit analysis includes blacklists, whitelists and Domain Name System (DNS) interrogation.
- IronMail queries a variety of blacklists containing domain names and IP addresses from known spammers.
- Whitelists specifically exempt senders and recipients from spam filtering. Particularly useful in the case of trusted business partners and contacts, whitelists use e-mail addresses, domain names and IP addresses of users who are exempt from filtering, which reduces false positives.
- IronMail's automated whitelist functionality provides a maintenance-free approach where legitimate e-mail addresses are automatically white-listed once the recipient has received e-mail from that sender a designated number times.
- DNS interrogation authenticates incoming connections to identify spam from hijacked e-mail servers. IronMail can be configured to deny connections for spammers if reverse DNS lookup fails to authenticate the domain of an incoming connection.

"CipherTrust's IronMail solution has been developed to provide such organisations with the protection that they need to ensure that incoming and outbound e-mail communications can be undertaken without being adversely affected by unwelcome third-party influences."

Butler Group

IronMail's Spam Detection Technologies



IronMail allows administrators to easily configure words and phrases and manage them in dictionaries, which are regularly updated by CipherTrust Research via Threat Response Updates (TRU).

Lexical Analysis

- Lexical analysis processes message content to identify spam. IronMail's lexical analysis is based on a combination of URL filtering, content filtering and Bayesian filtering.
- CipherTrust Research has identified thousands of URLs used in spam. These URLs are critical to spammers as they lead to a site where end-users purchase the spammer's product.
- IronMail allows administrators to easily configure words and phrases and manage them in dictionaries, which are regularly updated by CipherTrust Research via Threat Response Updates (TRU). IronMail contains a default anti-spam dictionary, as well as dictionaries targeted at confidential, malicious and pornographic content, and administrators may add, delete or edit this list as desired.
- Bayesian filtering creates evolving dictionaries which rate hundreds of thousands of words by their probability of being in a spam message.

Protocol Analysis

Protocol analysis identifies spam by recognizing abuse of or deviation from e-mail protocols. IronMail's protocol analysis is based on forgery detection, header analysis and domain spoofing detection.

- IronMail identifies message forgeries by analyzing the connection with a set of heuristic tests to mail headers, including:

  - Signatures of spam-generating software
  - Violation of e-mail protocols
  - Reverse DNS lookups
  - Invalid dates
  - Forged e-mail addresses.
- Header analysis analyzes custom fields generated by mail servers, particularly bulk mail engines, and gives administrators the ability to monitor and control custom fields used within an organization.
- Domain spoofing allows an enterprise to block messages that originate externally but report the messages originate from an internal domain. The accuracy of the technique is supplemented with the identification of approved relay servers.

TrustedSource allows IronMail to achieve the highest level of accuracy in determining valid e-mail and virtually eliminates false positives.

Authentication Protocols

Authentication protocols enhance IronMail's effectiveness by identifying legitimate e-mail by applying cutting-edge techniques, including CipherTrust's TrustedSource™ reputation lists and the Sender Policy Framework (SPF) sender identification standard.

TrustedSource is a DNS list of IP addresses created and maintained by CipherTrust. It is dynamically updated based on data received from the more than 7 million enterprise e-mail boxes protected by IronMail. CipherTrust Research uses proprietary analysis tools to determine IP addresses that demonstrate legitimate e-mail behavior and adds them to the TrustedSource database, which is available through the Threat Response System. TrustedSource allows IronMail to achieve the highest level of accuracy in determining valid e-mail and virtually eliminates false positives.

IronMail is the first product to offer support for the SPF protocol for legitimate, non-spamming e-mailers to validate their e-mail senders and prevent forgery.

IronMail is the first product to offer support for the SPF protocol for legitimate, non-spamming e-mailers to validate their e-mail senders and prevent forgery. SPF, which has now merged with Microsoft's CallerID protocol, protects end users from phishing, spam and viruses. With legitimate e-mailers designating a whitelist of their domains and IP addresses, IronMail's SPF/CallerID analyzes each e-mail on the correlation of the sender's IP address and claimed domain. IronMail recognizes the forged spam when these two essential elements do not match up.

IronMail now supports additional evolving standards for identifying valid e-mails, including the Domain Keys system utilized by Yahoo!

Traffic Pattern Analysis

Traffic pattern analysis evaluates message traffic and identifies patterns of behavior that indicate spamming activity. IronMail's traffic pattern analysis relies upon:

- CipherTrust's patented Anomaly Detection Engine (ADE) identifies patterns of spam and virus and worm propagation by monitoring mail flow behavior and observing anomalous or abnormal activity. This approach is particularly useful in protecting against spam-based denial of service attacks or spam-floods.

- Bulk Mail Detection monitors messages received by a large number of users around the world.
- Honey Pots identify spam messages delivered to fake or hidden e-mail addresses.

The combination of the Spam Profiler and IronMail's multi-faceted detection tools delivers the industry's highest detection rates and unparalleled accuracy.

Auto-learning

Auto-learning enables IronMail to continuously improve accuracy and eliminate false positives by learning from the users and the environment in which it operates. CipherTrust's patented adaptive learning algorithm enhances IronMail's effectiveness by analyzing selected end-user quarantines and adapting based on how the user handles quarantined messages.

Evolving to Meet New Threats

The combination of the Spam Profiler and IronMail's multi-faceted detection tools delivers the industry's highest detection rates and unparalleled accuracy. However, e-mail threats are ever changing, especially those generated by the highly profitable spam industry.

To insure IronMail's continued effectiveness, CipherTrust maintains a world class research and development organization.

CipherTrust Research & the IronMail Global Network

Over 1000 enterprise customers, including more than 30 percent of the Fortune 100, rely on IronMail's anti-spam and e-mail security solution. With over 7 million enterprise e-mail users, IronMail protects more e-mail users than any other enterprise solution on the market.

By pooling the latest e-mail trends and threats from its diverse customer base, CipherTrust has a world-view of enterprise e-mail traffic and behavior that benefits all IronMail users.

By pooling the latest e-mail trends and threats from its diverse customer base, CipherTrust has a world-view of enterprise e-mail traffic and behavior that benefits all IronMail users. As a new threat is identified on one network, all other systems are updated in real-time to protect against the threat.

CipherTrust also monitors other sources for information on emerging threats, ranging from open source projects that identify spam to leading industry groups such as the Anti-Spam Research Group of the Internet Research Task Force (IRTF).

This combination of an enterprise network effect and outside sources allows IronMail to identify new spam threats and e-mail variations the instant they hit the Internet.

Threat Response Updates

CipherTrust has created a renowned spam and e-mail security research lab by collecting information from IronMail deployments worldwide. Customers rely on CipherTrust's efficient Threat Response Update system to respond to threats in real-time.

The Threat Response Update system provides a constant stream of information to IronMail units in the field. Updates range from real-time policies and signatures to Genetic Optimization settings for the Spam Profiler. TRU updates ensure IronMail's continuous accuracy and effectiveness.

Built for the Enterprise

A complete anti-spam solution, IronMail is built for enterprise-class networks. Key enterprise features include:

- Low administration
- Spam traps and honey pots
- Enterprise spam-blocking actions, such as end-user quarantine and administrator quarantine.

When combined with the automatic updates through the Threat Response Update service, IronMail provides maintenance-free spam protection.

Zero Administration

IronMail is a zero-administration anti-spam solution. Through continuous automatic tuning and adaptive learning from user-accepted behavior, IronMail eliminates the need for e-mail administrators to become anti-spam experts. When combined with the automatic updates through the Threat Response Update service, IronMail provides maintenance-free spam protection.

Adaptive Learning

IronMail's adaptive learning systems allow an administrator to create fake e-mail addresses, or Honey Pots, not associated with an actual employee for the specific purpose of spam collection. Spam sent to this address is automatically added to the Bayesian spam pool. Honey Pots allow IronMail to maintain and improve effectiveness over time without administrator intervention.

Enterprise Spam-Blocking Actions

After identifying spam messages, IronMail provides nine available actions for spam disposal. Available actions include:

- Dropping the message
- Sending a blind copy (for example, to the HR or legal department)
- Rerouting the message
- Attaching a spam prefix to the subject of the message
- Five different forms of quarantine.

IronMail can label spam by modifying the message subject line, allowing end users to create their own personal policies for spam in their e-mail clients with rules that delete the message or send spam to specific folders.

IronMail enables end-user spam reporting to proactively protect against spam while minimizing or eliminating administrative overhead.

IronMail's end-user quarantine allows designated users to receive regular updates of quarantined messages. If a message has been incorrectly quarantined, the end user can release the message and IronMail will utilize the localized Bayesian systems to learn the marked message was legitimate.

For administrators, end-user quarantine eliminates the need to review quarantine queues for possible lost mail and to construct rules and policies in response to user feedback. They can select which users or groups of users need access to the user quarantine and which do not. All of this is accomplished without allowing suspect e-mail to pass through the gateway until it has been released by the user. Administrators can access the quarantine queue through a secure browser-based interface.

IronMail enables end-user spam reporting to proactively protect against spam while minimizing or eliminating administrative overhead. Many ISPs and enterprises provide a designated e-mail address for users to report spam messages, such as spamabuse@example.org, mail administrators are typically responsible for examining the messages and developing a rule to respond. This overhead usually results in ineffective spam management or hiring a dedicated staff.

IronMail's automated spam-abuse management technology eliminates this burden. IronMail accepts messages users forward to the designated "send spam" e-mail address and automatically process the messages to extract key identification characteristics. IronMail provides feedback to the Bayesian engine as it creates and enforces a new policy rule that blocks, quarantines or labels any future messages from this spammer based on the e-mail address, subject or IP address.

CipherTrust believes anti-spam is only one component of a complete enterprise e-mail security architecture.

Comprehensive E-mail Security

CipherTrust believes anti-spam is only one component of a complete enterprise e-mail security architecture. IronMail not only identifies and blocks spam, including phishing and spoofing messages, but also provides a complete solution to protect enterprise e-mail systems from other threats including denial-of-service attacks, intrusions and Web mail attacks.

Denial-of-Service Attacks

Enterprise networks are often the target of denial-of-service attacks for recreational hackers or malicious network intrusion. For corporations, denial-of-service attacks can result in lack of availability and compromised integrity of mail servers.

Denial-of-service attacks flood a mail server with more SMTP connections or SMTP instructions than the server can handle. Many mail servers and MTAs collapse under such attacks, by either crashing or allowing themselves to receive and execute unexpected commands, which are likely malicious in nature.

IronMail protects enterprise e-mail systems from denial-of-service attacks by scrutinizing inbound Internet e-mail packages for threats and managing overall volume. Using techniques such as dynamic throttling, IronMail can monitor and control inbound mail flow to prevent attacks from impacting mail server operation.

IronMail can prevent threats from impacting systems by detecting and blocking malicious code, unauthorized connections and other known attacks.

Intrusions

Intrusion occurs when unauthorized users gain access to an organization's infrastructure. As it relates to spam, this typically means that spammers break in to a mail server to send spam (mail relay) or harvest e-mail addresses. In some cases, spammers will also plant computer code on an organization's personal computers, which in turn become spam machines or "drones." Recent worms, such as MyDoom, Sobig and Swen are just a few examples of this technique in action.

Hackers and spammers gain access to systems by taking advantage of known weaknesses in an application's code. For example, hackers may open a legitimate communication channel with a Sendmail MTA by sending what at first looks like a legitimate e-mail. However, instead of sending a legitimate e-mail, the hacker sends malicious instructions that target weaknesses in Sendmail. The Sendmail MTA then runs the hacker's program, which can take control over Sendmail and instruct the MTA to redirect all mail to the hacker instead of the original recipients or send confidential files to a hijacked server. These actions have impact on the confidentiality and integrity of e-mail.

IronMail detects attacks such as malicious code and buffer overflows to protect the e-mail system. IronMail can prevent threats from impacting systems by detecting and blocking malicious code, unauthorized connections and other known attacks. Protocol enforcement is used by IronMail to identify new potential threats and disarm them before they can do damage.

By acting as a secure gateway; IronMail protects the entire e-mail system from all e-mail threats.

Web Mail Attacks

Web mail provides another common point of intrusion to e-mail systems. Many organizations today allow their mobile workers to access corporate e-mail through a Web browser by using Outlook Web Access (OWA) or iNotes. Web mail requires a Web server such as Microsoft's Internet Information Services (IIS), which is subject to numerous vulnerabilities, blended threats, viruses and worms.

IronMail provides a secure platform to protect Web mail. As a hardened e-mail appliance, IronMail acts as an application-specific firewall and allows only valid and safe connections to mail servers. IronMail is designed to block all manner of e-mail attacks, including buffer overflow, denial of service and exploits such as malformed MIME headers directed at internal servers. By acting as a secure gateway, IronMail protects the entire e-mail system from all e-mail threats.

Summary

Controlling spam is a critical requirement for enterprises today. IronMail's correlation engine, the Spam Profiler, ensures highly effective and accurate spam blocking. IronMail provides a comprehensive solution for e-mail security, encompassing hackers, intruders, policy and compliance, and viruses and worms, as well as spam. CipherTrust's research team and Threat Response Updates ensure that IronMail continues to protect against spam and other threats to ensure continuous effectiveness over time. IronMail's robust administration, and Genetic Optimization capabilities ensure administrators win the battle against spam.