



**“If at first you don’t succeed try and try again.”**  
**Words of wisdom when parenting a child; the modus operandi of the modern spammer.**  
**This paper examines the most effective technology for eliminating spam**  
**and discusses the shortcomings of existing approaches.**

## **SENDER ADDRESS VERIFICATION: SOLVING THE SPAM CRISIS**

Remember when you first “got mail?” Exciting wasn’t it...always seeing if one of your friends or family members sent you an animated electronic greeting or the newest joke. By the mid-nineties, email was living up to its promise as the greatest communication medium since the telephone. In the workplace email quickly became the communication vehicle of choice, enhancing worker productivity and facilitating the first globally distributed organizations.

Then came spam...

Seemingly overnight, email inboxes were inundated with solicitations to “meet singles in your area” and “refinance your home.” Subject headers read like inner city billboards. The once enjoyable act of checking email became infuriating for some, embarrassing for many and inconvenient for all. For the first time since the dawn of the Internet, email servers fell victim to the constant barrage of unknown peddlers. This year, companies will suffer billions of dollars in lost productivity because of spam.

Many feel that today’s anti-spam solutions have stemmed the tide. There are many companies in the spam-fighting business and most, if not all, claim to be hugely successful. Yet spam is *exponentially* more prevalent today than it was just 2 years ago. How can one conclude that today’s anti-spam solutions are working? This year spammers will use machine-generated programs to send *trillions* of unsolicited emails.

Thankfully, a new anti-spam technology has made its way into the market. This approach, known as Sender Address Verification or SAV, is poised to cripple spammer’s ability to deliver machine-generated email. SAV employs a patented methodology that asks a sender to verify their email address before a message is forwarded to a recipient’s inbox. SAV is easy to set up and provides tremendous value to both IT and business users. Most importantly, SAV eliminates 100% of spam and produces zero false positives. We will discuss more on SAV later in this paper.

### **THE WEAPONS OF A SPAMMER:**

#### **ANONYMITY, AUTOMATION, AND AN ARMS RACE MENTALITY**

There are 3 primary reasons why the problem of spam has exploded:

- 1) *Anonymity*: Creation of bogus, untraceable email accounts and domains from which to send spam, thereby preventing a “paper trail.”
- 2) *Automation*: Utilization of machines (mail servers) to auto-generate and send millions of emails in seconds.
- 3) *Arms Race Mentality*: The creation of exponentially more junk mail each day to ensure that the same number of spam “bullets” find their way through spam filters and reach their intended targets.

### **ANTI-SPAM FILTERS: A FLAWED APPROACH**

Filtering is a computing technique that employs artificial intelligence and complex algorithms to decipher “wanted” email from “unwanted” email. The two most common filtering techniques are “Bayesian” and “heuristic.” Both are sophisticated and intriguing, and both have failed miserably. Considering the exponential growth of spam and its financial impact in terms of lost employee productivity and wasted IT resources, it is clear that a better solution *must* be found.

***Sender Address Verification (SAV) is poised to cripple the spammer’s ability to deliver machine generated email.***

(continued, "Antispam Filters: A Flawed Approach")

**[Flaw] Filters are reactive, a fact that spammers can exploit in at 2 ways:**

- 1) Spammers are only accountable for the number of successful "hits" that are achieved by a particular message. Because spam is so inexpensive to generate and send, they have found the most effective way to overcome filter-based solutions is to dramatically increase the volume of unsolicited email. Therefore, spam volume continues to grow exponentially every year.
- 2) When the ever evolving style of "spam attacks" detects a breach in filtering "defenses," the point of weakness is exploited quickly in an effort to move as much spam as possible before filters react with an update and/or patch.

**[Flaw] Filters are either "too tight" or "too loose"**

As vendors or their customers tighten filters in hopes of blocking all spam, they begin to filter out important non-spam emails as well, an occurrence known as a "false positive." When filters are relaxed to limit the number of false positives, more spam emails slip through. This "catch 22" will continue to be an ongoing dilemma for companies that use anti-spam filters.

**[Flaw] Filters are being subsumed by SAV techniques**

Acknowledging their innate deficiencies, many filtering vendors are beginning to include a SAV layer in their anti-spam offerings. The current "soup du jour" is Sender Policy Framework (SPF). Unfortunately, with their substantial investment in artificial intelligence (filtering), many vendors are prohibited from abandoning this flawed approach. The result are product offerings that force customers to pay for filtering features that are no longer needed or effective.

**SENDER ADDRESS VERIFICATION:  
WINNING THE BATTLE AGAINST SPAM**

**THE DIGITAL DOORBELL**

A hallmark of our civilized society is etiquette. As children we are taught to always "knock" before entering a room with a closed door. SAV technology employs this approach to stop spam, requiring first time senders to identify themselves before their message is allowed to enter a recipient's inbox - a type of digital doorbell.

SAV's effectiveness is matched only by its simplicity. When persons with whom one has never corresponded send an

**SAV's effectiveness is matched only by its simplicity.**

email, a properly designed SAV system responds to the sender, in the intended recipient's name, asking the

sender to identify themselves by performing a simple task. This one-time verification request comes in the form of an email back to the sender. The simplest task requires the sender to press "REPLY" and "SEND" when they receive the request. Additional tasks, such as puzzle solving (captchas) can be employed if necessary to confirm a human sender. When the sender completes the verification request their email is automatically delivered. A delivery confirmation receipt is sent acknowledging that their email has been delivered and that their address has been automatically placed on the recipient's approved sender list. Once placed on this "whitelist" all future emails will be delivered directly to the recipient.

SAV removes the veil of anonymity enjoyed by spammers because the verification request is, by definition, an audit trail leading back to the sender. According to the Anti-Phishing Workgroup's May 2004 report, "...the actual percentage of spoofed phishing emails is likely higher than 95%." It is highly unlikely that spammers will respond to the verification requests, assuming that the return email address they provide is actually real, because in doing so they would be accepting responsibility for the spam that was sent. SAV turns the tables on the spammers back in favor of email recipients.

**"The biggest thing we can do to reduce spam is sender authentication."**

Brian Sullivan  
Senior Director for mail operations, AOL  
New York Times (23 June 2004)

**Sender Address Verification (a.k.a. Challenge/Response):  
One of Business 2.0's "Ten Technologies to Watch in 2004"  
Business 2.0 (7 January 2004)**

**ADVANTAGES OF SENDER ADDRESS VERIFICATION**

While there are many compelling arguments in favor of SAV, perhaps the most convincing are its 100% effectiveness and ability to help enterprises re-capture billions of dollars in lost productivity and wasted resources.

**[Fact] - SAV reduces server load and storage costs**

When implemented as a stand-alone network appliance SAV sits at the network edge, in front of the corporate mail infrastructure. Only email that should be delivered is actually allowed into the network. Spam is never allowed to reach the messaging infrastructure, thus limiting the burden on existing resources. In certain industries where government regulations mandate that all email is indexed and archived, a SAV enabled network appliance can free companies from incurring storage costs associated with spam.

**[Fact] - SAV never deletes legitimate emails**

Spam filters that use mathematical formulas to guess whether an email is legitimate regularly obscure valid email after mistaking it for spam (a false positive). SAV does not employ these techniques nor does it make these costly errors. SAV eliminates the guesswork by merely asking first-time email senders to "knock before entering."

**[Fact] - SAV mitigates future spam by exposing the sender**

SMTP (the backbone of Internet messaging) has no mechanism for verifying the validity of the email sender, thus making it an anonymous transport mechanism. There are promising technologies on the horizon, such as Sender Policy Framework (SPF) and Domain Keys. However, at this time the efficacy of either approach cannot be accurately measured due to lack of widespread industry adoption. SAV solves this basic problem not by trying to fix/monitor the actual correspondence that is sent via SMTP, but by closing the "loophole" in SMTP - the anonymity factor. SAV requires that senders of email either be pre-approved by recipients, or be willing to identify themselves.

**While there are many compelling arguments in favor of SAV, perhaps the most convincing is its 100% effectiveness.**

**DISPELLING MYTHS ABOUT SAV**

While the concept of SAV is quite simple to grasp, many experts have struggled to understand how SAV is implemented. This confusion has allowed a significant amount of misinformation to find its way into both the mainstream and IT trade press. Below are some common myths about SAV:

**[Myth] - SAV will double the amount of email traffic by flooding the Internet with verification requests.**

The misconception is that for every piece of email there will be a corresponding verification request. This is false.

- 1) Senders are only required to identify themselves a maximum of once per recipient. After they have been validated, their mail is delivered directly to the recipient. Moreover, global "whitelisting" and pre-approved sender lists limit the number of verification requests.
- 2) Spammers do not typically provide valid return email addresses. A properly implemented SAV system can detect this and withhold the request.

**[Myth] - SAV systems will flood each other with "ping pong" verification requests.**

At the root of any email processing mechanism is an email server. A basic characteristic of any modern email server is the prevention of "bounce" loops. A properly implemented SAV mechanism will, therefore, not be subject to "bounce" loops or message "ping pong."

