



Protective Addresses: New Identity-Based Method for Defeating Spam

Reflexion Networks, Inc.

September 2007

This white paper describes a new lightweight, identity-based credentialing model for eliminating spam that can be implemented unilaterally without any changes to the SMTP protocol.

The Continuing Blight of Spam Email

Spammers are a clever lot. Exasperating, maybe even infuriating, but clever, as shown by their repeated ability to work around conventional defenses to deliver their message. Despite the best efforts of smart people in the “white hat” world, email users still need new tools to take control of their inbox.

Spam defenses have traditionally relied on blocking messages based on the characteristics of content. While these techniques successfully block a great deal of spam, their ultimate effectiveness is undermined by the spammer’s ability to evade detection by altering content. As a result, content filtering is always a step behind, even with endless reinvestment.

Sender identification and reputation analysis techniques are being implemented, and hold a great deal of promise to improve overall effectiveness. Unfortunately, however, the overwhelming majority of spam is now generated by vast, evolving botnets, making it impractical to blacklist by IP address and a virtual certainty that some legitimate senders will face obstacles to getting their email delivered.

Email address-based techniques are also being implemented. Indeed, simple address analysis can be used to block the estimated 85% of all email traffic destined for “unknown users.” Such techniques have the advantage of being content-independent, and therefore, not subject to the limitations of filters. Some vendors take address-based techniques a step further, providing one-time use or “disposable” addresses as alternatives to one’s primary email address for public or high risk disclosures.

This whitepaper describes advanced new techniques that combine elements of sender identification with multiple addressing (aliasing) to provide a powerful content-independent means of assuring the delivery of mail from legitimate senders, while still blocking unwanted mail and senders. These techniques are embodied in what Reflexion calls Protective Addresses™, which are offered as an option in its multi-layered, managed email security service called Reflexion Total Control.

Fundamental Concepts

The fundamental concept behind Protective Addresses is that inbox control increases with the number of email addresses employed. Two email addresses are better than one, three are better than two, and so on, as far as the user wishes to extend the practice.

Protective Addresses change the paradigm of having all email, good and bad, arrive at a single email address, to one in which inbound mail arrives on as many different addresses as appropriate to achieve control over the inbox.

The validity of this concept is supported by three main considerations. *First*, the introduction of multiple To addresses permits the use of To-From address pairs as a means of identifying and classifying senders with much greater precision. Legitimate senders communicating on a valid pair can be assured delivery, regardless of content; all others can be subjected to additional screening to determine if delivery is warranted. The higher the proportion of mail arriving on valid address pairs, the lower the proportion of mail subjected to content filtering, which reduces false-positives.

Second, a range of access policies can be applied to each address and address pair to provide granular control over each sender's access privileges. With this degree of control, an address can be disabled for abusive senders, but "live on" for the community of legitimate senders who are accustomed to the address.

Third, this simple approach takes spammers' standard tactic of "spoofing" the From address, and turns it against them. In the Protective Address model, To-From address pairs serve as a sender-specific "key" – or what you might think of as an "email PIN" – to grant inbox access and assure delivery of the sender's email. With this "two factor" approach, when the spammer spoofs the From address, he must use it with the correct To address, which he is unlikely to know or guess; if he has a valid To address, he must use it with the correct From address, which he is again unlikely to know or guess. As a result, the common spammer practice of associating random From and To addresses actually makes the likelihood of achieving delivery infinitesimally small. In combination, these three considerations provide superior performance in both blocking spam and assuring delivery.

Importantly, the content-independent nature of Protective Addresses provides an effective complement to content-dependent defenses. In this model, inbox access is controlled by the system's assessment of a sender's validity, guided by user-specified policies, and not by the content or other characteristics of the message.

By attaching security to the one immutable context under the recipient's control – the delivery address – Protective Addresses establish a proactive defense against email abuse that cannot be circumvented by altering message content.

These concepts are not new. Email gurus have known for a long time that multiple addresses provide a very effective way of controlling access to one's inbox. Overall public awareness is now growing, too, with many people using alternate email accounts (typically from free email service providers like Google or Yahoo) in lieu of their primary address when they feel that a disclosure is at risk of generating spam (for example, when visiting an ecommerce site). Those who use substitute addresses are more comfortable disclosing an address on the Internet, because they know that if spam comes in, they can ignore or disable their supplemental account, without affecting legitimate mail arriving at their primary account.

Protective Addresses provide the same advantages with significant enhancements, including the fact that the model works for a single account, with a single inbox. Additionally, an automated system manages the use of Protective Addresses, making it simple to implement without any change in user behavior. As a result, email users always have the confidence to use email as aggressively as they please, with far less risk.

Using Protective Addresses

Protective Addresses take the form of a root address plus a suffix to the left of the @domain portion of the address. For example, if Jane Doe's primary address is jdoe@domain.com, she might use a Protective Address in the form jdoe.abcd@domain.com. The root address may be the user's primary address or an outbound alias, such as "j_doe," to further insulate the user's primary address from ill-meaning senders.

This addressing format may be used selectively or routinely, at the user's option, and blended with traditional defenses, including content filtering. In all cases, with any email client, users send and receive mail as they always have, but with added capabilities. When a message is delivered, it appears in the user's inbox, exactly as if it had been sent to his or her primary address.

As inbound and outbound mail flows through Reflexion's servers, the service automatically builds a database of the community of senders utilizing each Protective Address. This database of To-From address pairs provides the granular means of validating senders and regulating their access to the user's inbox. When inbound messages arrive at the gateway, Reflexion examines only the "Mail To" and "Receipt From" transport envelope addresses, not the message content. If a message is going to be rejected at this level, the service does so before paying the bandwidth cost for receiving the message itself. If the message passes Reflexion's address-based tests and other defenses, the Protective Address in the header is translated to the recipient's primary address. The message is then checked for viruses and cleared for final delivery to the user's local email server and inbox.

Each Protective Address may be used in one of three user-selectable states, which may be modified as necessary over time. These operating states specify how stringently the To-From address pair test is to be enforced to control delivery decisions, and include the following options:

1. **Public** – All email to a Public address will be accepted, regardless of sender or content (after scanning for viruses). This setting, which is typically chosen for Protective Addresses disclosed to legitimate senders, avoids the need for security on the address, at least in the early stages of use, and assures delivery.
2. **Protected** – Mail to a Protected address will be accepted only from a list of known senders, for example, only from senders at the domain where the address was initially disclosed. At the user's option, any mail from unrecognized senders may be quarantined as spam, returned to the sender for retransmission (as described later in the Total Control use case), or subjected to further analysis by Reflexion's Blended Defense.
3. **Disabled** – All mail sent to a Disabled address will be quarantined, vaporized or rejected as undeliverable, based on the user's preferences.

The typical default setting for all Protective Addresses is "public." This confidence is merited by the near universal truth that:

Legitimate contacts will never knowingly share your email address with a spammer, while spammers will only share your address with other spammers, never with legitimate contacts.

This maxim has been confirmed in practice by abundant user experience. If, however, a Protective Address begins to receive spam, the recipient can simply "protect" the address to limit its further use to the community of previous legitimate senders, which has been automatically tracked by Reflexion). In the extreme, a Protective Address can be "disabled" to prevent any further message deliveries.

Selective Use: Address-on-the-Fly™

Address-on-the-Fly (AOTF) enables senders to spontaneously disclose a Protective Address without interacting with the system in any way. For example, when placing an online order, one might use the address jdoe.merchantname@domain.com, where "merchantname" is the Protective Address suffix that the user chooses "on-the-fly."

When Reflexion's service identifies the first use of an AOTF in an incoming message, it records the To-From address pair, translates the address to the user's primary address, and delivers the message to the receiving MTA. At the user's option, the system automatically

2. Restricting use of the address solely to the community of prior legitimate senders (those who previously, successfully used the address).
3. Restricting use to the sender who first used the address, or only to users at that sender's same domain.
4. Disabling the address altogether.

Options 2 and 3 increase the level of address protection from Public to Protected status.

Fully-Automated Use: Total Control

While Protective Addresses provide valuable capability in purpose-specific, selective use, they are even more effective when used automatically for all new correspondents. In this mode, called Total Control, email exchanges take place on a Protective Address that is automatically assigned to each new sender.

In Total Control, if the system determines that the user is sending a message to a first-time correspondent, it automatically generates a new To address for the recipient's exclusive use, e.g., johndoe.45jz@domain.com, where "45jz" is the Protective Address suffix.

Alternatively, the system can be configured to use the recipient's domain as the suffix, e.g., johndoe.recipientdomain@domain.com. The latter approach personalizes the address to the correspondent, and tags all mail from senders at the same organization with the same suffix. If, however, the message is going to an existing correspondent, or correspondents, Reflexion automatically retrieves the proper Protective Address for each recipient, places it in the From envelope address, and routes the message for delivery.

Messages from legitimate but unexpected senders (i.e., first-time senders) who use a Public Protective Address will be successfully delivered, with the sender automatically added to the community of users of that Protective Address. If the address used by the sender is Protected, however, the system will optionally send back a change of address (CoA) notification, directing the sender to resend the message to an address that is automatically determined by the system. Because spammers typically don't reply to a challenge, respondents to a CoA will overwhelmingly be legitimate correspondents. As time progresses, and the use of Public Protective Addresses increases, the incident rate of CoA approaches zero for legitimate senders.

To the user, address assignment and management is completely transparent in both the inbound and outbound scenarios. The user does not see and is not required to manage Protective Addresses – Reflexion does all the work behind the scenes.

Users who want more control over access to their inbox may transition from Content Filtering to Total Control. Users typically start the transition by importing an Allow List of

their existing correspondents. Allow List development is accelerated using tools that automatically harvest one's address book and sent items from the email client. Administrators can round out the Allow List with global address and domain entries for known business contacts.

Once the Allow List is developed, mail from any other sender is either quarantined or tagged with "***Possible Spam**" in the subject line and delivered to the recipient's inbox. This process assures that all spam is tagged by default. If mail from legitimate sources is tagged, the recipient simply adds the sender to the Allow List by clicking on the control panel within the message.

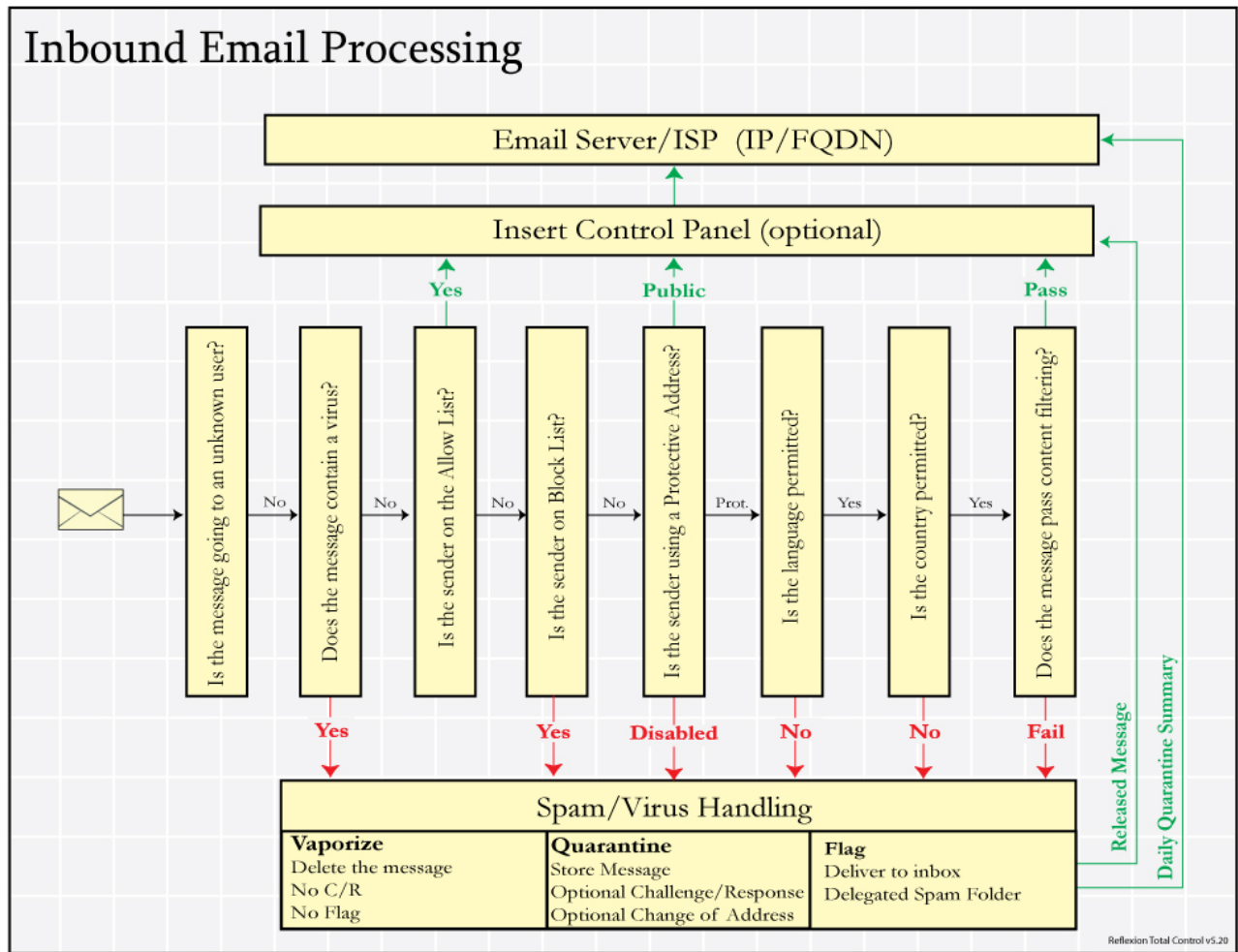
The typical transition only takes a few days to achieve the desired state in which all legitimate mail is arriving in one's inbox, and all spam is being tagged. At that point, the email administrator (or user, if permitted) can activate Total Control mode, after which the user will no longer see any spam, there will not be any need for a spam folder (unless the user desires one), and inbox access control will be completely and transparently managed and perpetuated by Reflexion. After completing the transition to Total Control, users tend to forget that the service is operating in the background.

Total Control is extremely effective in locking down one's inbox for access only by legitimate senders. This degree of control is very helpful during "Zero Hour" virus outbreaks, before anti-virus vendors have updated their signature collections, because infected messages are not likely to be sent using valid To-From address pairs and hence won't be granted inbox access. Nevertheless, Reflexion routes all mail through an anti-virus scanning engine.

Blended Defense

Reflexion blends Protective Addresses with other email defenses, such as content filtering, Allow Lists (whitelist), Block Lists (blacklist), and country and language screening, to construct a very effective, multi-layered defense, as shown in the accompanying diagram.

Reflexion's service is highly configurable by the administrator at the enterprise, user and address levels. This flexibility accommodates the widest range of user preferences and skill levels, and delivers superior effectiveness. Experience shows that 90% or more of all legitimate senders are either using a Protective Address or on the user's whitelist. As a result, email from only 10% of legitimate senders is subjected to content filtering, which reduces the false-positive rate by an order of magnitude.



How Will Spammers React?

Spammers have proven themselves to be very adept at working around content filtering defenses, and there is no reason to assume that they won't be equally creative in dealing with Protective Addresses. However, several factors weigh in favor of Protective Addresses. *First*, spammers must develop new techniques, as their traditional skills of manipulating content will no longer work. Given the filtering "monoculture," the path of least resistance is to continue with their current techniques, at least until Protective Addresses become the dominant model.

Second, spammers may try to flood a domain with variants of all likely root addresses and miscellaneous suffixes, in hopes of achieving a delivery. If this occurs, recipients have their own options of increasing the security on Protective Addresses or upgrading to Total Control operation. Additionally, part of the effectiveness of botnets stems from the fact that each zombie machine may avoid detection by sending just a few messages each day. If each zombie must send significantly more email, they are more likely to arouse suspicion, which increases the likelihood of inspection, detection, and remediation.

Third, even if the spammer succeeds in stumbling upon a valid To-From address pair, the user has the option of blending Protective Addresses with other defenses. For example, users can upgrade the scrutiny of their inbound traffic by augmenting a Protective Address with block listing, content filtering, and/or permitted languages and countries screening. Furthermore, the user has the option to “Disable” a Protective Address that becomes compromised and polluted. Experience has shown that a single unfortunate address disclosure can result in as many as 10,000 – 20,000 spam emails per month, all of which will be blocked by simply disabling the offending “To” address.

Benefits of Address-based Email Security

The Protective Address model does not base inbox access decisions on judgments about message content. As a result, the model complements traditional content-based techniques for dealing with spam, and yields important performance advantages, including:

1. More accurate classification of senders reduces (or eliminates) false positives and false negatives.
2. Zero susceptibility to content manipulation techniques, such as image and PDF spam.
3. Effective for any national language (including double byte character sets).
4. Performance doesn't erode over time.
5. No maintenance or tuning required.

The Protective Address model also complements other identity-based approaches by delivering the following advantages:

1. Operates effectively and independently without requiring all of one's correspondents to implement the same approach; easily handles messages from non-participant sources.
2. Reduces opportunities for spammer “workarounds,” such as using registered service providers, or sending spam from “zombie” desktops that use registered ISPs to create “false negatives.”
3. Reduces administrative overhead through lightweight credentialing.

Finally, Protective Addresses provide email users with a variety of other advantages. *First*, they provide users with an unlimited supply of substitute addresses for use in place of their primary address, such as in discussion forums, on web sites, in press releases, or in print. This practice helps to preserve the long-term integrity of one's primary address by avoiding

new sources of spam that might result from risky disclosures. *Second*, Protective Addresses enable users to identify the specific address disclosures that result in spam. Related tools provide the means of blocking this spam from one's inbox without filtering. *Third*, this technique provides a useful means of associating incoming email with a specific address disclosure, for example, to connect specific messages to a marketing campaign, press release, or job posting.

Summary

The Protective Address model provides a new form of lightweight identity-based email security that enjoys a number of advantages over other spam blocking methods:

1. The model provides email users with unparalleled control over access to their inbox. Control is not abdicated to third parties or overruled by pay-to-play mechanisms.
2. The model adds a more holistic dimension to traditional defenses, assuring the delivery of wanted mail from legitimate senders, as well as blocking mail from unwanted senders.
3. When used aggressively, Protective Addresses eliminate virtually 100% of spam without false positives.
4. Individual enterprises can adopt Protective Addresses unilaterally and take the full benefit without any external participant or protocol change.
5. There is no impact on legitimate mail while these new techniques are being adopted.
6. Protective Addresses are available today, and are quick and easy to deploy through an affordable managed service.

For more information about Protective Addresses, or to react to the ideas presented in this paper, please contact productmanager@reflexion.net.