How The Titan Key Can Eliminate The Global Spam Problem

A white paper from Titan Key Software

Version 1.5

October 10, 2003

Contents

Introduction

The spam problem continues to worsen because all other attempts to solve it have not addressed the root cause: all properly addressed email is unconditionally accepted. As a result, all other anti-spam software gives the spammer confirmation that the recipient address is working and does nothing to reduce the wasted bandwidth used to transmit spam. The ISP bears the brunt of the cost of carrying spam while their customers grow more frustrated.

The Titan Key is the only technology on the market that is engineered from the ground up to solve the root cause in that it *conditionally* accepts email. Rejected spam is stopped *before it is even sent*. The resulting benefit is that spammers discard emails protected by The Titan Key because they no longer work and bandwidth is liberated because no spam is transmitted at any point over the network. For the ISP, their networks no longer carry spam, and customers are rewarded for loyalty because the longer they stay with the same ISP, the fewer spammer databases they will be listed on.

Only The Titan Key actually prohibits spammers from sending spam. We feel it is the one technology that can actually eliminate the spam problem, permanently.

The root cause of the problem: email is unconditionally accepted

All Internet email uses the SMTP (Simple Mail Transfer Protocol) standard, one of the first Internet applications created, formalized around 1982. SMTP was created for a community of researchers, perhaps numbering in the thousands. The underlying assumptions that created SMTP were based on non-profit activities. The community using SMTP was inherently trusted. The resulting standards were extremely insecure to say the least. SMTP email is not encrypted and can easily be "spoofed", allowing one to masquerade under another email address.

The assumption that affects us the most today, however, was that all email is inherently valuable and should be read. And because of this assumption, SMTP will accept email from any source so long as it is properly addressed. The result? Viruses and worms embedded in email are commonplace. And of course, the biggest problem of them all: Spam.

Favorable conditions that fuel the problem

The root cause of the problem would not be enough on its own. There are other factors that have been brought into the arena resulting in today's spam problem.

Email has become a core communication function

The workday of today's knowledge worker centers on processing email. Email is used for the great majority of external *and internal* communications. In addition, many organizations have created automated workflow operations that use email as their primary messaging vehicle. Workers begin their morning by going through their inbox, and then check for messages throughout the day. Email has become a "heartbeat" function in today's workplace and the spam-based productivity loss has reached epidemic proportions.

Easy access to email addresses

Email addresses are everywhere. They are published on millions of Web pages, discussion groups, chat rooms, message boards, online magazines, company directories, business cards, etc. Email addresses are as proliferate as phone numbers. Email databases can be purchased for a little as $1 for 100,000 addresses.

Low cost to send, easy to get good ROI

When you combine cheap bandwidth, powerful processors, lack of security, and a **very Simple**-Mail-Transfer-Protocol, you get the ability to send millions of emails for nearly zero cost. As a spammer, it's almost impossible to *not* turn a good profit.

Lack of email privacy adds to the spam problem

The root cause of spam is creating a privacy nightmare. Because all properly addressed email is unconditionally accepted, one can argue that SMTP email inherently violates privacy. Intrusion via email is the default action. This lack of privacy contributes to other problems to further degrade productivity.

Unfriendly opt-out procedures

Web sites make it easy to opt-in for communication, but oh so difficult to opt-out. Users have to click on links to Web sites that don't always work, remember long-forgotten passwords, and God help them if they registered with an old email address that forwards messages.

Database mismanagement
Of course, just because one opts-out does not mean that they won't receive any more email. It just means they are marked in the database to not receive email. One can only hope that the software does not have bugs, the operators run the proper query, and the company is not tempted to send an email to everyone on the list because of something "really important". There are countless cases where users have submitted their email address, indicated they did **not** wish to receive "special offers", and of course still received them.

And just because one has opted out of an email database doesn't mean their address can't be sold or repackaged for other purposes.

Undesired personal email
Users are so frustrated with spam they are too busy to complain about unwanted personal email. We all receive unwanted jokes, warnings about viruses that aren't true, instructions to remove files that result in crashing our systems, pleadings to write to our congressmen, and great stock tips, to name a few. These emails may come from people we know and would rather not hear from, but we simply don't have the heart to tell them that we really don't like the intrusion.

Resulting problems for ISPs

Unfortunately, the ISP is bearing the brunt of spam's costs. Spam volume directly opposes the ISP business model. Customer loyalty is discouraged and customer costs increase over time.

Customer loyalty is discouraged
The longer an email address is in use, the more databases it will spread to and the more spam it will receive. Depending on the personal habits of the subscriber, the volume of spam becomes unbearable over time. In a final act of desperation, customers will abandon their email account (and possibly the ISP) to stop the flow of spam. This customer "churn" has a powerful negative impact on the ISP bottom line.

Bandwidth is wasted
Spam content is universally despised but the ISP still has to pay for the bandwidth to carry it.

Unfortunately all other anti-spam software does nothing to stop spam-driven bandwidth waste.

Overhead increases
As the spam volume continues to grow, so do the costs to carry it such as additional maintenance, handling customer support complaints, or paying for additional bandwidth.

Why the spam problem will continue go grow unabated with all other anti-spam approaches

The ineffectiveness of traditional anti-spam technologies is self-evident. Spam has continued to grow at an alarming rate and the general consensus is that "We're losing" (see http://www.clickz.com/emailstrategies/perm/article.php/2175751). There are many reasons why conventional anti-spam approaches will not solve the spam problem.

The root of the problem remains unsolved
All other anti-spam approaches do nothing to address the root problem. Properly addressed email is still unconditionally accepted and all subsequent technologies to filter spam are, by definition, *reactive*. We're treating the symptoms and ignoring the root cause.

Addresses are validated
When spammers send out mass-email, they do not know for the most part if their email is being filtered or deleted. But with all other anti-spam software, spammers still know that their email is being received. And because they know the address is valid, they will continue to send spam and attempt to sell it to other spammers.

The spamming business is not based on target marketing. Spammer's don't segment their lists to reach targeted demographics. Their success is directly based on raw volume. An email address that works is an asset to be re-used as much as possible.

Spam is still sent over the network
Because other anti-spam software has not solved the root problem and spam is still transmitted whether it ends up getting filtered or filed, network bandwidth is still wasted. ISPs still have to carry the traffic, and most users still have to download spam. And regardless of how sophisticated the other anti-spam solutions become, they will never reduce the amount of spam sent.

Constant vigilance required
Because other anti-spam approaches are reactive and do not stop spam *before* it is sent, spam is beginning to acquire the one-upmanship characteristics of viruses. Spammers are constantly researching how to get around filtering algorithms and other anti-spam firms will be continuously countering those efforts. The moment a user of traditional software lets their guard down will be the moment spam will instantly return.

Users still have to review spam
The dirty little secret of all the other anti-spam approaches is that despite all their claims *you still receive **all spam**!* Users are given a quarantine folder that holds suspected spam and must go through that folder to make sure that no false positives (good email that was treated as spam) exist.

Email privacy remains a problem
The Internet community is so consumed with combating the spam problem that they do not notice the secondary harmonic of the *privacy* problem. Traditional anti-spam software simply does not even begin to address the issue of privacy violations.

How The Titan Key Works

Since 1999, our staff has engineered a technology that directly solves the root of the problem. With The Titan Key, email is only *conditionally* accepted. The results are dramatic.

Simply put: There is no spam.

The consequential benefits of a well-engineered solution combine to define a new email paradigm. We call it *The Birth of Email Privacy.*

The Titan Key installs as the primary MTA (message transfer agent) of a given domain's email server. This means that any Internet server first talks to The Titan Key in order to send email.

Here's how it works:

1. The spammer attempts to send an email message.

2. If The Titan Key does not recognize the sender's address, it responds with a "No such user" error message, indicating to the sender that the "TO" address is not valid.

3. The connection is severed. No email contents are ever transmitted. This “hard bounce” typically directs most mass e-mail software to flag the email address for database removal.

4. The Titan Key™ then sends an invitation email to the sender's address asking them to validate themselves as a person. Typically, spammers do not have a valid return address. Those that do cannot economically look through the return mails and perform the validation step because it must be done manually.

5. For a spammer, the process ends. The target user apparently no longer exists because there is no such email address.

6. People who desire legitimate contact go through the validation step and are asked to resend their email, which then passes transparently. Subsequent emails do not require validation.

How The Titan Key Maintains its database of Known Senders

The Titan Key's conditional acceptance logic only allows email from Known Senders to pass through transparently. It dynamically maintains this database so that only new, unknown senders (an extremely small percentage of user's total legitimate email volume) must go through the invitation/validation process.

- When a user of The Titan Key sends an email, all recipients of that email are automatically added to the database of known senders.
- The Titan Key comes with utilities for Microsoft Outlook® that will extract email addresses from any Outlook folder and add them to the database of Known Senders, minimizing any unnecessary invite/validate operations.
- When new senders successfully complete the invite/validate process, they are automatically added as a known sender.

The Titan Key is a "set and forget" operation. Unlike all other anti-spam products that require ongoing maintenance from the user to flag spam, or review a quarantine folder containing suspected spam, The Titan Key requires no further effort. There is simply no more spam.

How The Titan Key Handles online orders or subscriptions

Other whitelist-based, anti-spam software has a difficult time in dealing with online orders or newsletters. Because the sender's email address is not known, order confirmations and newsletters end up in a quarantine folder instead of the user's inbox, requiring the user to manually add the email to their whitelist. Some newsletters further complicate the matter by using slightly different sender email addresses for each issue. This requires users of other software to either manually add each issue to their whitelist or to create special rules or exceptions to allow these special emails to pass through.

The Titan Key has an elegant solution to the problem, known as a KeyMail address. A Keymail Address looks and works just like other email addresses. It allows the user to give out an email address that will transparently pass through The Titan Key without requiring validation yet will only work for a given individual or organization.

Here's how it works:

1. The end user desires to sign up for a newsletter or place an online order or a similar situation where their email address is required yet the sender's address is not known.

2. The Titan Key gives the end-user a "KeyMail", a special coded email address and the user gives submits this instead of their normal, protected email address.

3. The vendor sends their newsletter or online order confirmation to the KeyMail and it passes through The Titan Key directly to the end-user without error or invitation/confirmation. All subsequent newsletters or order notices also pass through.

4. The KeyMail is now programmed to only allow email from this particular sender or sender's domain to pass through. Should any other sender attempt to use the KeyMail address, it will return with a "no such user" error message and will not send an invitation/validation email.

5. The Titan Key user may deactivate the KeyMail address at any time, disallowing any further emails sent to that address. This frees the end-user from the hassles of unsubscribing from newsletters and completely addresses any privacy concerns because the KeyMail simply no longer functions.

For the first time in Internet history, The Titan Key's KeyMail technology gives the end-user complete control over who can use their email address and how it is to be used. The Titan Key represents the "Birth of Email Privacy" that finally puts the user in control of their inbox.

How The Titan Key solves the root cause of the spam problem by *conditionally* accepting email

The core of our solution directly corresponds to the core of the problem. The Titan Key's patented process is the first that *conditionally* accepts email. It is the only technology where a user's email address works for friends but does not work for spammers.

Before the Titan Key, properly addressed email was unconditionally accepted. With The Titan Key, properly addressed email is accepted *only if the recipient has given permission.*

This is a radical departure from today's handling of email yet is in full compliance with the SMTP standards.

The benefits resulting from solving the root cause

As with any solution that addresses the root cause, the benefits are significant and immediate.

Spammers cannot send spam

Because The Titan Key user's email address literally does not work for spammers, by definition of the SMTP standards, *they cannot even send the spam.* No other software can make this claim.

Network bandwidth is liberated

Because spam cannot be sent, all of the network bandwidth that was previously wasted is now available for productive use. For the ISP, the savings are significant. Close to 50% of today's email is spam. No other anti-spam software completely frees bandwidth like The Titan Key.

Customer loyalty is *rewarded*
The Titan Key shatters the loyalty dis-incentive that spam has created. The "no such user" error message that The Titan Key returns to mass-email software typically directs it to flag the email address for deactivation or removal from the database. Invalid email addresses waste processing time and are worthless to a spammer. The sheer volume of spammer databases require that they eliminate email addresses that no longer function.

The net result to a user of The Titan Key is that over time, their email address will be on fewer spammer databases. This is a 180 degree reversal of the previous trend. The benefit to ISPs is significant. Because The Titan Key dynamically builds a database of "known senders" while at the same time it blocks spammers and reverses propagation of their email address on spammer databases, *customer ISP subscriptions become more valuable over time.* Unlike traditional anti-spam approaches, The Titan Key rewards customer loyalty by strengthening the subscriber's privacy capabilities over time.

No false positives, no quarantine folders to inspect
Because no spam is sent, there are no folders to inspect. And because email is immediately rejected or accepted, there is no such thing as a false positive! The tremendous benefit is that *all email in the inbox is by definition desired by the end-user.*

For someone that has been receiving volumes of spam for a long time, there is a deep sense of liberation immediately after The Titan Key is installed. The inbox is free of spam and every email is relevant!

Immediate feedback to sender
No other software gives the sender immediate feedback on how their email has been handled. Many times this causes problems because a sender is expecting a response assuming the recipient has received their email and when in fact the sender's email has been quarantined as spam.

If a sender's email is rejected by The Titan Key, the sender will receive a genuine error message *every single time.* This lets them immediately know that their email is rejected. It puts the burden of communication on the sender. One cannot expect a response if the email is known to have not been sent.

All privacy issues solved
The Titan Key gives the user full control over their email address. The end-user now decides *who has permission to send email*.

- The only email ever received is that which the end-user has either implicitly or explicitly permitted.
- The user can instantly decide to disallow further emails from any desired sender, freeing them from any burdens related to uncooperative opt-out procedures.
- Email addresses protected by The Titan Key are worthless if traded with anyone other than the validated sender. This greatly reduces the chance that email addresses will be bought or sold *because they are worthless in the hands of a different sender.*
- Users of The Titan Key may optionally decide to not give a particular sender the invite/validate email. Because the sender only receives the error message, *it is impossible for the sender to ever send email to that user again.* No other software empowers the user in such a profound way.

Why The Titan Key is the best chance to stop the spam problem

The mission and purpose of The Titan Key is simple.

Eradicate the spam problem.

The Titan Key is engineered from the ground up to fulfill that purpose. We believe it is the only software that has a solid foundation on which to permanently stop spam.

Only solution that actually stops spam
All other software first accepts spam, and then takes measures to filter it in some way. Only The Titan Key stops spam *before it is ever sent.* This has a profound effect on spammers. Consider this: If every Internet user installed spam filtering software, spammers would still be able to send spam, choke bandwidth, and attempt to circumvent the filtering rules. However, if every Internet user installed The Titan Key, *spammers could not send spam.*

Provides active feedback that spamming is not working
All other anti-spam software lets spammers know the email address is valid. Therefore, spammers continue to send spam. The Titan Key gives spammers immediate feedback that their email did not go through because the email address is no longer working. Whether they remove the email address from their database or not may be arguable, but one thing is for sure, they do know that their email was never received, much less opened. If you were a spammer with a database of 100,000 emails and found that 90,000 of those addresses were bad (no longer working), how many times would you keep sending out those 90,000 emails?

Eliminates spam-related network bandwidth
Wasted bandwidth is a significant byproduct of the spam problem. The Titan Key elegantly solves this problem because *no spam is ever transmitted at any point.* Not a single byte of spam is sent to any server protected by The Titan Key.

Fundamentally changes the email paradigm
With The Titan Key, the world will never be the same

- The burden of respecting privacy concerns will fall squarely on the sender, not the recipient.
- Valid email addresses will be highly treasured because they imply that the recipient has actively approved future communications.
- Email addresses can no longer traded as commodities because they only function for previously approved senders.
- Senders will have to consistently and properly identify themselves, otherwise they must undergo the invitation/validation process.
- And of course, finally, **THERE WILL BE NO SPAM.**