

Fighting SPAM using PKI

 The article was obtained at the following URL: <http://www.kfwebs.net/articles/article/36>
 The article might be distributed further as long as it is provided as it is, with the credits stated.
 The Article was written and first published by KF Webs, at <http://www.kfwebs.net>
 #####

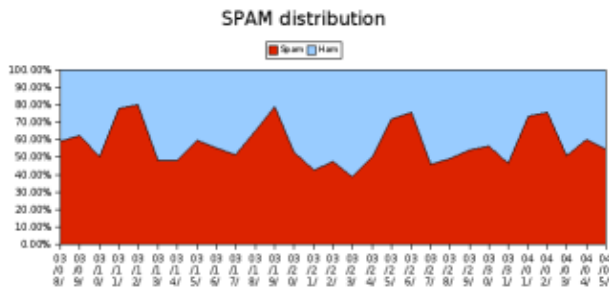
*Spam is an increasing problem for most, and personally statistics shows that somewhere between 50 and 60 per cent of the emails yours truly get are SPAM. Thankfully measures are being taken to reduce this problem.
 Added: 2006-04-06 13:03:12 - Modified: 2006-09-23 23:20:54 - Level: Beginner*

Table of contents

- 1. Introduction
 - 1. The Social Problem
- 2. What is DNS
- 3. What is PKI
- 4. PKI and DNS
- 5. How can you fight SPAM using PKI
 - 1. Whitelists and blacklists
- 6. Different standards
 - 1. Public Key Association
 - ◇ What is GNU Privacy Guard
 - 2. Sender Policy Framework
 - 3. DomainKeys
- 7. Conclusion

Introduction

Spam is an increasing problem. A multitude of working hours are wasted by employees sorting through spam messages and many are starting to get fed up by the ever-increasing amount. The spam versus ham distribution on one of the low-traffic (500 messages a day) email servers under KF Webs control is as follows:



An average of 58% of the emails received by the server is SPAM-messages.

The Social Problem

As long as it is profitable to send SPAM messages, people will continue doing so. The only way to truly fight SPAM is for it not to be profitable, and to do so one have to educate users not to click spam links, for their own good with regards to phishing as well to reduce the overall amount of SPAM.



Until that will happen, however you have to take measures to reduce the problem for yourself. Anti-spam solutions such as Spamassassin and dspam are helpful in reducing the problem, but still more has to be done. There is where this article hopefully helps understanding some available and coming technologies.

What is DNS

DNS is the abbreviated for of Domain Name System. When you visit a website such as kfwebs.net your computer sends a request to translate the domain name, kfwebs.net, from a human readable form into a computer readable form, referred to as an IP-address. In the time of writing the IP address of kfwebs.net looks like 213.161.224.2.

What is PKI

PKI is short for Public Key Infrastructure. The concept is that, unlike in most daily life situation where you use the same key to both lock and unlock e.g. a door, you have two keys, one for locking and one for unlocking. Technically this is called asymmetrical key cryptography. The equivalent of an ordinary lock would be called symmetrical key cryptography.

The reason for this is amongst other things that you can safely transmit the locking key, referred to as a public key. While you still keep the unlocking key, the private key. So you make the public key available for everyone, but only you keep the private key yourself.

With an analogy to real life. Say you live in a busy street and are worried that someone might get into your house. Using PKI you can give a locking key to your neighbors in case you forget to lock the door one day while walking around from your house.

A free implementation basing itself on PKI is OpenPGP. You can use OpenPGP free by using GnuPG. You can read more about how to secure your communication at secure-my-email.com

PKI and DNS

By storing a PKI certificate in the DNS record it is possible to verify that an email is coming from the server it is coming from. This would require the message to be digitally signed, and the receiving email server would have to verify the signature using the public component of the PKI certificate.

Only the holder of the private component of the PKI cert would be able to digitally sign a message that can be verified by that public key component. And that enables the theory to be utilized in a number of schemes. Before we proceed we will go into a little more detail with regards to the different terms used in this article.



How can you fight SPAM using PKI

The primary concern of most existing standards is not to stop spam, but to stop forgery. That is if you receive an email that claims to be from alice@abc.com it really is from abc.com. As it is today anyone can claim to be from anyone, so if I want to send an email to someone claiming to be from abc.com although my real address is kfwebs.net I can do so.

This is why there is a need for authentication schemes such as OpenPGP in order to ensure that the sender is whom he or she claims (s)he is.

Implementing cryptographical services on the mailserver (referred to as the Mail Transfer Agent (MTA) from now on) will help in ensuring the authenticity of the sender-MTA by verifying the message signature on a receiving-MTA. This only ensures the domain authenticity, and not the authenticity of the sender, you will still want to use a scheme such as OpenPGP for that.

Whitelists and blacklists

First after you can be sure that the email actually originate from the mailserver it claims it come from you can use whitelists and blacklists for email properly. A typical approach for spammers is to use the same sender address as receiver address. This way the email seems to both originate from and being sent to e.g. bob@bobsdomain.com, getting past any whitelist he might have for bobsdomain.com, even though the email itself could have been sent from anywhere.

Different standards

Public Key Association

Public Key Association(PKA) is a scheme that base itself out of [RFC4398: Storing Certificates in the Domain Name System \(DNS\)](#) which got published in March 2006 and obsoletes RFC 2538.

The abstract of the RFC says as follows:

Cryptographic public keys are frequently published, and their authenticity is demonstrated by certificates. A CERT resource record (RR) is defined so that such certificates and related certificate revocation lists can be stored in the Domain Name System (DNS).

The mentioning of PKA implementation shows up in the release notes of GNU Privacy Guard

The GnuPG release announcement for version 1.4.3 contained the following:

Implemented Public Key Association (PKA) signature verification.

This uses special DNS records and notation data to associate a mail address with an OpenPGP key to prove that mail coming from that address is legitimate without the need for a full trust path to the signing key.



What is GNU Privacy Guard

[GnuPG](#) is the GNU project's complete and free implementation of the OpenPGP standard as defined by RFC2440 . GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kind of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications.

Sender Policy Framework

Quoting openspf.org for explaining what the sender policy framework does:

Have you ever gotten spam from yourself? I have, and I've been thinking hard about how to stop it! I didn't send it. It came from a spammer. If we could stop spammers from forging mail, we could easily tell spam from ham and block the bad stuff.

SPF makes it easy for a domain, whether it's an ISP, a business, a school or a vanity domain, to say, "I only send mail from these machines. If any other machine claims that I'm sending mail from there, they're lying."



When an AOL user sends mail to you, an email server that belongs to AOL connects to an email server that belongs to you. AOL uses SPF to publish the addresses of its email servers. When the message comes in, your email servers can tell if the server on the other end of the connection belongs to AOL or not.

And that's it! SPF aims to prevent spammers from ruining other people's reputations. If they want to send spam, they should at least do it under their own name.

And as a user, SPF can help you sort the good from the bad. Reject mail that fails an SPF check. Use it to help your spam filters make a decision. Have confidence that mail that SAYS it's coming from your bank, your credit card company, or the government really is!

If you do get spam that passed an SPF check, then you know you should hold the sending domain responsible for the message.

The sender policy framework depends on a TXT record in the DNS zone. The DNS entry for KF Webs could look like

```
kfwebs.net. IN TXT "v=spf1 a mx ~all"
```

You can read more about the SPF at en.wikipedia.org

DomainKeys

DomainKeys, abbreviated DKIM, is currently being used by amongst others Google in its gmail service and Yahoo. An example of a mail header is:

```
DomainKey-Signature: a=rsa-sha1; q=dns; c=noFWS;  
s=beta; d=gmail.com;  
h=received:message-id:date:from:to:subject:cc:mime-version:content-type;  
b=Ud2KRmZ1JjQ8GeDzW+HGGu6QOYo+TF1TWlznSQE48j5cEESiUIhS4+cMLbH0iuSNEBvsS2b  
(wrapped)  
v1TQsCw7lnMkHxDLuccFGc033TReCVYdiAmbQVoEspFYGjl79pYW0+RHyp1AAZ96fTs+4h1S  
(wrapped)  
WeNJ4B3fuHMOAIJPa4k81hS+F9MoE=
```

antispam.yahoo.com says the following about Domain Keys

DomainKeys: Proving and Protecting Email Sender Identity

Email spoofing - the forging of another person's or company's email address to get users to trust and open a message - is one of the biggest challenges facing both the Internet community and anti-spam technologists today. Without sender authentication, verification, and traceability, email providers can never know for certain if a message is legitimate or forged and will therefore have to continually make educated guesses on behalf of their users on what to deliver, what to block, and what to quarantine, in the pursuit of the best possible user experience.

DomainKeys is a technology proposal that can bring black and white back to this decision process by giving email providers a mechanism for verifying both the domain of each email sender and the integrity of the messages sent (i.e., that they were not altered during transit). And, once the domain can be verified, it can be compared to the domain used by the sender in the From: field of the message to detect forgeries. If it's a forgery, then it's spam or fraud, and it can be dropped without impact to the user. If it's not a forgery, then the domain is known, and a persistent reputation profile can be established for that sending domain that can be tied into anti-spam policy systems, shared between service providers, and even exposed to the user.

For well-known companies that commonly send transactional email to consumers, such as banks, utilities, and ecommerce services, the benefits of verification are more profound, as it can help them protect their users from "phishing attacks" - the fraudulent solicitation for account information, such as credit card numbers and passwords, by impersonating the domain and email content of a company to which users have entrusted the storage of these data. For these companies, protecting their users from fraud emails translates directly into user protection, user satisfaction, reduced customer care costs, and brand protection.

For consumers, such as Yahoo! Mail users or a grandparent accessing email through a small mid-western ISP, industry support for sender authentication technologies will mean

Conclusion

As long as SPAM remains profitable spammers will continue. Educating users is the most important way of fighting spam in the long term perspective. In the short-term perspective technical solutions can be used to help reduce the effect of spamming.

This article introduces three different solutions to fight forged sender domain addresses that can be implemented by server administrators. Users can use schemes such as OpenPGP to ensure the authenticity of the sender.



Related articles: