



# Email Best Practices

Kevin Chege

# Why your email setup is critical

- Billions of SPAM emails are generated every day
- The tips here can help you to reduced the chances of you receiving SPAM email or inadvertently being the source of SPAM emails
- Because email is so efficient, its now used to send malware, ransomware, worms etc.
  - For example: WannaCrypt!

# SPF

- SPF – Sender Policy Framework
  - SPF allows administrators to specify which hosts are allowed to send mail from a given domain by creating a specific SPF record (or TXT record) in the Domain Name System (DNS).
- *@ IN TXT "v=spf1 include:gmail.com ip4:1.2.3.4 mx -all"*
- The above will only allow mail from IP 1.2.3.4 and any server in the domain with an MX record
- If not sure use a generation tool online
  - <http://www.mtgsy.net/dns/spfwizard.php>

# Domain Keys Identified Mail (DKIM)

- DKIM (DomainKeys Identified Mail) is an authentication mechanism to help protect both email receivers and email senders from forged and phishing email.
- It is intended to prevent forged sender addresses in emails, a technique often used in phishing and email spam.
- DKIM allows the receiver to check that an email claimed to come from a specific domain was indeed authorized by the owner of that domain which is done using cryptographic authentication.
- Verification is carried out using the signer's public key published in the DNS. A valid signature guarantees that some parts of the email (possibly including attachments) have not been modified since the signature was affixed

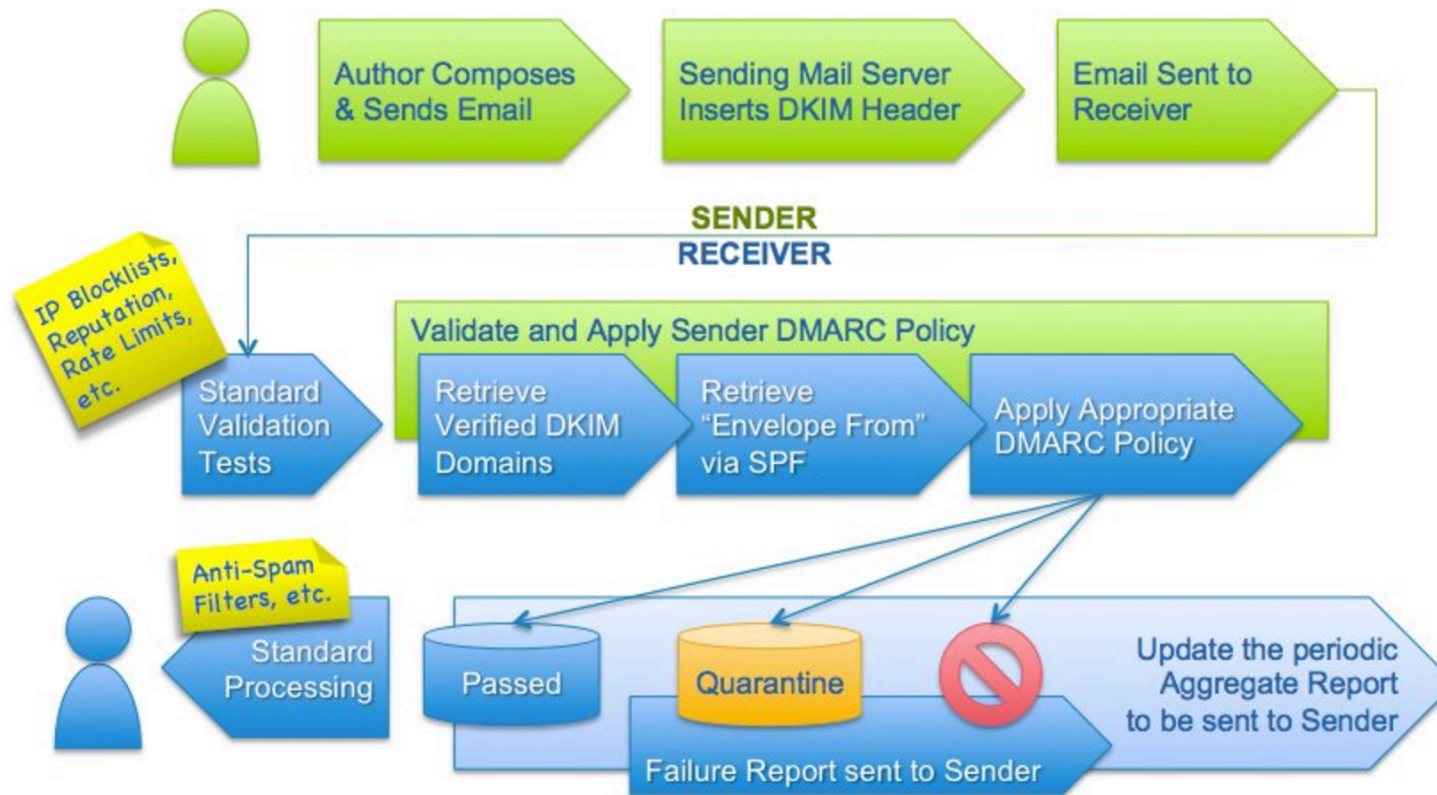
# DMARC -

- which stands for “Domain-based Message Authentication, Reporting & Conformance
- It builds on the widely deployed [SPF](#) and [DKIM](#) protocols, adding linkage to the author (“From:”) domain name, published policies for recipient handling of authentication failures
- Another IETF standard designed to combat growing spam
- More at <http://dmarc.org>

# Why is DMARC important

- Allows Domain owners to:
  - Signal that they are using email authentication (SPF, DKIM)
  - Provide an email address to gather feedback about messages using their domain – legitimate or not
  - A policy to apply to messages that fail authentication (report, quarantine, reject)
- Allow Email receivers to:
  - Be certain a given sending domain is using email authentication
  - Consistently evaluate SPF and DKIM along with what the end user sees in their inbox
  - Determine the domain owner's preference (report, quarantine or reject) for messages that do not pass authentication checks
  - Provide the domain owner with feedback about messages using their domain

# DMARC FlowChart



<https://dmarc.org/overview/>



# SPF, DKIM and DMARC

- All published in DNS!
- SPF sample: `$dig TXT facebook.com`  
`"v=spf1 redirect=_spf.facebook.com"`
- DKIM sample: `$dig google._domainkey.protodave.com TXT`  
`google._domainkey.protodave.com. 3600 IN TXT "v=DKIM1; k=rsa;`  
`p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAhArxYH88+A76Gk7/8ENefN5RhMFhoYJp8T3KLPYY`  
`pejDI45PKWTO+2r8ZJZOtuk7tsG07bmJyU8PFvU48Lf1xtb4WcFxxKKjd7N5MF6JcHD51Xb8XDAJA2ldqxH4hBbw9`  
`dRjsT7WBFXbp2x6MSWxgi9f1w+7Z2IFG+AtUjrf8/9N3gLieaZKZT1SEhR8TnhfOm"`  
`"FG0LfMyS0YtfHKrkUkBCEmWBPisB2CcZBShKr6/T8/UB/oZF8XMRd0NOsru9MGx9Yp89jIYS5YRuvbA0/TLgOOi`  
`qrSU5Ms1egMwfFyy4BMDUKayZzF6BxNPc/+UoFrYHKRZpyD/kEd4FXNEddlksQIDAQAB"`
- DMARC sample: `dig TXT _dmarc.google.com`  
`"v=DMARC1;p=reject;pct=100;rua=mailto:postmaster@dmarcdomain.com"`

# Reverse Records

- Have reverse records (PTR) for your mail server so that it is resolveable from the IP
- Mandatory by most servers these days
- Used to verify authenticity of the sending mail server
- The IP Address must resolve back to the mail server name
- You can have multiple reverse records
- You can have an SPF record that states that any IP that has a reverse record can send email from your domain
- *IN TXT "v=spf1 ptr:domain.co.tz ip4:1.2.3.4 mx -all"*

## Use Anti Spam and Anti Virus software

- Will reduce overall spam and email received
- You can also have a mail “firewall” or gateway aka Mail Filter to stop spam before it reaches your server
- Some softwares are:
  - SpamAssassin (AntiSpam) – renowned antivirus
  - ClamAV (AntiVirus) – renowned antivirus
  - MailScanner and Amavisd (rely on the above)
- When setup try a penetration testing site to see how well your server can protect you from SPAM and Viruses

# GreyListing

- Valid mail servers will have no problem if the receiving gives a soft error (4xx)
- They will attempt to send the mail again after some time
- Greylisting configured on a receiving mail server will give a soft error (4xx) to the sending server and store the IP/Hostname of the sending server in a file
- If the sending server returns again after some time (can be specified usually 5min) the email is accepted
- Used as a measure to deny mail from bots that are compromised to send mass mail. They often do not try again if the server did not accept the mail

# Accept only well formatted messages

- Sender must be a valid name not an IP ie not [user@192.14.5.6](#)
- Mail server HELO name must be resolvable ie FQDN
- Server identification must resolve ie HELO/EHLO name must be resolveable
- Email should be from a valid email address format eg: from [tom@example.com](#) and not from tom@example

# Security

- Run secure pages from the mail server and secure SMTP to clients
  - Secure Webmail – port 443
  - Secure SMTP – port 465/587
- Force clients to use secure IMAP or Secure POP
  - Secure POP – port 995
  - Secure IMAP – port 993
- Require authentication on your mail server before a mail enters the queue from a sending client aka SMTP AUTH
- Lock down your box and block all unnecessary ports

# Use Blacklist databases

- Use DNSBL – DNS Based Blackhole Lists or RBL (Real Time Blackhole lists) to deny mail from well known spamming machines
- Some well known good ones are
  - SORBS – <http://sorbs.net>
  - SPAMHAUS – <http://spamhaus.org>
  - SPAMCOP – <http://spamcop.net>
  - MANITU – <http://manitu.net>

# Require strong Passwords

- Advise users to use strong passwords or passphrases for their email
- Alphanumeric passwords are better than normal passwords ie combine letters with numbers
- Passphrases are even better, more difficult to break



# Backup and Redundancy

- Have multiple MX records so that your server is not the only one able to receive mail for you
- Backup your mail, use tools like Rsync to copy mail to another server as often as you can
- Ensure your DNS records (MX, NS etc ) are correct and test them when you complete you setup
- Use online tests like
  - <http://intodns.net>

# The question of Ethics

- As an email administrator, its easy to view other people's email at any time with admin rights
- Emails are intended by the sender for the recipient(s) and many senders are oblivious to the fact that their email can be intercepted along the way
  - Hence the need for encryption 😊
- As an email administrator, you should be be professional and maintain ethics and etiquette 😊

# References

- Wikipedia
- [http://www.linuxmagic.com/best\\_practices](http://www.linuxmagic.com/best_practices)
- Further reading:
  - DMARC: <https://dmarc.org/>
    - <https://en.wikipedia.org/wiki/DMARC>
  - SpamAssassin - <http://spamassassin.apache.org/>
  - ClamAV - <https://www.clamav.net/>
  - AmavisD - <https://www.ijs.si/software/amavisd/>
  - <https://protodave.com/security/checking-your-dkim-dns-record/>