Email

- DKIM (DomainKeys Identified Mail)
- DMARC (Domain based Message Authentication, Reporting and Conformance)
- SPF (Sender Policy Framework)

DKIM (DomainKeys Identified Mail)

Introduction

> **"** DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect forged sender addresses in emails (email spoofing), a technique often used in phishing and email spam. [source](#)

Description

DKIM is a more advanced method than [SPF (Sender Policy Framework)](#) for combating email spoofing. It uses [Public-Key cryptography](#) to digitally sign each email. A mail server generates a keypair and the public key is then added as a DNS record for that domain. Using the private key the mail server affixes a digital signature to each email. The receiving [Mail Transfer Agent (MTA)](#) can then lookup the public key using the DNS record matching the sending domain and validate the signature.

Example

As an example, the host `mail.swigg.net` is used for sending emails. If has the following DNS record.

Domain	Type	Value

| mail._domainkey | TXT | v=DKIM1; h=sha256; k=rsa; p=MIICIjANBgkqhkiG9w0BAQEFAAOC Ag8AMIICCgKCAgEA0SF9l7b0bMcB3pt HM6LbV+rZ/rz1SmHyNCKzBrB6rs433 avNHFO4bbs//NG9ZvrCqeElC4NlXPO0 VLl8Vbor9dA7HVcSct5aH9/qRWUMfE3 LEH9cBVytVAm3/ICgHN6qhWKbnPxK// zh5tmzgdcTKuWyiqhLSECbX63q3gWy uXYMJKqr/BzEq0fzLJymHCfaWkG3MI02 pRp68HgpVcpvx2G/t3BKz50BrZVOlSS E9Gi7wbb9jrdeGLwBYIBD4LR+QkVIr8 z+ptCMfg+XOfJzLDsBNBUHnBFT/7N3/ Ub9BNxsLBltZX3mAWNQQY/n31SC7ik 9qs3t6lt22er1jo3WZqjWxBM4xseynUv fn4Lgcp+XQAZCWRQIHr2hwrX4KO1m K/vvvb/dS+NmCNXmWkDvzerVPBCXd fBn+1nbnAsv0vzBuf2yELfRkAIuQRE/P RpeETXAjoayYsVePpOtJn5co0tuiOwbj Uf+9hkNO1a3aN/jrK41BDJrGoNjvul3k WZX1Tz42lCQ168x6tuR5ImB5jJFlgGJz +dC5wY8Gmt4hCf1GPW6g7RJpaGUXT EFAEAE0iECsMjg2/Tm2Sb/H4phN/F2A nF4bkju548Yg73X37tVCkLejMgwH7TT gyQvZ/nXhsE4q31YrNZSNnWZMV+9z/ yJyQvVmTXsOoDAIfkqxfcCAwEAAQ== |

DMARC (Domain based Message Authentication, Reporting and Conformance)

Introduction

> DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. The purpose and primary outcome of implementing DMARC is to protect a domain from being used in business email compromise attacks, phishing emails, email scams and other cyber threat activities. source

Description

The owner of a domain can, by means of a DNS record, publish a policy that states how to handle e-mail (deliver, quarantine, reject) which is not properly authenticated using SPF (Sender Policy Framework) and/or DKIM (DomainKeys Identified Mail).

Read More

Example

As an example, swigg.net is setup with the following DNS record.

Domain	Type	Value
_dmarc	TXT	v=DMARC1; p=quarantine; rua=mailto:dustin@swigg.net; ruf=mailto:dustin@swigg.net; sp=quarantine; ri=86400

This rule can be read as telling MTA (Mail Transfer Agents) the following.

Component	Description
p=quarantine	treat mail that fails DMARC check as suspicious
rua=mailto:dustin@swigg.net	send aggregated reports to `dustin@swigg.net`
ruf=mailto:dustin@swigg.net	send forensic reports to `dustin@swigg.net`
sp=none	treat mail that fails DMARC check as suspicious for subdomains
ri=86400	send reports every 24 hours (86400 seconds)

SPF (Sender Policy Framework)

Introduction

> " Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of the email. SPF alone, though, is limited only to detect a forged sender claimed in the envelope of the email which is used when the mail gets bounced. Only in combination with DMARC can it be used to detect the forging of the visible sender in emails (email spoofing), a technique often used in phishing and email spam. source

Description

SPF is the most basic email authentication method. It involves simple DNS records that allow you to specify what servers email can originate from for the domain specified in the email envelope.

Read More

Example

As an example, `swigg.net` is setup with two SPF rules.

Domain	Type	Value
@	TXT	v=spf1 mx include:_spf.google.com include:me.com -all
*	TXT	v=spf1 mx:swigg.net -all

These two entries can be read as follows:

1. Any email ending in `@swigg.net` has to originate from one of the MX records defined for swigg.net **or** from a Google/Apple server defined in *their* SPF policy. Any other server sending email on behalf of this domain will be rejected.

2. Any email ending in `@*.swigg.net` has to originate from one of the MX records defined for swigg.net. Any other server sending email on behalf of these domains will be rejected.