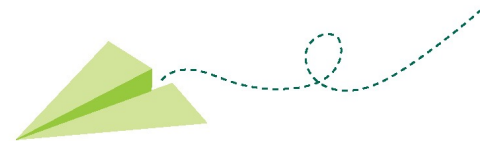




CENTRAL
MISSISSIPPI

Connect | Educate | Inspire | Secure





DNSSEC and Email Reputation

DNSSEC, SPF, DKIM, and DMARC Setup



CENTRAL
MISSISSIPPI

Agenda

- » Domain Name System Security Extensions (DNSSEC)
- » Sender Policy Framework (SPF)
- » DomainKeys Identified Mail (DKIM)
- » Domain-based Message Authentication, Reporting and Conformance (DMARC)



Domain Name System Security Extensions (DNSSEC)

- » A suite of extension specifications for securing data exchanged in the Domain Name System (DNS) in Internet Protocol (IP) networks
- » It provides cryptographic authentication of data, authenticated denial of existence, and data integrity
- » Doesn't provide availability or confidentiality



Definitions

- » Key Signing Key (KSK)
 - Used to sign other DNSKEY records containing zone signing keys (ZSK)
- » Zone Signing Key (ZSK)
 - Used to sign other records
- » DS record
 - A message digest of the KSK
 - It's a record used to identify the DNSSEC signing key of a delegated zone

Creating the ZSK and KSK

» Uses the `ldns-keygen` command

- Part of the OpenBSD LDNS utilities package
- Create the key with an algorithm specified using the “-a” option
- The “-k” option is used to create a key signing key

Files Output by Idns-keygen

» Creates 3 files

- .key file with the public DNSKEY
- .private file with the private keydata
- .ds with the DS record of the DNSKEY record.



Signing the Zone

- » Uses the `ldns-signzone` command
 - Part of the OpenBSD LDNS utilities package
 - The command creates a new zonefile that contains RRSIG and NSEC resource records
 - Use of NSEC3 is specified using the “-n” option
 - Salt for the zone signing is provided by the “-s” option

Configuration for nsd(8)

zone:

name: "isc2chapter-cms.org"

zonefile: "master/isc2chapter-cms.org.signed"

notify: 2001:19f0:5c00:1331:5400:4ff:feb7:50fb sys1.rbcarleton.net.

provide-xfr: 2001:19f0:5c00:1331:5400:4ff:feb7:50fb sys1.rbcarleton.net.



Generating the DS Zone Entry

- » Uses the `ldns-key2ds` command
 - Part of the OpenBSD LDNS utilities package
 - Transforms a public DNSKEY Resource Record (RR) to a DS RR
 - The “-n” option can be used to send the DS RR to the standard out instead of a file
 - The “-f” option is used to ignore the SEP flag
 - The “-2” option is used to use SHA256 as the hash function



DS Record TLD Submission

» GoDaddy example

- Key Tag
- Algorithm
- Digest Type
- Digest



Zone Resigning

- » Necessary when updating DNS
- » Uses the `ldns-signzone` command as when initializing a zone



Sender Policy Framework (SPF)

- » An email authentication method that ensures the sending mail server is authorized to originate mail from the email sender's domain
- » Authentication only applies to the email sender listed in the "envelope from" field during the initial SMTP connection



Example SPF Record

600 IN TXT "v=spf1 ip4:143.244.220.150 a mx -all"

- » v = version
- » ip4 = for matching the sender address
- » a = indicates the sender has an address record that matches the senders address
- » mx = indicates the sender has an address record that matches the mail servers address
- » -all = for all IPs not matched by prior mechanisms



DomainKeys Identified Mail (DKIM)

- » An email authentication method designed to detect forged sender addresses in email
- » DKIM signing provided by the OpenBSD opensmtpd-filter-dkimsign package



Setting up filter-dkimsign

- » Generate a private key
- » Generate public key for DNS
- » Add the DNS record
- » Configure the mail server to sign email



Domain-based Message Authentication, Reporting and Conformance (DMARC)

- » An email authentication protocol designed to give email domain owners the ability to prevent email spoofing
- » It extends SPF and DKIM



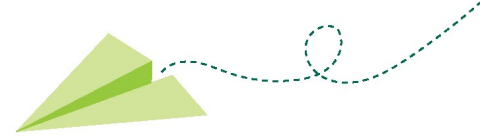
Example DMARC record

```
_dmarc 600 IN TXT "v=DMARC1;p=reject;sp=reject;pct=100;adkim=r;aspf=r;fo=1;ri=86400;rua=mailto:dmarc@rbcarleton.net"
```

- » v = version
- » p = policy
- » sp = subdomain policy
- » pct = percentage of bad email that the policy applies to
- » adkim = DKIM policy alignment (r for relaxed)
- » aspf = SPF policy alignment (r for relaxed)
- » fo = Failure reporting options
- » ri = requested interval between aggregate reports
- » rua = URI to send aggregate reports to (an email address)



Questions



CENTRAL
MISSISSIPPI

References

» Domain Name System Security Extensions (DNSSEC)

- Wikipedia article “Domain Name System Security Extensions”
 - https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- OpenBSD Idns-keygen(1), Idns-signzone(1), and Idns-key2ds(1) manual pages from the Idns-utils package
- OpenBSD nsd(8), nsd-control(8), and nsd.conf(5) manual pages

» Sender Policy Framework (SPF)

- Wikipedia article “Sender Policy Framework”
 - https://en.wikipedia.org/wiki/Sender_Policy_Framework

» DomainKeys Identified Mail (DKIM)

- Wikipedia article “DomainKeys Identified Mail”
 - https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail
- OpenBSD nsd-checkzone(8) man page
- From the the opensmtpd-filter-dkimsign package
 - OpenBSD filter-dkimsign(8) man page
 - /usr/local/share/doc/pkg-readmes/smtpd-filter-dkimsign

» Domain-based Message Authentication, Reporting and Conformance (DMARC)

- Wikipedia article “DMARC”
 - <https://en.wikipedia.org/wiki/DMARC>

