How safe is your domain?

Michael Kehoe
Sr Staff Security Engineer
Agenda

01 $ whoami
02 Introduction
03 DNS & Domain threat models
04 Top 1000 domain statistics
05 Registrar protection
06 Nameserver safety
07 DNS records for mail
08 Other best practices
09 Demo: Domain-Labs.com
10 Q & A
$ whoami
$ whoami

• Sr Staff Security Engineer - Confluent
  • Cloud Architecture & Reliability

• Previously:
  • Sr Staff SRE @ LinkedIn
  • PhoneSat intern @ NASA

• Background in:
  • Networks
  • Microservices
  • Traffic Engineering
  • KV Databases
  • Incident Management

• Twitter: @michaelkkehoe
• LinkedIn: linkedin.com/in/michaelkkehoe
• Website: michael-kehoe.io
Introduction
Threat-models for DNS & Domains
## Basic DNS Threat model

<table>
<thead>
<tr>
<th></th>
<th>Denial of Service/ Availability</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>• DNS records are resolvable during outage/ DDoS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Spoofing/ Authentication</th>
<th></th>
</tr>
</thead>
</table>
| 02 | • Pretending to be someone else (i.e mail spoofing)  
• Typosquatting/ Bitflipping/ Homoglyph on domains |   |

<table>
<thead>
<tr>
<th></th>
<th>Tampering/ Integrity</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>• Modifying DNS responses in-transit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Repudiation/ non-repudiation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>• Verified mail senders</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Information disclosure/ Confidentiality</th>
<th></th>
</tr>
</thead>
</table>
| 05 | • Intercepting DNS traffic  
• Intercepting mail or other layer-7 services |   |
Top 1000* domain statistics

* Cloudflare Radar Top 1000 domains (only 929 domains provided full results)
How many domains are following all best-practices?
Domain Locks

- **17%**
  - Implement all controls
  - All 6 Server Lock & Client Locks are implemented

- **38%**
  - Implement half of controls
  - All 3 Client Locks are implemented

- **36%**
  - Implement one control
  - 1 Client lock is implemented

- **9%**
  - No controls implemented
  - No server lock or client lock is implemented
Nameserver Safety

- **25%**
  - Utilize diverse nameservers
  - Utilize more than 1 DNS provider

- **75%**
  - Do not have diverse nameservers
  - Only use 1 provider

- **5%**
  - Implement DNSSec
  - Protects the integrity of DNS responses

- **95%**
  - Do not implement DNSSec
  - Responses could be tampered with
Mail Server Safety

- **68%**
  - Have a SPF record
  - Specify which IPs can send mail for your domain

- **58%**
  - Have a DMARC record
  - Policy for unauthenticated messages

- **0.2%**
  - Implement TLSA
  - Authenticates public key of certificate with the TLS connection

- **1.5%**
  - Implement MTA-STS
  - Policy for determining if inbound mail must be encrypted
Misc Controls

8%

Implement security.txt
Lets the public know how to report security issues

25%

Implement CAA
Lists which Certificate Authorities can issue a certificate against your domain
What are the best practices?
Registrar Protection
Registrar Protection

Enable all locks
Ensure that your domain can only be modified through established procedures with the registrar.

Enable 2FA
Utilize (non-SMS) 2FA to provide extra security for account credentials.

Implement IP controls
Only allow your IP space to access your domain registrar.

Integrate SSO
If possible, authenticate with your domain registrar through your existing SSO solution.
Registrars that support server-locks

Known supporting registrars

- MarkMonitor, Inc.
- NOM-IQ Ltd dba Com Laude
- CSC CORPORATE DOMAINS, INC.
- RegistrarSafe, LLC
- Cloudflare, Inc.
- Nameshield SAS
- RegistrarSEC, LLC
- (Shanghai) Co., Ltd.
- Lexsynergy Limited
- Safenames Ltd
Nameserver Safety
Name Server Safety

- **Implement DNSSec**
  Ensure that DNS results for your domain are not modified by MITM attackers

- **Use multiple DNS providers**
  Remove a single point of failure and reduce the risk of DDOS/failure taking down your domains DNS resolution
DNS Records for Mail
DNS Records for Mail

1. SPF
   Specify what IP addresses can send email addresses for your domain

2. DMARC / DKIM
   DMARC: Policy for authenticating email and reporting
   DKIM: Provides authentication for email senders using public-keys

3. TLSA
   DNS record that is a SHA256 hash of the certificate public-key

4. MTA-STS
   Policy stating your domain requires authentication and encryption for SMTP connections.

5. SMTP-TLS
   Enables standard reporting on senders ability for secure email delivery to your domain.

6. BIMI / VMC
   An open standard that allows email senders to use their brand logo in emails.

https://email-security-scans.org/
https://support.google.com/mail/answer/13130196
https://www.mailhardener.com/
### Records for domains that do not send email

| SPF   | TXT      | Host: yourdomain.com  
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Value: v=spf1 -all</td>
<td></td>
</tr>
</tbody>
</table>

| DMARC | TXT      | Host: _dmarc.yourdomain.com  
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Value: v=DMARC1;p=reject;sp=reject;adkim=s;aspf=s;fo=1;rua=<a href="mailto:dmarc@anotherdomain.com">mailto:dmarc@anotherdomain.com</a></td>
<td></td>
</tr>
</tbody>
</table>

| DKIM  | TXT      | Host: *._domainkey.yourdomain.com  
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Value: v=DKIM1; p=</td>
<td></td>
</tr>
</tbody>
</table>

| MX    | MX       | Host: yourdomain.com  
|-------|----------|----------------------|
|       | Priority: 0  
|       | Value . |  

https://www.gov.uk/guidance/protect-domains-that-dont-send-email
Other best security practices
Implement security.txt
Let people know where/how to report security issues

Implement CAA records
Restrict what CA's can issue certificates for your domain

https://securitytxt.org/
https://docs.digitalocean.com/products/networking/dns/how-to/create-CAA-records/
Demo: domain-labs.com
Scan your site now

Security Report Summary

Site: https://michael-kehoe.io/
IP Address: 99.83.231.61
Warning: Grade capped at A, please see warnings below.

Advanced: Great grade! Perform a deeper security analysis of your website and APIs:

Warnings

Content-Security-Policy
This policy contains `unsafe-inline` which is dangerous in the script-src directive. This policy contains `unsafe-inline` which is dangerous in the style-src directive.

Raw Headers
domain-labs.com

Scan your domain now

Recent Scans
- yahoo.com - 65
- yahoo.net - 35
- youtubecookie.com - 30
- youtube.com - 40
- zemanta.com - 27
- zoom.us - 35

Hall of Fame
- yahoo.com - 65
- paypay.com - 55
- g0t.com - 50
- chaturbate.com - 50
- classdojo.com - 50
- dipict.com - 50
- ebay.com - 50
- google.com - 50
- hotmail.com - 50
- linkedin.com - 50

Hall of Shame
- anythinktech.com - 5
- appsflyersdk.com - 5
- browser-intake-datadoghq.com - 5
- c0000.com - 5
- imotive2.com - 5
- imotech.tech - 5
- kishi.tech - 5
- itwebstatic.com - 5
- onetrust.io - 5
- palmplaystore.com - 5
Scan your domain now

Safety Report Summary

Domain: yahoo.com
FLD: yahoo.com
Authorative Zone: yahoo.com
Report Time: 2023-06-14 00:58:51.343804
Score: 65/79

Domain Registration and Registrar

domain_lock_check: PASS 10/10 Found all 6 domain locks at FLD: yahoo.com
domain_registrar_dnssec: FAIL 0/5 [yahoo.com] Failed to find a valid DNSSEC WHOIS record

DNS Records

bimi_record_check: FAIL 0/5 Failed to resolve a BIMI record at: default._bimi.yahoo.com.
domain_txt_verification: PASS 5/5 Found google-site-verification TXT record
dmarc_record_check: PASS 5/5 Successfully found DMARC record at: _dmarc.yahoo.com.