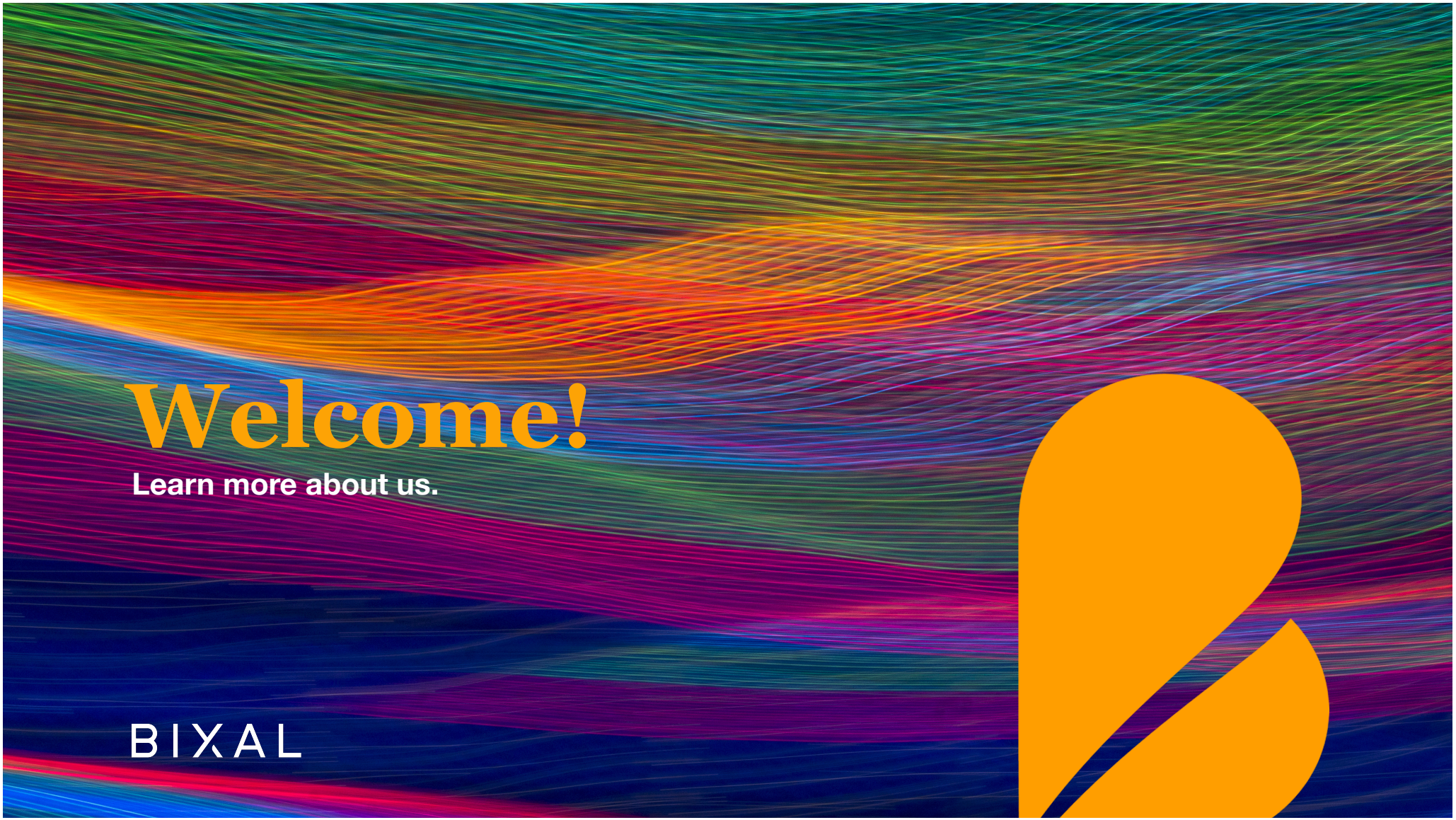
DNSSEC and the Web

How to improve security and reliability for the Web with DNSSEC

BIXAL | John Franklin, 20 February 2022

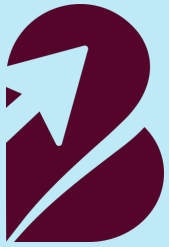

Welcome!
Learn more about us.
BIXAL

We are Bixal, an organization determined to leave a positive impact on the lives of people everywhere.

We believe in the potential of our government to deliver on this mission at a scale like nothing else in the world.

Bixal is a diverse group of strategists, designers, engineers, and thinkers.

Strategic Communications



Human-Centered Design

Agile Development

Modernized Learning

Data Science and Analytics

Cloud Computing

Want to join our team?

Apply through our website:

www.bixal.com/careers

Don’t see what you’re looking for?

Submit your resume through our “General Opportunities” position.

A Short DNS Primer

DNS: How does it work?

- Query / Answer
  - Q: `www.bixal.com. A?`
  - A: `www.bixal.com. => CNAME d2id3snkxmh9hv.cloudfront.net.`

- Server Types
  - Forwarding resolver – passes the query on to another resolver.
  - Recursive resolver – performs multiple lookups to find the answer.
  - Authoritative server – serves the resources records for one or more zones.

DNS Nomenclature

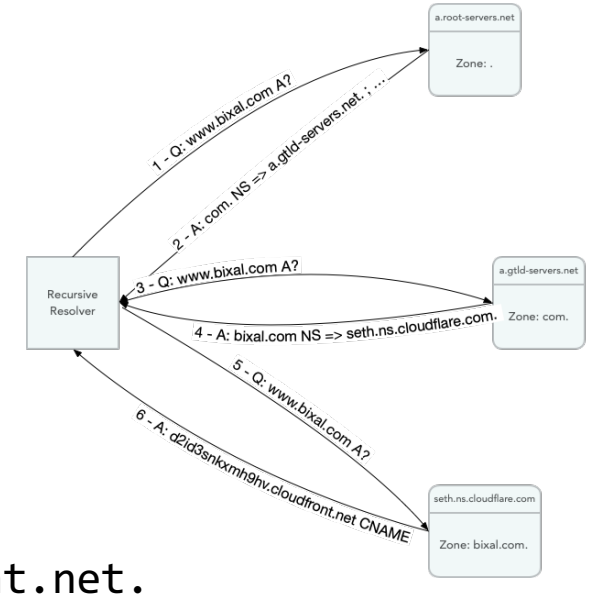
- Domain – A namespace, e.g., bixal.com or com.
- Zones – A collection of Resource Records (RRs) under a common domain.
- Resource Records – Individual records in a zone.
  - `www IN A 1.2.3.4`
  - `bixal.com. IN MX 10 mx.bixal.com.`
- Root zone – The zone for the root domain “.” (dot)

DNS: Recursive Resolvers

- Q: `@a.root-servers.net. www.bixal.com. A?`
- A: `com. NS a.gtld-servers.net.`

- Q: `@a.gtld-servers.net. www.bixal.com. A?`
- A: `bixal.com. NS seth.ns.cloudflare.com.`

- Q: `@seth.ns.cloudflare.com. www.bixal.com A?`
- A: `www.bixal.com. CNAME d2id3snkxmh9hv.cloudfront.net.`



DNS Resource Records (RRs)

- SOA – Start of Authority
- NS – Name Server
- A – IPv4 address
- AAAA – IPv6 address
- TXT – Text (free form)
- MX – Mail Exchange (where to send emails for a domain)
- CNAME – Canonical Name

DNS Overview

- Built to be a global, distributed lookup engine.
  - Because hosts.txt didn’t scale. (No shock there.)
- Security? Why? It’s public data!
- Three Pillars of Security:
  - Confidentiality – only those with permission can read the data.
  - Integrity – only those with permission can create the data.
  - Availability – what good is data you can’t access?

DNS: A Problem of Integrity

- In 2008, Dan Kaminsky discovered a cache poisoning attack.
  - Attackers could change the IP addresses returned for a hostname.
  - The “fix” doesn’t fix it, just makes it 65k times more difficult.
- Need a way to verify the integrity of data returned.
- Digital signatures!
  - RFC 4033 describing DNSSEC was published in March 2005.

Encryption & Digital Signatures

Encryption 101

- Symmetric encryption
  - Same key encrypts and decrypts.
  - Fast – Modern CPUs include extensions to support AES.
- Asymmetric encryption
  - Requires a key pair.
  - Anything encrypted with one can ONLY be decrypted with the other.
  - Designate one “private”, and one “public”.
- Digital signature
  - Create a checksum of the data, encrypt with the private key.
  - Receiver creates same checksum, compares with encrypted copy.

DNSSEC

- Add digital signatures to the RRs.
- Publish public keys as their own RR.
- Adds new RRs
  - RRSIG – Resource Record signature
  - DNSKEY – Public signing key for a zone.
  - DS – Delegation signer, a hash of the DNSKEY (KSK).
  - NSEC/NSEC3 – “Next SECure” records (proves non-existance of RRs)

DNSSEC Queries

- Q: `@ns.bixal.com www.bixal.com. A?`
- A:

```
www.bixal.com. CNAME d2id3snkxmh9hv.cloudfront.net.

www.bixal.com. RRSIG CNAME 13 3 bixal.com.
  fsgSbrY5DrPbZsC2UzC9sDdnmSFYBy1qKDnQCuTJFcglqfBHFRX8AXtF
  7+PIekHk0qTdJRfOQqpogLk1E5bW7Q==
```

Why do I care?

- Cache poisoning attacks redirect users before you see them.
  - Hard to detect!
- Federal government is working to enable DNSSEC across .gov.
  - https://fedv6-deployment.antd.nist.gov/cgi-bin/generate-gov
- If your DNS provider supports DNSSEC, deployment is trivial.
  - If they don't, consider changing DNS providers. Seriously.
- Improved infrastructure security and website performance.
  - Wait, what? Web site performance?

Secure DNS Resources

SVCB and HTTPS RRs

- SVCB – Service Binding
  - IETF Internet-Draft
  - Define service aliases or service parameters.
  - Provide server ECHConfigList for ECH (Encrypted Hello) messages.

- HTTPS – SVCB specifically for HTTPS

```
$ORIGIN bixal.com
@ HTTPS 0 d2id3snkxmh9hv.cloudfront.net.

$ORIGIN cloudfront.net.
d2id3snkxmh9hv HTTPS 1 . alpn=h2,h3 ech="abc..." port=8443
d2id3snkxmh9hv HTTPS 2 d2id3snkxmh9hv-legacy alpn=http/1.1 port=443
```

DANE

- DNS Authentication of Named Entities
- Leverages the DNSSEC trust to extend to system certs and keys.

- TLSA – Define the cert or CA cert for the host.
  - Prevent forged SSL certs
- SSHFP – SSH Fingerprint
- SMIMEA – S/MIME certificate for email address.

DANE – TLSA

- Defines:
  - a cert that is used for a service OR
  - a cert that signs the end cert.
- Usable for any service that uses TLS.
- Signals mandatory TLS usage, like HSTS.
- Examples:
  - `_143._tcp.mail  TLSA [cert]`
  - `_22._tcp.jump-proxy  TLSA [cert]`

DANE – SSHFP

- Defines the host SSH Fingerprint
- No more TOFU!
- Create with `ssh-keygen -r <hostname>`

```
jump-proxy IN SSHFP 1 1 81dd539758c46c2dd8efdaa8c1499c3deac820a3
```

DANE – SMIMEA

- Defines the S/MIME certificate for an email address.
  - “hostname” is partial sha256 for user name.
- Pros: can publish S/MIME certs
- Cons:
  - Can easily determine valid email addresses
  - Email address becomes case-sensitive

- `C93f1e…1c1afd6._smimecert.bixal.com. SMIMEA [cert]`

DNSSEC

- What can it do for you?

  - Better ensure users get to your site.
  - Alias the apex of your domain to a load balancer.
  - With emerging protocols (http/2, quic), make the connections faster.
  - Better secure the ops infrastructure hosting your site.

Go forth and secure!

Thank You

BIXAL