DNSSEC

Kyle Rankin
Director of Engineering Operations
Artemis Internet, Inc.

http://greenfly.org/talks/security/dnssec.html

Agenda

- Introduction
- How DNS Works
- DNS Security Issues
- How DNSSEC Works
- DNSSEC Terminology
- New DNSSEC Record Types
- DNSSEC Look-aside Validation
- Implementing DNSSEC
- Current DNSSEC Adoption
- DANE
- Questions?

How DNS Works

- Primary job: converting hostnames to IPs
- Client sends request to local DNS server
- "What is the IP for www.greenfly.org?"
- DNS server starts recursive query
- To play at home: dig +trace www.greenfly.org.

Tracing a Recursive Query

1. **ns1.someisp.com** to **root**: *www.greenfly.org?*
2. **root** to **ns1.someisp.com**: *I don't know, ask a org nameserver. Here are their addresses...*
3. **ns1.someisp.com** to **org**: *www.greenfly.org?*
4. **org** to **ns1.someisp.com**: *No clue, but ns1.greenfly.org and ns2.greenfly.org know about it. Here are their addresses...*
5. **ns1.someisp.com** to **ns2.greenfly.org**: *www.greenfly.org?*
6. **ns2.greenfly.org** to **ns1.someisp.com**: *64.142.56.172*
7. **ns1.someisp.com** to **OS**: *64.142.56.172*
8. **OS** to **browser**: *64.142.56.172*

DNS Security Issues

- DNS designed to be an open, friendly service
- DNS queries and responses are not encrypted
- Domain names sometimes look alike (google.com vs googIe.com)
- Companies can't always register their name on all TLDs (artemis.com)
- Many DNS servers (open resolvers) will perform recursive queries for anyone who asks
- Open resolvers heavily used in modern DNS amplication DDOS attacks
- DNS subject to MitM attacks
- DNS spoofing/cache poisoning attacks.

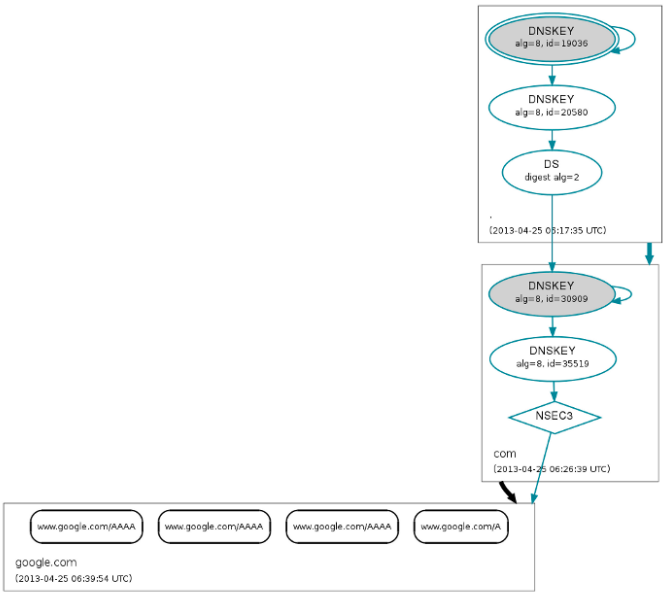
DNSSEC Addresses

- DNS designed to be an open, friendly service
- DNS queries and responses are not encrypted
- Domain names sometimes look alike (google.com vs googIe.com)
- Companies can't always register their name on all TLDs (artemis.com)
- Many DNS servers (open resolvers) will perform recursive queries for anyone who asks
- Open resolvers heavily used in modern DNS amplication DDOS attacks
- ~~DNS subject to MitM attacks~~
- ~~DNS spoofing/cache poisoning attacks.~~

How DNSSEC Works

- Some similarities with CA system
- Uses public-key cryptography to sign every DNS record for a zone
- DNS servers generate key pair, sign records with private key
- Root DNS servers have key pair, DNSSEC-enabled
- DNSSEC-enabled TLDs get key signatures signed, published by root DNS
- DNSSEC-enabled zones get key signatures signed, published by TLD
- DNSSEC-capable resolvers anchor trust in root DNS keys
- When DNSSEC records resolve, chain of trust is followed
- If record tampered with, signature won't match
- If record doesn't exist, absence is also signed.

Trust graph for www.google.com



DNSSEC Terminology

- RR - Resource Record: smallest unit of data in a zone (A, NS...)
- RRSET - Complete Set of Resource Records (all NS records or A records for a name)
- KSK - Key-Signing Key. Signs DNSKEY records in a zone
- ZSK - Zone-Signing Key. Signs all of the other records in a zone
- SEP - Secure Entry Point. Flag set in key to denote it as a KSK
- Separate KSK, ZSK not required, but best practice
- Allows larger KSK, easier rotation of ZSKs.

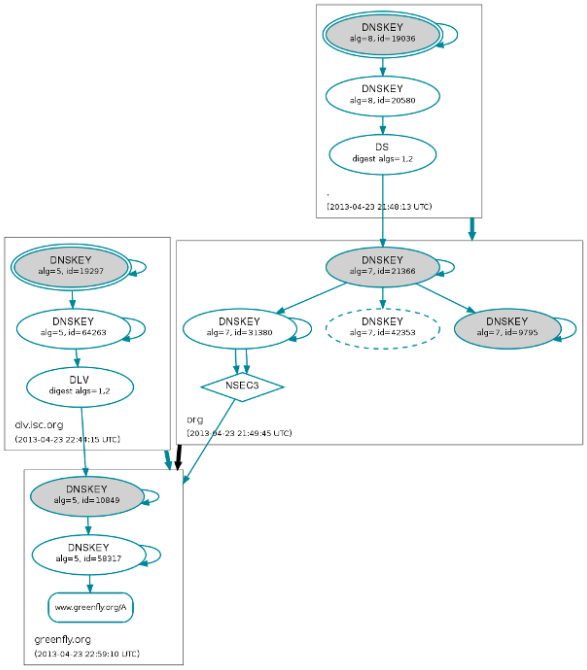
New DNSSEC Record Types:

- DNSKEY - A public key for the zone, either KSK or ZSK
- RRSIG - Resource Record Signature, contains a signature for an RRSET
- NSEC - Next Secure, used in "negative answers" to prove whether a name exists or not
- NSEC3 - Next Secure (version 3). Like NSEC, protects against "zone walking"
- DS - Delegation Signer. Contains KSK signature and submitted to zone parent as part of chain of trust
- DLV - DNSSEC Look-aside Validation. Much like DS records, used when DS records not supported.

DNSSEC Look-aside Validation

- Work-around solution until DNSSEC is fully adopted by TLDs
- Or if a registrar doesn't support DNSSEC
- Changes trust anchor from root to a third-party, like dlv.isc.org
- Requires DNS resolvers to add/trust third-party keys.

Trust graph for www.greenfly.org



Implementing DNSSEC

- Create KSK and ZSK

```
$ dnssec-keygen -a RSASHA1 -b 2048 -n ZONE -f KSK greenfly.org
$ dnssec-keygen -a RSASHA1 -b 1024 -n ZONE greenfly.org
```

- Include references to keys in zone file (db.greenfly.org):

```
$INCLUDE Kgreenfly.org.+005+10849.key ; KSK
$INCLUDE Kgreenfly.org.+005+58317.key ; ZSK
```

- Sign the zone using KSK and ZSK:

```
dnssec-signzone -o greenfly.org -k Kgreenfly.org.+005+10849 \
  db.greenfly.org Kgreenfly.org.+005+58317.key
```

- Or if using DLV:

```
dnssec-signzone -l dlv.isc.org -o greenfly.org -k Kgreenfly.org.+005+10849 \
  db.greenfly.org Kgreenfly.org.+005+58317.key
```

Implementing DNSSEC Continued

- Configure BIND to use signed zone:

```
zone "greenfly.org" {
  type master;
  file "/etc/bind/db.greenfly.org.signed";
  allow-transfer { slaves; };
};
```

- Enable DNSSEC in BIND masters and slaves:

```
options {
  dnssec-enable yes;
  dnssec-validation yes;
};
```

- To validate DLV zones, add additional BIND option and trusted key:

```
options { dnssec-lookaside . trust-anchor dlv.isc.org.; };
trusted-keys {
        dlv.isc.org. 257 3 5 "BEAAAAPHMu/5onzrEE7z1egmhg/WPO0+juoZrW3euWEn4MxDCE1+lLy2 brhQv5rN32RKtMzX6Mj70jdzeND4XknW58dnJNPCxn8+jAGl2FZLI
};
```

Sample DNSSEC Query Result

```
$ dig +dnssec www.greenfly.org

; <<>> DiG 9.8.1-P1 <<>> +dnssec www.greenfly.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13093
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.greenfly.org.               IN      A

;; ANSWER SECTION:
www.greenfly.org.       900     IN      A       64.142.56.172
www.greenfly.org.       900     IN      RRSIG   A 5 3 900 20130523213855 20130423213855 58317 greenfly.org. cZS1G2Jj3FNBOUrU4W+LbpCJ1vVa+3yos1ni5VOpct4x41WvXGQNoh1G /uFFJ62YRYXskL/c17wiAEIqsJOO/wzekSKFWAoiJ3zWO5119c/8KPGF 7LzmEumdAVW2MmrPVu+PKGfi1P1fofjwJLbgVhyYqepbbD8xv3bmg0Np YnM=

;; AUTHORITY SECTION:
greenfly.org.           900     IN      NS      ns2.greenfly.org.
greenfly.org.           900     IN      NS      ns1.greenfly.org.
greenfly.org.           900     IN      RRSIG   NS 5 2 900 20130523213855 20130423213855 58317 greenfly.org. d/7E3iCxzS/qBSOl/x7m/yWqbl5mUGH7tVw/j7U/qyC7D9YZJIXNp3J uU8vueo09cZf+yjwHusdWDWgdW8mkAVoGRSK/azoY4o2xRBvt8ZSpf3a BqmNIHzROZkf6BOrx6Nqv6SnpSGoNLQBoEc90FvDFe/NSI27LBTIxCv4 3UQ=

;; ADDITIONAL SECTION:
ns1.greenfly.org.       900     IN      A       64.142.56.172
ns2.greenfly.org.       900     IN      A       75.101.46.232
ns1.greenfly.org.       900     IN      RRSIG   A 5 3 900 20130523213855 20130423213855 58317 greenfly.org. VDeJS1fEYRwHkjRnCvmDXFHneG3Fhw15mCSALT8m8fOtQkNroI8t0qu3 K8Tdt4q8/t1JYucpwQbpjsR3f+rmJcOt4L7HSVA/1LHajOqA+Wn2XH8L Rp01qVkeBIZ7g+K7LY2XRU3DGSzbeFUKrViqtakbTQxZ9o3Oj6ZqLOPv 0nQ=
ns2.greenfly.org.       900     IN      RRSIG   A 5 3 900 20130523213855 20130423213855 58317 greenfly.org. dUU/6bbc6sHoS1+e2uGwoEXLMGyr4Qaedk3E74ArnUOb4VViBd3CxvGF SPG2QK3AggDv8z3+9Wm6NA11oTFcuIGnbBarxDQIrbERHFfcSQaekvSR UcSSD7wft9YO7UTIiQrc8LkItXZAKd72Gy1ZP4mhhLxwwOIh1HshQ9d2 uTY=

;; Query time: 196 msec
;; SERVER: 64.142.56.172#53(64.142.56.172)
;; WHEN: Fri Apr 26 16:13:22 2013
;; MSG SIZE  rcvd: 817
```

Current DNSSEC Adoption

- DNSSEC Deployed at root zone on July 15, 2010
- 463 Total TLDs in root zone
- 271 TLDs are signed
- 265 TLDs have trust anchors published as DS records in the root zone
- 4 TLDs (.ee, .kg, .th, .ua) also have trust anchors published in the ISC DLV Repository
- (Data from ICANN TLD DNSSEC report accurate as of 2014-02-22.)

DANE

- DANE (DNS-based Authentication of Named Entities) proposed on top of DNSSEC
- Defined in RFC 6698
- DANE authenticates TLS w/o CAs using DNSSEC-signed keys
- Shifts trust from CAs to root DNS, TLDs, and DNS admin
- Supported in Chrome since 2011
- Supported in Firefox with add-on.

Questions?

Additional Resources

- Collection of DNSSEC information: http://dnssec.net/
- ISC's DLV Documentation: https://dlv.isc.org
- RFC4033: DNS Security Introduction and Requirements: https://tools.ietf.org/html/rfc4033
- RFC4034: DNSSEC Resource Records: https://tools.ietf.org/html/rfc4034
- RFC4035: Protocol modifications for DNSSEC: https://tools.ietf.org/html/rfc4035
- RFC4641: DNSSEC Operational Practices: https://tools.ietf.org/html/rfc4641
- DNSSEC HOWTO: http://www.nlnetlabs.nl/publications/dnssec_howto/
- ICANN TLD DNSSEC Report: http://stats.research.icann.org/dns/tld_report/
- DNS Visualizer: http://dnsviz.net
- http://greenfly.org/talks/security/dnssec.html