DNS security extensions

ENOG IV / RIPE NCC Regional Meeting

23 – 24 October 2012, Moscow

Security related RR

- CERT
- TLSA, SMIMEA* (DANE)
- CAA*
- SSHFP
- SPF

PKIX problems

- Self-signed certificates (~48% web servers)
- A lot of local CA
- Big number of CA (>160) without any confidence in their security level
- Many different CA storages on every system
- A lot of preinstalled CA
  - Hard to delete compromised CA from default lists
  - Local CA`s are not able to get into default CA lists
    - I.CA (cz.) is one of the examples
- Certificate validation problems
- There are number of "fake" certificates around for valid domains, including Google, Paypal, etc.

Some known problems with CA

- DigiNotar CA disaster - poor security, systems were not isolated or audited
- ComodoGate Case - fake certificates for google, yahoo, skype, mozilla, etc. possibly state-driven attack (Iran), more than 500 rogue certificates!
- Trustwave CA - delegation to third parties for decryption of the proxied https traffic
- Current model allows any of these CAs to issue a certificate for any domain name

Certificate validation problems

- Unpredictable behavior if access to CLR URL is broken
- Adds latency to HTTPS
- Can block access to the web site in case of DDOS to CRL server
- OCSP responder having similar issues

Vendor-specific workarounds

- Google DNS bases certificate catalog
  - dig +short 405062e5befde4af97e9382af16cc87c8fb7c4e2.certs.googlednstest.com TXT – "14867 15062 74"
- DNSSEC stapled certificate in Chrome
  - Validates DNSSEC chain embedded at certificate
- Conspiracy Mozilla extension
  - Track certificate changes

Storing Certificates in the DNS

- **CERT** RR described in RFC 4398
  - Allows to store X.509 certificates/CRLs or OpenPGP certificates/revocation
- CERT support added at BIND 9.7 and NSD 3.0.5
- Client behavior is not specified precisely
- Not implemented in browsers and other common software
- Implemented in GnuPG 1.4.3 and later
  - There are also some unofficial methods for OpenPGP exists like a publishing TXT record under _pka namespace
  - See http://www.gushi.org/make-dns-cert/HOWTO.html

DNS-based Authentication for Named Entities [1]

- Before: Trusted CA → Certificate → Domain
- DANE use cases
  - CA constraints
    - Specified certificate should be in any PKIX certification path of presented certificate
  - Service certificate constraints
    - Specified certificate should match presented certificate, but it also should pass PKIX certification path validation
  - Own trust anchor
    - Presented certificate should pass PKIX path validation if specified certificated used as a trust anchor
    - Specified certificate should match presented certificate, PKIX path validation is not preformed in this case
- New **TLSA** RR for _port._protocol. domain
    - *_443._tcp.www.example.com. IN TLSA (0 0 1 d2abde240d7cd3ee6b4b28c54df034b9 7983a1d16e8a410e4561cb106618e971)*

DNS-based Authentication for Named Entities 2

- DANE binds certificates with domain names
- CA binds certificates to authorities, organizations, persons, locations

DNS-based Authentication for Named Entities [3]

- DANE protocol and use cases defined in RFC 6394, 6698
- DANE for S/MIME in drafts
  - SMIMEA RR
    - MFXHI33O._smimecert.cloudedlynx.org. IN SMIMEA (anton in Base32 →MFXHI33O)
- DANE for POP3, IMAP and SMTP in drafts
  - Defines client behavior

DNS-based Authentication for Named Entities [4]

- DANE can be a key feature for DNSSEC development growth
- Service owners should be confident in their DNS operator

- DANE implementations:
  - add-on for Firefox
  - implementation for NSS (Network Security Services by Mozilla)
  - Visit dane.verisignlabs.com if you browser supports DANE
- NSD 3.2.11, BIND 9.8.3

Certification Authority Authorization

- CAA RR –
  - specifies CA's authorized to issue certificates for domain and specific properties for them
  - performed by a certificate issuer before issue of a certificate
  - only reducing risk of unintended certificate mis-issue
- Different to TLSA that
  - used to check issued certificates
  - performed by a client
- CAA RR currently in drafts

End of the CA dinosaurs’ era?

- Not for all cases…
  - Very large existing infrastructure
  - Organizations (banks & etc.) and authorities (governments) CA
  - Organization and person validation
  - Extended validation, biometric data, etc.
- And…
  - It will take a time to upgrade existing software
  - DNSSEC is still not widely implemented

What you can do?

- Add IPv6 support to your DNS infrastructure
  - A lot of major local companies (registrars, hosting companies) hadn’t done it yet
    - 4 of 25 ru./рф. registrants have IPv6-enabled NS servers
- Add DNSSEC to your infrastructure domains
- Move SPF from TXT to SPF RR or keep them both
- Protect your services with CERT, TLSA, SSHFP records
- Allow your customers to do the same
  - Add SPF, SRV, NAPTR, CERT, TLSA, SSFP, etc. support
  - Allow custom type records if possible
  - Allow clients to make their own secondary NS servers

Anton Baskov
<anton@ministry.int.ru>

DNS security extensions at ENOG IV
23 – 24 October 2012, Moscow

Based at ENOG III presentation by Anton Baskov *<anton@ministry.int.ru>* and Alex Samorukov *<samm@net-art.cz>*