All over DNS BoF

ENOG III / RIPE NCC Regional Meeting

22 – 23 May 2012, Odessa

BoF Agenda

- Regional ENUM status update
- DNS – Addressing, Security
- DNS RPZ
- FRED and other NIC.CZ activities
- Tunnels over DNS

- We have only one hour for presentations and discussions

ENUM BoF / ENOG II

- Russia
  - In consideration of the Ministry
  - Number portability announced by Dmitry Medvedev
- Ukraine
  - Delayed
- New addressing

ENUM / Ukraine

- Опытная эксплуатация планируется в III квартале 2012 года
- Разработаны основные регуляционные документы, которые были упомянуты на прошлом ENOG, но оказалось, что необходимо разработать большее количество приложений для реализации проекта
- Проект по переносимости тормозится из-за позиции Администрации связи, которая затягивает согласования
- Вопрос находится на контроле в Администрации Президента. Ожидаем организационно-административные выводы

DNS

- DNS
  - World largest distributed database: reliable, distributed, secure, w caching & ….
- Why application developers & end users treat DNS as only database for A and MX records?
  - Addressing: SRV, NAPTR, URI … DDDS
  - Security: DNSSEC, CERT, DANE, SSHFP, SPF, …
- Application developers don’t use all DNS possibilities even in cases where DNS designed for
- DNS operators doesn't provide such possibilities to end users

Addressing / Examples

- OpenID
  - DNS → HTTP (99% useless) → OpenID via HTML headers
  - DNS → OpenID via NAPTR
- URI Discovery
  - Contact data with NAPTR (like ENUM)
    - A lot of users currently have own domains that can be used as ID (for example provided by service operators like blog engines)
  - Services discovery & etc.
    - NAPTR+, URI, SRV

Addressing

- SRV: specify location for known services
  - _protocol + domain → host, port
- NAPTR: URIs mapping
  - domain → list of (service + …) + URI (regexp from domain) or SRV or host
- S-NAPTR: stores application service + protocol information for a given domain
  - domain → list of (service + protocol) + link to SRV record or host
- URI RR*: querying known service URIs mappings
  - _protocol + domain → URI
- U-NAPTR*: mapping application URIs for a given domain
  - extends S-NAPTR with URI as a target
  - domain → list of (service + protocol) + URI in addition S-NAPTR

* - drafts

Security

- CERT
- TLSA (DANE)
- 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 chaine embedded at certificate
- Conspiracy Mozilla extension
  - Track certificate changes

Storing Certificates in the DNS

- RFC4398 allows to store X.509 certificates/CRLs or OpenPGP certificates/revocations used by OpenPGP software
- Support for CERT resource records has been added to the Bind 9.7 DNS server.
- Implemented in GnuPG 1.4.3 and later
- Client behavior is not specified precisely
- Not implemented in browsers and other common software

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 (52) 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
- DANE for S/MIME in consideration
- 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)

End of the CA dinosaurs' era?

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

Pail Vixie
<paul@redbarn.org>

Anton Baskov
<anton@ministry.int.ru>

Sergey Myasoedov
<kaa@kaa.ru>

Jaromir Talir
<jaromir.talir@nic.cz>

Alex Samorukov
<samm@net-art.cz>

All over DNS BoF at ENOG III

22 – 23 May 2012, Odessa