Anton Baskov
<ab@antonbaskov.ru>

DNS-based Authentication of Named Entities (DANE)

ENOG 9

29 – 30 May 2015

Anton Baskov
<ab@antonbaskov.ru>

DANE – Аутентификация через DNS

ENOG 9

29 – 30 Мая 2015

Известные проблемы

- Самоподписанные сертификаты
  - примерно 48% веб серверов
- Огромное количество местных центров сертификации
  - Государственные, отраслевые и корпоративные центры сертификации
- Большое число «общеизвестных» CA
  - Более 200 предустановленных CA в Apple OS X Yosemite
  - Есть ли к ним доверие?

Известные проблемы

- Несколько хранилищ сертификатов доверенных CA в каждой системе
- Огромное число предустановленных CA в каждом из них
  - Сложно удалить скомпрометированный CA из подобного списка
  - Местным CA достаточно сложно попасть в подобные списки

Известные проблемы

- Каждый центр сертификации может выдать сертификат на любое имя (домен, организацию)
  - Таким образом появляются подложные сертификаты для сервисов Google, Paypal и т.п.
- Сложность проверки сертификата на отзыв
  - Задержка при соединении
  - Вопросы доступности CRL

CERT RR

- Запись CERT описана в RFC 4398
  - Позволяет хранить как сертификаты X.509, так и ключи OpenPGP
  - (Однако) Поведение клиента не определено!
- CERT RR поддерживается популярными DNS серверами
  - начиная с BIND 9.7 и NSD 3.0.5
- Не поддерживается браузерами и иными популярными приложениями
  - За исключением GnuPG
    - см. http://www.gushi.org/make-dns-cert/HOWTO.html

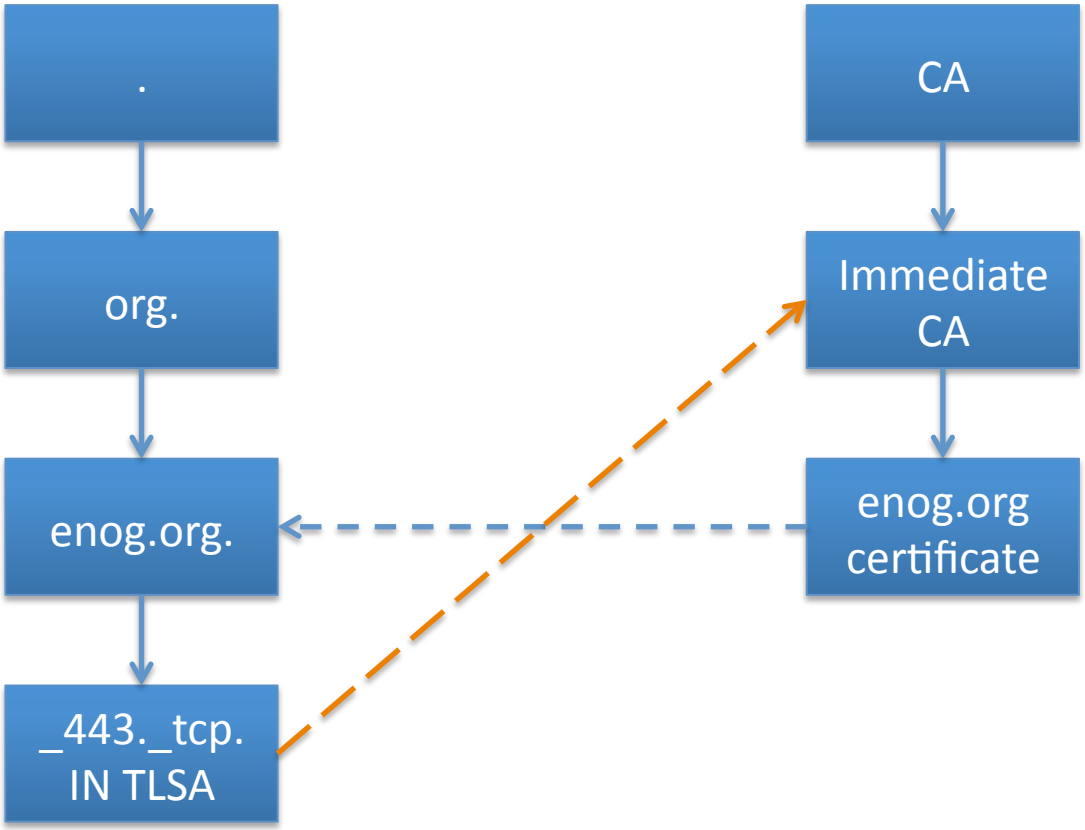
Certification Authority Authorization

- CAA RR
  - Указывает центр сертификации, которому можно выдавать сертификаты для данного домена
  - Дополнительный уровень проверки со стороны центра сертификации перед выдачей сертификата
  - Служит для уменьшения вероятности выдачи сертификата мошеннику
- DANE
  - Используется для проверки сертификата на стороне клиента
- RFC 6844

DANE

- PKIX: Доверенный CA → Сертификат → Ресурс (домен)
- DANE: Цепочка доверия DNSSEC → Домен → Ограничение на доверенный сертификат

DANE


.
org.
enog.org.
_443._tcp.
IN TLSA
CA
Immediate
CA
enog.org
certificate

Варианты использования

- Варианты использования DANE
  - Ограничение по CA
    - Указанный сертификат должен находится в цепочке сертификации представленного сертификата
  - Ограничение на сертификат
    - Представленный сертификат должен не только совпадать с указанным сертификатом, но и пройти проверку согласно цепочке сертификации
  - Собственный доверенный сертификат
    - Представленный сертификат должен пройти проверку согласно цепочке сертификации, если указанный сертификат являлся бы единственным доверенным сертификатом
    - Если представленный сертификат совпадает с указанным, то проверка цепочки сертификации не производится

DANE

- DANE связывает сертификат с доменом
- Центр сертификации удостоверяет иные сведения, указанные в сертификате
  - Например, принадлежность сертификата организации или физическому лицу, место выдачи и т.п.

DANE / TLSA RR

- _port._protocol.domain + **TLSA** RR
  - *_443._tcp.www.example.com. IN TLSA (0 0 1 d2abde240d7cd3ee6b4b28c54df034b9 7983a1d16e8a410e4561cb106618e971)*

  - RFC 6398: *DANE Transport Layer Security (TLS) Protocol – TLSA*
  - RFC 6394: *Use Cases and Requirements for DANE*

DANE / SRV*

- DANE for SRV
  - Defines client behavior
    - _xmpp-client._tcp.example.com. SRV 1 0 5222 im.example.net.
    - _5222._tcp.im.example.net. TLSA ...
  - См. draft-ietf-dane-srv

DANE / MX*

- DANE for SMTP
  - Defines client behavior
    - example.com. IN MX 10 mail.example.net.
    - _25._tcp.mail.example.net. IN TLSA ...
  - См. draft-ietf-dane-smtp-with-dane

DANE / S/MIME*

- S/MIME
  - <local-part-hash*>._smimecert.<domain> + **SMIMEA** RR
    - *db3cda86d4429a1d39c148989566b38f7bda0156296bd364ba2f878b._smimecert.antonbaskov.ru. IN SMIMEA*
      - *ab@antonbaskov.ru*
      - *UTF-8 lowercase SHA-2 224 HEX*
  - См. draft-ietf-dane-smime

DANE / OpenPGP*

- OpenPGP
  - <local-part-hash*>._smimecert.<domain> + **OPENPGPKEY** RR
    - *fb977b8b4d5903b85055620603._openpgpkey.antonbaskov.ru. IN OPENPGPKEY <Base64 Public Key>*
      - *ab@antonbaskov.ru*
      - *UTF-8 lowercase SHA-2 256 HEX truncated from right side to 28 octets*
  - См. draft-ietf-dane-openpgpkey

DANE

- DANE требует внедрения DNSSEC
- DANE требует доверия к оператору DNS

Конец эры центров сертификации?

- Не совсем…
  - Корпоративные, отраслевые и правительственные центры сертификации
  - Удостоверение владельца сертификата
    - Организации или физического лица
  - Extended validation, biometric data, etc.
- И кроме того
  - Обновление программного обеспечения затянется на долгий срок
  - DNSSEC до сих пор широко не распространён

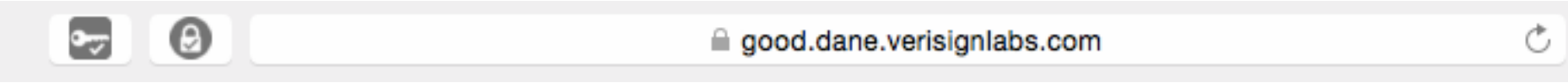
Практическая часть

Поехали!

Реализации

- HTTPS
  - DNSSEC/TLSA validator from NIC.CZ
- XMPP
  - Prosody mod_s2s_auth_dane
- SMTP
  - POSTFIX
- OpenPGP
  - openpgpkey-milter (encrypt outgoing emails on MUA/MTA side)
- S/MIME
  - Smaug (Verisign) / Smaug Thunderbird Plugin

Установите расширение браузера



- Установите DNSSEC/TLSA validator от NIC.CZ
  - Отображает состояние DNSSEC и TLSA
  - Safari, Chromium, Firefox, Internet Explorer, Opera
  - https://www.dnssec-validator.cz/pages/download.html
- Проверьте правильность установки
  - http://dane.verisignlabs.com/

Структура TLSA RR

- *_port._protocol.domain TTL IN TLSA 0 0 1 d2abde240d7cd3ee6b4b28c54df034b9 7983a1d16e8a410e4561cb106618e971*

- *Порт и протокол транспортного уровня*
  - *_443._tcp. – HTTPS*
  - *_5222._tcp. – XMPP S2S*

Структура TLSA RR

- Certificate usage
  - CA constraint = “0”
  - Service certificate constraint = “1”
  - Trust anchor assertion = “2”
  - Domain issued certificate = “3”
- Selector
  - Full certificate = “0”
  - Public key only = “1”
- Matching type
  - Exact match = “0”
  - SHA-256 hash = “1”
  - SHA-512 hash = “2”
- Data

0. Ограничения на CA

- Выполняется обычная проверка по цепочке сертификации
  - Корневой или промежуточный сертификат должны находится в списке доверенных сертификатов
- Указанный сертификат должен быть в цепочке сертификации

1. Ограничение на предъявляемый сертификат

- Выполняется обычная проверка по цепочке сертификации
  - Корневой или промежуточный сертификат должны находится в списке доверенных сертификатов
- Указанный сертификат должен совпадать с предъявленным

2. Указание доверенного сертификата

- Указанный сертификат является единственным доверенным сертификатом
- Выполняется проверка по цепочке сертификации при соблюдении вышеуказанного условия

3. Непосредственное указание сертификата

- Указанный сертификат должен совпадать с предъявленным
- Проверка по цепочке сертификации не производится

Сертификат

- SHA 256 – 32 октета
- SHA 512 – 64 октета
- Открытый ключ
  - 1024 бит = 128 октетов
  - 4096 бит = 512 октетов
- Сертификат
  - 4096 бит – примерно 1400 октетов

Создаем запись TLSA

- Terminal
  - **ldns-dane (ldns)** ← recommended
  - dane (sshfp)
  - tlsa (hash-slinger)
- Web
  - https://www.huque.com/bin/gen_tlsa
  - https://ssl-tools.net/tlsa-generator

В нашем случае

- https://test.enog.ru/
- test.enog.ru → 89.184.82.95
- Self-signed certificate

Итого:

- test.enog.ru. IN A 89.184.82.95
- _443._tcp.test.enog.ru. IN TLSA 3 0 1 …
  - ldns-dane create test.enog.ru 443 3 0 1
  - Domain issued certificate – 3
  - Full certificate – 0
  - SHA-256 – 1

Anton Baskov
<*ab@antonbaskov.ru*>

Вопросы?

ab@antonbaskov.ru