NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ

Internet Week 2010 DNSOPS.JP BoF

Phreebird Suite Introduction

2010年11月25日

NRIセキュアテクノロジーズ株式会社
MSS事業本部MSS事業部
ITセキュリティアナリスト

中島　智広 (@shima_nakatomo)

〒105-7113
東京都港区東新橋1-5-2 汐留シティセンター

おことわり

- 本資料はBoFでの情報共有を目的として作成した資料です
- 内容には配慮していますが正確性については保証できません
- 重大な誤りに気づいた場合は下記までご連絡いただけると幸いです
  ※修正をお約束するものではありません

nakashima@nri-secure.co.jp

Phreebird Suite

- Dan Kaminsky氏が発表したDNSSECを容易に実装するためのツール
  - ゼロコンフィギュレーションで動作するDNSSEC Proxy
    (既存のDNSの前段に設置することでDNSSEC対応が完了)
  - 小型軽量・高速がウリ(Phreebird単体でソースコード1400行)
  - いくつかの実験的な機能を実装
    - DNS over HTTP
    - DNS over X.509 over SSL
  - BSDライセンス

特徴

- 受け取った問い合わせクエリを背後のDNSに中継
- DNSからの応答に対してオンザフライで署名し問い合わせ元に回答
- 一度署名したレコードはキャッシュを保持して再利用
- 鍵はすべてのゾーンで同一のものを使用
- NSEC3の実装は騙し(White Lies)
- NSEC3 DoSへの対策としてRate Limitを実装
- 親ゾーンに登録するDSはクエリを投げて取得

導入手順@CentOS5.5

■インストール

```
# wget http://j.mp/9vI6L6
# tar zxpvf phreebird_suite_1.02.tar.gz
# cd phreebird_suite_1.02
# ./depbuild.sh
# make;make install
```

■鍵の生成

```
# phreepheed -g
```

■起動

```
# phreepheed -b 127.0.0.1:50053
```

※Listenポートが被らないようnamedは50053をListenしている想定

デモ

1. DNSに直接問い合わせ

```
# dig -p 50053 @localhost www.dnsesclab.org +dnssec
```

2. Phreebirdに問い合わせ

```
# dig @localhost www.dnsseclab.org +dnssec
```

3. Validatorで再起問い合わせ

```
# dig @validator www.dnsseclab.org +dnssec
```

4. DS/DNSKEYの取得

```
# dig @localhost dnsseclab.org ds  or  dnskey
```

5. Validatorで再起問い合わせ(存在しないドメイン)

```
# dig @validator hoge.dnsseclab.org  +dnssec
```

デモ（DNSに直接問い合わせ）

```
# dig -p 50053 @localhost www.dnsesclab.org +dnssec
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41405
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;www.dnsseclab.org.          IN      A

;; ANSWER SECTION:
www.dnsseclab.org.      3600    IN      A       182.48.47.26

;; AUTHORITY SECTION:
dnsseclab.org.          3600    IN      NS      ns2.dnsseclab.org.
dnsseclab.org.          3600    IN      NS      ns1.dnsseclab.org.
(以下略)
```

デモ（Phreebirdに問い合わせ）

```
# dig @localhost www.dnsseclab.org +dnssec
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21153
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;www.dnsseclab.org.          IN     A

;; ANSWER SECTION:
www.dnsseclab.org.     3600   IN     A      182.48.47.26
www.dnsseclab.org.     3600   IN     RRSIG  A 7 3 3600 201012222354(略)
;; AUTHORITY SECTION:
dnsseclab.org.         3600   IN     NS     ns1.dnsseclab.org.
dnsseclab.org.         3600   IN     NS     ns2.dnsseclab.org.
dnsseclab.org.         3600   IN     RRSIG  NS 7 2 3600 201012222320 (略)
(以下略)
```

デモ（Validatorで再起問い合わせ）

```
# dig @validator  www.dnsseclab.org +dnssec
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37076
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1

;; QUESTION SECTION:
;www.dnsseclab.org.          IN     A

;; ANSWER SECTION:
www.dnsseclab.org.     1847   IN     A      182.48.47.26
www.dnsseclab.org.     1847   IN     RRSIG   A 7 3 3600 20101222(略)
;; AUTHORITY SECTION:
dnsseclab.org.         1847   IN     NS     ns2.dnsseclab.org.
dnsseclab.org.         1847   IN     NS     ns1.dnsseclab.org.
dnsseclab.org.         1847   IN     RRSIG   NS 7 2 3600 201012221 (略)
```

デモ（DSの取得）

```
# dig @localhost dnsseclab.org ds
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33307
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;dnsseclab.org.                 IN      DS

;; ANSWER SECTION:
dnsseclab.org.          3600    IN      DS      55382 7 1 99EC5167D2828ABBC
6E3AECECCFFF9A20764EE6E
dnsseclab.org.          3600    IN      RRSIG   DS 7 2 3600 20101223004908
20101125004908 55382 dnsseclab.org. glgzVX5+ShhjHrlRhKHp9oNa3zLh
voKfP3DyKxwJG6x3/g42KxfXU3r5 UmyCExLsGde42INnSWSe+ERM(略)
```

デモ（DNSKEYの取得）

```
# dig @localhost dnsseclab.org dnskey
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47401
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;dnsseclab.org.                 IN      DNSKEY

;; ANSWER SECTION:
dnsseclab.org.          3600    IN      DNSKEY  256 3 7 AwEAAb8js87tbU/I1/J
RI/HxDy4HWf30W4Zrx/V04E198OR6+h/Bbmtz o8lvTdzA35JYuj4VqNW(略)
dnsseclab.org.          3600    IN      RRSIG   DNSKEY 7 2 3600 2010122223
0555 20101124230555 55382 dnsseclab.org. djZODWqvB4izucM5t3aXf(略)
```

!?

デモ（DNSKEYの取得）※他ドメインでの例

```
# dig isc.org DNSKEY
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54465
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;isc.org.                       IN      DNSKEY

;; ANSWER SECTION:
isc.org.                7072    IN      DNSKEY  256 3 5 BEAAAAPWwlvZf0cyC(略)
isc.org.                7072    IN      DNSKEY  257 3 5 BEAAAAOhHQDBrhQ (略)
isc.org.                7072    IN      RRSIG   DNSKEY 5 2 7200 20101220230155
20101120230155 12892 isc.org. Sfuc6cOzgrK+9Fb0xz+rdvz3jCYVNL9T(略)
isc.org.                7072    IN      RRSIG   DNSKEY 5 2 7200 20101220230155
20101120230155 14457 isc.org. jnNw3duXbcD2wMkWzC32wrwqUjKdN(略)
```

ZSK

KSK

デモ（Validaterで存在しないドメインを再起問い合わせ）

```
# dig @validator hoge.dnsseclab.org +dnssec
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 4681
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;hoge.dnsseclab.org.            IN      A

;; Query time: 30 msec
;; SERVER: 182.48.47.65#53(182.48.47.65)
;; WHEN: Thu Nov 25 12:35:37 2010
;; MSG SIZE  rcvd: 47
```

!?

デモ（存在しないドメイン）※他ドメインの例

```
# dig @validator hoge.edu +dnssec
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 37832
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

;; QUESTION SECTION:
;hoge.edu.                      IN      A

;; AUTHORITY SECTION:
edu.                    898     IN      SOA     a.edu-servers.net. nstld.verisign-grs.co
m. 1290656409 1800 900 604800 86400
edu.                    898     IN      RRSIG   SOA 7 1 900 20101202034009 20(略)
 4BJHN8D5BNN7IIN1LPPSF6S0NE7GEOSI.edu. 898 IN RRSIG NSEC3 7
286400 20101202023446 20101125022446 44056 edu. MJq0IQP4wYpv(略)
 (以下省略)
```

デモ（存在しないドメイン）※NSEC3の騙し

```
# dig @localhost hoge.dnsseclab.org |fgrep "IN NSEC3"
66g7ts2is7hvngjtgok247l89d9tkvls.dnsseclab.org. 0 IN NSEC3 1 0 1 1290
66G7TS2IS7HVNGJTGOK247L89D9TKVLU A RRSIG

nsvipjbg4f4hp3jiq9bburhuq2kev2th.dnsseclab.org. 0 IN NSEC3 1 0 1 1290
NSVIPJBG4F4HP3JIQ9BBURHUQ2KEV2TI RESERVED0 A NS CNAME
SOA NULL WKS PTR HINFO MX TXT AAAA LOC SRV NAPTR CERT DS
SSHFP IPSECKEY RRSIG NSEC DNSKEY DHCID NSEC3 NSEC3PARAM
SPF

aialm6ugrp79gkjhbdq6miibc6tinsqf.dnsseclab.org. 0 IN NSEC3 1 0 1 1290
AIALM6UGRP79GKJHBDQ6MIIBC6TINSQH A RRSIG
```

ほぼ同じ

ほぼ同じ

ほぼ同じ

何を引いても固定

デモ（ldns_chase）

```
# ldns_chase www.dnsseclab.org
      |---www.dnsseclab.org. (A)
         |---dnsseclab.org. (DNSKEY keytag: 55382 alg: 7 flags: 256)
            |---dnsseclab.org. (DS keytag: 55382 digest type: 1)
               |---org. (DNSKEY keytag: 61598 alg: 7 flags: 256)
                  |---org. (DNSKEY keytag: 21366 alg: 7 flags: 257)
                  |---org. (DS keytag: 21366 digest type: 2)
                  |   |---. (DNSKEY keytag: 40288 alg: 8 flags: 256)
                  |       |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
                  |---org. (DS keytag: 21366 digest type: 1)
                     |---. (DNSKEY keytag: 40288 alg: 8 flags: 256)
                        |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
All OK
www.dnsseclab.org.      3597    IN      A       182.48.47.26
       243772704       IN      RRSIG   A 7 3 3600 20101222165448
20101124165448 55382 dnsseclab.org. (略);{id = 55382}
```

実験的試み

- DNS over HTTP
  - GETメソッドでBASE64エンコードしたDNSクエリを発行
  - DNS over UDPに比べて遜色ないパフォーマンス(QPS)が出るらしい
  - Dan Kaminsky氏が所属するRecursion Ventures社でサービス提供

- DNS over X.509 over SSL
  - 詳細不明

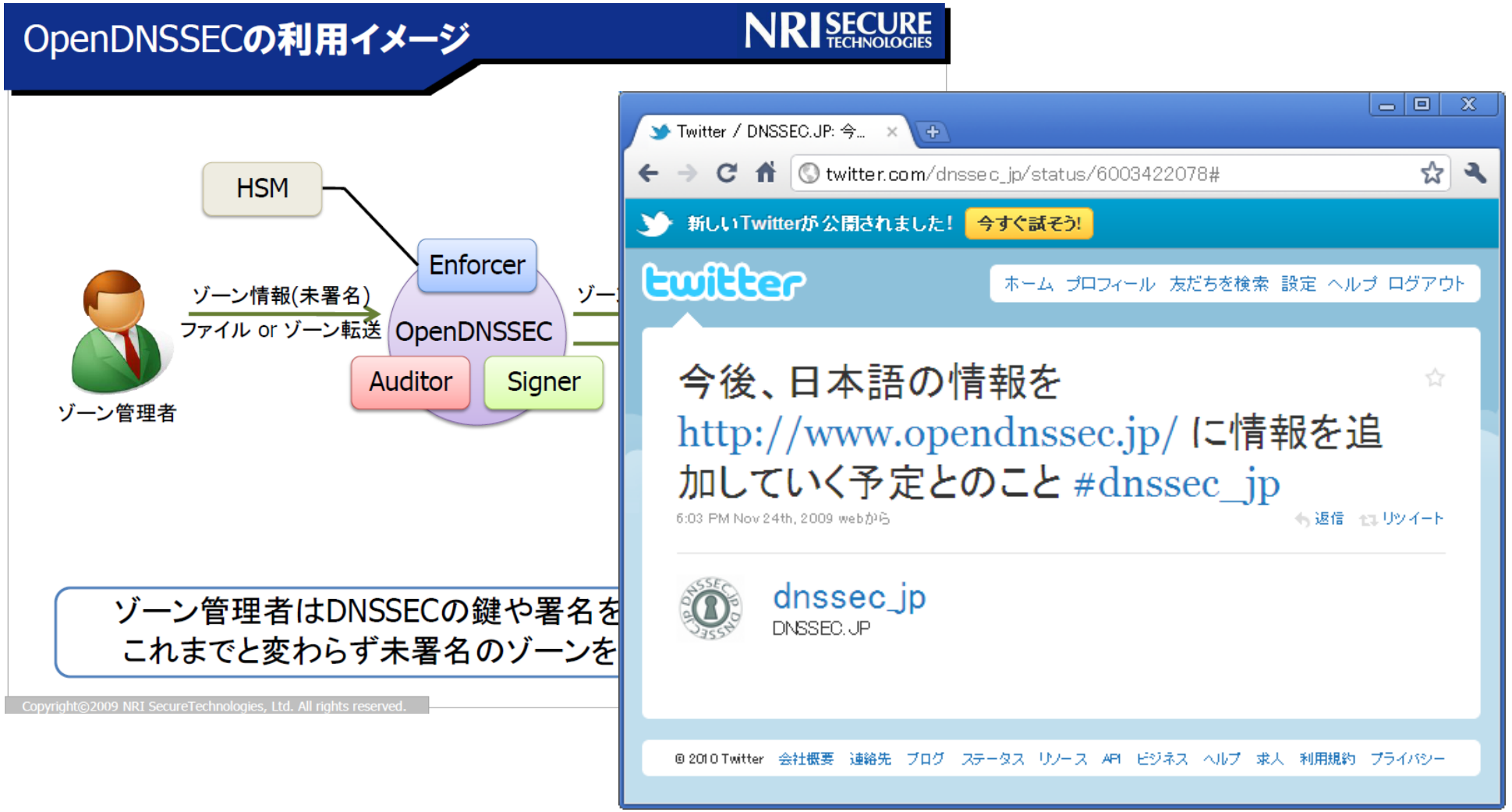
まとめ

- ゼロコンフィギュレーションを実現するための割り切りが凄まじい
  - ZSKは単一のものを全ゾーンで使用
  - KSKが無い
  - NSEC3は騙し(White Lies)
- サービス提供には使えない

	Phreebird Suite	BIND/NSD+α
導入の容易さ	○	△
鍵管理	DNS全体で一つ	ゾーン毎に作成・管理
鍵交換	不明	手動・自動・半自動
DNSSECの完全性	×	○
メンテナンス	？	○
脆弱性対応	？	○

おまけ

おぼえていますか？



OpenDNSSEC.JPのコンテンツ整備始め（てもらい）ました

■謝辞：川原大幸さん(住商情報システム株式会社)

参考

- Phreebird Suite 1.02
  - http://s3.amazonaws.com/dmk/phreebird_suite_1.02.tar.gz
- PHREEBIRD SUITE1.0:
  INTRODUCING THE DOMAIN KEY INFRASTRUCTURE
  - http://www.slideshare.net/dakami/phreebird-suite-10-introducing-the-domain-key-infrastructure
- Black Ops of Fundamental Defense:
  Introrucing the Domain Key Infrastructure
  - http://www.slideshare.net/RecursionVentures/dki-2

NRIセキュアテクノロジーズ