DNSSECソフトウェアアップデート
+
DNSSEC普及状況調査

NTTネットワーク基盤技術研究所
佐藤 一道

本日のお題目

- DNSSECソフトウェアアップデート
  - DNSSEC周辺のソフトウェアの紹介
    - サーバ
    - 運用ツール
    - 開発者向けライブラリ
- DNSSEC普及状況調査
  - 下位ゾーンのDNSSEC普及状況調査結果の報告
    - Alexa人気ランキング掲載サイトのDNSSEC対応状況

DNSSECソフウェアアップデート

調査資料

- DNSSEC Roadmap
  - Shinkuro Incから発行された資料
    - 権威サーバの運用者、キャッシュサーバの運用者、サービスプロバイダなど、様々な目線からDNSSECの現状や展望などが記載されている
    - 参考URL: http://www.dnssec-deployment.org/wp-content/uploads/2013/03/roadmap-021313-v21.pdf
  - 第3章”First Layer: DNSSEC Tools & Implementation”の調査を実施

DNSSEC対応サーバ/サービス

NTT

- 最近開発されたサーバとしてYadifaが挙げられる
  - 開発者は他サーバと比較して省メモリ、高速であると主張

開発元	権威サーバ	キャッシュサーバ	備考
BT Diamond	IPControl	IPControl	
Cisco	--	Prime Network Register	
cz.nic	knot-dns	--	
EURid	Yadifa	--	
F5	Big-IP Global Traffic Manager	Big-IP Global Traffic Manager	DNSを用いたロードバランサ（アプライアンスボックス）
Infoblox	Infoblox	Infoblox	
ISC	BIND	BIND	
Microsoft	Windows Server 2012	--	
NLnet Labs	NSD	unbound	
Nominum	Nominum ANS	Vantio Caching Platform	
PowerDNS	PowerDNS Authoritative Server	--	PowerDNS recursorは DNSSEC検証未対応
Secure64	DNS Authority	DNS Cache	
Verisign	ATLAS	--	サービスとして提供

運用ツール (1/2)

- フリーで利用できる鍵管理、署名の自動化ツールはまだまだ少ない
  - OpenDNSSEC、DNSSEC-Toolsが挙げられる
    - 商用利用に耐え得るツールとしてはOpenDNSSEC一択か?
  - DNSSEC-Toolsは更新頻度も高く、今後の活動に期待

ツール	開発元	機能
OpenDNSSEC	.se, Cira, Nominet	鍵生成および更新、署名の自動化など
dnssec-keygen dnssec-signzone	ISC	鍵生成、署名 (BIND付属)
ldns-keygen ldns-signzone	NLnet Labs	鍵生成、署名 (ldns付属)
pdnssec-keygen pdnssec-signzone	Roy Arends	鍵生成、署名 (DNSSEC perltools付属)
Secure64 DNS Signer	Secure64	鍵生成および更新、署名の自動化 (Secure64製OS上で動作)
Zonesigner	Sparta, Inc.	鍵生成、署名 (DNSSEC-Tools付属)
Rollerd	Sparta, Inc.	鍵更新、再署名の自動化 (DNSSEC-Tools付属)
jdnssec-keygen jdnssec-signzone	Verisign Labs	鍵生成、署名 (jdnssec-tools)

運用ツール (2/2)

- DNSSEC検証結果の可視化ツールが増えてきている
  - 可視化ツールはエラー要因の特定に非常に有効
    - サーバログ、digやdrillだけではトラブルシュートは難しい
  - 特にDNSVizは秀逸
    - Webアプリケーションであり、問題箇所の特定が容易
    - DNSSEC-Nodes、lookupはUIが分かり難く、またスタンドアロンアプリケーションであることがネック

ツール	開発元	機能
dnscheck	.se	DNSSEC検証の他、委任の正当性などのチェック
validns	Anton Berezin	署名済ゾーンファイルのチェック
Donuts	Sparta, Inc.	署名済ゾーンファイルのチェック (DNSSEC-Tools付属)
Nagios Plugin	The Measurement Factory	RRSIGの有効期限のチェック
SecSpider	UCLA	DNSSEC検証、接続性、Path MTUなどのチェック
jdnssec-verifyzone	Verisign Labs	署名済ゾーンファイルのチェック (jdnssec-tools付属)
DNSViz	Sandia National Laboratories	DNSSEC検証結果の可視化
DNSSEC-Nodes	Sparta, Inc.	DNSSEC検証結果の可視化
DNSSEC-Check	Sparta, Inc.	キャッシュサーバのDNSSEC対応状況チェック
logwatch	Sparta, Inc.	DNSSEC関連メッセージの出力 (logwatchにパッチを適用)
lookup	Sparta, Inc.	DNSSEC検証結果の可視化

DNSSEC検証ライブラリ

NTT

- DNSSEC関連の開発ライブラリは充実している
  - メジャーな言語は概ねカバーされている
    - Perl、Python、Ruby、Java、C

ツール	開発元	機能
Net::DNS::SEC	CPAN	Net::DNSにDNSSEC関連機能を追加したPerlライブラリ
libunbound	NLnet Labs	DNSSEC検証機能を含む名前解決関連のC言語ライブラリ
DNSPython	Nominum	DNSSEC検証機能を含む名前解決関連のPythonライブラリ
libval libsres	Sparta, INC.	C言語用のDNSSEC検証ライブラリ
Dnsruby::Dnssec	Nominet	DNSSEC検証機能を含む名前解決関連のRubyライブラリ（DNSSEC Roadmap未掲載）
DNSJava （DNSSEC対応版）	Nominum	DNSSEC検証機能を含む名前解決関連のJavaライブラリ（DNSSEC Roadmap未掲載）

まとめ

- DNSサーバ
  - 新規参入サーバは少ない
    - 既存サーバとの差異化が難しく、開発のモチベーションが湧かない?
- 運用ツール
  - 鍵管理や署名の自動化ツールにおいて、フリーで利用できるものはまだまだ少ない
    - OpenDNSSEC、DNSSEC-Tools
  - 可視化ツールが増えてきている
    - 検証失敗(Bogus)の要因特定に役立つと思われる
    - 個人的にはDNSVizがオススメ
- 開発者向けライブラリ
  - メジャーな言語のライブラリは一通り揃っている
    - Perl、Python、Ruby、Java、C
  - 実際にDNSサーバを立てなくとも、DNSSEC検証用のテストツールなどは比較的容易に組めると思われる

DNSSEC普及状況調査

はじめに

- DNSSECの”真の普及”とは? (個人的意見)
  - 1. 多くのユーザが利用している有名ドメイン名が、DNSSEC対応すること
    - Google、Facebook、Twitterなど
  - 2. 多くのユーザが利用しているキャッシュサーバがDNSSEC検証機能をONにすること

- 下位ゾーンの普及状況を調査
  - 上記の1にフォーカスし、有名ドメイン名のDNSSEC対応状況を調査することでどの程度”真の普及”が進んでいるかを明らかにする
  - 2に関してはデータ収集が困難であるため調査は未実施
- 現在の普及状況におけるDNSSEC検証回数の推定
  - キャッシュサーバでDNSSEC検証をONにした場合、どの程度の頻度で検証が発生するかを推定
  - DNSSEC検証をONにすることでどの程度負荷が上がるかの参考値を算出したい

調査概要

- 普及状況調査
  - 人気100万サイトのドメイン名に対して名前解決を行い、その応答を分析
    - 署名付ドメイン名数
    - 署名付ドメイン名のTLD分布
  - 署名付ドメイン名のDNSSEC検証を行い検証結果を分析
    - Secure、Insecure、Bogus数

- DNSSEC検証回数推定
  - DNSSEC対応のドメイン名の人気ランク、TTLから1秒あたりの検証発生回数を推定

データセット、収集方法

- 人気サイトリスト
  - Alexa Top100万リストを利用
    - http://s3.amazonaws.com/alexa-static/top-1m.csv.zip
    - 2013/5/19のリストを利用
- 名前解決結果
  - $ dig +dnssec +traceで上記リストに含まれる全てのドメイン名の名前解決を実施
  - tcpdumpでDNSパケットをキャプチャ
- DNSSEC検証結果
  - DNSSEC検証をONにしたBINDを用意
    - バージョンは9.7 (CentOS 5.9のパッケージを利用)
    - (もちろんオープンリゾルバではありません)
  - $ dig @localhost +dnssecで名前解決の結果得られた署名付ドメイン名のDNSSEC検証を実施
  - tcpdumpでDNSパケットをキャプチャ

Alexa Top 100万リストの名前解決結果

- 100万ドメイン名のうち、約98.5万の応答を取得
  - うち約96万がNoError応答
- 応答が取得できなかった1.5万のドメイン名について
  - 権威サーバまで到達できなかったなど

応答コード	応答数
NoError	959,252
NXDomain	18,113
Refused	4,033
FormErr	2,093
ServFail	1,361
不明	15,148
合計	1,000,000

NoError応答の詳細分析を実施

DNSSEC対応ドメイン名数の調査結果

- 署名済ドメイン名数
  - 全ドメイン名の約0.8%と署名済ドメイン名は少ない

署名済ドメイン名数	全ドメイン名数	署名率
7,636	959,252	0.80%

- 署名済ドメイン名のDNSSEC検証結果
  - 署名済ドメイン全てがSecureではなく、約1/4がInsecure
  - Bogusなドメイン名も僅かに存在
    - 思ったよりも少ない印象

	ドメイン名数	検証結果の割合	
		対署名済ドメイン名数	対全ドメイン名数
Secure	5,827	76.31%	0.61%
Insecure	1,799	23.56%	0.19%
Bogus	10	0.13%	0.00%

人気ランクの高いDNSSEC対応ドメイン名

- 最もランクの高いドメイン名はpaypal.com
  - PayPalでの決済は安心安全
- Alexaランク上位の署名付ドメイン名の中には有名サービスは多く含まれていない
  - DNSSECの真の普及は進んでいないように思われる

Alexaランク	ドメイン名	検証結果
53	paypal.com.	Secure
174	mozilla.org.	Secure
191	comcast.net.	Secure
340	domaintools.com.	Insecure
369	nih.gov.	Secure
767	ca.gov.	Secure
858	irs.gov.	Secure
1,076	comcast.com.	Secure
1,124	state.gov.	Secure
1,203	weather.gov.	Secure

Alexaランク	ドメイン名	検証結果
1,596	noaa.gov.	Secure
1,651	ed.gov.	Secure
1,666	centrum.cz.	Secure
1,935	www.gov.uk.	Insecure
1,993	directtrack.com.	Insecure
2,422	berkeley.edu.	Secure
2,476	cdc.gov.	Secure
2,479	whitehouse.gov.	Secure
2,486	fbi.gov.	Secure
2,627	iheart.com.	Insecure

Bogusドメイン名について

- Bogusとなった原因をDNSVizを用いて調査
  - http://dnsviz.net/
- DNSVizの結果と本調査結果が異なるケースが存在
  - spilxl.dk、akvo.orgについてはキャッシュが空の状態で検証を行うとBogusであり、root、TLDのキャッシュがある状態で検証するとInsecureとなる
  - dotarai.co.thは任意の検証タイミングでBogus

ドメイン名	調査結果	DNSViz結果	原因
spilxl.dk.	Bogus	Insecure	信頼の連鎖切れ
barneysfarm.com.	Bogus	Bogus	署名の有効期間超過
challenge.gov.	Bogus	Bogus	DNSKEYと上位DSが異なる
akvo.org.	Bogus	Insecure	信頼の連鎖切れ
vsevjednom.cz.	Bogus	Bogus	署名の有効期間超過
dotarai.co.th.	Bogus	Secure	署名の有効期間超過?
aqarategypt.com.	Bogus	Bogus	DNSKEYと上位DSが異なる
mandataire-voiture-neuve.fr.	Bogus	Bogus	署名の有効期間超過
macrowebs.com.	Bogus	Bogus	DNSKEYと上位DSが異なる
trt1.jus.br.	Bogus	Bogus	DNSKEYと上位DSが異なる

DNSSEC対応ドメイン名のTLDごとの普及状況調査

- DNSSEC対応ドメイン名をTLD別に集計し、TLDごとの普及状況を調査

- Alexaリストに含まれる全ドメイン名のTLD分布
  - ユニークTLD数は85
  - comが100万のうちの半数以上を占め、net、ru、org、deと続く

TLD	Alexaリスト出現数
com.	528,239
net.	56,119
ru.	47,858
org.	39,294
de.	22,829
uk.	18,340
cn.	18,275
br.	17,713
jp.	17,039
pl.	13,322

DNSSEC対応ドメイン名のTLDごとの普及状況

NTT

- 署名付ドメイン名数はcomが最も大きいが、母数(Alexaリスト出現数)が大きいため署名率は低い
  - Secure率も高いとは言えない
- cz、nl、govは母数に対して署名数が比較的大きく、またSecure率も高い
  - チェコ、オランダはDNSSEC先進国と言える
- brは署名率は低いものの、Secure率は最も高い
- seはInsecure率がSecure率を上回っており、czやnlと比較すると普及は進んでいないように思われる
  - 思ったよりもSecure率が低い印象

TLD	(A) Alexaリスト出現数	(B) 署名付ドメイン名数	(C) Secure数	(D) Insecure数	(E) Bogus数	署名率 (B÷A)	Secure率 (C÷B)	Insecure率 (D÷B)	Bogus率 (E÷B)
com.	528,239	1,733	1,039	691	3	0.33%	59.95%	39.87%	0.17%
cz.	4,696	1,469	1,397	71	1	31.28%	95.10%	4.83%	0.07%
nl.	8,339	1,420	1,376	44	0	17.03%	96.90%	3.10%	0.00%
se.	3,467	828	309	519	0	23.88%	37.32%	62.68%	0.00%
br.	17,713	628	624	3	1	3.55%	99.36%	0.48%	0.16%
gov.	793	316	299	16	1	39.85%	94.62%	5.06%	0.32%
net.	56,119	212	141	71	0	0.38%	66.51%	33.49%	0.00%
org.	39,294	165	104	60	1	0.42%	63.03%	36.36%	0.61%
eu.	4,057	110	85	25	0	2.71%	77.27%	22.73%	0.00%
fr.	9,028	99	91	7	1	1.10%	91.92%	7.07%	1.01%
be.	2,402	60	51	9	0	2.50%	85.00%	15.00%	0.00%
edu.	2,814	56	49	7	0	1.99%	87.50%	12.50%	0.00%
de.	22,829	50	41	9	0	0.22%	82.00%	18.00%	0.00%
nu.	404	47	0	47	0	11.63%	0.00%	100.00%	0.00%
rs.	670	40	0	40	0	5.97%	0.00%	100.00%	0.00%

DNSSEC検証回数の推定

- 現在の普及状況における、DNSSEC検証ONの場合のキャッシュサーバの検証回数を推定
  - ユーザ数を1〜10,000,000で変化させた場合の、DNSSEC検証回数を推定
    ⇒ NW規模ごとの検証回数の推定

- 推定方法
  - 検証回数 = あるドメイン名の応答がキャッシュされていないときに問い合わせを受ける回数
  - ドメイン名ごとの問い合わせ頻度、TTLを考慮して検証回数を推定
    - メジャードメイン名はキャッシュが切れてすぐに問い合わせがある可能性が高く、検証回数は多くなる
    - マイナードメイン名はキャッシュが切れてもすぐに問い合わせがあるとは限らず、検証回数は少なくなる
    - TTLが短いドメイン名ほど検証回数は多くなる
    - TTLが長いドメイン名ほど検証回数は少なくなる
  - 詳細な推定方法は参考スライドを参照

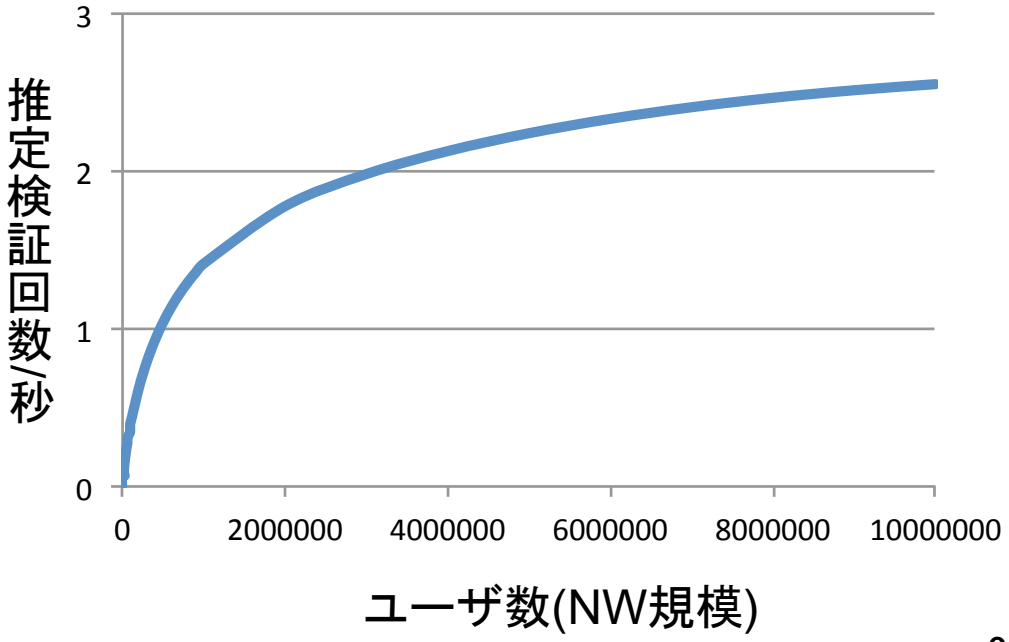
推定における前提条件

- 対象ドメイン名およびリソースレコード
  - Alexaリストに掲載されたドメイン名を対象とする
  - リソースレコードはAレコードのみを対象とする
    - AとそのRRSIGレコードのTTLは同一
- ドメイン名の問い合わせ傾向
  - 人気ランクn位のドメイン名への問い合わせ数は1位の1÷n回
    - ドメイン名へのクエリ数は人気ランクに反比例する
  - 人気ランク1位のドメイン名へのクエリ数は1人1日50回、かつ30%のユーザが問い合わせる

DNSSEC検証回数の推定結果

- 現状では、DNSSEC検証をONにした場合においても検証による キャッシュサーバのリソース消費量の極端な増加は見られないと思われる
  - ISPなど、100万ユーザ規模(大規模NW)では、1秒間あたり1回強検証が発生
  - 社内NWなど中小規模のNWでは1秒間あたりの検証回数はほぼゼロ
    - 数分〜数10分に1回程度検証が発生する程度

ユーザ数（NW規模）	推定検証回数/秒
1	0.00
10	0.00
100	0.00
1,000	0.01
10,000	0.07
100,000	0.40
1,000,000	1.41
10,000,000	2.55



まとめ

- Alexa Top 100万リストのDNSSEC対応状況の調査を実施
  - 最も人気あるDNSSEC対応ドメイン名はpaypal.com、続いてmozilla.orgが続く
  - ただし、人気サービスのDNSSEC対応はまだまだ進んでいないように思われる
  - TLD別に見るとチェコ、オランダのドメイン名は普及が進んでいる

- DNSSEC検証ONにおける検証回数を実施
  - 大規模NWにおいても、秒間あたりの検証回数は1回程度と多くはない
  - 現状では、検証をONにすることによるリソース消費量は急激に増加することはないと思われる

参考：検証回数の推定方法 (1/2)

- ドメイン名へのクエリ数が平均λ回/秒のとき、t秒の間にk回問い合わせを受ける確率は以下で求めることができる

$$P(k) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}$$

- 検証が発生する確率 = 問い合わせ時にキャッシュされていない = TTL秒間に0回問い合わせを受ける確率であるため、t = TTL、k=0となる

$$P(0) = e^{-\lambda \times TTL}$$

- 上記確率より、あるドメイン名dの平均クエリ数/秒をλ_d、TTLをTTL_dとすると平均検証回数/秒Cは以下となる

$$C(d) = \lambda_d \times e^{-\lambda_d \times TTL_d}$$

- よって、全てのドメイン名について平均検証回数/秒を算出し、総和を取ることで検証回数を求めることができる

$$C_{total} = \sum_{d \in D} C(d)$$

参考：検証回数の推定方法 (2/2)

- ドメイン名ごと平均クエリ数/秒の算出方法
  - ドメイン名へのクエリ数は人気ランクに反比例する*性質を利用
    - 人気ランクn位のドメイン名へのクエリ数は1位のクエリ数の1/nとなる
  - 人気ランク1位のドメイン名へのクエリ数は1人1日50回、かつ30%のユーザが問い合わせると仮定
    - ユーザ数m人、人気ランク1位の1日のクエリ数は50×(m×0.3)
  - 上記から、ユーザ数mのNWにおける、人気ランクn位のドメイン名dへの秒間平均クエリ数λ_dは以下となる

$$\lambda_d = \frac{50 \times (m \times 0.3)}{n} \div 86400$$

*J. Jung , E. Sit , H. Balakrishnan , R. Morris, DNS performance and the effectiveness of caching, IEEE/ACM Transactions on Networking (TON), v.10 n.5, p.589-603, October 2002.