# DNSSECの理想と現実
## ーそのIPアドレス管理への影響ー

太田昌孝
東京工業大学情報理工学研究科
mohta@necom830.hpcl.titech.ac.jp

# 概要

- 通常のDNSは既に十分安全
  - DNSSECの必要性は消滅
  - 特に、アドレス逆引きは安全
- DNSSECのサーバ側の運用は容易
  - 手間が増え、ドメイン管理の手数料は上がるが
- DNSSECのリゾルバ側の運用は不可能
- リゾルバ側の運用不可能性を放置したまま
  - サーバ側の運用資金を要求するのは、詐欺

# DNSSECの理想

- DNSは危険！？
  - DNSに本当のセキュリティを！？
  - 公開鍵暗号技術の導入
    - これで、DNSは暗号学的にセキュア！？
  - 1995年（？）に開発開始
- 最初のRFC（RFC2065）は1997年に発行
  - 1999年に改訂版（RFC2535）、問題あり
  - 2005年に二訂版（RFC4033～5）、DS追加等
  - 順調に進化？

# DNSSECの現実

- いくつかのドメインでは導入
- 利用者側には全く相手にされず
  - 労多くして、益なし
- 理想的な環境ではリゾルバも動作するが
  - 現実的な環境での実運用は、事実上不可能
    - メッセージサイズ、NAT、時刻、、、
- DNSSECの暗号学的前提
  - TTP（Trusted　Third　Party）が信頼できる
    - TTPが暗号学的に信頼できるわけではない

# 現行DNSのセキュリティ

- 現行DNSはWeakly　Secure
  - 問と答をメッセージIDで照合
    - 問のメッセージIDの推測が難しく、問や答が途中のISPで盗聴も改竄されなければ、偽の答を排除可能
  - リゾルバが最初に使うネームサーバが信頼できるなら
    - 順次紹介されるネームサーバも信頼できるはず
  - 現行DNSは、各ISPと各ネームサーバ管理者（各ゾーン管理者）が信頼でき、問と答が照合できるなら、セキュア

# 現行DNSのセキュリティの弱点と対策

- 追加情報(特にグルーA)のオーソリティ問題
  - ネームサーバが与える追加情報は信用できない
    - 子ゾーン内のグルーAしか認めない(やりすぎだが)
- メッセージIDは16ビットしかないので
  - 誕生日攻撃により容易に偽の答を挿入可能
    - 256回程度の試行で、高確率で攻略可能
    - TCPではシーケンス番号により安全、UDPは問のソースポート番号を乱雑化

# 現行DNSのセキュリティの現状

- 現行DNSは、ちゃんと実装すれば一応安全
  - もはや、DNSSECは不要？
- とはいえ、ソースポート番号の乱雑化だけでは多少不安
  - TCPなら安心・安全
    - 重い？
  - DNSSECでは、TCPがどのみち必要
  - なら、TCPだけあればよく、DNSSECは不要

# DNSSECの開発経過

- D. Eastlakeが最初のドラフトを作成
  - セキュリティの専門家であって、DNSには無知
    - RR単位での認証くらいは、説明すれば理解できた
    - CNAME、レフェラル、メッセージ長等、DNSのデリケートな点は、いくら説明しても無理解
      - 多くは今では修正されたが、メッセージ長は手つかず
        - » DNSKEY　RR集合は、KSKとZSKがごっちゃなため巨大で、512Bに収まらず
        - » EDNSで救済できるはずだったが、、、もはや、1500Bに収まるかどうかも、怪しい

# DNSSECの仕組み

- セキュアなゾーンは秘密鍵をもち、それで、
  - ゾーンのデータに署名
- 親ゾーンの秘密鍵で
  - 子ゾーンの公開鍵に署名
- あるゾーンの公開鍵を持ったリゾルバは
  - そのゾーンや子孫のセキュアなゾーンのデータを認証可能
- 署名には署名の時刻と有効期間あり

# DNSSECのセキュリティの前提

- 暗号学的前提
  - ゾーンの秘密鍵が悪用されない
    - ゾーン管理者は、いわゆるTTP(Trusted Third Party)
  - セキュアな時刻が利用可能
- プロトコル的前提
  - ５１２バイトを遥かに超えるメッセージ受信が可能
- どの前提も、常に成立するとは期待できない

# TTPは信用できるのか？

- 暗号学的には、何の保証もない
  - 暗号学的には、TTPが信頼できるというのは仮定であって、結論ではない
- ゾーン管理者が信頼できないなら
  - DNSデータがセキュアじゃないのは当然
    - DNSSECは、もともと大層なセキュリティは提供しない
    - メッセージIDやISPが信頼できなくても、ゾーン管理者さえ信頼できれば、答が信頼できる、と言う程度
    - 苦労に見合うセキュリティなのか？

# セキュアな時刻同期

- RFC2535によると、NTPというのがあるらしいが、、、
  - だから？
  - 運用は？
  - セキュアにしろというけど、鍵は？
- RFC4033~5では、言及なし
  - もはや、誰も何も考えてない？

# ５１２バイトを超えるメッセージ

- EDNS拡張をみんながサポートすれば、、、
- NATでは、相手にされていない
- NATによっては、IPフラグメントがまともに動かない
- NATでの、ポート５３へのTCPは？

| Make/Model | | DHCP DNS | No Proxy | UDP Proxy Transport Tests | | UDP Proxy DNSSEC Tests | | | | TCP Proxy |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Out of the Box Usage Mode | Route DNS to Upstream Resolver | Proxy DNS over UDP | A. EDNS0 Compatibility | B. Signed Domain Compatibility | E. Request Flag Compatibility | D. Checking Disabled Compatibility | C. DNSSEC OK Compatibility | Proxy DNS over TCP |
| 2Wire | 270HG-DHCP | Proxy | OK | OK | FAIL | OK | OK | FAIL | FAIL | FAIL |
| Actiontec | MI424-WR | Proxy | OK | OK | FAIL > 512 | OK | OK | OK | OK | FAIL |
| Apple | Airport Express | Proxy | OK | OK | FAIL > 512 | OK | FAIL | FAIL | FAIL | OK |
| Belkin | N (F5D8233) | Proxy | OK | OK | FAIL > 1500 | OK | OK | OK | OK | FAIL |
| Belkin | N1 (F5D8631) | Proxy | OK | OK | FAIL > 1500 | OK | OK | OK | OK | FAIL |
| Cisco | c871 | Route | OK | OK | FAIL > 512 | OK* | OK* | OK* | OK* | FAIL |
| D-Link | DI-604 | Proxy | MIX | OK | FAIL > 1472 | OK | OK | OK | OK | FAIL |
| D-Link | DIR-655 | Proxy | OK | OK | OK | OK | OK | OK | OK | FAIL |
| Draytek | Vigor 2700 | Proxy | OK | OK | FAIL > 1464 | OK | FAIL | FAIL | OK | FAIL |
| Juniper | SSG-5 | Route | OK | OK | OK | OK | OK | OK | OK | FAIL |
| Linksys | BEFSR41 | Varies | OK | OK | FAIL > 1472 | OK | OK | OK | OK | FAIL |
| Linksys | WAG200G | Varies | OK | OK | OK | OK | OK | OK | OK | FAIL |
| Linksys | WAG54GS | Varies | OK | OK | OK | OK | OK | OK | OK | FAIL |
| Linksys | WRT150N | Varies | OK | OK | FAIL > 512 | OK | OK | OK | OK | FAIL |
| Linksys | WRT54G | Varies | OK | OK | FAIL > 512 | OK | OK | OK | OK | FAIL |
| Netgear | DG834G | Proxy | OK | OK | FAIL > 512 | OK | FAIL | FAIL | MIX | FAIL |
| Netopia | 3387WG-VGx | Proxy | OK | OK | FAIL > 512 | OK | FAIL | FAIL | FAIL | FAIL |
| SMC | WBR14-G2 | Proxy | MIX | OK | FAIL > 512 | OK | OK | OK | OK | FAIL |
| SonicWALL | TZ-150 | Route | OK | n/a | n/a | n/a | n/a | n/a | n/a | n/a |
| Thomson | ST546 | Proxy | OK | OK | FAIL > 512 | OK | OK | OK | OK | FAIL |
| WatchGuard | Firebox X5w | Varies | OK | FAIL | FAIL | FAIL | FAIL | FAIL | FAIL | FAIL |
| Westell | 327W | Proxy | OK | OK | FAIL | OK | OK | FAIL | FAIL | FAIL |
| ZyXEL | P660H-D1 | Proxy | OK | OK | FAIL > 1464 | OK | OK | OK | OK | FAIL |
| ZyXEL | P660RU-T1 | Proxy | OK | OK | FAIL > 1464 | OK | OK | OK | OK | FAIL |



Table 2. Test Result Summary

http://www.internetdagarna.se/arkiv/2008/www.internetdagarna.se/images/stories/pdf/domannamn/Steve_Crocker_administrationofdnssec.pdf

# Summary Results

| | OK Out of the Box | Configurable | Client Routable | Unusable | Total |
|---|---|---|---|---|---|
| DHCP Behavior | | | | | |
| A. Route | 3 | | | | 3 |
| B. Proxy then Route | 2 | 4 | | | 6 |
| C. Proxy; changeable | 1 | 5 | | | 6 |
| D. Proxy; not changeable | | | 7 | 2 | 9 |
| Total | 6 | 9 | 7 | 2 | 24 |

http://www.internetdagarna.se/arkiv/2008/www.internetdagarna.se/images/stories/pdf/domannamn/Steve_Crocker_administrationofdnssec.pdf

# DS (Delegation Signer)の迷走 RFC2535ー＞RFC4033～5

- 子ゾーン鍵の署名を
  - 子ゾーンで持つと、親子の通信が大変？
    - どうせ通信は必要なので、たいした問題ではない
  - 親ゾーンで持たないと、セキュアでない子ゾーンをそうと認証するために、子ゾーンに負担?
    - もともとの要求が破綻
      - DNSSECを要求するなら、セキュアじゃない答は役立たず
  - 親ゾーンで持たないと、親の鍵変更時の子ゾーンへの連絡が大変
    - だとすると、ルート鍵の変更は事実上不可能

# 親鍵変更の通知と ルート鍵の変更の通知

- 子鍵の署名を子が持つと
  - 親鍵変更で、子の持つ署名の変更が必要
    - 親から子への連絡が大変？
    - 親子ゾーンの管理者間の連携は元々必須なので、問題なし
- ルート鍵は、リゾルバが持つ
  - ルート管理者とリゾルバ管理者は、一般に無関係、何の連携もない
    - ルート鍵変更時のリゾルバ管理者への連絡は、無理
    - 秘密鍵が漏れた場合や、鍵変更を一度逃した場合は、自動更新は無理

# DNSSEC vs CDN

- CDNでは1ドメイン名に数十のAを持ち、一時にはそのうち数個を返すことがよくある
  - 答として、数十から数個を取り出すの全ての組み合わせにすると、必要な署名の数が爆発するが
    - 組み合わせを限定すれば、実用上何も問題はない
  - 問題は、Aの答と署名のマッチング
    - Aの答に対応する署名が付随していない場合
      - 自分の持つ答に対応する署名を得ることは、不可能

# DNSSEC運用の現状の概要
# リゾルバ側

- NATとの相性
  - 一部のNATではDNSSEC利用不可
- CDNとの相性
  - DNSSECでは、毎回異なる答は返せない
- 時刻同期
  - そこまで手がまわっていない
- ルート鍵変更
  - 各種提案はあったが、絶望的

# DNSSEC運用の現状の概要
# サーバ側

- NATとの相性
  - NAT?なにそれ？
- CDNとの相性
  - 署名は用意できる
- 時刻同期
  - 手であわせれば、十分
- ルート鍵変更
  - 変えるだけ

# そもそもDNSSECを どう使うのか？

- 最初は、キャッシュ汚染問題だけだったはず
  - 既に解決済み
  - では、DNSSECのメリットは？
- DNSSECを必要とするなら
  - セキュアじゃないゾーンからの答は？
    - 信頼できない以上、全く使えないはず
  - DNSSECが使えない環境では
    - 何もできないはず

# DNSSECと逆引き

- DNSSECを使えば、ゾーン管理者さえ信頼できれば
  - ISPの盗聴やパケット改変があっても大丈夫
  - ゾーンの根元や幹線ISPは、まあ信頼していいかもしれないが、、、
    - 問題は、末端(組織内等）のISPやゾーン
    - 末端ISPは末端逆引きゾーンの管理者なので
      - ゾーン管理者を信頼するなら、DNSSECは不要
- DNSSECが逆引きに必要なら
  - 逆引き登録がない場合は、何もできないはず

# そもそも
# 何のための逆引きか？

- アクセス管理をドメイン名で行う場合
  - 相手のドメイン名を知る必要あり
  - 正引き（ドメイン名ー＞IPアドレス）は、自称でしかない
  - IPアドレスー＞ドメイン名がどれだけセキュアでも
    - IPアドレスが信頼できなければ、意味なし
  - 相手のIPアドレスは、3ウェイハンドシェーク等で（ISPが信頼できれば）信頼できる
    - ISPが盗聴、改変すれば、詐称可能

# おわりに

- 普通のDNSは既に十分安心・安全
- DNSSECによりISPを信頼する必要なし
- DNSSECのサーバ側の運用は
  - 金さえかければ簡単
- DNSSECのリゾルバ側の運用は
  - 不可能
- DNSSECを逆引きで利用することは
  - 結局ISPを信頼することになり、無意味