IETF における標準化・ディプロイメント状況

関谷 勇司
東京大学 情報基盤センター / WIDE Project

2009年 IETF における標準化動向

- Routing 関連
- DNS 関連
- IPv6関連

Routing 関連

GROW WG

- BGP Graceful Shutdown
  - eBGP peer を packet loss なしに shutdown
  - BGP のコンバージェンスの間に packet が回るのが問題
  - コミュニティを利用して通知
    - AS 内部的には local-pref を利用して制御
  - 手続きを示したもの
- FIB Aggregation / Virtual Aggregation
  - ルータの FIB table が悲鳴をあげています
  - 同一 PATH で aggregation できるものを FIB にのせない
    - RIB -> FIB を抑制
  - Sub-prefix をもつルータに tunnel

SIDR WG

- Secure Inter-Domain Routing WG
- RPKI
  - Repository Structure
  - ROA (Route Origin Authorizations) validation
  - S-BGP や soBGP に利用
- 鍵サイズやマネージメント
- No RFC
- もともとは RPSEC を実現するための RPKI/ROA
  - だいぶ遠回りしているように見えるけれど
  - まだ標準化 / デプロイメントは見えてこない

SAVI WG

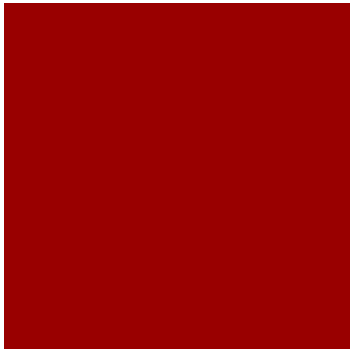
- Source Address Validation WG
  - SAVI for Stateless Address Autoconfiguration
  - SAVI for DHCP
  - SAVI for Secure ND
  - SAVI for Delegated IPv6 Prefixes

  - SAVI switch による実装 ？
    - BB ルータやエッジスイッチによる解法
  - たくさん出て来てますが。。。
  - あまり決まっていない
    - どれも複雑過ぎる気がします

IDR WG

- Inter-Domain Routing WG
- BGP Graceful Shutdown
- BGP Best Path Selection Additional Criteria
  - MPLS data plane
  - Path Availability Check
  - Add-paths (multiple paths)
- 4-octets AS
  - 移行のための手順
- BGP Advisory Message
  - BGP notification をつかって、相手の機器やオペレータにメッセージを送る
  - 電話やメールでやるより信頼性が高い？！

OPSEC WG



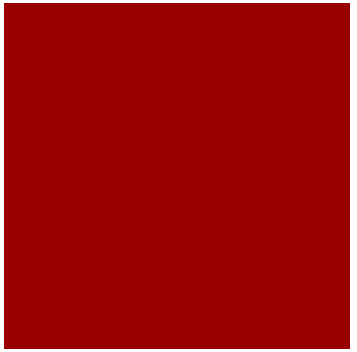
- Operational Security Capabilities for IP Network Infrastructure
- Routing Protocol Crypt Issues
  - Manual Keying の問題点
  - 単なる MD5 ではなく
  - OSPF でのシーケンス番号攻撃
- Security Assessment of the Internet Protocol version 4
  - TCP/IP (IPv4) の脆弱性に関するドキュメント
  - 今更言われても。。。って感じなものも

LISP WG

- Locator / ID Separation Protocol WG
- LISP framework
  - Deployment シナリオ
  - LISP/ALT
- LISP MAP Server
  - Interoperability Test も行われた
  - Cisco LISP / Lisp-Click / ZLisp /Open LISP
- FIB aggregation / Virtual Aggregation と同じような結果になっていくのでは

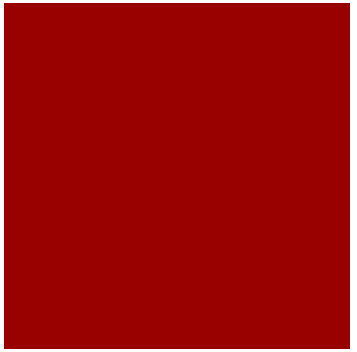
DNS関連

DNSEXT - forgery resilience



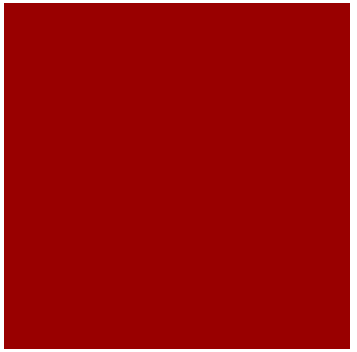
- DNS クエリのエントロピーを拡張する
  - DNS ping, dns0x20, RTT Banding ...
- キャッシュサーバでの上書き禁止
- DNS 実装側での工夫が必要
  - 積極的に手を入れるまでもないのでは。。。
  - Draft 的には IESG レビューに
- なんとなく立ち消えそう
  - 商用 DNS サーバは独自に実装し、BIND 等はあまり対応しそうにない

DNSEXT - EDNS0



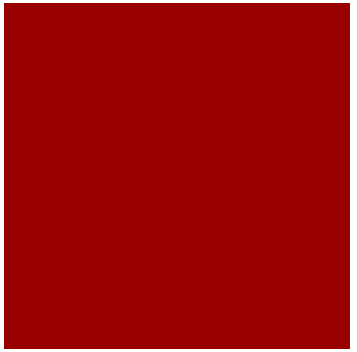
- EDNS0 のバッファサイズと MTU の関係
  - EDNS0 buffer size > MTU
  - 良い環境とはなり得ない
- EDNS0 と DNSSEC パケット
  - EDNS0 buffer size < 1220 の場合は DO (DNSSEC OK but) を無効にした方が良い？
  - EDNS0 buffer size > 1024 を通さないファイアウォール
  - EDNS0 is unreliable
  - TCP fallback

DNSEXT - DNSとTCP



- DNS レスポンスサイズ
  - DNSSEC によって増大
  - EDNS0 という解法もあるけれど。。。
  - すべてがサポートしているわけではない
- TCP で DNS クエリは現在 SHOULD
  - MUST にする？
  - 一部 CPE の DNX Proxy は TCP をサポートしない
  - Stateless TCP
  - Persistent Connection

DNSEXT - DNSSEC



- Trust Anchor Selection
  - Closest
    - TAR (Trust Anchor Repository) から選出
  - Any
    - どれでも利用できるものから
  - On-Tree
    - DNS tree から取得

DNSOP WG

- DNSSEC 鍵更新
- DNSSEC trust anchor
- IPv6 reverse zone
- IDN TLD
- Resolver Priming

DNSOP - DNSSEC

- DNSSEC 鍵更新
  - 鍵更新のためのフレームワーク定義
  - 通常時更新、緊急時更新
  - DPS (DNSSEC Signing Policy and Practice Statement) framework
  - dnssec-key-timing
- DNSSEC trust anchor
  - DNS プロトコルを利用して Trust Anchor を更新するための仕組み

DNSOP – IPv6 reverse zone

- draft-howard-isp-ip6rdns-01
  - No Response
  - Wildcard match
  - Dynamic DNS
  - Generate PTR on the fly
- 要するにいちいち書いてたらやってられない

DNSOP – その他

- IDN TLD
  - TLD に IDN が導入される
  - TLD が飛躍的に増大する
  - .中国 v.s. .中國
  - DNAME による Redirection
- Resolver Priming
  - draft-ietf-dnsop-resolver-priming-02
  - “Priming” という挙動を標準化
  - いつ、どのタイミングで、どのように

DNSSEC 関連の動き

- Trust Anchor Repository
  - Trust Anchor : DNSSEC 認証の起点を示す DNSKEY RR
  - TAR : DS RR を集めて保存
- DLV
  - DNSSEC Lookaside Validation
  - DLV RR を使い、Trust Anchor を自動的に発見
- Root Zone 署名
  - IETF76 にて状況報告 – Q&A セッション
  - 2009年12月1日に ICANN がゾーン提供開始
  - 2010年7月1日までに、全 ROOT DNS サーバが対応
    - http://blog.icann.org/2009/10/dnssec-signed-root-by-july-1-2010/

IPv6 関連

v6ops WG

- Requirements for IPv6 Customer Edge Router
  - いわゆる BB ルータへの要求
  - Prefix Delegation
- Rogue IPv6 RA
  - Problem Statement
  - RA guard
  - SeND を使えともありますが。。。
- 6to4 / Teredo / ISATAP
  - Routing Loops (ISATAP / 6to4)
  - 攻撃者がいればあぶないのはどれもいっしょ。。。

v6ops WG

- IPv6 in IX
  - IPv6 アドレスの使い分け
    - Routable v.s. non-routable
  - Arp sponge / ND sponge ？
    - Arp / ND を横取りして Bogus パケットを観測
- CGN for IPv6 transition
  - Incremental CGN

6MAN WG

- IPv6 Maintenance WG
- Handling Overlapping IPv6 Fragments
  - IPv6 フラグメントパケットの再構築方法
  - セキュリティ的な問題
- Address Selection Design Team
  - アドレス選択アルゴリズムのコンフリクト (RFC3484)

6MAN WG

- A Recommendation for IPv6 Address Text Representation
  - IPv6 アドレステキスト表記の方法
- Use of /127 IPv6 Prefix Length on P2P Links Not Considered Harmful
  - P2P リンクでは /127 を。。。

BEHAVE WG

- NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
- DNS64: DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
- Stateful IPv6/IPv4 Translation
- Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)