事前資料

DNSの可用性と完全性について考える

はじめに

今回のセッションは

「キャッシュポイズニング」

をターゲットにして議論したいと思います。

DNS プロトコルが
あまり詳しくない方は、

１日目の
「DNSチュートリアル」

に是非参加してください。

より深く本セッションに参加できます

現在の状況を整理しようか

事前資料

キャッシュポイズニングにおける DNSプロトコルの問題点

- データの完全性を保証していない。
  - 受け取ったデータが正しいデータか確認できない。
- なりすましが容易
  - 主に使うのがUDPプロトコル
- パケット識別のエントロピーが低い
  - 攻撃の成功が容易

問題に対するアプローチ

- データの完全性を保証していない。
  - DNSSECを実装することで、完全性をある程度担保
- UDPプロトコル
  - 今のところなし
    - FULL TCP化という声もある
- パケット識別のエントロピーが低い
  - ソースポートのランダム化によりエントロピーを足す

今の現状は？

日本国内の状況
（私の主観も入ります…）

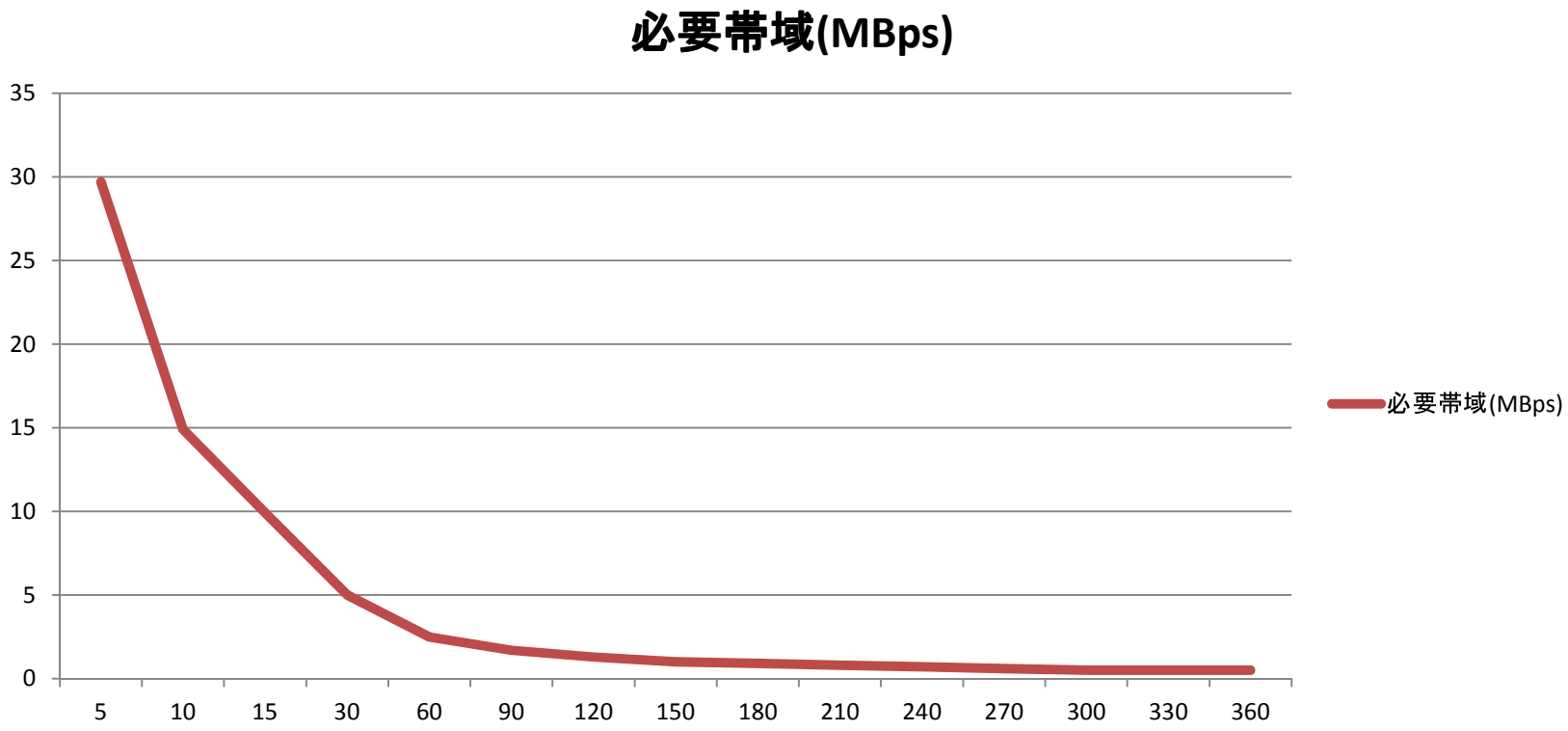
- DNSSECの実装
  - 権威DNSサーバ側
    - 日本国内ではほとんど普及していない。
    - アウトソーシング系で対応しているのは私が知る限り3社程度
    - DS取り次ぎしてくれる事業者も少ない
  - キャッシュDNSサーバ側
    - 権威よりはマシだが、ISP契約回線数ベースで見ると1割行くか行かないか。
    - Google Public DNSが対応しているので、実際はもっと多いはず。
- パケット識別のエントロピーが低い
  - ソースポートのランダム化によりエントロピーを足す
    - ISPのキャッシュDNSサーバの対応状況は、契約回線数ベースで見ると、ほぼ対応していると考えていい。（要は大手は全て対応済み）
    - キャッシュDNSサーバ台数だと、数割固定ポートが残ってるような

みんな大好き
ソースポートのランダム化の効果

- モデルケース
  - 権威DNSサーバ2台（アドレス2つ）
  - 毒入れパケットのサイズ（200byte)
- ポート固定の場合
  - 必要なデータ量は
    - 2*65535*200 = 約25MB
- ポートランダムの場合
  - 必要なデータ量
    - 2*65535*64000*200 = 約1.5TB

ソースポートがランダムな時の毒入れに必要なリソース

- 帯域(Mbps)＝y, 時間（日）＝xとすると以下のような感じ



ソースポートがランダムな時の毒入れに必要なリソース

- 帯域(Mbps)＝y, 時間（日）＝xとすると以下のような感じ

時間	5	10	15	30	60	90	120	150	180	210	240	270	300	330	360
必要帯域	29.7	14.9	9.9	5	2.5	1.7	1.3	1	0.9	0.8	0.7	0.6	0.5	0.5	0.5

- 半年0.9Mbpsの攻撃を行えば理論上は毒入れできる。

キャッシュDNSサーバの運用者が
頼みにしている

ソースポートのランダム化の
効果ってこれぐらいなんだけど。

他のレイヤーの人たちはどう感じます？

国内であまり論じられてない観点

- 中間者攻撃
  - 日本だと通信の秘密という大原則があるからあんまり考えられてないけど
  - 例えば経路ハイジャックされて、権威DNSサーバのパケット吸い込まれたらどうする？

国内であまり論じられてない観点

- DNSを利用している側
  - DNSで偽の応答が返る可能性があるのって認知されてる？（サービスの運用者とか）
  - もしかして、キャッシュポイズニングされても問題なかったりするのか！
    - なんか保険とか有るらしいよ？

キャッシュポイズニングって
DNSSECで解決できるんだけど
なんでやらないの？

答え

可用性が犠牲になるから
（とみんな思ってる）

DNSSECの可用性の問題

- 権威DNSサーバ側
  - 鍵交換とか署名とか定期的に行う必要がある。
  - DS取り次ぎミスしたら2時間～１日止まる
- キャッシュDNSサーバ側
  - 権威DNS側の運用ミスすると、検証しているキャッシュDNSだけSERVFAILする。
    - あんまり普及してないので「あんたんとこだけページ開けない」クレームの発生 (NASAとか)
  - TLDのゾーンの運用失敗が発生した時の影響が大きすぎる。

DNS運用者の多くは

可用性のリスク ＞ 完全性のリスク

だと思ってる。
そうだよね。

本当にそうかは
本編にご期待ください。

セッション当日に議論したいこと

- DNSを日頃使ってる方に
  - 今の状況の毒入れのリスクは許容範囲？
    - 毒入れされても仕方ないよねって思える？
  - DNSSECによる可用性の低下は許容範囲？
- 権威DNS運用者の人たちに
  - これが解決できれば導入できるよ、とか！
- キャッシュDNS運用者の人たちに
  - みんなで検証すれば怖くない？