短いTTLのリスク

DNS DAY - Internet Week 2006

2006年12月6日
民田雅人
株式会社日本レジストリサービス
(2006年12月27日修正版)

DNSプロトコルの脆弱性

- DNSはUDPなので、嘘データを入れやすい
  - 16bitのIDを推測して当てる
  - 送信元のソースアドレスをフェイク
- 既知の脆弱性(2002年11月初出)
  - http://www.kb.cert.org/vuls/id/457875
  - 「DNS再入門」(IW2002のDNS DAY)でも紹介
- この確率は意外に高い
  - いわゆる「誕生日のパラドックス」

従来から知られていた脆弱性

- http://www.kb.cert.org/vuls/id/457875
  - オープンなキャッシュサーバに対して、大量のリクエストを出す
  - 同じサーバに対して、偽装したDNS応答パケットを、IDをランダムに変えながら送る
  - それなりの確率でキャッシュ・ポイズニング(毒入れ)が成立する
- 実際に可能であるが、大量のクエリのリクエストのおかげで、検出しやすい

ここで説明する脆弱性

- DNS RRのTTLが短いと、キャッシュサーバの問合せ頻度は高くなる
  - 例えばTTLが30秒のサイト(実際に存在する)で、高アクセスなサイトだと、30秒間隔で、確実にキャッシュサーバからの問い合わせが発生する
- 気長に嘘のDNS応答をキャッシュサーバに送り続ければ、**そのうち**当たる

「そのうち」が**意外に短い**

攻撃のストーリ

- 攻撃者はアクセスの多いサイトで
  TTLが短いものを狙う
  - どこのキャッシュサーバでもかまわない
  - 気が付かれないようにこっそりと攻撃したい
- 同時に複数のキャッシュサーバへ
  嘘の応答を定期的に送り続ける
- 時間の問題で、どこかのキャッシュサーバへの毒入れが成功する

どこかのキャッシュサーバへ毒入れが成功する確率

$$P_S = 1 - \left(1 - \frac{R \times W}{N \times Port \times ID}\right)^V$$

R: 攻撃対象1台あたりに送るパケット量(pps)
W: 攻撃可能な時間(Query⇒AnswerのRTT)
N: 攻撃対象レコードを保持するコンテンツサーバの数
V: 攻撃対象のキャッシュサーバ数
Port: Query portの数(BINDの場合固定なので1)
ID: DNSのID (16bit = 65536)

毒入れが1回でも成功する確率

$$P_{CS} = 1-(1-P_S)^A$$

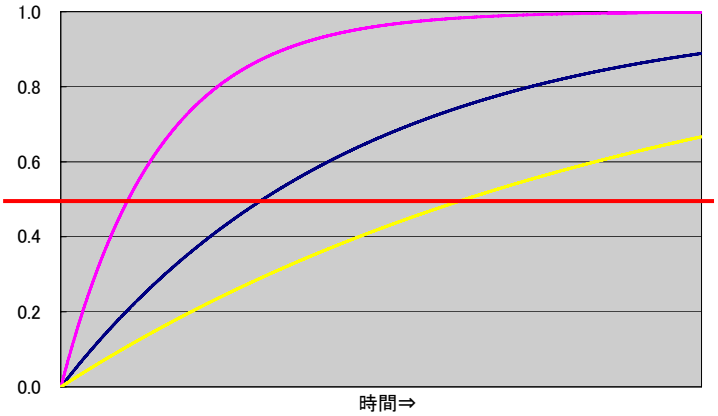
$$= 1-\left(1-\left(1-\left(1-\frac{R\times W}{N\times Port\times ID}\right)^V\right)\right)^{\frac{T}{TTL}}$$

$$= 1-\left(1-\frac{R\times W}{N\times Port\times ID}\right)^{\frac{V\times T}{TTL}}$$

A:攻撃数(=T/TTL)

T:攻撃時間　TTL: DNSレコードのTTL

毒入れが1回でも成功する確率の時系列変化



確率が0.5を超えると毒入れが成功しても不思議ではない

internetweek.jpの計算結果

- AレコードのTTL　86400秒
- Authoritative Server　2台
- 1台あたりの攻撃レート　**100pps**
- 攻撃対象のキャッシュサーバ　100台
- RTT(えいやで20msとする)　20ms
- 確率0.5を超えるまでの時間　約15ヶ月

ある人気サイトの計算結果

- AレコードのTTL　30秒
- Authoritative Server　2台
- 1台あたりの攻撃レート　**10pps**
- 攻撃対象のキャッシュサーバ　100台
- RTT　20ms
- 確率0.5を超えるまでの時間　**38時間後**

問題点のまとめ

- TTLが短いと、
  低レートでも攻撃が成功する確率が高くなる
  - 低レートの攻撃は検出しにくい
  - 攻撃が高レートになれば、
    より短時間で攻撃が成立する可能性がある
- DNSプロトコルそのものに起因する
  - もしIDが32bitやそれ以上であれば攻撃困難
- キャッシュサーバの実装によっては攻撃困難
  - クエリポートが固定か、そうでないか

キャッシュサーバの実装

- クエリポートが固定
  - BIND系全て
  - Windows 2000 ServerのDNSサービスは固定
    Windows Server 2003は未調査
- クエリポートが変わるもの
  - dnscache (djbdns)
  - PowerDNS recurser

DNSコンテンツ設定側で毒入れ確率を減らすために

- 極端に短いTTLは可能な限り避ける
- TTLを短くしなければならない場合、ネームサーバの数を多くする
  - ただし、大きな効果は期待できない
  - 他のパラメータの調整はコンテンツ設定側では不可能

根本解決のために

- Ingress Filterの導入 (BCP38 RFC2827)
  - インターネットに対して、ソースアドレスに嘘をついたパケットを送出できなくする。(さまざまな攻撃を防止できるようになる)

ISPの方、是非お願いします

- DNSSECの導入
  - DNSの応答パケットが正式のものか虚偽のものかを判断でき、虚偽の応答を捨てることができる

JPRSはDNSSEC導入に取り組んでます

参考文献

- draft-hubert-dns-anti-spoofing-00
  - 特定(1台)のキャッシュサーバを攻撃した場合について記述してある

Q and A

JPRS
JAPAN REGISTRY SERVICES