DNS Response Rate Limiting (DNS RRL)

IIJ 山口崇徳

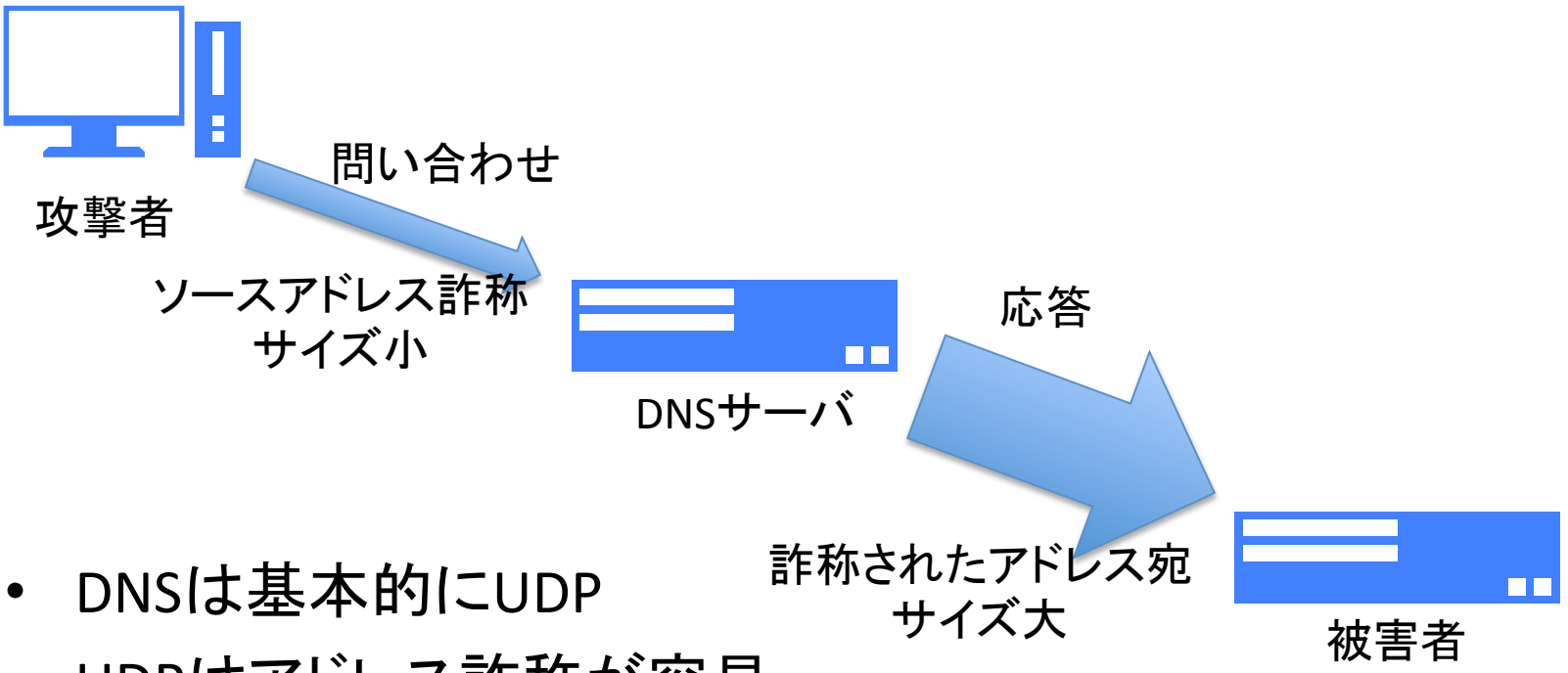
いきなりすいません。
本日はDNSSEC 2013スプリングフォーラムですが、

DNSSECの話はしません。

DNS amplification attack

- 先日「重複をお許しください」が出ましたね
  - http://jprs.jp/tech/notice/2013-04-18-reflector-attacks.html
  - JPRSだけでなく、JPNIC、JPCERT、警察庁などからも同様の注意喚起
- DNS amp、DNSリフレクター攻撃などとも呼ばれる
- 3月のSpamhaus/Cloudflare事件が記憶に新しいが、手法自体は古くから知られたもの
  - JPRSのアナウンスは今回が初めてではない(2006/3/29)
  - 以前2chもこれで落とされたらしい(2010/3/1)
  - 公になっていないだけで、日常茶飯事

復習: DNS ampとは



- DNSは基本的にUDP
- UDPはアドレス詐称が容易
- 少量のトラフィックを送るだけで、被害者のネットワーク帯域を飽和させることができる
  - botnetを使うとより効率的

DNS ampの踏み台となる条件

- アドレス詐称しやすいUDPで、かつ応答パケットが大きくなる
  - 必ずしもDNSである必要はない
  - 理屈の上ではSNMP ampとかも可能
- これまではキャッシュDNSサーバが踏み台に多く使われた
  - オープンリゾルバは大きな情報を外部から容易にキャッシュさせることができる
  - 権威DNSサーバは外部から情報をいじれない
- 近年、DNSの応答サイズは増大傾向
  - SPF、DKIM、そしてDNSSEC
  - わざわざ外部から仕込まなくても、権威DNSサーバの側で勝手に大きな情報を登録してくれる
- DNSSECな権威サーバはDNS ampの踏み台に利用しやすい

踏み台にされないようにするには

- キャッシュDNSサーバは、組織内部から利用できればよい
  - 外部からアクセスできないように制限する
  - RFC5358: Preventing Use of Recursive Nameservers in Reflector Attacks
- 権威DNSサーバは世界中からアクセスできなければならない
  - アクセス制限できない
  - どうしよう?

権威サーバのamp対策

- 権威DNSサーバに問い合わせてくるのはキャッシュDNSサーバ
- ひとつのキャッシュDNSサーバの下にユーザがたくさん
  - ひとつのキャッシュサーバから大量の問い合わせがやってるくること自体は異常ではない
  - 問い合わせの数で制限するのは危険
- キャッシュサーバとはキャッシュするサーバである
  - キャッシュが生きている間は、同じことを権威サーバに問い合わせてくることはないはず
  - 短時間に同じ問い合わせが大量にやってくるのは異常
  - こいつを止めてやればいいんじゃね?

Response Rate Limiting

- ということで…
- 本来ならキャッシュしてるはずの情報を何度も何度も繰り返し聞きにきてないかチェック
- そういうものがあれば、攻撃とみなして応答を制限する
  - 詐称されたアドレスに大きな応答を返さなくなる

- キャッシュDNSサーバでRRLを導入するのは危険
  - キャッシュサーバのクライアントはキャッシュ機能を持たないものが多いので、何度も同じ名前を聞きにくることは異常とはいえない

Query Rate Limitingじゃないの?

- はい、response rateなんです
  - 単位時間あたりの「応答数」を制限する
- 問い合わせそのものを制限するのではなく、その問い合わせ内容を調べた上で、応答について制限する
- どう違うの?
  - example.com/ANYの問い合わせを大量に受けてDNS ampが疑われる場合に、これに対する応答は制限しつつも www.example.com/A に対してはちゃんと応答する
  - 1.example.com、2.example.com、3.example.com、…のような、問い合わせる名前を毎回変えながら攻撃するような場合にも対処
    - ワイルドカードの問い合わせやNXDOMAINで大きな応答を返すのを抑制

RRLの実装

- BIND
  - 9.7〜9.9 に対する(ほぼ公式の)パッチ
    - http://ss.vix.su/~vjs/rrlrpz.html
    - RHEL6のRPMは適用済み(RHSA-2013-0550)
  - BIND 9.10、BIND 10で正式採用予定
- NSD
  - 3.2.15 で対応
  - configure --enable-ratelimit
- KnotDNS
  - CZ NICが開発してる権威DNSサーバ
  - 1.2.0-rc3 で対応

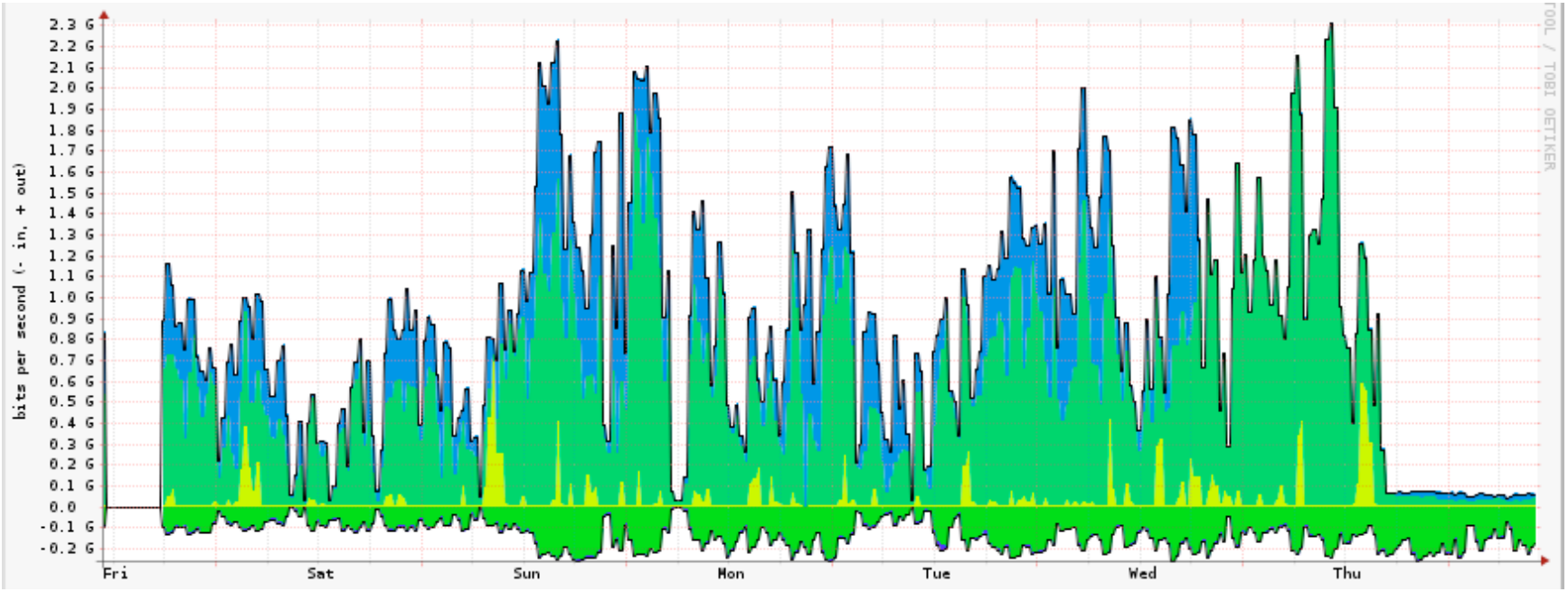
RRL発動時の挙動

- 設定したresponse rateを越えて問い合わせが来た場合、応答を返さない
  - …だけではない
- 1/2の確率で応答を返す(SLIP)
  - が、通常の応答ではなく、TC(truncated)ビットをonにして応答する
    - TC = TCPで問い合わせをやりなおせ
  - アドレス詐称していないホストがRRLで誤爆されたとしても、何度かリトライしてslipした応答を受けとれればTCPで名前解決可能
    - TCPは詐称困難なのでRRLの制限対象外
  - slip応答は問い合わせパケットと同じサイズ(増幅しない)
  - BIND + rrl patchではslipする確率を設定で変更可能
    - NSDは変更不可

デモ

- RRLが有効な権威DNSサーバに同じ問い合わせを大量に投げてみるよ!
  - アドレス詐称まではしませんが、制限される様子は観察できます

RRLの導入効果



- http://lists.redbarn.org/pipermail/ratelimits/2012-December/000144.html より
- Affilias (.org や .info のレジストリ) の実測値
- outbound が max 2.3Gbps → 70Mbps

注意点(1)

- amp攻撃そのものを抑止するものではない
  - RRLの制限発動までは増幅された応答を詐称アドレスに返す
  - RRL発動後も(増幅はしないけど)slip応答は返す

- 制限対象はIPアドレスごとではなく、ネットワークごと
  - v4は/24、v6は/56 (BIND + rrl patch; 設定で変更可)
  - v4は/24、v6は/64 (NSD; 設定で変更不可)
  - DNS ampはホストの脆弱性を突くのではなく、ネットワーク帯域を埋めるのが目的の攻撃なので、防御もネットワーク単位でおこなう必要がある
- 同じ/24の範囲内にキャッシュサーバが複数あると、同時に制限対象になってしまう

注意点(2)

- 負荷上昇
  - 応答レートを常に記録しておく必要があるので、amp攻撃がおこなわれていないときでも常時数%のパフォーマンス低下
- パラメータチューニング
  - 設定値が不適切だと、詐称してないクライアントを制限したり、逆にampをまったく防がなかったりすることもありうる
  - …のだが、どの程度の値が適切かという知見の集積が少ない
  - 考えなしに実施するとよろしくない

で、RRLでハッピーになれるの?

- うーん…
- 大きな応答を返す1万台の権威サーバのそれぞれに対して1query/secで詐称クエリを投げると…
  - 個々の権威サーバから見ればクライアントあたり1qpsでしか問い合わせが来ないのでRRLは発動しない
  - が、全体では1万qps
- 大きな応答を返す権威サーバを大量に用意することができれば、RRLを回避しつつ十分な威力でamp攻撃できる
  - DNSSECが普及すればするほどampに適した権威サーバも増える
- RRLは一時しのぎにしかならない
  - 次の対策を考えておく必要がある
  - 根本的にはBCP38 (RFC2827) Network Ingress Filtering の実施

まとめ

- DNS amp対策が必要なのはキャッシュDNSサーバだけではない
  - DNSSECは権威サーバでも大きな応答を返して増幅率が大きくなるので、ampの踏み台に利用しやすい
- RRLを導入することでampを軽減できる
  - 単位時間あたりの同一応答数を制限
  - ampを防止するわけではない
- 根本的解決ではない
  - RRLを回避する攻撃も想定される
  - BCP38を実施して詐称アドレスを拒否する
    - キャッシュDNSに対するamp攻撃やTCP SYN flood攻撃にも効果あり
    - http://www.bcp38.info/

(参考) DNS Dampening

- もうひとつのDNS amp対策手法
  - http://lutz.donnerhacke.de/eng/Blog/DNS-Dampening
- クライアントごとにペナルティポイントを計算
  - 問い合わせタイプごとにポイント加算(ANYを聞いてきたらxx点)
  - 応答サイズによってポイント加算
  - 一定時間経過ごとにポイント減算
- ポイントが一定値を越えたら問い合わせを捨てる
- RRLより誤爆しやすいが、問い合わせる名前を変えながらのamp攻撃に強い
- BIND用patchあり
  - http://altlasten.lutz.donnerhacke.de/mitarb/lutz/bind-9.9.2-dampening.patch

参考URL

- Response Rate Limiting in the Domain Name System (DNS RRL)
  - http://www.redbarn.org/dns/ratelimits
- DNS Response Rate Limiting (DNS RRL)
  - http://ss.vix.su/~vixie/isc-tn-2012-1.txt
- DNS Response Rate Limiting as implemented in NSD
  - http://www.nlnetlabs.nl/blog/2012/10/11/nsd-ratelimit/
- Defending against DNS reflection amplification attacks
  - http://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf
- DNS Rate Limiting
  - http://www.guug.de/veranstaltungen/ffg2013/talks/DNS_Rate_Limiting__Matthijs_Mekking.pdf
- Defending against DNS Amplification Attacks
  - https://indico.dns-oarc.net/indico/getFile.py/access?contribId=4&resId=0&materialId=slides&confId=0