DNS rebinding attackの対策と考察

力武　健次
情報通信研究機構 インシデント対策グループ
2007年11月19日
dnsops-jp BoF @ Internet Week 2007

DNS rebindingって?

- DNSの指すオブジェクトを変えること
- JavaScriptはホスト名のみで認証
- 攻撃者が外部のホスト名から内部を指したらどうなるか
  →DNSの通りに見に行ってしまう
- ∴同じホスト名で外部と内部両方にアクセスする可能性が発生する

JavaScript Same-Origin Policy

- アクセス範囲をドメイン（ホスト）名で規定
- 同じプロトコル，ホスト，ポートで許可

http://x.example.com/a.html	オリジナル	
http://x.example.com/dir/b.html	許可	
https://x.example.com/c.html	不許可	プロトコル
http://x.example.com:81/d.html	不許可	ポート
http://y.example.com/e.html	不許可	ホスト

代表的な攻撃シナリオ

1. ホスト名Xを外部アドレスAに設定
2. Aからのスクリプトを読ませる
3. ホスト名Xを内部アドレスBに設定
4. 2.で読んだスクリプトからホスト名Xでアクセスしに行く
5. 4.のアクセスは内部アドレスBに行く

→ファイアウォール越えのアクセスができる

JavaScript以外の攻撃対象

- ブラウザのプラグイン一般
  （ブラウザとは別の認証判断をしている）
  Java (LiveConnect, Applet)
  Flash Player
  Adobe Acrobat
  その他たくさん
- Same-origin policyであれば攻撃対象

攻撃にかかる時間

- 95%の信頼度で
  LiveConnect (JVM): 40〜60msec
  Flash Player 9: 200msec
  IE6, IE7, Firefox 1.5/2, Safari 2: 1sec
  LiveConnect (without JVM): 1.3sec
  Opera 9: 4 sec
  （スタンフォード大の論文[1]より）

攻撃への対策は手薄

- DNS pinning
  - 一度DNSを引いたら一定時間保持
  - (TTLには関係ない名前解決時の処理)
- しかしpinning無効手法の多くが既知
  - IE6/IE7/Firefox 1.5/Opera 9/Safari 2
- Flash PlayerではXML policyで攻撃可
  - SWFムービーに任意の内容を送り込める

攻撃されたホストの利用法

- ファイやウォール越え
  - プライベートネット内資源の探索
  - localhostをソースIPにしたホスト内部攻撃
  - ホスト内部のサービスの外部からの不正利用
- ソースIPアドレスの不正利用
  - グローバルアドレスを持ったホストを攻撃
  - →踏み台攻撃 (SPAM, なりすまし一般)

どれくらい攻撃に成功したか

- Web上の広告を見てもらった[1]
- 成功率は約91%
  - Flash Player, LiveConnect, Java+proxy
  - Flash Player 9の86.9%に対して攻撃成功
- グローバルIPを安く乗っ取れる
  - 10万個のIPアドレスを100米ドル以下で入手
  - botnetを借りるより安そう

DNS的対策(1)

- プライベートネットワーク対策
  - dnswall[2]
    - CNAME禁止
    - A/AAAA RRの応答を検査する
    - プライベートアドレスならNXDOMAINにする
- グローバルアドレスだったら?
  - ...内部と外部の区別方法が別に必要

DNS的対策(2)

- 逆引きの認証を行う
  アドレスが本当にそのホストかどうかの判定
  例: ホスト 11.22.33.44に対して
  auth.44.33.22.11.in-addr.arpa IN A 11.22.33.44
  とした上で
  abc.example.org.auth.44.33.22.11.in-addr.arpa
  が IN A 11.22.33.44 と定義されていれば認証
- すでにJavaで実装済みだが...
  Flash Playerなどではまだらしい

DNS的対策は実は難しい

- DNSSECなどの認証では解決不可
  authoritative zoneの中身は信じるしかない
- レジストラは何ができるか?
  事後対策ぐらいしかできないだろう
- DNSソフトウェアは何ができるか?
  プライベートアドレスは無碍に拒否できない
  (プライベートネットワークの運用ができなくなる)

Webの本質的な問題

- pinningは次の1行で無効になってしまう
  document.domain = document.domain;
  (DNSを引きに行ってしまう)
- HTTP Host Headerのチェックもあるが...
  これで嘘をつかれても対抗手段がない
- JavaScript等のアクセス許可問題に帰着
  そもそも誰でも信用して，というのが間違いか?

参考文献

[1]スタンフォード大の論文
ACM CCS 2007で発表
http://crypto.stanford.edu/dns/
[2]dnswallのソース
http://code.google.com/p/google-dnswall
[3]金床氏のメモ
http://wizardbible.org/33/33.txt