DNS の抱えるセキュリティ・リスクと対策

力武 健次
独立行政法人 情報通信研究機構
情報通信部門 セキュリティ高度化グループ
rikitake@nict.go.jp

1 概要

DNS（ドメイン名システム）は，nict.go.jp のようなドメイン名と，IP アドレスなどのネットワーク資源を結びつけるための広域分散データベースである．Web や電子メールなど，ほとんどのインターネット・アプリケーションの動作は DNS の信頼性に依存している．

このような重要な役割を DNS が果たしているにもかかわらず，DNS は外部からの攻撃に対して弱く，防御体制は十分とはいえない．本稿では DNS が現在抱えるリスクと対策について述べる．

2 DNS の認証問題と DNSSEC

DNS の中身である RR（リソースレコード）は，システム運用上不可欠な情報を含む．しかし，RR に対する認証は，ドメイン名の木構造に準じた上位 DNS サーバへの手動による下位サーバのアドレス登録という弱い形でしか行われていない．IP アドレスやパケットが第 3 者により偽造できる現在，このような弱い認証は簡単に破られてしまう．また，スパイウェアなどにより OS の DNS 参照制御情報を書き換えて，偽のサーバへ誘導する手法をフィッシング詐欺などで使う事例が増えている．

これらのドメイン乗っ取り行為に対する対抗策の 1 つとして，DNSSEC [1, 2, 3] がある．DNSSEC では，DNS サーバの提供する RR 群に PKI（公開鍵暗号基盤）を使い管理した署名鍵を用いてデジタル署名を行うと共に，サーバの委任関係を RR 署名鍵への署名の連鎖として表現することで，DNS の提供するドメイン名空間全域にわたって RR 情報の正当性を保証することが目的である．DNSSEC を用いることで，ドメインの乗っ取りの大部分は防ぐことができる．

しかし，DNSSEC はリゾルバとサーバ両方の大幅な拡張を必要とすること，またドメイン名管理組織が連携して世界規模の PKI を維持しなければならない必要性から，その実装はまだ進んでいない．DNSSEC の早期の実装は急務だが，それまでの間は OS の不正書き換え防止やトラフィック監視など他の手段でドメイン乗っ取りを防ぐ必要がある．

3 DNS の通信路への攻撃

DNS のデータ交換はほとんどを UDP に頼っており，本質的に DDoS（分散サービス拒否攻撃）を防ぐ手段はない．性能に余裕のない小規模なサーバが DDoS 攻撃対象になればドメイン全体へのアクセス停止を引き起こす．

また，DNS のリゾルバーサーバ間通信やサーバの情報更新，サーバ間の情報複製に際しては，DNS の暗号化拡張 [4, 5] や SSH, rsync といった安全なファイル転送手段で保護できるものの，これらは未だ普及していない．このような環境下では，DNS の交信への攻撃は致命的な結果となる．

4 DNS 構成システムへの脆弱性攻撃

DNS サーバは公開運用が前提であり，その脆弱性は広く攻撃の対象となる．最も一般的な実装である BIND の脆弱性 [6] は，多くの情報システムの停止を引き起こした．

また， DNS は多数のキャッシュを利用して性能向上を図っている．しかし，このキャッシュの状態保持を悪用し，匿名通信路として使う技法も開発されている [7]. このように DNS システムとしての所定の動作が脆弱性となり得る場合，修正は容易ではない．

その他にも，多くの DNS サーバが不適切な設定による脆弱性を内包しており [8]，運用管理上の問題も見過ごすことはできない．

5 まとめ

DNS に起因するリスクの軽減には DNSSEC 等認証手段の導入は急務である．既存手法による通信路の保護や端末サーバ双方の適切な運用管理も正常な DNS 動作には不可欠である．

参考文献

[1] Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S.: DNS Security Introduction and Requirements (2005). RFC4033.

[2] Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S.: Resource Records for the DNS Security Extensions (2005). RFC4034.

[3] Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S.: Protocol Modifications for the DNS Security Extensions (2005). RFC4035.

[4] Vixie, P., Gudmundsson, O., Eastlake, D. and Wellington, B.: Secure Key Transaction Authentication for DNS (TSIG) (2000). RFC2845.

[5] Wellington, B.: Secure Domain Name System (DNS) Dynamic Update (2000). RFC3007.

[6] CERT/CC: Multiple Vulnerabilities in BIND. CERT Advisory CA-2002-31, http://www.cert.org/advisories/CA-2002-31.html.

[7] anonymous: DNS Covert Channels and Bouncing Techniques. http://archives.neohapsis.com/archives/fulldisclosure/2005-07/att-0472/p63_dns_worm_covert_channel.txt.

[8] Pappas, V., Xu, Z., Lu, S., Massey, D., Terzis, A. and Zhang, L.: Impact of Configuration Errors on DNS Robustness, *Computer Communication Review*, Vol. 34, No. 4, pp. 319–330 (2004). Proceedings of SIGCOMM 2004.