DNS サーバ・セキュリティ

Internet Week 2003 DNS Day

神明 達哉

株式会社 東芝 研究開発センター

内容

- DNS **におけるセキュリティ上の課題**
  - **データの詐称、サービス妨害** (DoS)**、「プライバシー」、セキュリティホール**
  - **具体例とその対応**
- DNS **セキュリティに関するプロトコル**
  - TSIG、SIG(0)、DNSSEC
- **一般的な動作原理が中心**
  - **個別の設定方法は後半で紹介**
  - **一部、おもに** BIND **を対象に具体的な例も示す**

用語

- リゾルバ
  - DNS のクライアント
- キャッシュサーバ
  - 反復的 (recursive) に問い合わせ、結果をキャッシュするサーバ
  - リゾルバからの問い合わせを受けて、権威サーバに問い合わせる
- 権威 (authoritative) サーバ
  - DNS のゾーンを管理するサーバ

DNS データの詐称: 概要

- 不正な DNS データを犠牲者に与える
  - 典型的には応答の改竄
  - いろいろ悪用可能
    - ネットワークの横取りや DoS など
- 様々な方法で可能
  - パケットの横取り
  - 問い合わせパケットの推測
    - パラメータ (QID, UDP port) を推測し、詐称した応答を返す
  - キャッシュ汚染
    - ゾーン外グルーによる方法など

パケットの横取り

- 例: 問い合わせのパケットを盗み見て、先に偽の応答を返す
- 常に成功するわけではない
  - 攻撃者のネットワーク上の位置に依存する
    - パケットの盗聴が可能、かつ
    - 正規のサーバより先に応答を返せる
  - 公共端末のあるような場所では可能性あり

問い合わせパケットの推測

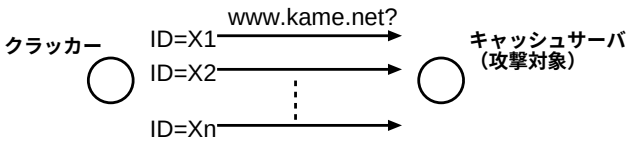
- DNS 応答パケットのパラメータ
  - 問い合わせの名前: (例)"www.toshiba.co.jp"
  - 問い合わせ ID: 16 ビット
  - 問い合わせ元 UDP ポート: 16 ビット
- すべてのパラメータを推測し、先に応答を返せれば攻撃が成立
  - 名前: 攻撃者が制御可能
  - ID: 多くの実装で乱数利用
    - …が、その精度はまちまち
  - UDP ポート: 実装によっては固定
    - e.g. BIND キャッシュサーバ

「誕生日攻撃」による総当たり的方法 (1)

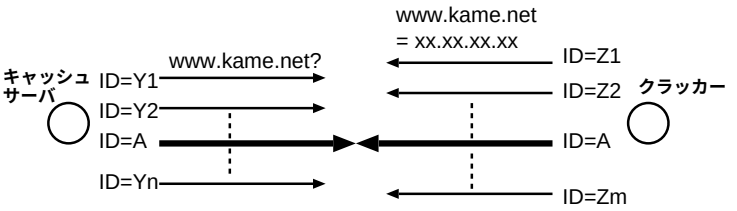
- http://www.kb.cert.org/vuls/id/457875
- 0. UDP ポートは固定または推測可能とする
- 1. 大量の問い合わせをキャッシュサーバへ送信
  - 名前は固定、ID は変化させる
- 2. キャッシュサーバが大量の問い合わせを送信
- 3. 大量の偽の応答をキャッシュサーバへ送信
  - ID を変化させる
  - 2 と 3 で対応する ID があれば攻撃が成立

「誕生日攻撃」による総当たり的方法 (2)

- クラッカーからキャッシュサーバへの問い合わせ



- 一致する組み合せがあれば攻撃成立



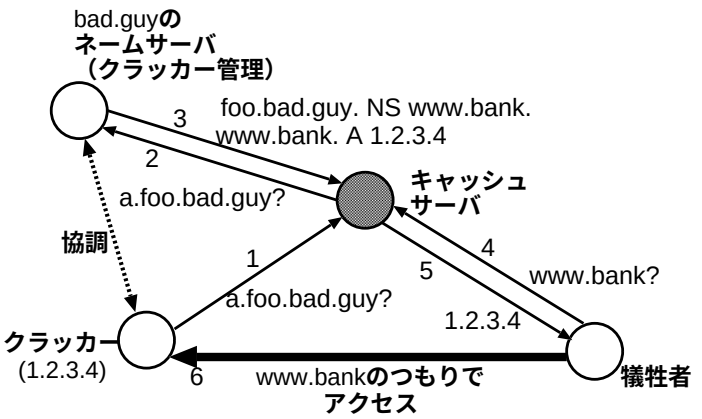
「誕生日攻撃」による総当たり的方法 (3)

- 強力だが、制限あり
  - クラッカーがキャッシュサーバへ問い合わせを出せるのが前提
  - アクセス制御で攻撃可能な範囲を狭められる
- 攻撃の成立しやすさは実装によって異なる
  - UDP ポートを毎回変える実装では、それも推測する必要あり
    - djbdns など
  - 同一名前の問い合わせを一つにまとめる実装に対しては大量の問い合わせは無意味
    - BIND9 など

キャッシュ汚染

- 古典的なデータ詐称方法
  - 古い BIND の実装に対しては簡単に実現できる
  - 過去に多くの被害例あり
- 1. クラッカーが管理するゾーンへキャッシュサーバを誘導する
  - 直接問い合わせる/mail/web bug などの方法で可能
- 2. グルーレコードを用いて他人のドメイン名を乗っ取る

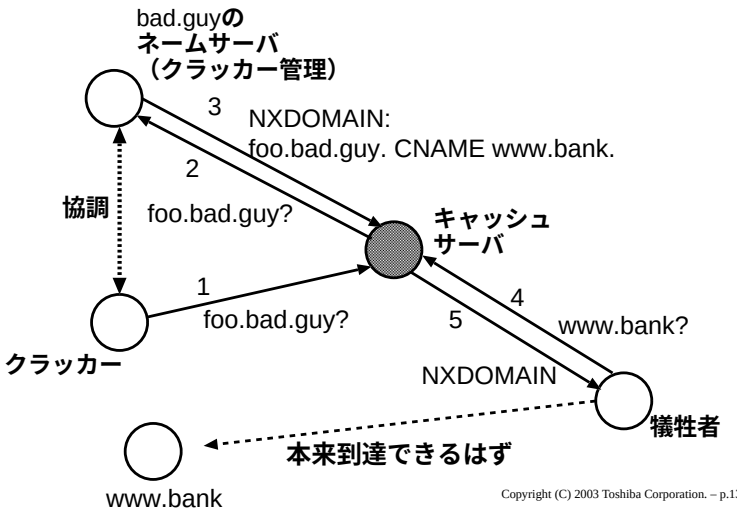
キャッシュ汚染: 動作例



否定的応答によるキャッシュ汚染

- CNAME と否定的応答 (NXDOMAIN) の組み合せによる汚染
  - DoS につながる
  - BIND 8.3.6/8.4.2 以前に脆弱性あり
    - BIND8 最新版、BIND9 は安全
- 1. キャッシュサーバをクラッカーのゾーンへ誘導
- 2. CNAME の先を他人のドメイン名に向け、NXDOMAIN を返す

否定的応答によるキャッシュ汚染: 動作例



DNS データの詐称: 対応方法

- 完全な解はない
  - 横取りや推測、総当たりによる攻撃を完全に防ぐのは不可能
  - DNSSEC はプロトコル上は「完全」に近いが、普及に難
- 限界を理解した上で、適切な対応を
  - 汚染防止のアルゴリズムを持つキャッシュサーバ利用
    - 最近の多くの実装は対応済み
  - 適切なアクセス制御
  - DNS の結果に頼りすぎない
    - (例) 名前ベースのアクセス制御をしない

サービス妨害攻撃 (DoS): 概要

- 単純な DoS
  - 大量の問い合わせによる帯域・計算資源の妨害
  - 有名な例: ルートサーバへの DoS
    - 2002 年 10 月 21 日
    - 一部のルートサーバが動作不全に
- キャッシュサーバに対する DoS
  - キャッシュのメモリをあふれさせる
  - キャッシュ用ハッシュアルゴリズムへの攻撃
    - S. Crosby, "Denial of Service via Algorithmic Complexity Attacks", USENIX Security 2003

サービス妨害攻撃 (DoS): 対応方法

- ネットワークサービスにおける宿命
  - 根本的な解はない
  - 必要以上に恐れても仕方ない
- 一般的な対症療法
  - サーバ構成の冗長化
  - アクセス制御 (とくにキャッシュサーバの場合)
- キャッシュサーバの場合の追加対応
  - サーバ設定におけるリソース制限
    - 例: BIND9 の max-cache-size オプション
  - 安全なハッシュアルゴリズムを持つ実装の利用
    - BIND 9.2.3 など

その他の DoS (1)

- IPv6 対応が不十分な DNS ロードバランサで発生
  - AAAA への問い合わせに対し、常に否定的応答 (NXDOMAIN) を返す
- 悪用すると、意図的に NXDOMAIN をキャッシュさせられる
  - 1. キャッシュサーバに対して先に AAAA を問い合わせる
  - 2. NXDOMAIN がキャッシュされる
  - 3. A を問い合わせてもキャッシュされた NXDOMAIN が返ってくる
- 対象ゾーンの管理者、キャッシュサーバ利用者の双方が被害者

その他の DoS (2)

- 本質的には実装のバグ
  - ロードバランサの置き換え/アップグレード以外の解はない
- 詳細
  - http://www.kb.cert.org/vuls/id/714121
  - draft-morishita-dnsop-misbehavior-against-aaaa-00.txt

DNS の「プライバシー」問題

- ゾーン全体の内容の「漏洩」
  - 第三者によるゾーン転送
    - 例: dig @203.178.141.194 kame.net axfr
  - ゾーン転送の盗聴
  - DNSSEC を利用したデータ開示
    - NSEC RR によってゾーン全体のデータの鎖が得られる
- 特定サーバの実装名・バージョンの開示
  - BIND の"version.bind"

「プライバシー問題」は問題か？

- DNS の専門家の立場: 問題ではない
  - DNS の (ゾーン) データは本来公開データ
  - 公開しているサーバの名前はいずれ知られる
    - アドレスベースの総当たり攻撃も可能
  - 名前を知られて困るなら DNS に登録すべきでない
- ゾーン転送のアクセス制御は必要か
  - アドレスベースおよび TSIG 利用
  - 「プライバシー問題」の完全な解ではないが、それなりの意味もある
    - DoS 防御およびゾーン転送自体を守る
  - まずは正しい理解、後は各管理者の判断

DNS 実装のセキュリティホール

- 最近の例
  - CERT CA-2002-19
    - BIND リゾルバのバッファオーバーラン
  - CERT CA-2001-02
    - BIND8 サーバのバッファオーバーラン
  - 攻撃の実例も多数あり
- DNS におけるセキュリティホールの影響
  - サーバ: システムの乗っ取りにつながる
    - 特権ポートのために管理者権限が必要
  - リゾルバ: 更新作業が大変
    - 基本的なシステムライブラリの一部
    - どこで使われてるかわからない

セキュリティホールへの対策

- 安易な解はない
  - 基本はまめなメンテナンス
- 日常的な対策
  - 適切なアクセス制御
    - 例: キャッシュサーバへの問い合わせはローカルサイトからのみ許す
  - 不要な特権の放棄
    - 特権ポートを開いた後は管理者権限を放棄できる

DNS セキュリティに関するプロトコル技術 (1)

- TSIG
  - RFC 2845
  - **サーバ同士、またはサーバ・リゾルバ間の通信を認証**
    - **動的更新、ゾーン転送などで利用**
  - **共通秘密鍵で** DNS **メッセージ全体に署名**
- SIG(0)
  - RFC 2931
  - **動機・用途は** TSIG **と同じ**
    - SIG RR **を使った公開鍵方式**
  - **実装は不十分**

DNS セキュリティに関するプロトコル技術 (2)

- DNSSEC
  - RFC 2535、draft-ietf-dnsext-dnssec-xxx
    - I-D **版は** RFC2535 **との互換性なし**
  - **公開鍵方式による** DNS **データの電子署名**
    - **データ詐称に対する完全な解を提供**
  - **普及は難しい**
    - **原則としてルート以下のすべてのゾーンに署名が必要**
    - **クライアント側の対応にも課題**

まとめ

- DNS におけるセキュリティ上の問題
  - データの詐称、DoS、一般のセキュリティホール
- 完全な対策はない
  - データ詐称、DoS: 本来防ぐのが難しい
  - 「プライバシー」問題: こだわるメリットは薄い
- やれるところから
  - 適切なアクセス制御
  - サーバのリソース管理
  - 安全なバージョンの利用

