DNSプロトコルの脆弱性

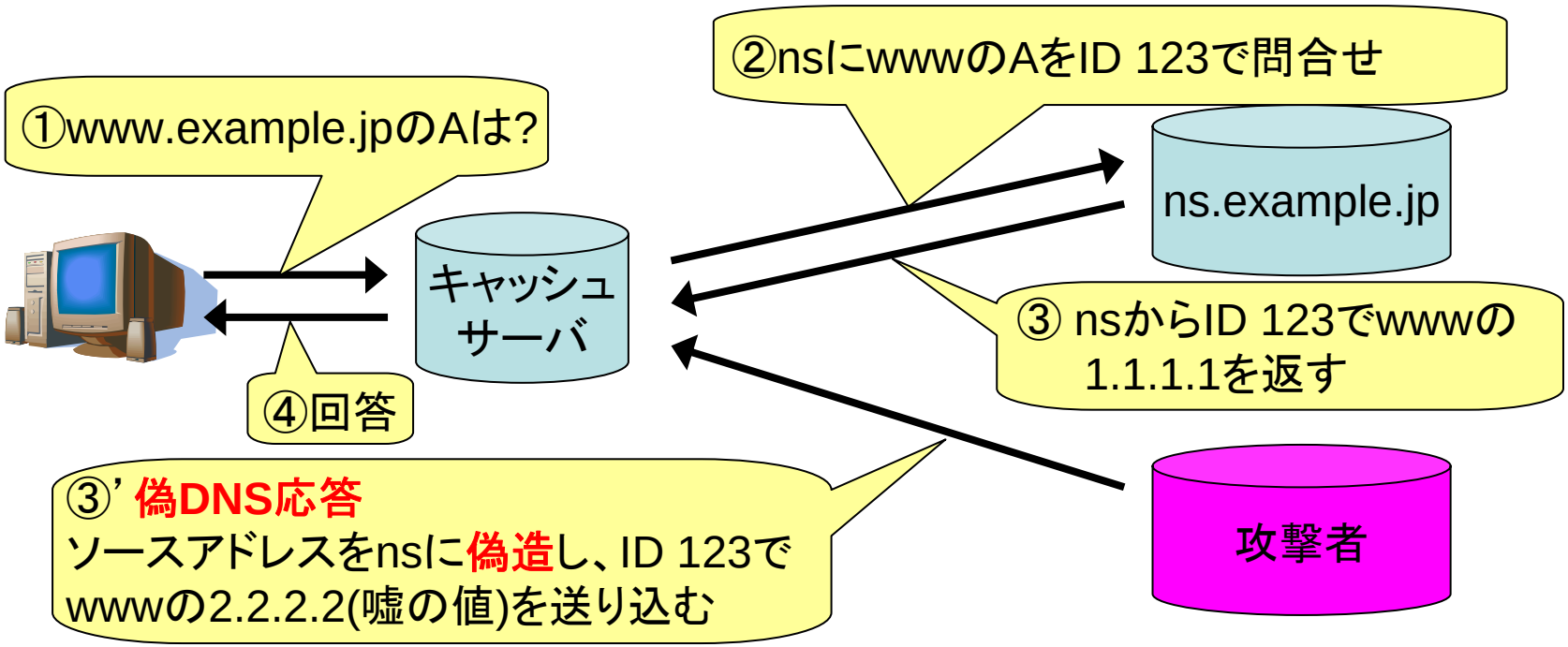
民田雅人
株式会社日本レジストリサービス
2008-07-09
dnsops.jp BoF @ 品川

DNSプロトコルのおさらい

- 問合せと応答の単純な往復
  - この名前のIPアドレスは?
    ⇒ IPアドレスはXXXXだよ
- トランスポートは主にUDP
  - 条件によってTCPになることもある
- 問合せパケット　　クエリ名+ID+etc...
- 応答パケット　　クエリ名+ID+回答+etc...

ID:　識別のための16bitの値

毒入れ



- ③より先に③’の偽DNS応答が送り込まれると、キャッシュサーバは嘘情報をキャッシュする
  - ④で嘘をクライアントに送る
- クライアントPCは、偽のサイトへ誘導される

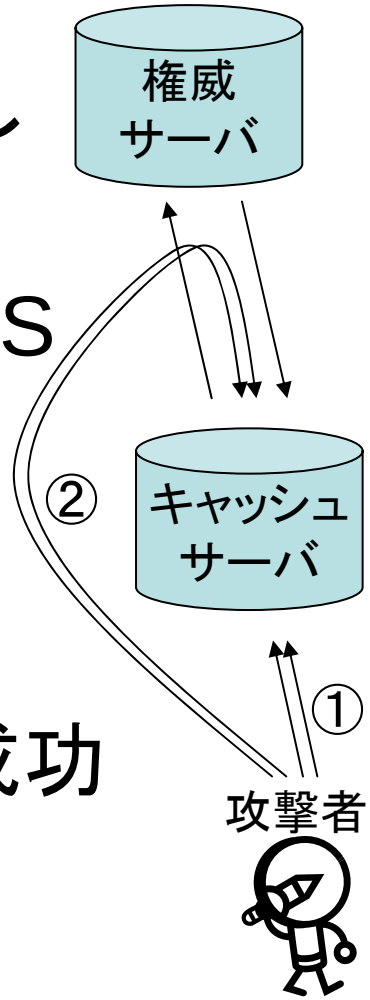
毒入れの手法

① オープンなキャッシュサーバに対して何か問合せを送る

② 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

– クエリ名とソースアドレスは自明

IDが正規応答と一致すれば攻撃が成功



DNSプロトコルの脆弱性

- CERT VU#457875で警告
  - **2002年11月**初出
  - 参考：http://www.kb.cert.org/vuls/id/457875
- ソースアドレスを偽装しやすい
  - DNSはUDPを主に使う
- IDは16bit**しか**ないため意外に当たりやすい
  - 毒入れの成功確率は、想像以上に高い

キャッシュサーバへ
毒入れが成功する確率

$$P_S = \frac{R \times W}{N \times Port \times ID}$$

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権威サーバの数

Port: Query portの数

ID:　DNSのID (16bit = 65536)

Port番号1種類の固定で計算

R	W(ms)	NS	Port	ID	確率
10000	10	2	1	65536	0.000762939
100000	10	2	1	65536	0.007629395
200000	10	2	1	65536	0.015258789
500000	10	2	1	65536	0.038146973
10000	40	2	1	65536	0.003051758
100000	40	2	1	65536	0.030517578
200000	40	2	1	65536	0.061035156
500000	40	2	1	65536	0.152587891

本日(7/8)のBIND 9へのパッチ

- リゾルバ(キャッシュサーバ)の問合せポートが固定になっているのを、クエリ毎に乱数を使って変更する
  - 純粋に確率を下げるものであり、DNSプロトコルの脆弱性そのものを対処するものでは無い

さて、その効果は?

Port番号可変(60000種類)で計算

R	W(ms)	NS	Port	ID	確率
10000	10	2	60000	65536	0.0000000127
100000	10	2	60000	65536	0.0000001272
200000	10	2	60000	65536	0.0000002543
500000	10	2	60000	65536	0.0000006358
10000	40	2	60000	65536	0.0000000509
100000	40	2	60000	65536	0.0000005086
200000	40	2	60000	65536	0.0000010173
500000	40	2	60000	65536	0.0000025431