「Visual DNS Attack」を用いた DNSキャッシュポイズニングの仕組み

今井研究室　後藤祥仁

1

目次

- 用語解説
  - DNS
  - DNSキャッシュポイズニング
- デモについて

2

DNS(Domain Name System)

- ドメイン名とIPアドレスを相互変換するサービス(今回はドメイン名→IPアドレスについて言及する)
  - IPアドレス…TCP/IPネットワークに接続されたコンピュータや通信機器の一台ごとに割り当てられた識別番号
  - 例)　www.google.com⇔172.217.31.164
- 権威サーバ(コンテンツサーバ)とDNSキャッシュサーバを使ってDNSサービスを実現している
  - 権威サーバ…ドメイン情報を管理するサーバ
  - DNSキャッシュサーバ…クライアントユーザに代わって権威サーバに問い合わせを行うDNSサーバ
    - 一毎回権威サーバに問い合わせると効率が下がるため
    - キャッシュサーバに一時的に保存する必要がある

3

DNSキャッシュポイズニング

- キャッシュサーバが権威サーバに問い合わせし、権威サーバから返答が来る前に偽の情報をキャッシュサーバに送り込む攻撃
- 攻撃されると、同じドメイン名でも違うサイト(サーバ)に誘導されてしまう

4

例えば…

ドメイン名	IPアドレス
www.google.com	172.217.31.164
www.yahoo.co.jp	182.22.25.124

ドメイン名	IPアドレス
www.google.com	172.217.31.164
www.yahoo.co.jp	172.217.31.164

5

とりあえず覚えてほしいこと

- DNS
  - ドメイン名のIPアドレスを教えてくれる
- DNSキャッシュポイズニング
  - 攻撃が成功すると、同じURLでも違うサイトに飛ばされる

6

デモについて

- デモで行うこと
  - DNSの動き
  - DNSキャッシュポイズニングの動き
- ボタンを押すことでそれぞれ実行できる

7

8

デモに移ります

9