Infoblox
CONTROL YOUR NETWORK

DNS: Defense and Attack

Paul Ebersman
pebersman@infoblox.com, @paul_ipv6
RIPE66, Dublin, 13-17 May 2013

© 2013 Infoblox Inc. All Rights Reserved.

DNS is you

© 2013 Infoblox Inc. All Rights Reserved.

DNS is who you are on the internet

- **If your DNS zone isn't available:**
  - No email
  - No website
  - No internet services…

© 2013 Infoblox Inc. All Rights Reserved.

Robust DNS is worth money

Even managers/executives now see value of robust DNS

© 2013 Infoblox Inc. All Rights Reserved.

DNS Hijacking

© 2013 Infoblox Inc. All Rights Reserved.

- **Registry/Registrar security**
- **Who owns nameservers**
- **Who can update zone data and how**

© 2013 Infoblox Inc. All Rights Reserved.

Attacking your cache

© 2013 Infoblox Inc. All Rights Reserved.

Cache Poisoning

- **What is it?**
  - Inducing a name server to cache bogus records
- **Made possible by**
  - Flaws in name server implementations
  - Short DNS message IDs (only 16 bits, or 0-65535)
- **Made easier on**
  - Open recursive name servers
- **Consequence**
  - Man in the middle attacks

© 2013 Infoblox Inc. All Rights Reserved.

How Random - Not!

- **Amit Klein of Trusteer found that flaws in most versions of BIND's message ID generator (PRNG) don't use sufficiently random message IDs**
  - If the current message ID is even, the next one is one of only 10 possible values
  - Also possible, with 13-15 queries, to reproduce the state of the PRNG entirely, and guess all successive message IDs

© 2013 Infoblox Inc. All Rights Reserved.

Birthday Attacks

- **Barring a man in the middle or a vulnerability, a hacker must guess the message ID in use**
  - Isn't that hard?
  - As it turns out, not that hard
- **Brute-force guessing is a birthday attack:**
  - 365 (or 366) possible birthdays, 65536 possible message IDs
  - Chances of two people chosen at random having different birthdays:

$$\frac{364}{365} \approx 99.7\%$$

  - Chances of n people (n > 1) chosen at random all having different birthdays:

$$\bar{p}(n) = \frac{364}{365} \times \frac{363}{365} \times \ldots \times \frac{366 - n}{365} \qquad p(n) = \left(1 - \bar{p}(n)\right)$$

© 2013 Infoblox Inc. All Rights Reserved.

Birthday Attacks (continued)

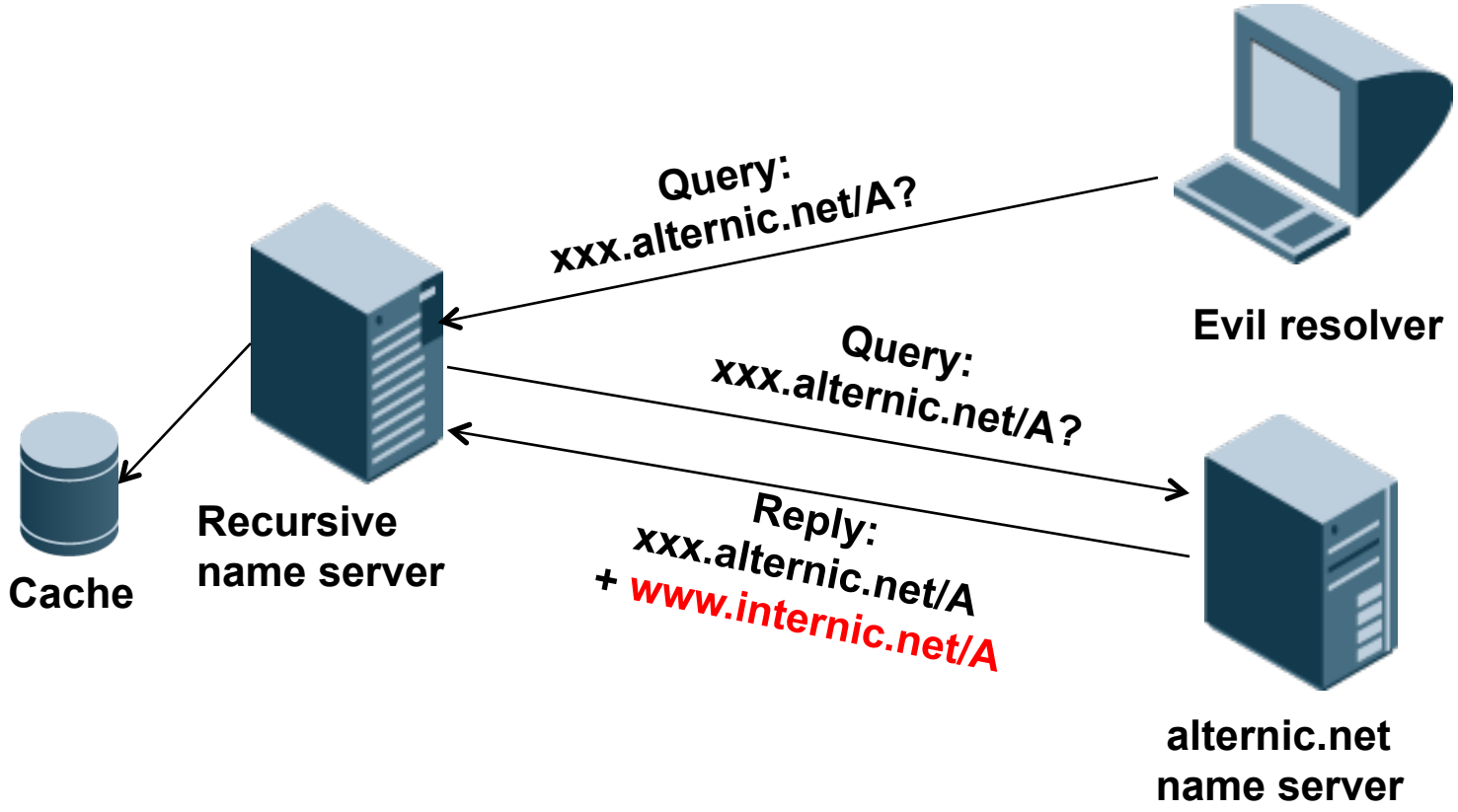
People	Chances of two or more people having the same birthday
10	12%
20	41%
23	50.7%
30	70%
50	97%
100	99.99996%

Number of reply messages	Chances of guessing the right message ID
200	~20%
300	~40%
500	~80%
600	~90%

© 2013 Infoblox Inc. All Rights Reserved.

The Kashpureff Attack

- **Eugene Kashpureff's cache poisoning attack used a flaw in BIND's additional data processing**

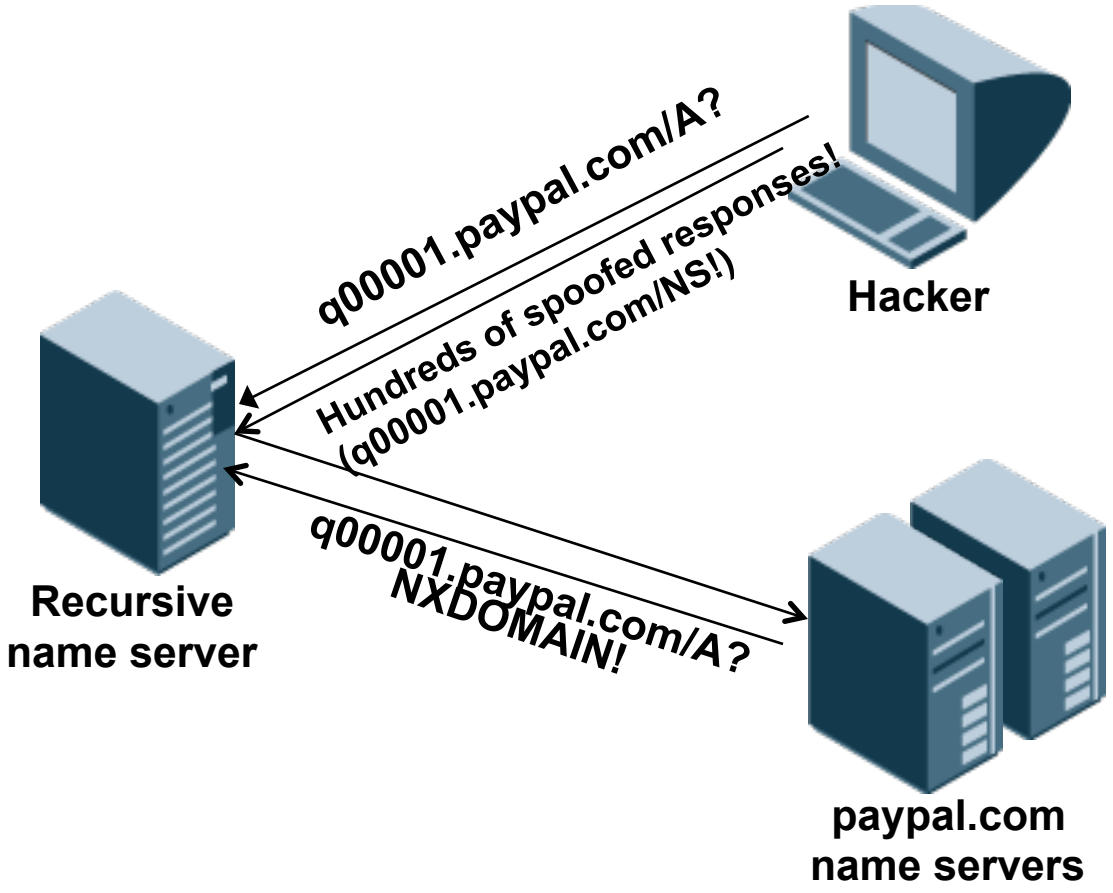


Infoblox

© 2013 Infoblox Inc. All Rights Reserved.

The Kaminsky Vulnerability

- **How do you get that many guesses at the right message ID?**



© 2013 Infoblox Inc. All Rights Reserved.

The Kaminsky Vulnerability (continued)

- **How does a response about q00001.paypal.com poison www.paypal.com's A record?**
- **Response:**

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61718
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
ADDITIONAL: 1

;;; QUESTION SECTION:
;q00001.paypal.com.          IN      A
;;; AUTHORITY SECTION
q00001.paypal.com.          86400   IN      NS      www.paypal.com.
;;; ADDITIONAL SECTION
www.paypal.com.             86400   IN      A       10.0.0.1
```


© 2013 Infoblox Inc. All Rights Reserved.

Saved by the Second Law of Thermodynamics

- **To make it more difficult for a hacker to spoof a response, we use a random query port**
  - In addition to a random message ID
  - If we use 8K or 16K source ports, we increase entropy by 13 or 14 bits
  - This increases the average time it would take to spoof a response substantially
- **However, this is not a complete solution**
  - Spoofing is harder, but still possible
  - Evgeniy Polyakov demonstrated that he could successfully spoof a patched BIND name server over high-speed LAN in about 10 hours

© 2013 Infoblox Inc. All Rights Reserved.

Defending your cache

© 2013 Infoblox Inc. All Rights Reserved.

Defenses

- More randomness in DNS msg IDs, source ports, etc.
- Better checks on glue
- DNSSEC

© 2013 Infoblox Inc. All Rights Reserved.

Overwhelming your authoritative servers

© 2013 Infoblox Inc. All Rights Reserved.

Sheer volume

- **Botnet attacks in 10s of Gb's**

© 2013 Infoblox Inc. All Rights Reserved.

High Yield Results

- **Asking for DNSSEC records**
- **Using NSEC3 against you**

© 2013 Infoblox Inc. All Rights Reserved.

How to defend your servers

© 2013 Infoblox Inc. All Rights Reserved.

Harden your server

- Perimeter ACLs
- Higher capacity servers
- Clusters or load balanced servers

© 2013 Infoblox Inc. All Rights Reserved.

Spread yourself out

- Fatter internet pipes
- More authoritative servers (up to a point)
- Anycast
- HA

© 2013 Infoblox Inc. All Rights Reserved.

DNS use by the bad guys

© 2013 Infoblox Inc. All Rights Reserved.

DNS use by bad guys

- **Command and control**
- **DNS Amplification**
- **Fastflux**
  - single flux
  - double flux
- **Storm, Conficker, etc.**

© 2013 Infoblox Inc. All Rights Reserved.

Protecting your users via DNS

© 2013 Infoblox Inc. All Rights Reserved.

Dealing with malware

- **Prevent infections (antivirus)**
- **Block at the perimeter (NGFW, IDS)**
- **Block at the client (DNS)**

© 2013 Infoblox Inc. All Rights Reserved.

RPZ DNS

- Uses a reputation feed(s) (ala spam)
- Can be IP or DNS based ID
- Fast updates via AXFR/IXFR
- Protects infected clients, helps ID them
- Can isolate infected clients to walled garden

© 2013 Infoblox Inc. All Rights Reserved.