DNSSEC:

WHAT IT MEANS FOR DNS SECURITY AND YOUR NETWORK

Agenda

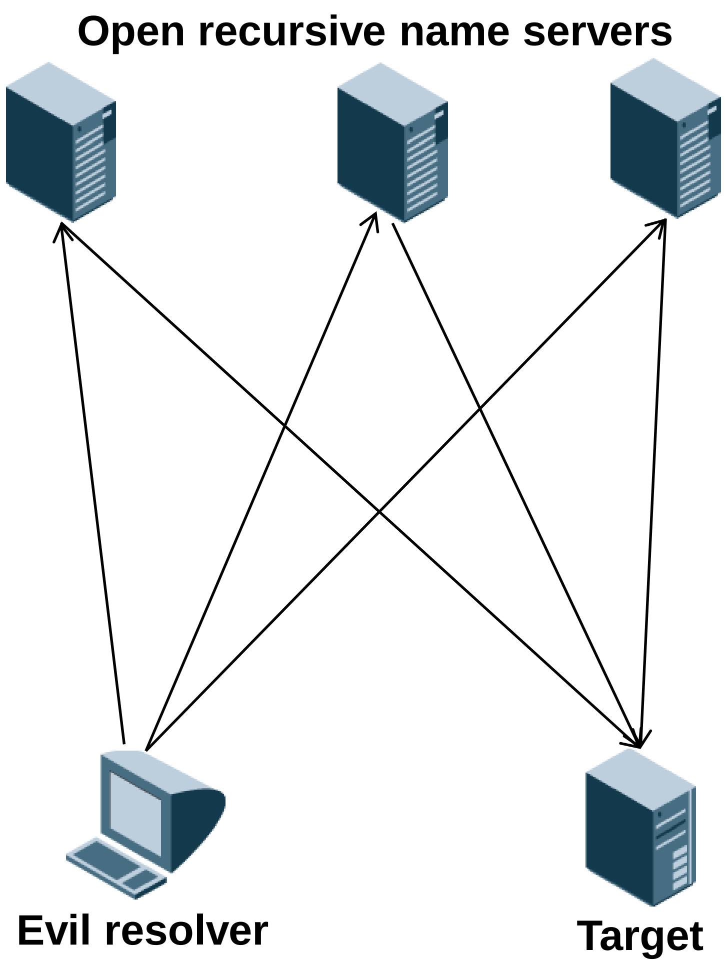
- Threats to DNS
- DNSSEC overview/history
- DNSSEC today
- DNSSEC in more detail
- DNSSEC best practices/recommendations
  - Architectural
  - Operational
- References

TOP 4 SECURITY THREATS TO DNS

1. Distributed Denial of Service (DDoS)
2. Malicious open recursive name servers
3. Web Proxy Auto Discovery protocol
4. Cache poisoning

DISTRIBUTED DENIAL OF SERVICE

- DDoS: Brute force attack
- Name servers are high-profile targets
- Queries spoofed from target's address

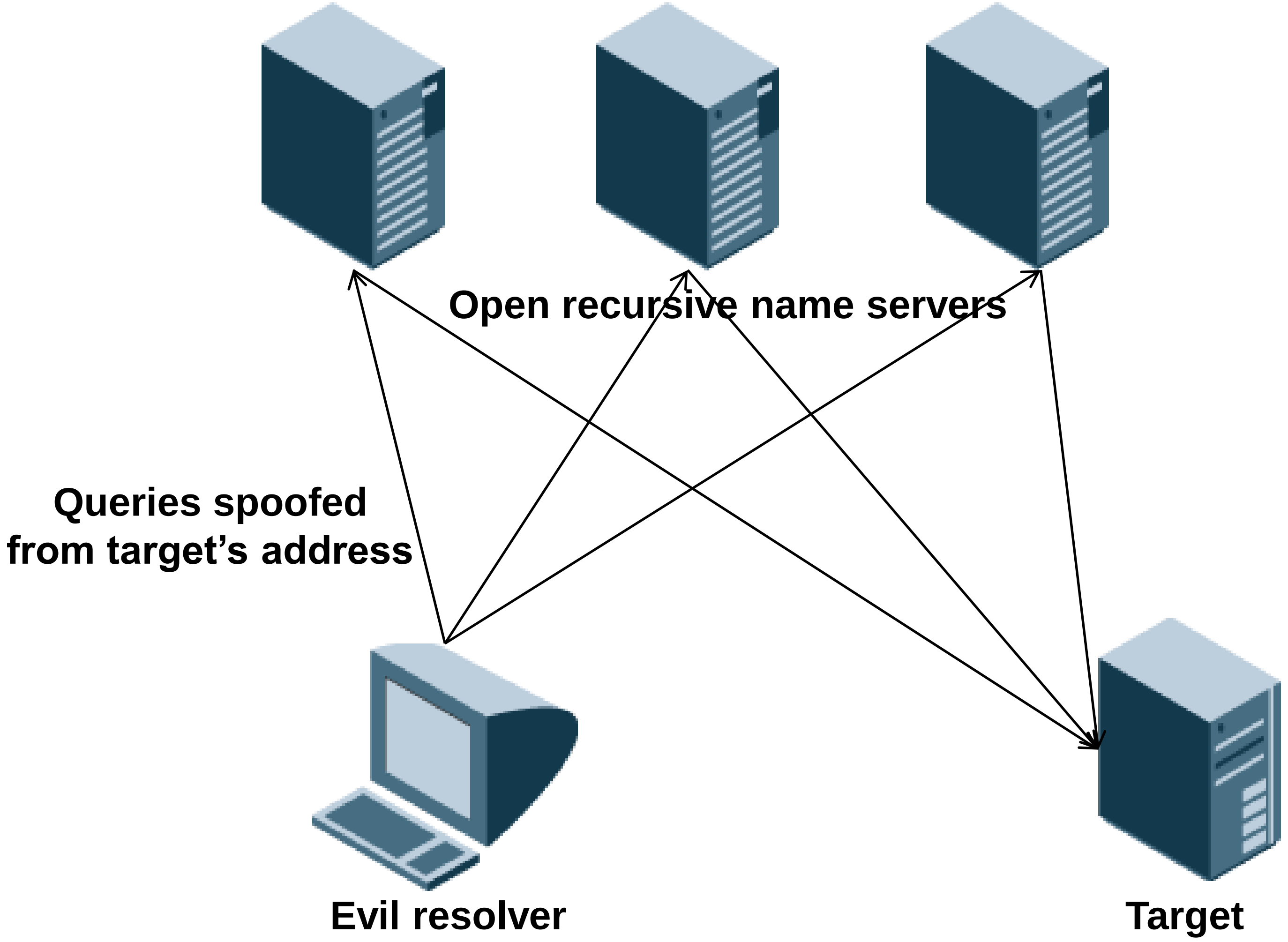


Queries spoofed from target's address

Distributed Denial of Service

- What is it?
  - Attacks that use many, cooperating Internet hosts to swamp a target
- Name servers are a high-profile target for DDoS attacks
  - They're critical
  - Everyone needs them
  - You can't hide them (authoritative name servers, anyway)
- Ironically, some of the most popular accomplices to enlist in a DDoS attack are
  - Name servers
    - In particular, open recursive name servers
- What's it matter?
  - You could be attacked
  - You could become an accomplice in an attack through inaction

DNS Amplification



AMPLIFICATION

- Simple amplification: . (root) NS RRs:
  - *dig ns* . (heck, just *dig* works, too)
  - Query: 45 bytes, reply: 300 bytes
  - Amplification: ~7x
- Amplification with DNSSEC: signed.infoblox.com's DNSKEY RRs
  - *dig dnskeysec.infoblox.com. +dnssec*
  - Query: 76 bytes, reply: 2894 bytes
  - Amplification: ~38x!
- A little more math:
  - 1000 qpsx 2894 bytes/open recursor = 2.9 MBps/open recursor = 23.2 Mbps
  - 1000 open recursors = 23 Gbps

AN AMPLIFIED RESPONSE

```
[wit:~] cricket% dig +dnssecsigned.infoblox.com. dnskey

; <<>>DiG 9.4.1-P1 <<>> +dnssecsigned.infoblox.com. dnskey
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46654
;; flags: qraa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;signed.infoblox.com.                    IN          DNSKEY

;; ANSWER SECTION:
signed.infoblox.com. 3600      IN        DNSKEY      257 3 5 AwEAAZvf8cRF9fIQim+x3vFqbKMq2uBAI2g79UApMupGNnpMncHKbzYg
C4mn7n8GZU6QNXyWaep7g2wXQJatV4xS8JKUxXMm0S3+0mXVKPgU4otL JTSdPt+RQPxEtWLcmtT0v648OTypu2VNx7NhphBt91iQxwsI960bXHTG
mgiIQjBCy9wI6SD3Ay4dsZauDO/y/JJowIN+fbKnwXW7FM1bIaz/Iubg d/JKC7ofbI4jqSzrLtyIMDWYHV8xPVI6hsIPUda4ZSxXVAN4DZiIKSN6
YcEfOaRZ1aG+g1QtsWpduspM1zXTB2srVvZkLf1TCq1g7g48Hn742QWu sxaafZT+x5kxOEKhZ4Zt/6mUue3EOgKDGWu+5tbwc+VdjDW95hfPcvDn
1UD2MHq4dD3dUgWngy5paXM1PTsy8geXVQUcA5iJ5dFAjsL0oduXKs8D RneMDIUYOMInbzHO3gv0v+QBRz6XPsEUcifq8kwzwO1LVg3HMSIiOKYq
Ix9E8KWt0QOCr1lSsceNoxIIi1f6sckFzNTZKpqfEa4zobtSBkdeokHv aMIAxaTuW1lqT7gVUvVJ8k7EnFaIh6yHJ8ObfFyrKHwspkAQg19NFzi2
kpM8uGGkPsVb4ijJYK7kuyRenLWUR0ySuiMd44xj9W2TABwT7MMtZ1n6 xqZC+kT9+UPP79+9
signed.infoblox.com. 3600      IN        DNSKEY      256 3 5 AwEAAecjDQ+J+v8pKPxOh1Q34O5pjEXFQbQyaYIv3sh3AEaC5IREv+Ij
a6dZP15NbuMOEXLIU1WuTiEqvdh1wn6Py4vNgh1hZn4zHRcUFs/HW1tH igmLeXx9auur+N9j3kdezpdjtIK5dRcrTg3L0D8NIMjGck/4brscPVat
knEYIPtxb5v+UX+8JWdEcB2/TqKj2BWQogsGmDwf1zVeAjE2V0BV5VzM 4CF2oHpGitRSV6KI+fL3Zm7P/qD7gfkjVe7b6WTh9aqz/Y5a8P61DNPX
1d+BaN8ehpEeVmCQj3EGfZ/f1WMgUiWGIlj/SirX8HniVmUZ/IMmoJhd cmgkcAXDJDLsakdy4XehZPiEj2ClAwTnVgNkUDkYN2tm2io+IHAq7kq8
xWijxnJ463+OUxQTQg0+0m2ar3s7LPxbdpUrk+0er2emG4vBMiLw6cm4 kVw4g6EFB9CeybQzwK8ZVIfPvQfI/ON1yvVU8sAHw78yYXPE1MIVYUB3
jKqoa3NPJXDyaG9sGKBJvWJMS0PpH5OxOEvnRNC2SCIWRLHhvnjJZypQ hyunDYicKC2nI3Ia3t3E9xIFcIAAOWSWkMIPhoIYXcJuKSjxatx/K95Y
m0QnJvx8AXhrcD0iZpY66+4owJkoobcDGnnnsW636DlCcBD76zjd5vWs ShIk5/ak0MbLcCIf
signed.infoblox.com. 3600      IN        RRSIG       DNSKEY 5 3 3600 20080410205926 20080311205926 16366 signed.infoblox.com.
hwIdf2sPFwO9mIXlNhPakpfPh4lSoZkzyKO9dKIj4XjgH7Qj+N0Z94Kl Q5I8+tTgctge+n1W7/I0r62OhehotjS1PZyzidsn9cVLdBzypnoe6FJQ Q728xl5059arIlKx5aNXP7s9wDnBcifo9hRqiC8u+Ib/AfI4CHa2a4X4
0avwS9kQKoskkJJ5gqmi9PMwsZWtvXK9rTAt8Gw1vZb2bbAekeS3Zhh/ UhCPaITlm5NGtbjhXKS4fzDPCFvthya0dhp9e5ZnUBvBGYrnvi5qVS1c
LgiTDPZ5+0KNYFiwrpEdQ9IFfwGJvzYQY5ZaAtI8j4b/dYOcIgI9LqhR bqzKasBdZon0G0LI3wk0BJ8UCQ2giFraI2jAo7hG5GXzGDaTEwjHtKs+
oUpI7ZWUCInicgx5iQS9KZ1iyxo14EwCAeqstheYAYLbCIdF7xrNYa0H tslqDRSvurbtTQLqGpw6eWbGJshAv8xaU3GG5sLExyWWV5fiDzvEahiK
eYnsM2dLs7VtwEWcC/uJMwTQ7jIC4m68JVBUMz8guvvIH1aLvo0uyzSx pkLY8UTr0HQZ9/08wQj/9T9yUc/0iw4jk7b8/zv2vRrfvIAvG+JyEzUB
Gy4e/DE9N+NNOnRSkOnIuIAMkVhKmvG5QN9Yx/ep1tj/SbyYuTIdasQW Mqk33UjnDmw=
signed.infoblox.com. 3600      IN        RRSIG       DNSKEY 5 3 3600 20080410205926 20080311205926 43077 signed.infoblox.com.
4xHNTjo4J0ykRMAx0IfEbjhjcIBIkFxfKIyI2TFYOmJx17LeA6m8TUyL uUyFXb3BWSaFgCEjDOLChoSfZ1Ak24BG49djP9j0OJ5K9Zvj64GefTG2
NID+WYW8LRIrzmpYkW4nvZRDX672KfsjMyDWAkwmh4lNjqXsoUUoRReS qvZ+OfINpFKCVdTWz1xEasXc2J2yQgONLdALcEVCTB/ppUxr/yZAySQY
IIyMnayBzYPcG9C1as5MILHKuwQIdz50q2IBcPmXGqwRLW9gHU1gHNBU BWbsjBRSnxU6TvP9z00w3HWhuXHTGW+gQiiJVhyTJeEFrOSocxrnL7M5
AGG5D3mzaBZDqcLFaxjkvGG+LfM9xgK441xaFsCmIc0ZaQEY/ffuninP vvMCpJOuNQsT7ZB+XFbtN5Go0x5ybtnqIbkdOzp6N8WzBz83kdX4WVes
s4w9qfDQF/uEV5Yg2bKbS54osja9Eo/CpbIX1cI6yXDqrD5Ak4veTaFZ cVMjqBC/+t1q5g9kSZwwmOu5EOazsn99b5rS/MTf+q8ByrWR99B0scb9
987bIT0CLXhHirA9+NJ7Wk4hOpdrTEq33uCmZVsJocZ4HVLyh3W4n2Ao RQ+1I/GWFf/0pQeg6iI+QsbGOyeksrhY6JGH518k79DN6OyVaQIwbbcg 8IrZ2Sd7fwM=

;; AUTHORITY SECTION:
signed.infoblox.com. 3600      IN        NS          bigmo.nxdomain.com.
signed.infoblox.com. 3600      IN        RRSIG       NS 5 3 3600 20080410205926 20080311205926 43077 signed.infoblox.com.
I+1eoP1MLxSYY+NySYmARuc9/n5y3XZNI8AdrG2xQBVegEDmKR4ojGs9 yYFxZxjYzAxDYB64oe/iCZJ810vOaXvJjxtMTYdxXiRof9KbNA4oyVST
4r33bHhpemwPjUcSquHIr/xLu+SIDJrrRzL90KUZX1wNNX+gNYFqgDs2 TRUjipgAB43hHtzHzaaMaSsxXhHSIxPn1vPeIq/2csorzFemYDL7/woD
e8ZmImsHIJv1bs4sCre1rAY+3HIsYH7zIRyLCRJDAjg7H+LX9o5PFDhQ OFXkom1OdqQhkGXgcLLRJmp2IqMsKxWc2uVdi8NnVYLzshwY7oVXtVdi
PKX+M4Bn01vMN7E/QrOA/4Ch7krQwSEgD8HN1hWp1sWuJH6Zc7JKbkDn axXgoUbqRIEcM5vqePPbgjiWY8s8gCfFpSSX/wsIivwM2KnVRR0WmpYI
e9WxO1948geLcENsIyDetVdBv/IqdQmfvmLRLosiLpWWeiWkbqXA/odh sAEoVW/x4xIIYyM8VroTPQLTZLsuNvrYsWzndiMzEaHmRSqvgoP6drZG
FzIv2LvILd2aFanjoX3xqo86qsPHK941Y/+FmBI2mKIVyCzaPi94P0zW z9BtLqMzJHCv3HW+kqVo9sPqd8hJ37vPsFWWZeARz1b/O80OhBgpVD8I u6SDfd0rBog=

;; ADDITIONAL SECTION:
bigmo.nxdomain.com.            86400     IN          A           192.168.0.1

;; Query time: 16 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sat Apr 12 16:55:06 2008
;; MSG SIZE  rcvd: 2846
```

MALICIOUS OPEN RECURSIVE NAME SERVERS

- About 68k globally
- Most return addresses for open web proxies in Russia and China
- Malware reconfigures Windows resolvers to use these name servers, redirecting traffic through these proxies

WEB PROXY AUTO DISCOVERY PROTOCOL

WPAD: A protocol that enables a web browser to automatically discover proxy servers

- Most modern web browsers (IE, Firefox, etc.) support WPAD
- If your search list contains domain names outside your control, the *wpad* lookup may return something unexpected, like *wpad.com*, *wpad.net* or *wpad.org*

CACHE POISONING

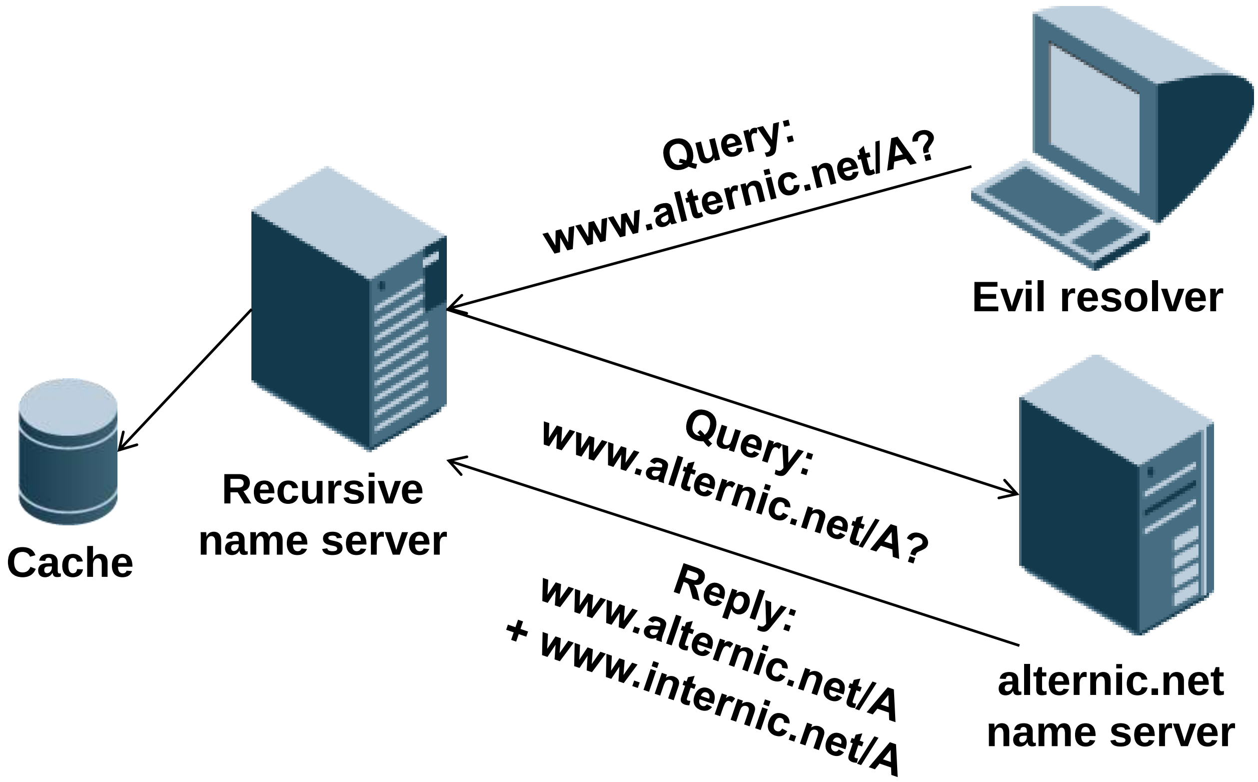
- Definition: Inducing a name server to cache bogus records
- Can re-direct unknowing users to malicious sites
- Compromises email, eCommerce, Web traffic, SaaS, … Everything!
- Made possible by flaws in name server implementations, limitations in DNS itself
- Easier on open recursive name servers

Cache Poisoning

- What is it?
  - Inducing a name server to cache bogus records
- Made possible by
  - Flawed name server implementations
  - Short DNS message IDs (only 16 bits, or 0-65535)
- What's it matter?
  - A hacker can induce your name server into believing something false
    - By caching bogus records
  - Your users might connect to the wrong web site and reveal sensitive data (passwords, account numbers) there
    - The "wrong" web site might look just like the real web site
  - Your users email might go to the wrong destination
    - Where it might just sit, or it might be copied or modified and then sent on

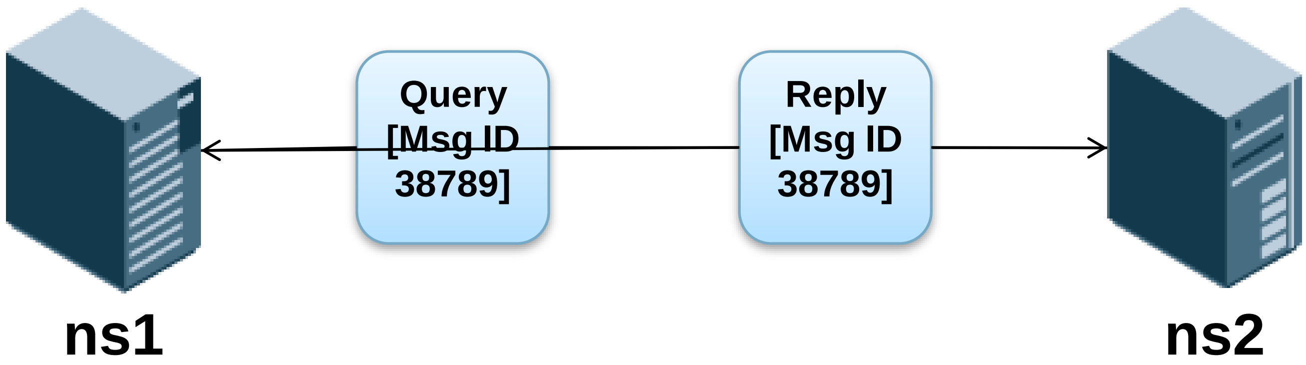
CACHE POISONING ILLUSTRATED

- This 1997 attack used a flaw in BIND's additional data processing
- Here's how the attack worked:



DNS MESSAGE IDS

- A DNS axiom:
  - The message ID in a reply must match the message ID in the query



Birthday (Brute Force) 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: 99.7%
  - Chances of a “birthday collision”:

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%

Birthday (Brute Force) Attacks (cont.)

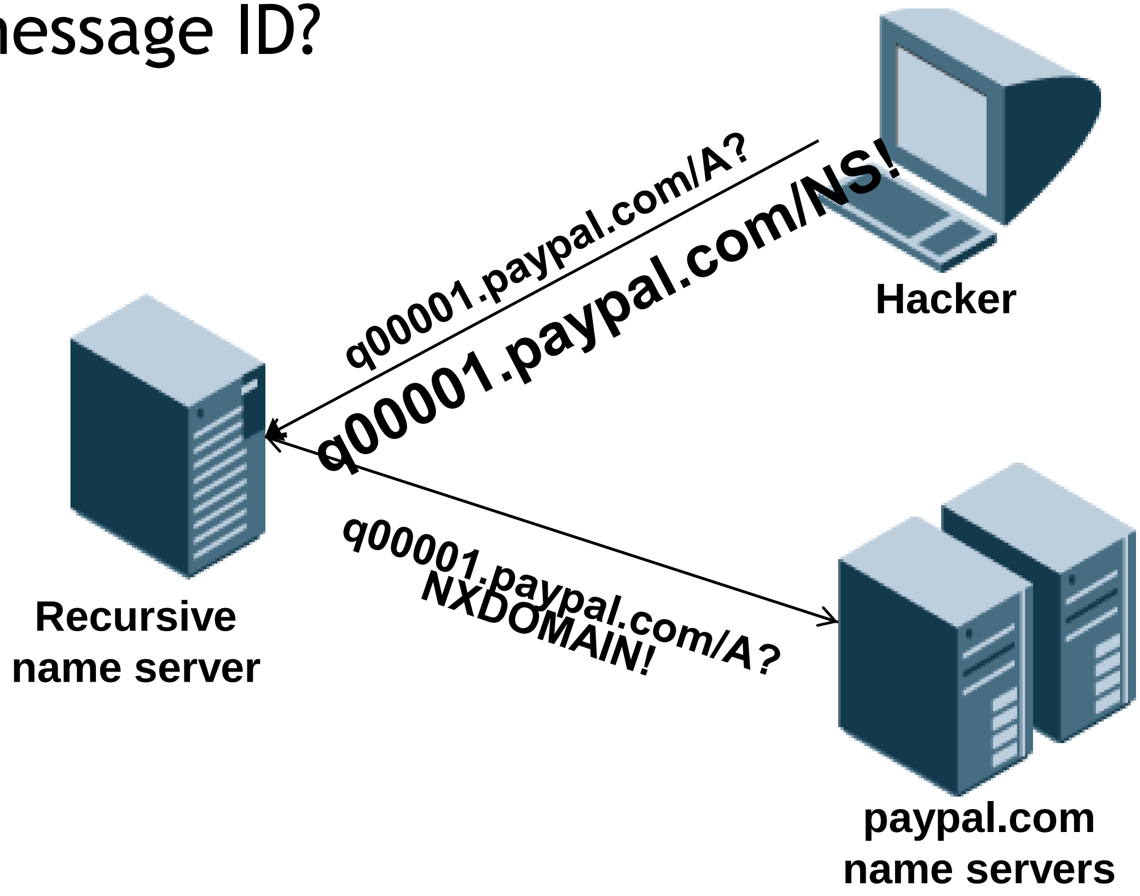
Number of reply messages	Chances of guessing the right message ID
200	~20%
300	~40%
500	~80%
600	~90%

IT GETS WORSE

- Security researcher Amit Klein of Trusteer found that flaws in BIND's message ID generator (PRNG) mean that most versions of BIND 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

THE KAMINSKY VULNERABILITY

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



THE KAMINSKY VULNERABILITY (CONT.)

- So what if the hacker's referral response wins?
- 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
```

THE KAMINSKY VULNERABILITY WAS A GAME CHANGER

Made clear how vulnerable the global DNS system really is

- Mobilized many (but not all) organizations to upgrade their DNS servers with patched DNS code
- The patch is a stop-gap – doesn't "fix" the vulnerability, just makes it harder / more expensive / more obvious to exploit
- A real fix requires adding security features into the DNS protocol – plus a number of operational and administrative processes
- Motivated many to advocate for DNSSEC adoption

DNSSEC OVERVIEW HISTORY

- Brief description of what DNSSEC does
- What DNSSEC doesn't do
- Historical background (development, adoption)
- Impediments to DNSSEC adoption

WHAT IS DNSSEC?

- DNS Security Extensions
- Uses public key cryptography to verify the authenticity of DNS zone data (records)

  - DNSSEC zone data is digitally signed using a *private* key for that zone

  - A DNS server receiving DNSSEC signed zone data can verify the origin and integrity of the data by checking the signature using the *public* key for that zone

DNSSEC IS IMPORTANT – BUT NOT A COMPLETE SOLUTION FOR DNS SECURITY

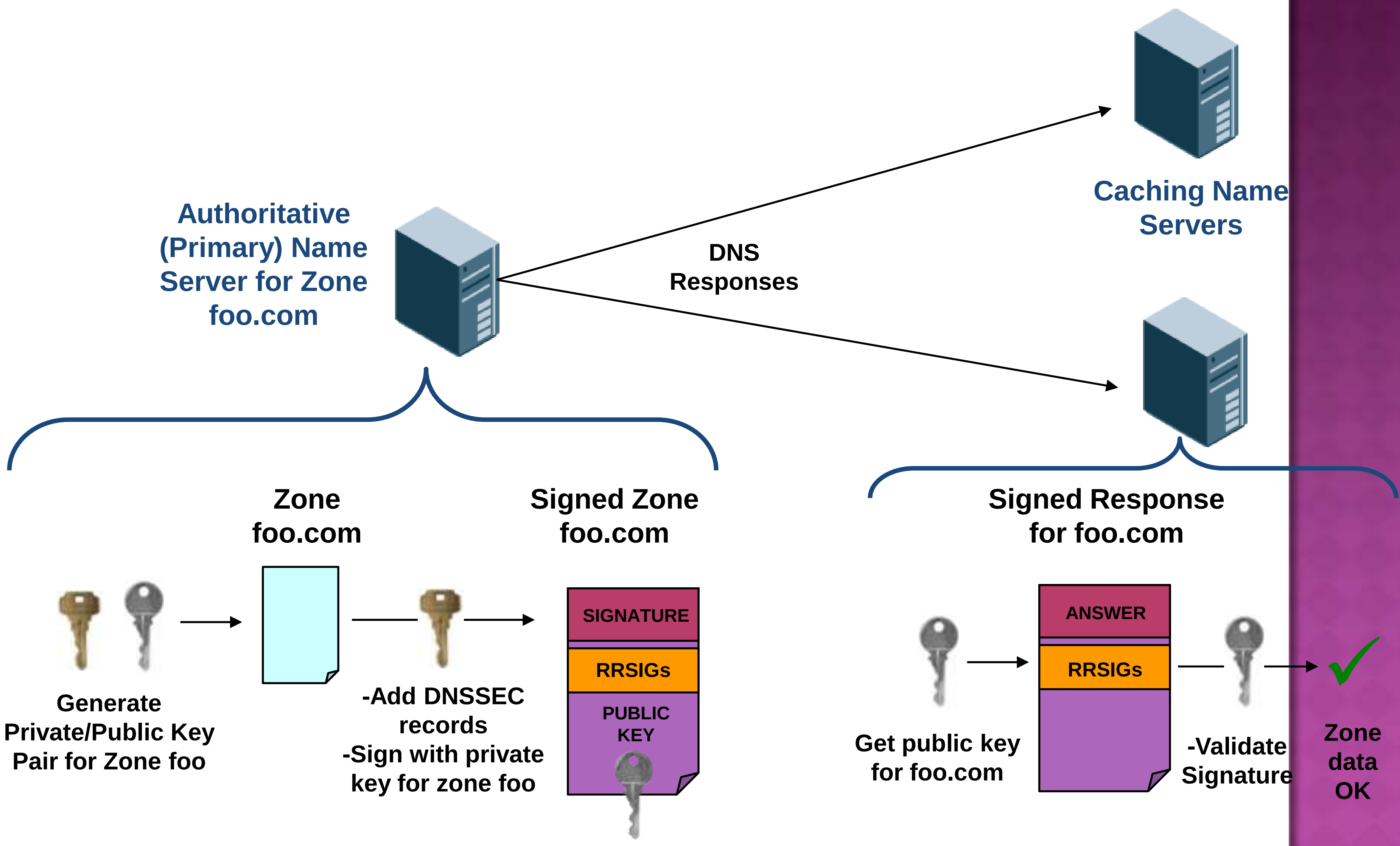
- DNSSEC doesn’t:
  - Protect against host threats (DDoS, buffer overruns in code, etc.)
  - Keep DNS data private
  - Insure correctness of DNS data

- The role of DNSSEC: Establish the legitimacy of data retrieved from the DNS
  - Protects end users from being redirected to malicious sites
  - Allows *any* data stored in the DNS to be validated as trustworthy

DNSSEC is Critical – For Securing Technologies Beyond Just DNS

- Most Internet technologies depend on untrusted data
  - E-Mail
  - Web
- Most Internet technologies depend on untrusted data, *even when they really should be authenticating it*
  - "Forgot My Password" systems provide login credentials over unencrypted email to a DNS-controlled destination
- Authentication flaws are tearing down the Internet
  - 60% of breakins that Verizon Business saw in 2008 were auth-related
- DNSSEC allows content to be authenticated as coming from a trusted source, *even when that source is a totally separate organization*
  - Just like DNS allows email to be delivered, *even when the destination is a totally different company*

DNSSEC IN PRACTICE



DNSSEC CHALLENGES

- DNSSEC operations are fairly straightforward, if a bit cumbersome *with present implementations*
  - Generating the public/private key pair, signing and verifying zone signatures
  - Must be done every time a zone is created or modified
- Big challenge: Securely distributing each zone's *public* key to the DNS servers that may need it
  - The best way to distribute keys: DNS!!!
  - But – a chicken & egg problem
- For DNSSEC to scale, automation and a "chain of trust" are required

WHAT HAS LIMITED DNSSEC ADOPTION?

- One major rewrite
- One substantial tweak to the rewrite (NSEC3) to deal with certain concerns
- Lack of understanding and expertise among network administrators
- Clumsy administrative tools
- Overhead (computational, memory, network traffic)
- Lack of signed top-level zones (essential to establish "chains of trust")
- Lack of a concrete threat (until now)

DNSSEC TODAY

- Adoption initially slow, but currently accelerating
- In parallel, US Federal Government moving towards deployment
- Several Top Level Domains currently signed
- Major gTLD's have issued statements about deployment plans and goals (com/net)
- .ORG is signed
- DNSSEC signed root zone has been available since 15 July 2010

DNSSEC IN THE US FEDERAL GOVERNMENT

- Office of Management and Budget (OMB) Memo 08-23 set deadlines for zone signing (externally facing zone only)
- Federal Information Security Management Act (FISMA) has complementary security controls for internal DNS as well as validation of DNSSEC responses
- The .gov key is available via the Interim Trust Anchor Repository (ITAR) *https://itar.iana.org/*
  - Has the public keys for all TLDs

DNSSEC IN US FEDERAL GOV: LESSONS LEARNED

- Registrar-registrant interaction requires a lot of planning and testing
- DNSSEC requires communication between network admins and IT security staff
- DNSSEC operations must be automated to be manageable – You'll either need to build or buy tools

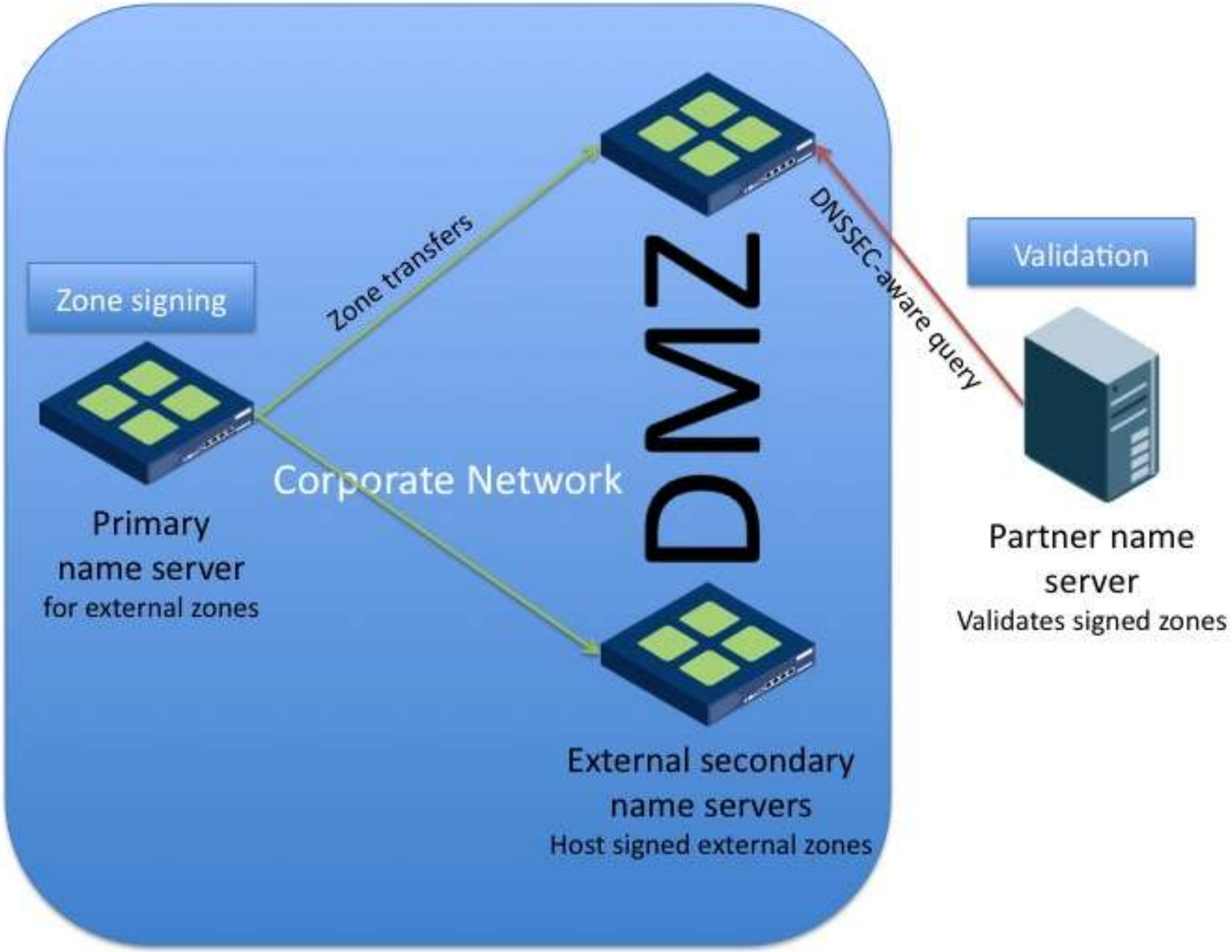
BASICS OF DNSSEC DEPLOYMENT BASED ON ROLE

- Authoritative (serving data)
  - Primary concerns:
    - Crypto key management
    - Content management
- Recursive (caching) Service
  - Primary concerns
    - Maintaining list of current trust anchors (until the root is signed)
    - Maintaining current level of service in the face of new cryptographic operations

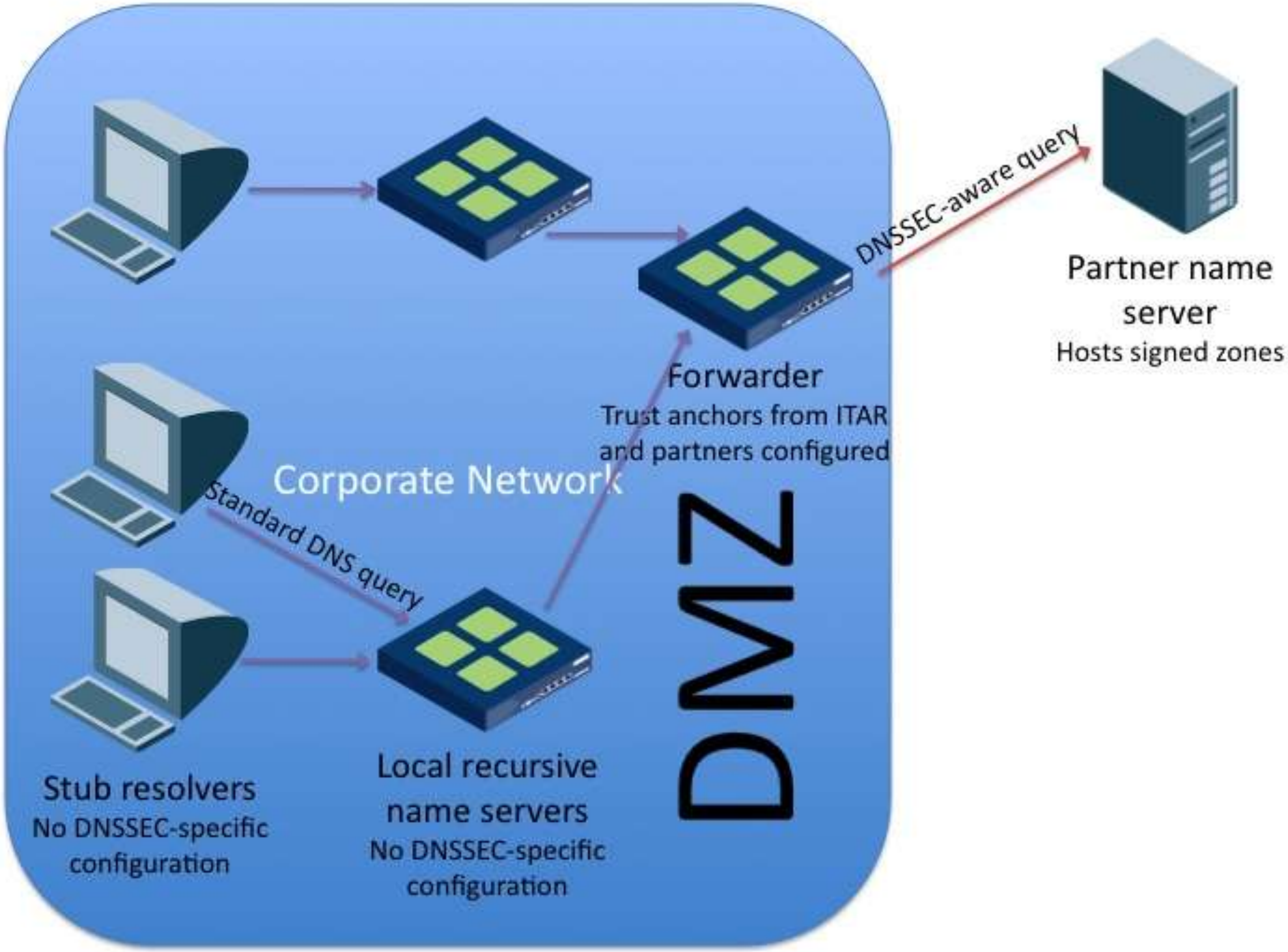
DNSSEC BEST PRACTICES / RECOMMENDATIONS

- Architectural Best Practices
- Operational Best Practices

ARCHITECTURAL BEST PRACTICES: AUTHORITY



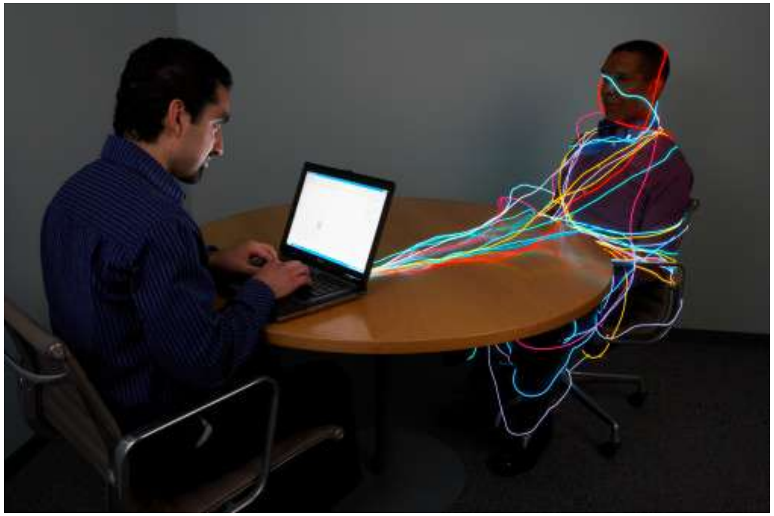
ARCHITECTURAL BEST PRACTICES: RECURSION



DNSSEC Operational Best Practices

- Establish a security policy for DNSSEC
  - Which zones need to be signed
  - Which servers will serve DNSSEC zones
  - When to expect signatures
  - Client-side policy (what happens if signature fails, etc.)
  - Key generation/management procedures
  - Crypto standards (key length, expiration, etc.)
- Design the DNSSEC implementation (best practices)
- Assess infrastructure and upgrade / configure equipment to perform DNSSEC as needed
- Recommendations:
  - Start with a pilot/trial, and test
    - Shadow existing operations
  - Sign authoritative production zones first, test, then configure validation on clients

DNSSEC OPERATIONAL BEST PRACTICES - RESOURCES



- From the IETF: RFC 4641 "DNSSEC Operational Practices"
  - Currently under revision in the IETF
- From NIST: Special Publication 800-81r1 "Secure Domain Name System (DNS) Deployment Guide"
- From various sources: Training materials
  - Most available via *http://www.dnssec.net/*

SOME TIMING RECOMMENDATIONS

- Start preparing now
- Blocking factors that have been suppressing adoption for years are finally falling
- This will ultimately represent the canonical defense against "Kaminsky" attacks
- Applications will be coming that will demand DNSSEC support
  - We can't fix everything, but if we can make a serious dent in the 60% of attacks that are traced back to authentication flaws, we'll have done good.

SUMMARY

- New DNS vulnerabilities (e.g. Kaminsky) expose major flaws in DNS security
- DNSSEC is the best available solution to address DNS flaws
- Momentum is increasing
  - Signed TLDs, plans to sign the root zone, etc.
  - OMB mandate
  - Vendor support
- Implementing DNSSEC starts with defining policies & assessing impact on organization & infrastructure
- Many challenges can be mitigated by implementing tools that automate DNSSEC

REFERENCES

For More Info

For additional updates on DNSSEC go to:

http://www.dnssec.net/

http://www.cricketondns.com

Information about DNSSEC for the Root Zone:

http://www.root-dnssec.org

DNS Security Center:

http://www.infoblox.com/library/dns-security.cfm