DNS Response Modification

David Piscitello
Senior Security Technologist
ICANN

Intended web experience

- Type a URL: http://www.example.com/index.htm
- Browser asks DNS to find IP address of this host
- If DNS finds the IP address then
  - It passes this IP address to browser
  - Browser connects to the site
  - If page exists, browser downloads page
  - Else browser displays “page not found”
- Else if host does not exist
  - DNS returns a “name error” to browser
  - Browser displays an error “Server not found” (or similar)

Response Modification alters this experience

- Type a URL: http://www.example.com/index.htm
- Browser asks DNS to find IP address of this host
- If DNS finds the IP address then
  - business as usual (well, maybe…)
- Else if DNS response is “name error” then
  - Respond in a way that is self-beneficial
  - Commonly done without notice and consent to user or domain registrant
    - Even when notice is provided, full disclosure of the security implications are not identified
  - The registrant does not benefit from and in some instances is harmed by the alteration

DNS Protocol Violation?

- RFC 1035 says name error is "only meaningful in responses from an *authoritative name server* "
  - The response is thus **more than an error indication**
  - **Response expresses content** that the authoritative name server expects the client to receive
- DNSSEC goes through great pains to provide *authenticated denial of existence* of DNS records
  - Why would we bother if non-existence was unimportant!!!

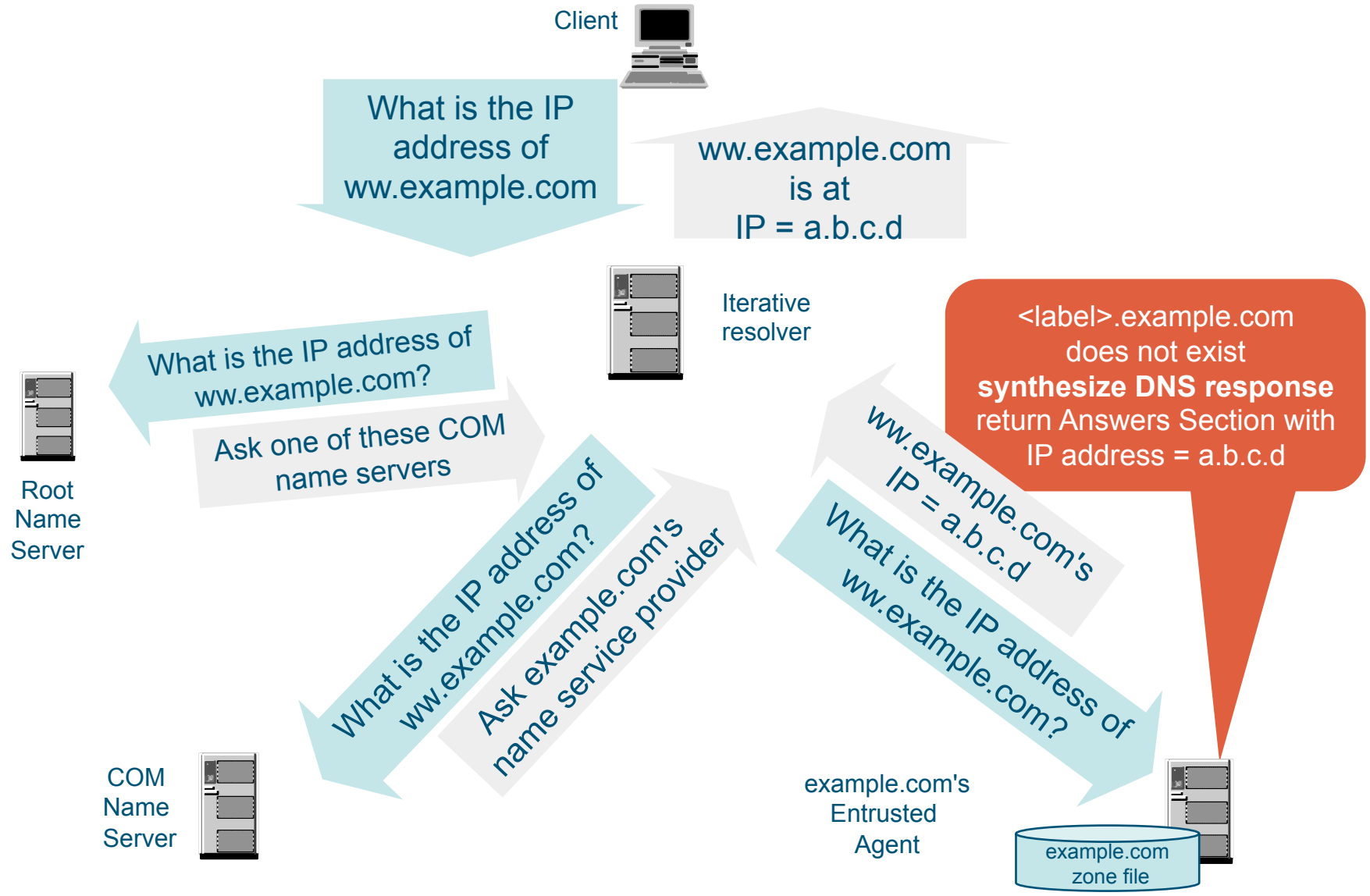
Who can make such changes

- Entrusted Agents
  - A DNS operator who provides authoritative name service on behalf of a registrant
  - Registrars, ISPs, trusted 3rd parties, registrant's IT
- Third parties
  - any DNS operator of any name server that processes the response along the return path from the authority name server to the client that issued the request

Form 1: Synthesized DNS response

- An Entrusted agent operating as a zone authority
  - Receives a name query from a client
  - Determines the name does not exist in the zone file
  - Returns a *name exists* response containing an IP address mapping the entrusted agent chooses
  - Common implementation is to include a *wildcard entry* in the registrant's zone file
    - All names not found resolve to an IP address the agent chooses

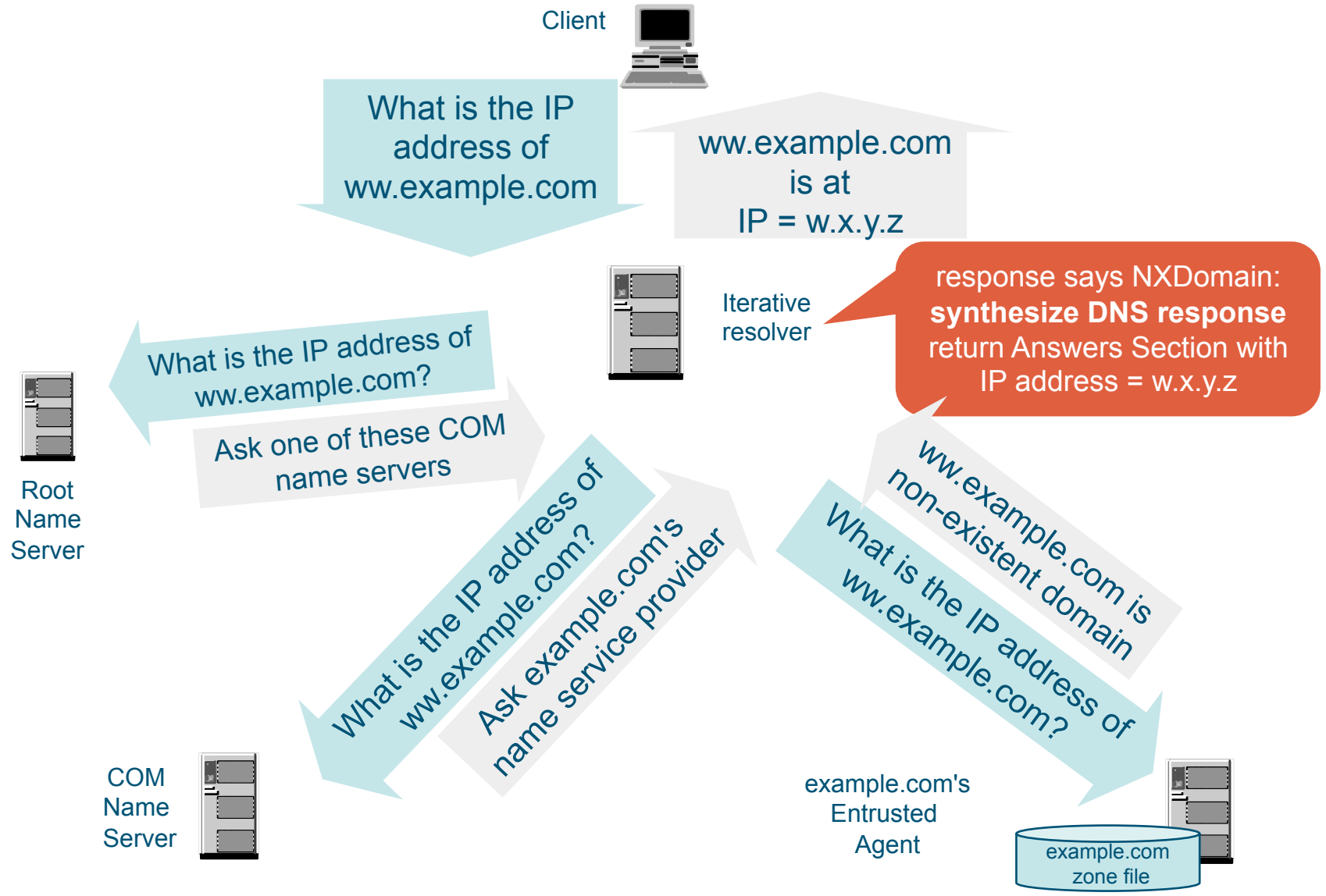
Synthesized DNS Response (Simplified)



Form 2: "On the fly" response modification

- A third party NS operator
  - Examines DNS responses messages it attempts to resolve for a client
  - When it encounters a *non-existent domain* response the resolver
    - Silently alters the response code from *non-existent to name found*
    - Inserts an IP address mapping the third party chooses

NXDomain Response Modification(Simplified)



Who has the means, motive and opportunity?

Who	How	Why
Sponsoring registrar	Entrusted agent (EA)	Promote business
Public DNS provider	Third party NS operator	Promote services
ISP	Third party NS operator or EA	Advertise
Web (proxy) operators	Third party NS operator	Affiliate advertising
"for fee" DNS provider	Third party NS operator or EA	"Enhance the user experience" ☺
Domain registrant	EA	Enforce a policy Remedial Education
Attackers	"own" a DNS server	Fun, fame, fortune…

How are users affected?

- A modified DNS response
  - Signals a different state of the zone to the user than the registrant intended
    - The non-existence of a name is not conveyed to the user
    - The user concludes the host is operated by the registrant
  - Can result in inconsistent responses
    - The response a user receives depends on the resolver it asks
  - Can cause address mapping conflicts when multiple NS operators alter responses
    - An authority may add a host that has been “redirected”
    - Resolvers caching a modified response for this name will return a different address from the one now in the authority zone file

How are domain registrants affected?

- A modified DNS response
  - Alters the content the domain authority intended to have delivered
    - Would you tolerate undisclosed modification of any other application content?
    - Why should DNS messages be treated differently from mail, IMs or voice?
  - Has business and brand implications
    - Redirection hosts benefit from the domain registrant's brand, reputation, site and link popularity, and sponsored link agreements…
- Operational instabilities
- Security implications ->

Security Implications

- A modified DNS response
  - Subverts a "parent trusts the subdomain" security assumption common to web applications
    - Applications assume that any host in my domain is trustworthy
  - Wrests security of hosts from the registrant
    - A host is named in your domain but secured by "someone else”
    - How can I test and audit for (regulatory) compliance and policy conformance if I don’t know or operate the hosts where my NXDOMAINs are redirected
  - **Creates opportunities for attack via a host you cannot secure**
    - Phishing via false site injection
    - Redirect hosts can intercept, monitor and analyze traffic (extract data)
    - Redirect hosts can intercept cookies to acquire personal, credit or bank data
  - Facilitates attacks against brand
    - Aren’t 3rd level labels you don't control as dangerous as 2nd level labels

Other issues

- **A Records today, what about tomorrrow?**
  - Assumption is that most NXDomain responses are for web sites so they lead to "eyeballs"
  - Imagine a future of modified DNS responses that includes MX, NAPTR, SRV and other resource records
- Dueling rewrites
  - DNS responses can be processed by many third parties
  - Any party downstream from a synthesized response can rewrite the response
  - Interesting problem for error resolution marketeers
- Is this the tip of the iceberg?
  - How long before responses from other application servers are “in play”?

SSAC Recommendations

- Synthesized responses at any level in the DNS have unanticipated and undesirable consequences for the registrant and user
- Registrants should choose an entrusted agent that asserts it will not modify DNS responses in its terms of service
- Registrants should study ways to provide end-to-end authenticated proof of non-existence of subdomains (DNSSEC)
- Entrusted agents should not inject DNS wildcards in a zone without informed consent and without fully informing the domain registrant of the risks this practices exposes
- Entrusted agents should provide opt-out mechanism that allows clients to receive the original DNS answers to their queries.
- Third parties should disclose that they practice NXDomain response modification and should provide opportunities for users to opt out