SSAC Public Meeting
Paris
24 June 2008

DNS Response Modification

What is a NXDomain response

- NXDomain = non-existent domain
- Same as a Name Error DNS response code
- RFC 1035 says "only meaningful in responses from an *authoritative name server* "
  - This makes is more than an error indication
  - It is *content* the authoritative name server expects the client to receive
- This content may be modified by
  - Entrusted Agents
  - Third parties

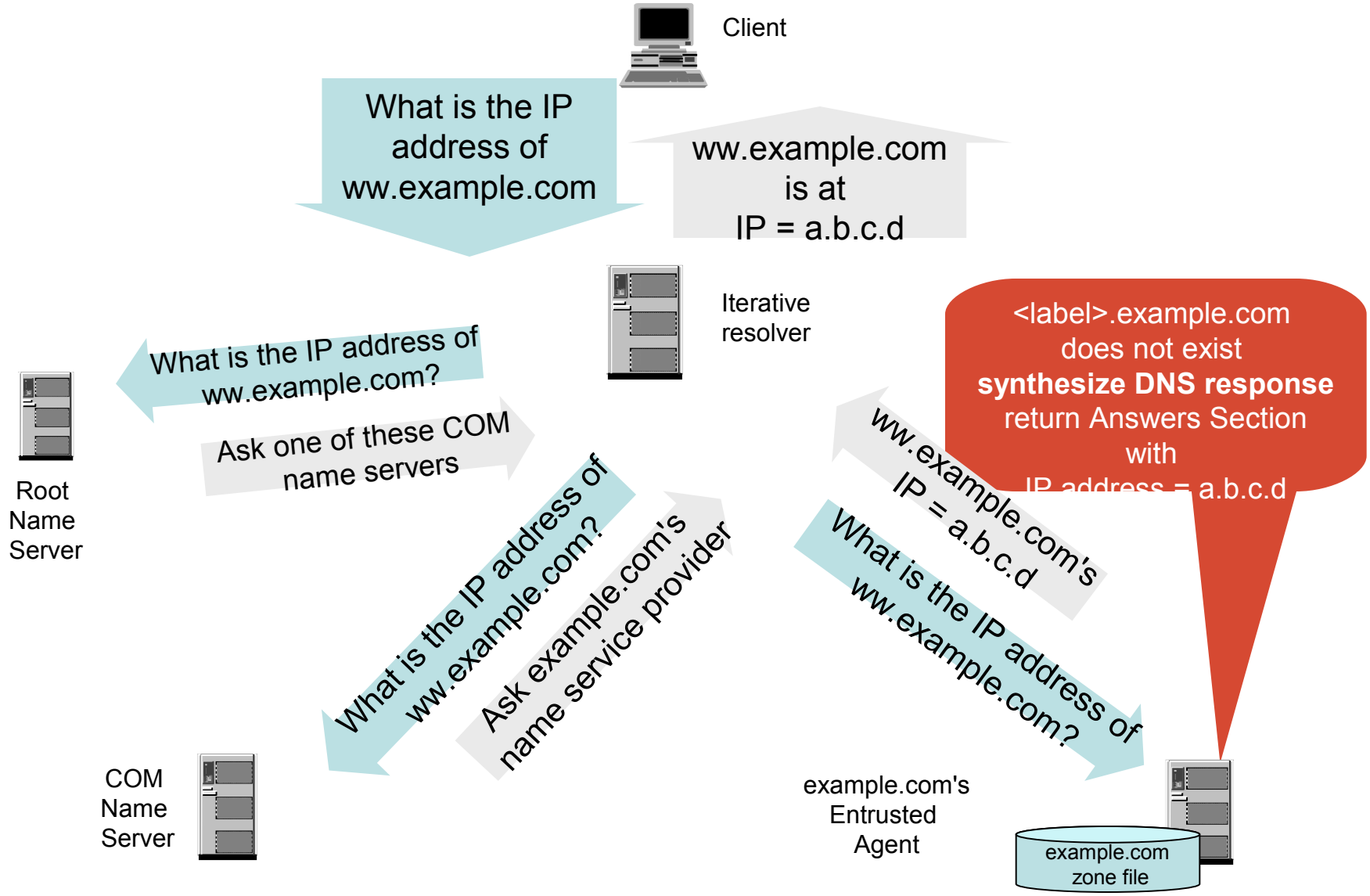
The Players

- Domain registrant
  - Registers the domain
  - In principle, controls what is included in the domain zone
  - In principle, controls the responses the domain's authoritative name server returns
- An entrusted agent
  - administers the zone for the registrant
  - operates the authoritative name service
- Third party NS provider
  - Operates (iterative) resolvers
  - Provides name resolution service to clients

Synthesized DNS response

- An Entrusted agent
  - 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 a zone file
  - All names not found in the zone resolve to an IP address the entrusting agent chooses

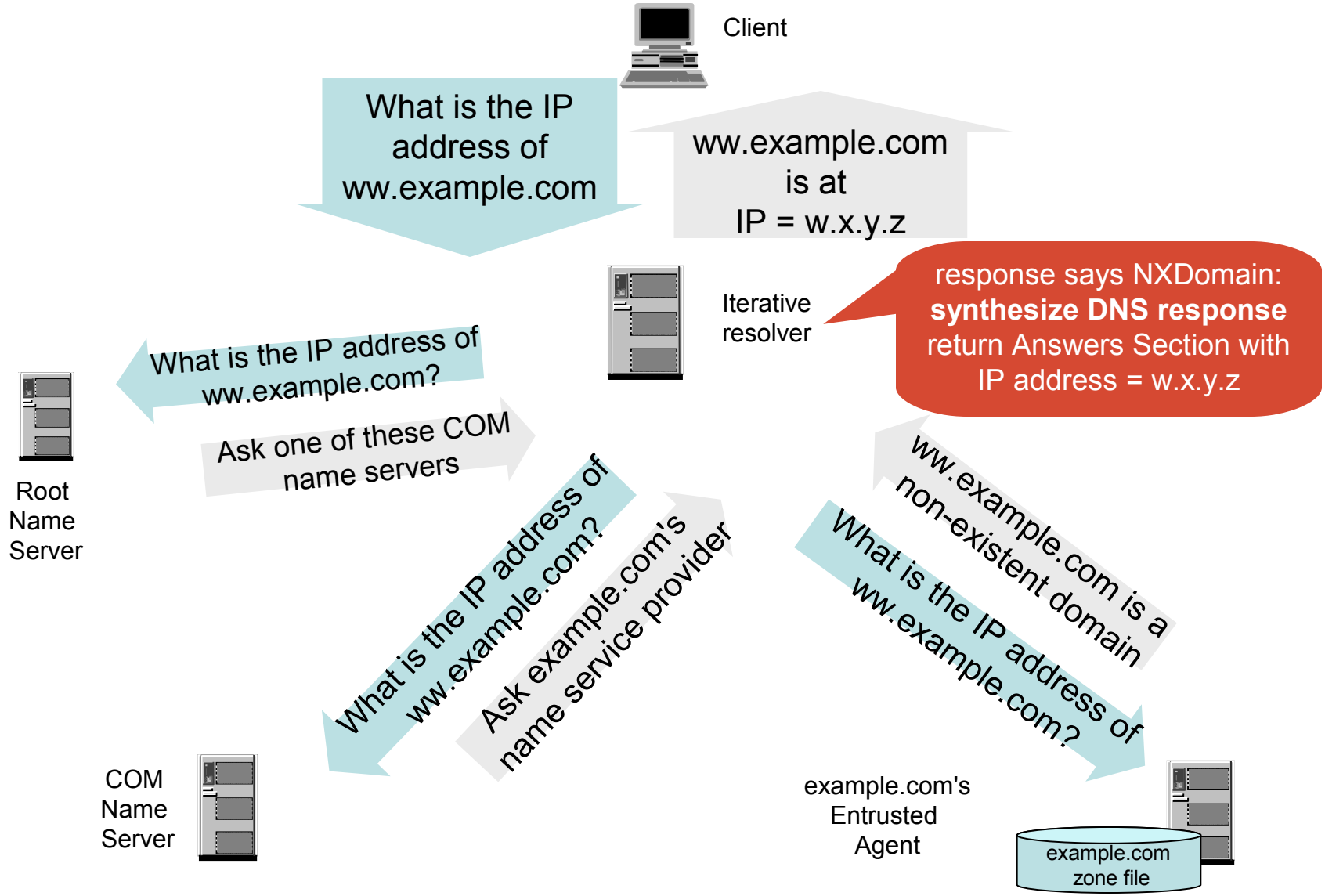
Synthesized DNS Response (Simplified)



NXDomain 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 it
    - 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	Promote services
ISP	Third party or EA	
Web (proxy) operators	Third party	Advertise
"for fee" DNS provider	Third party or EA	Affiliate advertising "Enhance the user experience" ☺
Domain registrant	EA	Enforce a policy Remedial Education
Attackers	"own" a DNS server	Fun, fame, fortune…

How are registrants and users affected?

- Altered and redirected in this manner, the DNS response
  - signals a different state of the zone to the user than the operating state
  - alters the content the domain authority intended to have delivered
    - Why should DNS messages be treated differently from mail, IMs or voice?
  - can cause DNS operational instabilities
    - the response a user receives depends on the resolver it asks
    - address mapping conflicts when multiple parties alter responses
  - creates business consequences for the registrant
    - Redirection hosts benefit from the domain registrant's brand, reputation, site and link popularity, and sponsored link agreements…
  - subverts a common "parent trusts the subdomain" security model
    - affects the registrant's compliance testing and auditing
  - wrests security of hosts from the registrant
    - a host is named in your domain but secured by whoever operates that host
    - Creates opportunities for attack via a host you cannot secure

And those attacker opportunities are?

- Phishing via false site injection at synthesized and modified subdomains
- Data extraction
  - Redirect host can intercept, monitor and analyze traffic
- Aribitrary cookie retrieval
  - Intercepted cookies may disclose personal, credit or financial data
- Attacks against brand
  - Are 3rd level labels you don't control any less dangerous than 2nd level labels that are offensive, defamatory, deceptively or typographically similar

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 synthesis that includes
  - MX records
  - NAPTR records
  - SRV records
  - …

Dueling rewrites

- Hey, it's only *content*… if the original content is already altered, why shouldn't I deliver my content instead?
- 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 businesses
  - Who owns this street corner…

Preliminary Recommendations

- SSAC has previously and repeatedly recommended against synthesizing DNS responses at the TLD level. Similar actions at subdomain levels should not be practiced.

Preliminary Recommendations

- Registrants can control how an entrusted agent answers a query for a name that does not exist in its zone file, via a trust and business relationship.
- Registrant should dictate whether its authoritative name servers return Name Errors or synthesized responses.
- Organizations that rely on accurate NXDomain reporting for operational stability 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, e.g., DNSSEC security extensions

Preliminary Recommendations

- Entrusted agents
  - should not use DNS wildcards in a zone without informing the domain registrant of the risks identified in this Report and elsewhere
  - should not generate wildcards and synthesized responses without the informed consent of the registrant
  - 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 customers to opt out.

Future Work

- How are other IP-based services affected when DNS responses do not match the content the registrant intends to have delivered?
- Are traditional operational assumptions rendered obsolete if error modification becomes common practice?
- How should trust be asserted or demonstrated if subdomains can be created by parties other than the registrant?