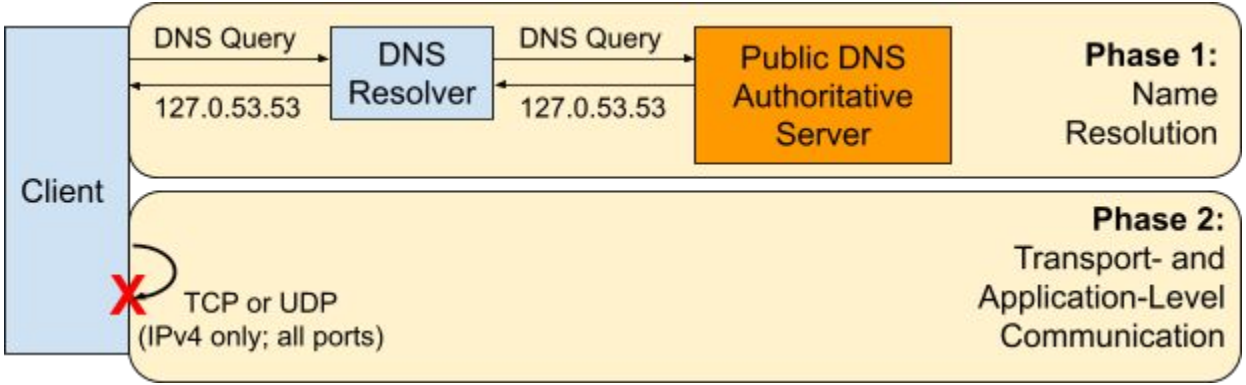
Comparison of Proposed Alerting and Data Collection Techniques

Casey Deccio

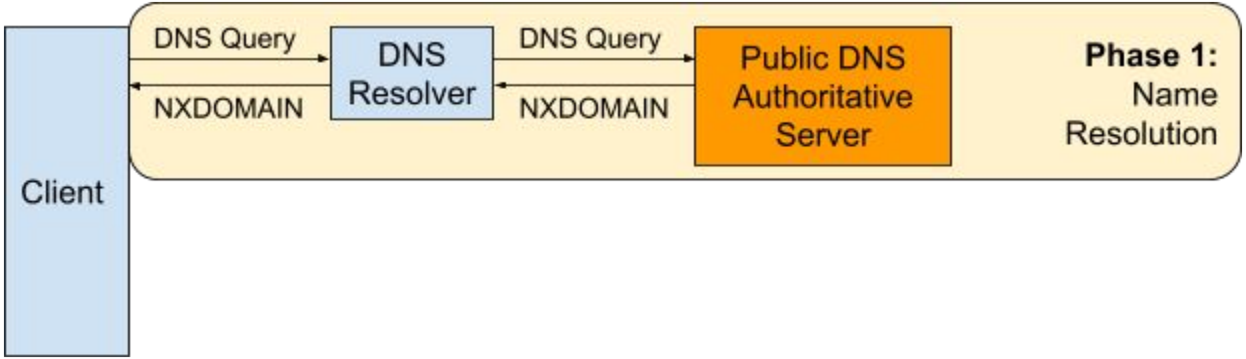
Purpose

- Clarify the risks and benefits of the different assessment mechanisms
    - Controlled Interruption (CI)
    - Active Collision Assessment (ACA)
    - Passive Collision Assessment (PCA)
- Identify purpose and contribution of ad-based and probe-based generated measurement techniques

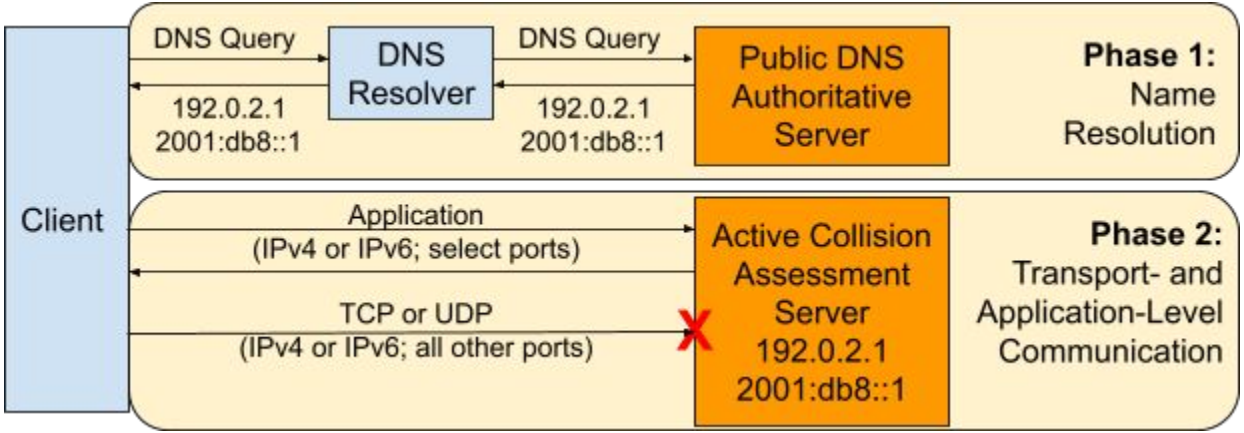
Controlled Interruption


DNS Query
DNS Resolver
DNS Query
Public DNS Authoritative Server
127.0.53.53
127.0.53.53
Phase 1: Name Resolution
Client
Phase 2: Transport- and Application-Level Communication
X
TCP or UDP (IPv4 only; all ports)

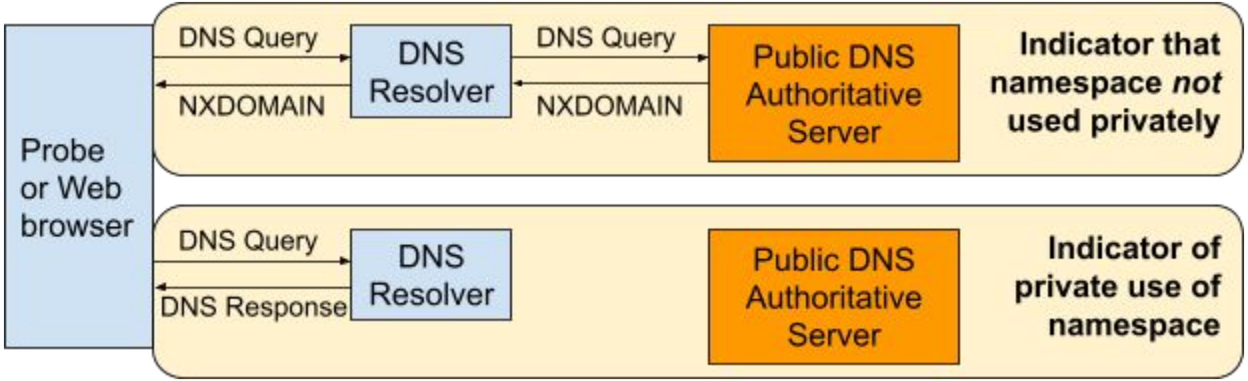
Passive Collision Assessment



Active Collision Assessment


Client
DNS Query
DNS Resolver
DNS Query
Public DNS Authoritative Server
192.0.2.1
2001:db8::1
192.0.2.1
2001:db8::1
Phase 1:
Name Resolution
Application
(IPv4 or IPv6; select ports)
TCP or UDP
(IPv4 or IPv6; all other ports)
Active Collision Assessment Server
192.0.2.1
2001:db8::1
Phase 2:
Transport- and Application-Level Communication

Atlas Probes



Probe or Web browser
DNS Query
NXDOMAIN
DNS Resolver
DNS Query
NXDOMAIN
Public DNS Authoritative Server
Indicator that namespace *not* used privately
DNS Query
DNS Response
DNS Resolver
Public DNS Authoritative Server
Indicator of private use of namespace

What is being compared?

- Alerting effectiveness
  - *What population of potentially affected users, systems, and applications are expected to be reached by the alerting mechanism?*
- Operational continuity, security, and privacy
  - *How might users or systems be negatively impacted by interruption to service or subjected to exploit or privacy violations?*
- User experience
  - *What is the experience of the end user, in terms of application behavior, path to resolution, etc?*
- Root cause identification
  - *How useful is the technique in leading users towards the root cause and a possible resolution?*
- Public response
  - *In what ways might the techniques be received in the public, with ICANN and others being accountable for complaints and fallout associated with design and execution of the mechanism?*
- Telemetry
  - *How much data is available to investigative parties, and what type of effort will it take to collect and analyze it?*

Alerting Effectiveness and Coverage

	CI	ACA	PCA
DNS Resolution of Queried Names	Resolution of queried names depends on DNS configuration and system mobility	Resolution of queried names depends on DNS configuration and system mobility	Queries names do not resolve
Application Coverage	Only applications using IPv4 are affected	Applications using either IPv4 or IPv6 are affected	No applications are affected

User Experience

	CI	ACA	PCA
Error Response - Application Experience	Quick-Response Error	Quick-Response Error or Timeout, depending on network configuration and application port	No Error
Error Response - User Experience	Application Dependent	Application Dependent	No Error
User Experience - HTTP / HTTPS Browsers	Not applicable	**HTTP:** unexpected content received **HTTPS:** TLS certificate errors	Not applicable
User Experience - Other Clients and Protocols	Not applicable	**Non-browser HTTP:** unexpected content received, other unknown errors **Applications that use TLS:** TLS certificate errors **SSH:** man-in-the-middle attack errors	Not applicable
User Experience - Local Firewall Alerts	Rare but possible	Not applicable	Not applicable

Operational Continuity; RCI; Public Reception; Telemetry

	CI	ACA	PCA
Operational Continuity, Security, and Privacy	**DNS Query Surveillance:** all qnames **Communication Interruption:** all **Application Inference:** none **Communication Interception:** none **Data Exfiltration:** none	**DNS Query Surveillance:** all qnames **Communication Interruption:** all **Application Inference:** all **Communication Interception:** select **Data Exfiltration:** select	**DNS Query Surveillance:** all SLDs, fraction of qnames **Communication Interruption:** none **Application Inference:** none **Communication Interception:** none **Data Exfiltration:** none
Root Cause Identification	**Low** - hint often not observed (34%) or not understood (24% - 50%)	**Low** - name collisions experienced in Web browsers are few (12 - 20%)	Not applicable
Public Response	**Neutral (94%)**, based on actual deployment experience	**Unknown, Possibly negative**, based on experience with Site Finder	No reactions anticipated
Telemetry	**DNS queries:** all qnames; end-system query volume masked by caching **Application:** no telemetry	**DNS queries:** all qnames; end-system query volume masked by caching **Application:** IPv4 and IPv6; TCP/UDP usage and destination ports; application-layer data	**DNS queries:** all SLDs, fraction of qnames, end-system query volume masked by caching **Application:** no telemetry

Generated Measurements of Collision Potential

- Two techniques proposed:
    - Ad-based measurement
    - RIPE Atlas probe measurements
- Contribution
    - Expose collision *potential* in networks where queries *would* collide if they were allowed to reach public authoritative servers.
- Limitations
    - They do not necessarily reflect actual activity by end users and systems.
    - They only address a subset of configurations and usage models.
    - Queries will include those from both actual end systems and the generated measurements.
    - Not all browsers and probes point at DNS resolvers that are used by end users and systems.
    - Any identifiers associated with query names must be embedded in the second label.
    - Data will only be gathered for networks that host a probe or browser that receives ads.

Impact on the Root Cause Analysis

- Several of the comparisons led to updates to the Root Cause Analysis report
  - Added new sections:
    - Section 3.4 - Web search results
    - Section 5 - Web search results analysis
  - Added two findings to section 10.2:
    - The public response to controlled interruption was overall neutral.
    - Name collisions were diverse, both in terms of the application involved and their root causes.
  - Updated one finding in section 10.2:
    - Controlled interruption is effective at disruption, but not at root cause identification.
  - Added Appendix B (Web search results for 127.0.53.53)
  - Updated references across the document