Visualization of DNS Dependencies and More

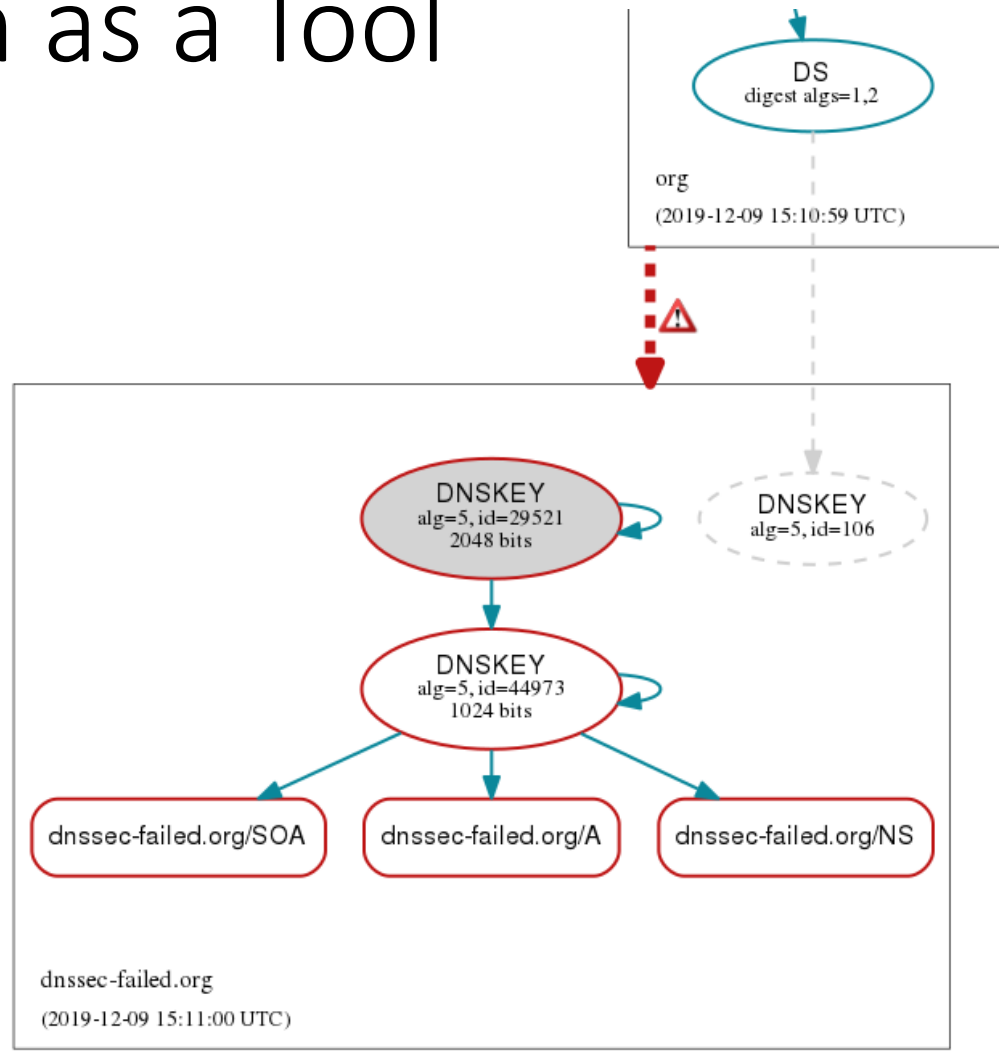
Casey Deccio

Brigham Young University

Graph-Based Visualization as a Tool

- Visual Awareness
  - Humans see trends or more clearly identify problems

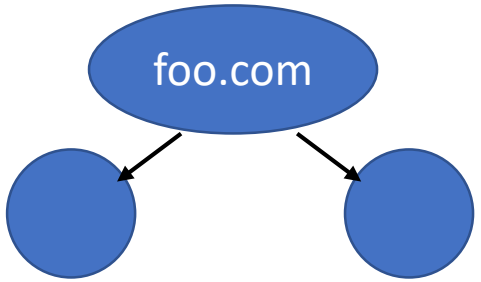
- Data Structures
  - Graphical data structures can be used for programmatic analysis



What Is Included?

Basic Components

- Direct Relationships
  - Dependency
  - Influence
  - Weight
- Groupings
- Boundaries

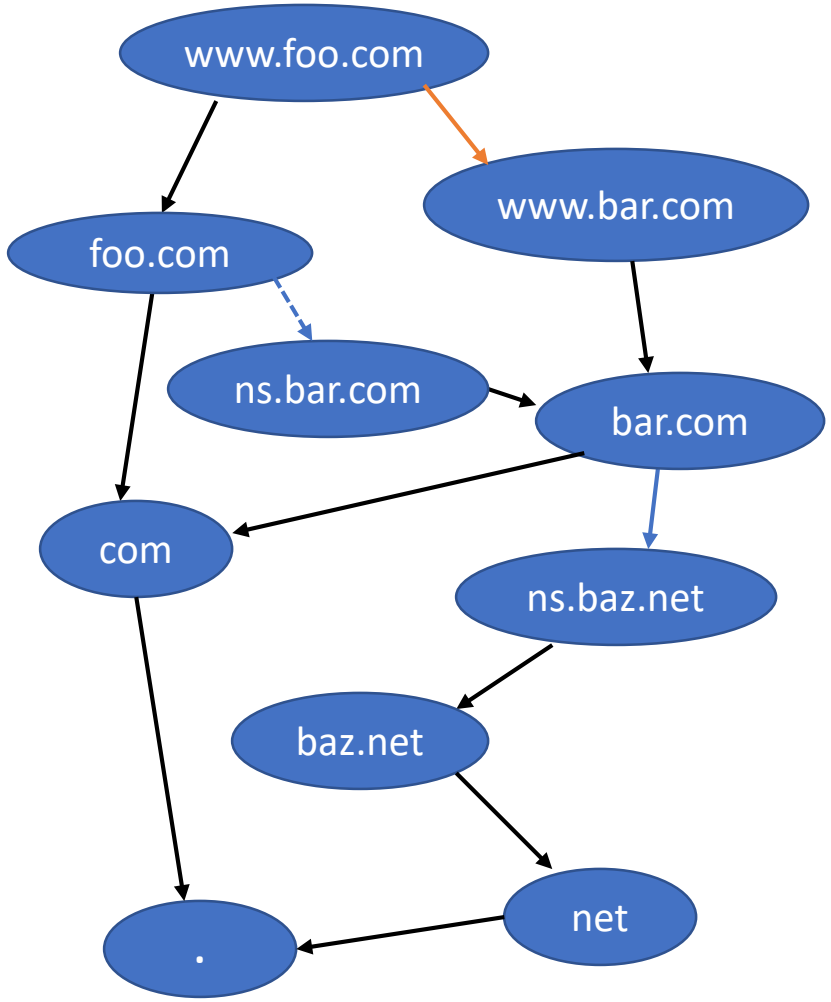


Inferences

- Common Ancestry
- Transitive Relationships

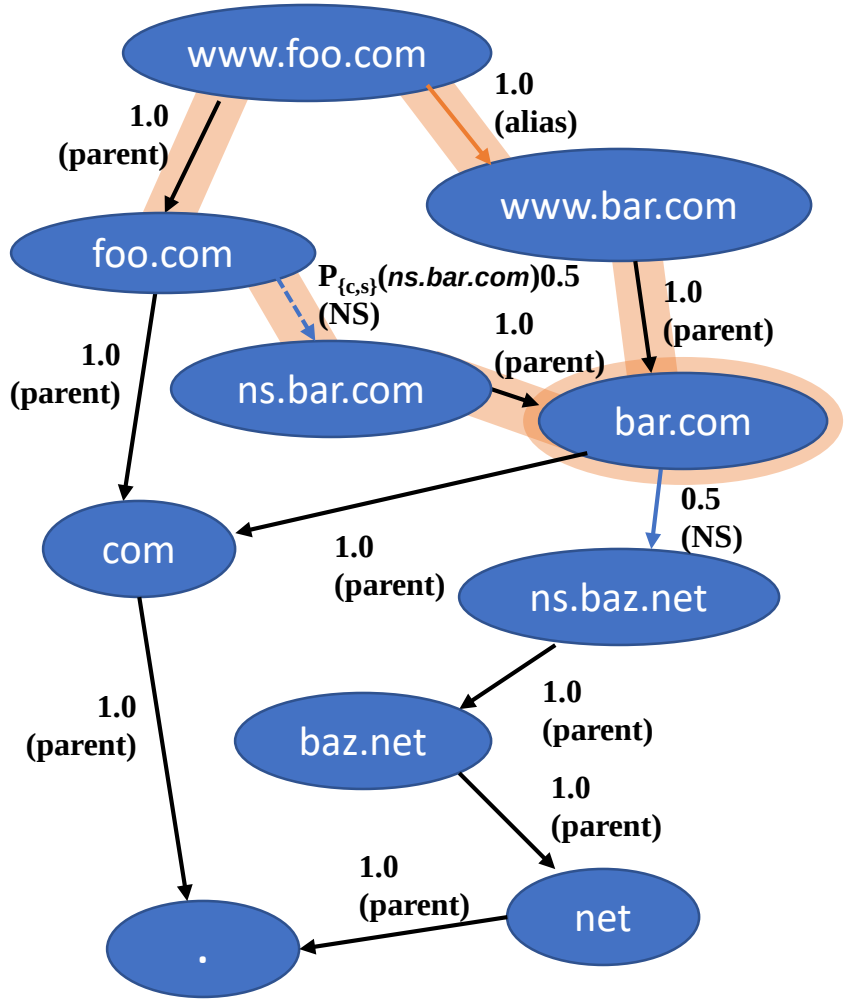
Example: Resolution Dependencies/Influence

- Nodes = domain names
- Edges = dependencies
  - Child to parent
  - Alias to target
  - Zone to NS targets



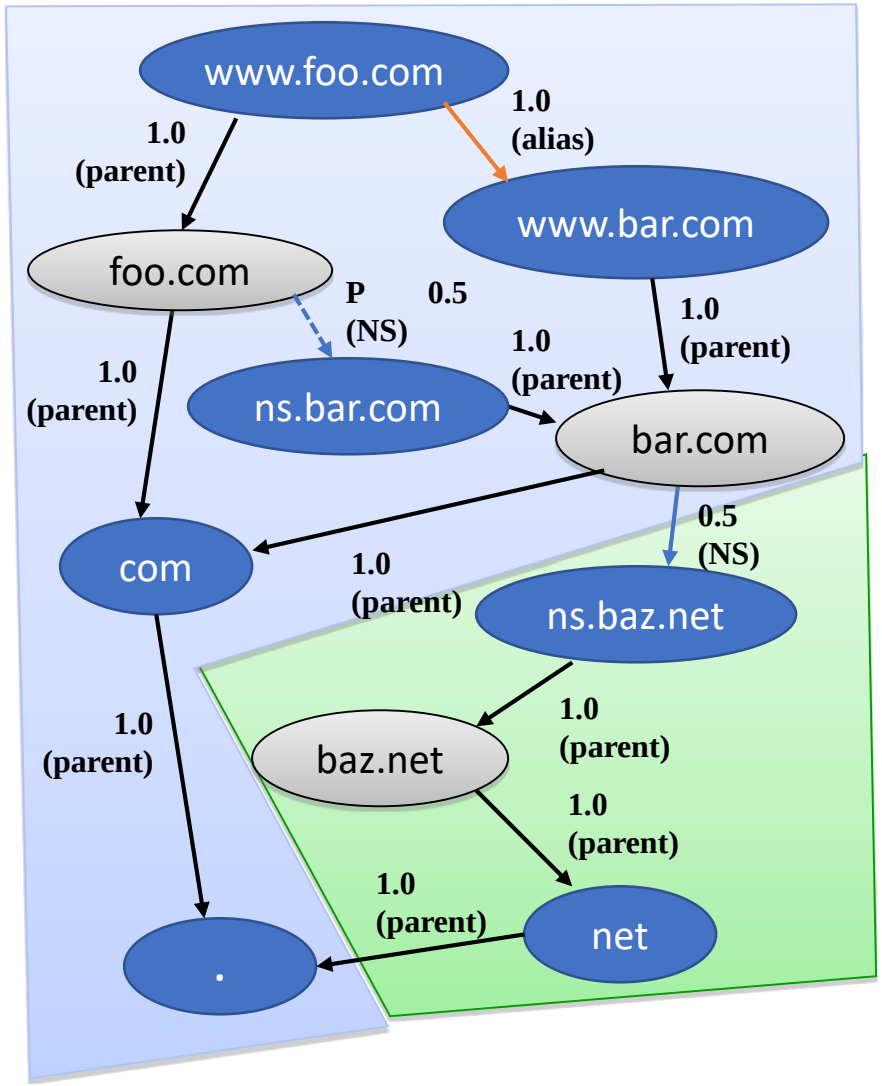
Quantifying Influence with Weights

- Follow edges on path using weights as probability



Defining Boundaries

- Zone Boundaries
- Administrative Boundaries
- Direct Configuration Boundaries

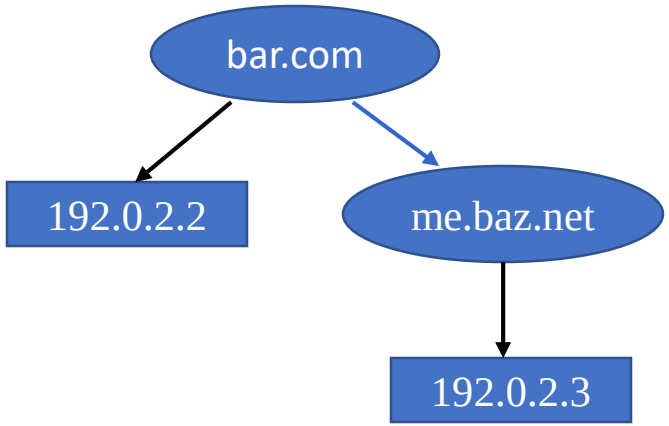


2010 Results

- Under normal circumstances:
  - Nearly all zones rely on fewer than 20 other zones
  - 80% of zones have no third-party influence

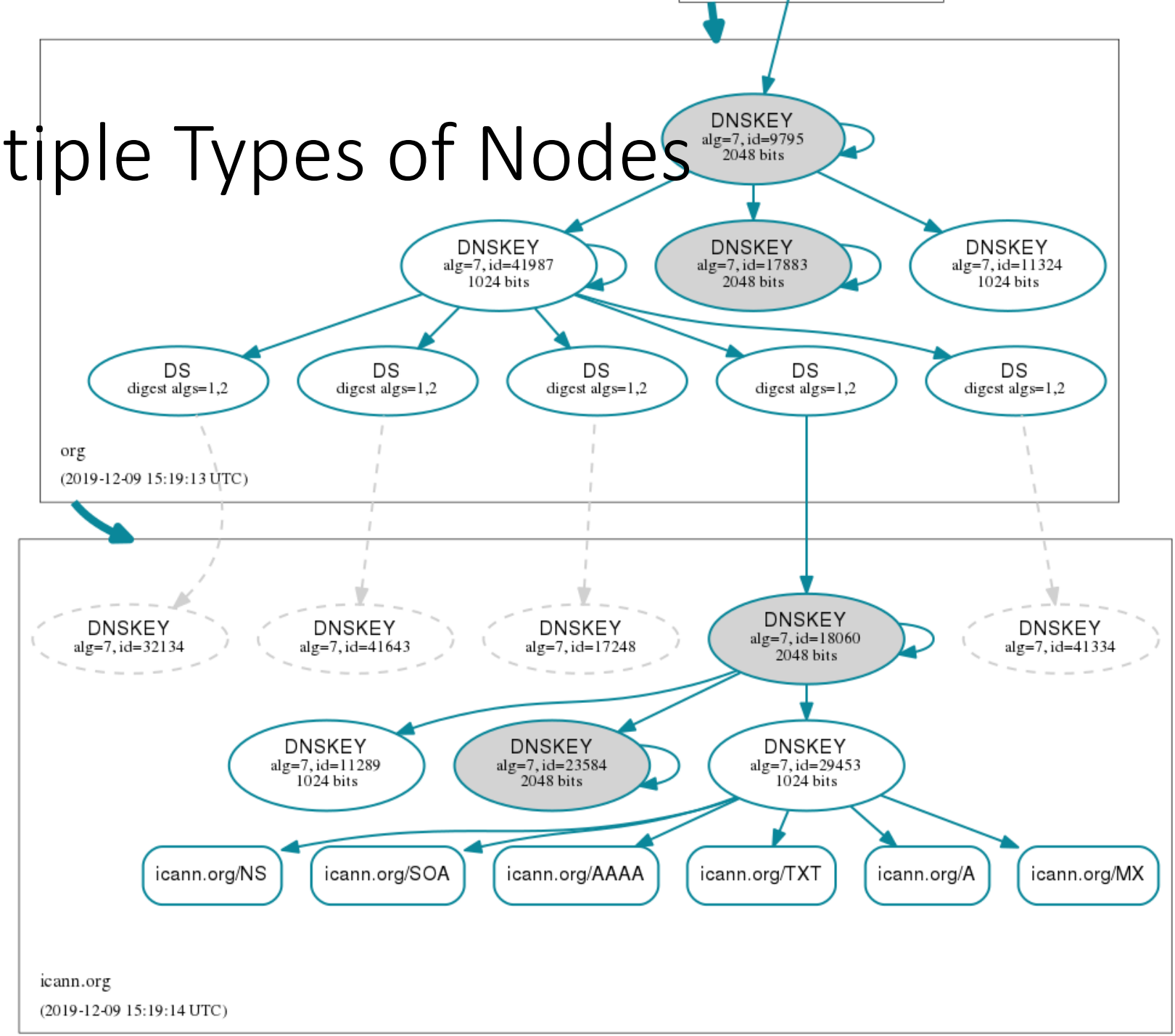
Connecting Multiple Types of Nodes

- Direct server dependencies:
  - **Zone-to-server:** Dependency of zone on server whose name has in-bailiwick glue record
  - **Name-to-server:** Dependency of name on address



Connecting Multiple Types of Nodes

- DNSSEC Dependencies



Other Types of Nodes / Relationships

- Geographic region
- ASN
- IP Reputation Category

Getting the Most Mileage / How does it scale?

- Meaningful use of symbols, styles, and labels
  - Emphasize the most important distinctions
- Aggregation
  - Must be based on basic relationships
  - Both quantitative and qualitative analysis