

# One small step for DNS

# One giant leap for Networking



Me: Siva Kesava R K  
t-sikaka@microsoft.com

Siva Kesava Reddy K<sup>\*†</sup>, Ryan Beckett<sup>§</sup>, Behnaz Arzani<sup>§</sup>, Todd Millstein<sup>\*</sup>, George Varghese<sup>\*</sup>  
<sup>§</sup>MNR Group, <sup>\*</sup>UCLA

## 1. Problem Statement

DNS misconfigurations have caused global outages.

### Microsoft DNS Outage, 2019



Microsoft engineers executed a delegation change

1



Error in change automation resulted in a server with empty zone files

2



3

"Oops! Domain doesn't exist"

"what's the IP address of database.windows.net?"

"65.55.23.107"

Can't access my database.



- Users experienced connectivity issues globally with several Microsoft services, including Azure Storage, Azure SQL Database, Microsoft 365 and Azure DevOps.
- ~25% of queries produced incorrect results
- Negative caching aggravated the situation
- Cascading effect - multiple other Azure and Microsoft services that depend upon these core services were also impacted

Can we verify the correctness of the DNS configuration changes before they are made?

## 2. Challenges

- Handling the scale of the DNS (microsoft.com domain alone has ~200 million entries)
- DNS look up is non-deterministic
- Modeling rewrites in DNS (CNAME & DNAME)
- Handling state explosion

## 3. Limitations of Prior Works



Time = ??



External Monitoring Service (EMS)



Querying Rate = ??

Time of change unknown to the EMS and it has to send real queries at frequent intervals

- Black-box testing can catch errors only after they are live
- Errors found are not comprehensive

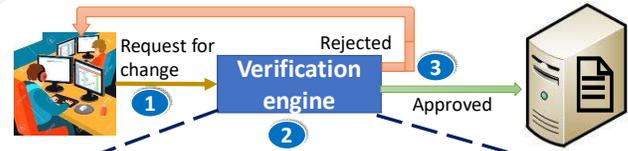
## Terminology

According to geography and organizational affiliation, administrator of a domain can delegate the responsibility for managing a subdomain to someone else. Each time an administrator delegates a subdomain, a new unit of administration is created and these units are called **zones**. The boundary between zones is a point of **delegation** in the DNS.

## 4. Approach

**Goal:** Verify correctness of the DNS configurations by statically checking properties on the zone files, for example, for all queries ending with "database.windows.net" the reply should be independent of the server contacted.

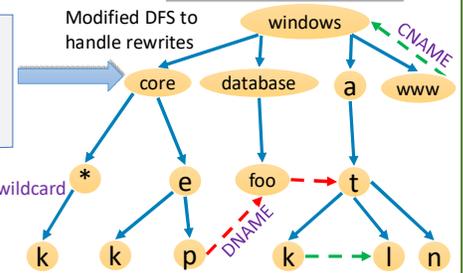
**Approach:** Categorize all queries into equivalence classes and execute them symbolically.



### Zone Files



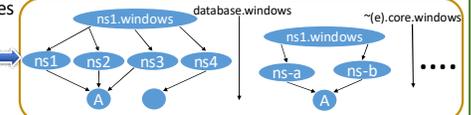
### Equivalence Class Generation Graph



### Symbolic Interpreter

Mimic the execution of a query & check for properties

Properties



Satisfied (Approved) Counterexamples (Rejected)

## 5. Ongoing Work

- Tackle the limitations of prior works by using a white-box approach with access to all the zone files under Microsoft domain
- Formalizing the model of the DNS.
- Formulating the desired properties and implementing the symbolic interpreter

<sup>†</sup>Contributed during an internship at MSR, Redmond