Cooperative Security Mechanisms for DNS

Prasant Mohapatra
University of California, Davis

http://www.cs.ucdavis.edu/~prasant

Project Goals
- Analyze and characterize DNS operation from a security standpoint
- Develop scalable cooperative solution for DNS security

Existing Challenges
- Complexity of DNS system
- Lack of uniform implementation

Our Approach
- Abstract DNS infrastructure as graph models from observed data; transform graph model into mathematical models
- Enhance DNS security with scalable and resilient solutions

Approach and Impact

New approach
- New methods for analyzing DNS dependencies
- Experimental work to derive general DNS model

Research Impact
- Incorporate mathematical models to predict DNS behavior
- Identify regions of weakness in DNS infrastructure

Technical Discussion
With years of operational experiences, there are few, if any, efforts attempt to model the behavior of the DNS infrastructure. Characteristics such as query/response integrity, latency, server interdependency and transitive trusts in DNS servers have been studied in limited context. As such, insufficient efforts have been invested into developing a comprehensive mathematical model that could describe the behavior of DNS system under different scenarios. Our current efforts focus on developing mathematical models for describing DNS system behaviors in different scenarios (e.g. epidemic spread, in the presence of cache poisoning) by leveraging DNS delegation chain information obtained through experiment.

Results
We have successfully developed a light-weight, scalable, and decentralized solution to detect cache poisoning, called DoX. Our current effort focuses on understanding the DNS dependency graph (partial graph shown to the right) so that we can understand the DNS structure better, enabling us to develop a more comprehensive security solution for the DNS infrastructure.