Critical Infrastructure
DNS Research Testbed

Wes Hardaker <hardaker@isi.edu>¹

joint work with Terry Benzel¹, Michael Elkins², John Heidemann¹, Yuri Pradkin¹, Abdul Qadeer¹

1: University of Southern California/Information Sciences Institute
2: Parsons
Evolution of the DNS Ecosystem

- 1985: DNS starts in academia
- 1995: Internet commercialization
- 1998: ICANN
- 2004: new TLDs
- 2016: NTIA transition
Changing Roles

• 1985: academic: applied research
• 1995: transition to “make it real”
• 2005: academia lacks perspective to contribute

can we benefit from complementary roles?
Results: Difficult Evolution Problem

• Advancing the DNS and DNSSEC is difficult
  – Protocol changes (e.g. NSEC5, DANE, …)
  – Code innovation (e.g. new server code)
  – Hardware changes (e.g. hardware-based dnssec)

• Safe experimentation on real traffic is difficult
  – Mirroring vs live feeds
  – Privacy concerns

• Thus: Internet naming research has stagnated
Our Solution: A Testbed Married With Operations

- Internet infrastructure at USC/ISI
  - DNS’s B-Root
  - Other zones and protocols
- Hardware for conducting experiments
- Software for collecting research traffic
- Software for analyzing and comparing traffic
  - Operational vs Testbed
- Software for replaying and retesting
Our Expected Architecture

The following diagrams depict our current high-level architectural plans
Typical Operational DNS Service
Adding a Parallel Testbed

FW -> Splitter -> FW -> Production

- Research Encoder Option Modules
  - UDP->TCP
  - UDP->HTTP
  - Anonymizer
  - Research Module

- Test
- User Hardware

- Research Decoder Option Modules
  - TCP->UDP
  - HTTP->UDP
  - De-Anonymizer
  - Research Module

Synchronization

Research Testbed
Other Data Sources

- FW
- Splitter
- FW
- Production
- Comparison & Verification
- Research Archive
- Traffic Generator
- Traffic Replayer
- Research Encoder Option Modules:
  - UDP->TCP
  - UDP->HTTP
  - Anonymizer Research Module
- Test
- User Hardware
- Research Decoder Option Modules:
  - TCP->UDP
  - HTTP->UDP
  - De-Anonymizer Research Module
- Research Testbed
- Synchronization
Example Usage Configurations

• Run in parallel
• Replay and generated traffic
  – Tuning and adaptation
• User zones hosted at the testbed
• Protocol conversions and testing
• Address based operational/test separation
Run in Parallel: Root or User Zones
Replay and Generated Traffic

Traffic Generator -> Traffic Replayer -> Research Archive

Research Encoder Option Modules:
- UDP->TCP
- UDP->HTTP
- Anonymizer
  Research Module

User Hardware

Test

Research Decoder Option Modules:
- TCP->UDP
- HTTP->UDP
- De-Anonymizer
  Research Module

FW -> Production

Research Testbed

Synchronization
Safe Experimentation

• Goal: testing new tires on a running car
  – Critical infrastructure cannot fail
  – But, research means trying new things

• Approach: new research infrastructure for...
  – experimenters evaluate real traffic
  – then compare experimental vs. production outputs
  – path to production after testing with automatic fail “out”

• Result: testing new things, safely
Community and Research Building

• A new research community
  – Outreach to broader research communities
  – Re-engaging academia
  – Outreach to operational communities

• Broaden the naming research agenda
  – Looking for input and feedback!

• New open-source software
  – For use by both researchers and operators
Overall Benefits

• Rekindle and grow academic involvement
• Accelerate innovation
  – new uses
  – more rapid evolution
• Collaboration with academia, industry, governments and NGOs
Timeline

• **Now:**
  – Gather Requirements
  – Funding
  – Community and collaborators

• **Soon:**
  – Hardware and software
  – Open to researchers for experimentation
Join Us

• **Looking for feedback**
  – http://ant.isi.edu/researchroot
  – Join our mailing list
  – Send us ideas, suggestions, feedback
  – And use cases!!!

• Join the community and attend our workshops