

Netalyzr NG: Measuring DNS, DNSSEC, and TLS from the Edge



Cyber Security Division 2012 Principal Investigators' Meeting

10/10/2012

Nicholas Weaver
Researcher
International Computer Science Institute
nweaver@icsi.berkeley.edu
510-666-2903



Topic and Team

- TTA #7: Network Mapping and Measurement
 - This proposal is focused on measuring DNS, DNSSEC, and TLS from the end users' network connections
- PI: Nicholas Weaver
 - Researcher at ICSI focused on network measurement and network security
- Co-PI: Christian Kreibich
 - Researcher at ICSI focused on network measurement and network security
- Network Security Group lead: Vern Paxson
 - Professor at UC Berkeley and Senior scientist at ICSI



Network Security and the Edge

- Security relevant network protocols must go to the edge
 - The final device needs confidence in DNS, the ability to validate DNSSEC, and create encrypted connections (TLS/SSH/VPN) to remote systems
 - But **can** systems access these protocols?
 - **Should** they have confidence?
- We must measure these properties from the edge of the network
 - On the users' computers
 - On the users' phones

What is *Netalyzr*?

- ***Netalyzr*** is a widely used, highly comprehensive network measurement, debugging, and survey tool
 - Runs in a Java-equipped browser with just 2 mouseclicks
 - Provides a command line client
 - Supports remote system debugging and embedding in other projects
 - Coming soon: Android client
 - Full functionality for mobile devices
- Wide usage offers a unique opportunity to deploy new client-side network measurements
 - 670,000 sessions from 470,000 IPs to date
 - Measurements have already provided significant insights into the edge network operation

Enabling Netalyzer to Evaluate Security Protocols

- Enhanced DNS Health Monitoring
 - Have previously detected several manipulations
- DNSSEC to the resolver
 - When resolvers do validate DNSSEC, what are the limitations? (e.g., algorithm support, clock drift)
- DNSSEC to the client
 - When clients need to validate DNSSEC, what are the limitations? (e.g., path issues, bad roots)
- TLS to the client
 - Detecting HTTPS manipulations
- Other enhancements
 - User survey for data release to PREDICT
 - Proxy traceroute to detect hidden proxies

DNS Health

- Netalyzr currently looks up ~90 important names on the client which are validated on our server
 - Already observed ISP-directed MITM attacks on search engines, DNSChanger conditions, and state-sponsored censorship
- An opportunity to add a substantial number of names to validate
 - Perhaps 50 to 100 more without substantial performance impact (could be sampled from a larger list)
 - Which names should be validated?
- DNS packet injection detection
 - DNS “hold-open” can detect packet injection

DNSSEC Validation on the Recursive Resolver

- Resolvers are beginning to validate DNSSEC
 - Is the path sound? Can the resolver receive the necessary information to validate in all cases?
 - What are the supported RRTYPEs?
 - What are the supported algorithms?
- Other correctness issues:
 - CD support and caching?
 - Clock drift?
- Requires creating a ***dynamic*** DNSSEC authority server
 - Create DNSSEC signatures over arbitrary data in real time

DNSSEC Validation and the Client

- The client must validate DNSSEC information
 - The recursive resolver should not be trusted
- Information from the recursive resolver...
 - Can the client actually obtain all DNSSEC RRSETs and RRTYPEs to enable DNSSEC validation? If not, why not?
- Information from the Internet...
 - Is there a proxy or firewall that interferes with DNSSEC requests? If so, does everything work right including DNSSEC data, alternate RRTYPES, large requests, truncation...
 - Can it be bypassed if broken?
- Do the roots and TLDs return DNSSEC information?

Monitoring TLS

- The client also needs to communicate securely
 - But can the encrypted communication actually take place?
- Can the client contact remote servers using TLS?
 - Both our own and major infrastructure (e.g. Google)
 - Are the certificates correct?
 - Or is there a proxy?
- Protocol-Agnostic proxy detection
 - Developing a “Proxy Traceroute” to detect hidden TCP terminating proxies regardless of protocol

Other features...

- User survey
 - Consent to export data to PREDICT
- JavaScript “Lite” version
 - Embed some DNS and other tests as an iFrame in web pages
- General enhancements
 - Attracting more users increases the quality of DNS, DNSSEC, and TLS measurements
- Measurements by request
 - Are there other network measurements which should be included?

Capabilities We Enable

- Users improve understanding of their connectivity...
 - ... and enable future research through collected data
- Network operators gain a valuable tool
 - A “two click” functionality and problem check
- DHS and the community learns the true state of the edge network
 - What works and doesn't work for DNS, DNSSEC, and TLS
 - What workarounds may work or won't work

Schedule & Deliverables

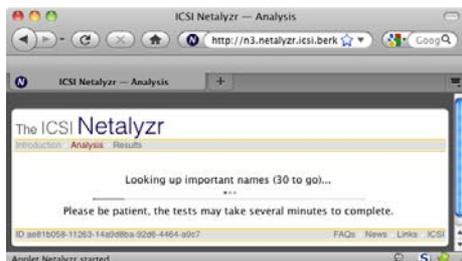
- 6 months:
 - initial dynamic DNSEC service
 - New test methodologies
 - User consent for data export to ***Predict***
- 12 months: Initial TLS checks
- 18 months: New tests based on feedback
- 24 months: Continued operation beyond the contract end
- Ongoing during the contract:
 - Other enhancements to Netalyzr
 - The better the tool -> more users -> more data
 - Data analysis, publications, and reports

Technology Transition

- Netalyzr will continue as a free-to-use service after the contract ends
 - The enhancements will act as additional benefits to users and network operators
- The DNS library will be released under a Berkeley-style license
 - Allows others to build applications which require dynamic DNSSEC signatures
 - e.g. a DNSSEC, single RTT timestamp service:
Query an arbitrary name and get back a signed RRSET
- Data with user consent will be exported to PREDICT

Netalyzr NG: Monitoring DNS, DNSSEC, and TLS from the edge

International Computer Science Institute



?

TLS Manipulated?

DNSSEC Working?

DNSSEC Manipulated?

Widespread Survey Of The Internet:
What Works?
What Doesn't?

Debugging Information:
What's Blocking DNSSEC From Working?

Operational Capability:

Network Testing Tool:

- + Detect Client DNSSEC problems
- + Detect DNS manipulation of critical names
- + Detect in-network TLS manipulations

Dynamic DNSSEC Authority:

- + Enables experimenting with dynamic DNSSEC

Network Measurement Information:

- + Detailed survey of DNSSEC's deployment **to the client**
- + Detection and analysis of manipulated DNS names
- + Detection and analysis of TLS manipulations on important sites

Network Measurement Results:

- + Reports on DNSSEC and TLS client availability
- + Suitable datasets for inclusion into PREDICT

Proposed Technical Approach:

Enhance Netalyzr to provide detailed probing:

- + Detect how DNSSEC is deployed to the client
- + Detect and probe manipulations of DNS
- + Detect and probe TLS manipulations
- + Requires creating dynamic DNSSEC server

Data analysis and Data Release:

- + Detailed reports on obtained measurement result
- + Support for manual generation of third party queries
- + Suitable data exported to PREDICT

TTA #7 is specifically concerned with measuring DNSSEC:

- + Netalyzr NG offers a **unique** vantage point for evaluating DNSSEC to the client both now and in the future
- + TLS is equally important for typical clients and growing more important as additional services (search, social media) transitions to https.

Schedule, Deliverables & Contact Info

Schedule: 24 months

- + 1-6 Months: Development and Deployment of DNSSEC tests and server
- + 7-12 Months: Development and Deployment of TLS validation
- + 13-18 Months: New tests based on feedback
- + 19-24 Months: Commercial Transition, Data Export

Deliverables:

- + Continued operation and analysis including reports
- + Dynamically Signing DNSSEC server
- + Suitable dataset into the PREDICT repository

Corporate Information:

International Computer Science Institute
Admin POC: Jaclyn Considine, jaci@ICSI.berkeley.edu
Technical POC: Dr Nicholas Weaver, nweaver@ICSI.Berkeley.EDU
1947 Center Street suite 600, Berkeley, CA, 94704. 510-666-2900

Extra Slides

How *Netalyzr* Operates

