CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS’

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

International Computer Science Institute

Dr Nicholas Weaver

September 18th, 2013

Homeland Security
Science and Technology

Team Profile

- The International Computer Science Institute
  - A non-profit (501(c)3) research lab affiliated with the University of California at Berkeley
- PI: Dr Nicholas Weaver
  - Network measurement, network security
    - Favorite paper title:
      “How to 0wn the Internet in Your Spare Time”
- Co-PI: Dr Christian Kreibich
  - Network measurement, network security
    - Favorite paper title:
      “Probe and Pray: Using UPnP for Home Network Measurements”
- Postdoctoral Researcher: Dr Narseo Vallina-Rodriguez
  - Network measurement, cellular networks
    - Favorite paper title:
      “Breaking for Commercials: Characterizing Mobile Advertising”

Customer Need:
Can DNSSEC Work?

- DNS (the Domain name System): Turns “www.example.com” into addresses
- DNSSEC (DNS Security Extensions): Adds cryptographic integrity
- DNSSEC on the authority-server side is a ***success***
  - Most major TLDs (top level domains, eg .com) support DNSSEC records
    - Thanks in no-small-part to DHS’s mandates
  - Thus we now have perhaps the most interesting Public Key Infrastructure (PKI) available, deployed and just waiting to be used
    - Free to use! A ***constrained path of trust!***
- DNSSEC on the recursive resolver is almost useless
- But ***can clients use DNSSEC?***
  - Can the end host ***directly or indirectly*** receive DNSSEC-signed data?
    - Are there workarounds?
  - Do DNSSEC validators ***operate correctly***?

Approach: Client Level Tests with *Netalyzr*

- DNSSEC to the recursive resolver provides only minor benefits
  - The recursive resolver is proven untrustworthy: It is the client which must validate DNSSEC
- If DNSSEC information needs to reach the client…
  - We must ***comprehensively test*** the client and recursive resolver
- Enter ***Netalyzr***:
  - A widely used free network measurement and debugging tool that runs in the user's web browser:
    - Now almost 1M sessions to date

DNSSEC to the Client

- Netalyzr previously ***proved*** that the recursive resolver can't be trusted
  - Thus DNSSEC ***must*** be validated on the client
- Can the client get the necessary information to validate DNSSEC?
  - Can it get it directly from the Internet?
    - Ask the roots for key material etc
  - Can it get it from the recursive resolver?
    - Either by using the DO (I want DNSSEC) in requests or by a fallback mechanism of asking for RRSIGs
- Tests have now been integrated into Netalyzr

DNSSEC on the Recursive Resolver

- If the recursive resolver validates DNSSEC, does it validate DNSSEC ***correctly?***
  - – Is the clock accurate?
  - – What algorithms are supported?
    - What is the fate of unsupported algorithms?
  - – A whole host of corner cases…
- Building a ***dynamic*** DNSSEC server
  - – Some tests can only be constructed by generating responses on the fly
- Coupled with new tests, should enable comprehensive examination of the recursive resolver

The (Well Deserved) Demise of Java in the Browser

- Java in the web browser is (deservedly) dying:
  - Java represents a massive security hole due to its sandboxed-structure:
    Many key APIs are effectively running "sudo"
    Any bug which enables a sandbox bypass -> P0wned user
- Fortunately, Android is Java
  - Netalyzr on Android offers even more visibility
    - Still get onto the wifi networks
    - Additional cellular visibility

Other Areas to Measure

- Measuring TLS (Transport Layer Security, aka “HTTPS”) certificates:
  - Query several sites for the TLS certificates
  - Upload the certificates to our server
  - Check with the ICSI TLS Observatory to see if the Certificate Authority is known for that site
    - Effectively “Certificate pinning by observation”
- Cellular radio behavior
  - A hidden source of cellular network performance issues

Benefits: Fully Understanding DNSSEC to the Client

- Can clients receive DNSSEC information? If not, what workarounds?
  - For routing records: A/AAAA/MX etc:
    Bypass the recursive resolver if DNSSEC validation fails
  - If you want to use DNSSEC for key distribution in new protocols, ***also*** include the DNSSEC chain in the protocol as an option
- Also other security protocols:
  - How many clients are behind TLS proxies? Buggy web proxies?

Competition

- Academic research surveys using advertisements:
  - Can probe validation (based on “pass or fail” JavaScript)
    - “Measuring the Practical Impact of DNSSEC Deployment” by Lian et al
      - Limited by static DNSSEC configuration: Can’t measure clock drift or failover
  - Can ***not*** probe the path needed for client-side validation
- Commercial bandwidth testers (e.g. speedtest.net)
  - Have the client base but a much more limited focus on “performance”
  - Have a much more difficult revenue model
    - As researchers we are “paid” in data…

Current Status

- Testing the DNSSEC to client path:
  - Full test suite deployed and operational for several months:
    - Many clients have an either/or problem: either they can’t get DNSSEC from the Internet (common for hotels/coffee shops) or they can’t get it from the recursive resolver (common for bad home gateways)
    - A few clients fail completely: >1% failure rate
- DNSSEC server status:
  - Domain is live, dynamically signing records
    - Need to add NSEC/NSEC3 support and then start building tests
- Android client: near release-ready
- ***Predict*** data release: Developing partial anonymization strategy, signing memorandum of understanding when revised MOU available

Next Steps

- Continue development:
  - DNSSEC server validation suite
    - Javascript version for advertisement-based testing
  - TLS certificate queries
  - Android release
- Technology transition: ***keep running Netalyzr***
  - Developing Netalyzr requires substantial resources
  - Simply operating Netalyzr requires only a little EC2 time

Contact Information

- Nicholas Weaver
  - nweaver@icsi.berkeley.edu
    - PGP key: http://www1.icsi.berkeley.edu/~nweaver/data/nweaver_pub.asc
  - International Computer Science Institute:
    1947 Center Street suite 600
    Berkeley, CA, 94704
    (510)-666-2903