DNSSEC-Tools

Russ Mundy
SPARTA, Inc
DNSSEC-Tools

• SPARTA has developed a number of tools and libraries for DNSSEC
  – http://www.dnssec-tools.org
• Effort is sponsored by US DHS
• Components:
  – Infrastructure: DNSSEC Libraries, Perl Modules, ...
  – Tools for managing DNSSEC Zones
  – Demonstration Applications, Utilities, ETC
  – Educational Materials
DNSSEC-Tools Support

- Core Libraries and Modules
- Zone Management Tools
- Resolver Management Tools
- Developer Tools
- DNSSEC-Aware Application Patches
- DNSSEC Debugging Tools
- Documentation
DNSSEC-Tools: Libraries

• DNSSEC validator library
  – Verifies DNS(SEC) data at the library layer
  – Portable-ish (getting more so)
  – Based on libbind
  – Thread-safe
  – Reentrant
  – Can pull data directly or from a local caching resolver
  – BSD Licensed

• Net::DNS::SEC::Validator
  – Perl module that wraps around libval
Libval\_shim

- LD\_PRELOAD-based approach for adding DNSSEC capability to existing applications
- The shim library implements most of the commonly-used resolver functions
  - Applications that use these functions can automatically become DNSSEC-capable if they run within an LD\_PRELOAD environment with libval\_shim.
  - Many applications (including Firefox) are known to work out of the box with libval\_shim.
Validation Library API

- draft-hayatnagarkar-dnsext-validator-api-06.txt
  - Defines an API for interfacing with a validation library
  - Allows clients to state their policy
  - Allows clients to get DNS and validation results
    - High-level: `val_gethostbyname` and friends
    - Low-level: `val_resolve_and_check` and friends
    - Policy: `val_create_context` and friends
  - Implemented in DNSSEC-Tool's libval
- Not yet an IETF Working Group document
Zone Management Tools

• Zonesigner
  – Signs zones in one step
  – Wrapper around BIND zone signing utilities
  – Defaults do the “right thing”

• Rollerd
  – Automatic key-rollover and signing daemon
  – Regular scheduled calls to zonesigner

• Donuts
  – DNS Zonefile extensible error checker

• Mapper
  – Graphical map generator of zone data
Check Your Zonefile: DoNutS

Zone Errors

Below are the errors found when analyzing the zones

Questions

Results:

reverseddates-ns.test.dnssec-tools.org:

- Rule Name: DNSSEC_SUB_NOT_SECURE
- Level: 3
- Error: sub-domain reverseddates-ns.test.dnssec-tools.org is not securely delegated. It is missing a DS record.
- Details: Tests for the existence of a DS record in a zone for sub-domains. If not present then the sub-domain is not being securely delegated to.

nods-ns.test.dnssec-tools.org:

- Rule Name: DNSSEC_SUB_NOT_SECURE
- Level: 3
- Error: sub-domain nods-ns.test.dnssec-tools.org is not securely delegated. It is missing a DS record.
- Details: Tests for the existence of a DS record in a zone for sub-domains. If not present then the sub-domain is not being securely delegated to.
Check Your Zonefile: DoNutS

# donuts --level 8 -v example.com.signed example.com

--- loading rule file /usr/share/donuts/rules/dnssec.rules.txt
  rules: DNSSEC_RRSIG_TTL_MATCH_ORGTTL DNSSEC_MEMORIZE_NS_RECORDS DNSSEC_MISSING_NSEC_RECORD
  DNSSEC_MISSING_RRSIG_RECORD DNSSEC_RRSIG_NOT_SIGNING_RRSIG DNSSEC_RRSIG_FOR_NS_GLUE_RECORD
  DNSSEC_NSEC_FOR_NS_GLUE_RECORD DNSSEC_RRSIG_SIGEXP DNSSEC_NSEC_TTL DNSSEC_DNSKEY_MUST_HAVESAME_NAME
  DNSSEC_DNSKEY_PROTOCOL_MUST_BE_3 DNSSEC_BOGUS_NS_MEMORIZE DNSSEC_MISSING_RRSIG_RECORD
  DNSSEC_RRSIG_TTL_MUST_MATCH_RECORD DNSSEC_MISSING_NSEC_RECORD DNSSEC_RRSIGSIGNER_NAME_MATCHES
  DNSSEC_NSEC_RRSEC_MUST_NOT_BE_ALONE DNSSEC_RRSIGS_MUST_NOT_BE_SIGNED DNSSEC_MEMORIZE_KEYS DNSSEC_RRSIGS_VERIFY
--- loading rule file /usr/share/donuts/rules/parent_child.rules.txt
  rules: DNS_MULTIPLE_NS DNSSEC_SUB_NOT_SECURE DNSSEC_DNSKEY_PARENT_HAS_VALID_DS DNSSEC_DS_CHILD_HASMATCHING_DNSKEY
--- loading rule file /usr/share/donuts/rules/parent_child_temp.txt
  rules: DNSSEC_SUB_NS_MISMATCH
--- loading rule file /usr/share/donuts/rules/recommendations.rules.txt
  rules: DNS_REASONABLE_TTLS DNS_SOA_REQUIRED DNS_NO_DOMAIN_MX_RECORDS
--- Analyzing individual records in example.com.signed
--- Analyzing records for each name in example.com.signed
  example.com:
    Rule Name: DNS_NO_DOMAIN_MX_RECORDS
    Level: 8
    Warning: At least one MX record for example.com is suggested

  sub2.example.com:
    Rule Name: DNSSEC_SUB_NOT_SECURE
    Level: 3
    Error: sub-domain sub2.example.com is not securely delegated. It is missing a DS record.

results on testing example.com.signed:
  rules considered: 28
  rules tested: 25
  records analyzed: 52
  names analyzed: 8
  errors found: 2
Use Mapper to view zone status (before)
Use Mapper to view zone status (after)
Resolver Management Tools

• Trustman
  – Trust Anchor Management Daemon
  – Detects key-rollovers of configured trust anchors
  – Implements RFC5011 for proper rollover

• Logwatch
  – Monitors system logs for bind DNSSEC errors
  – Patch integrated into the latest version of logwatch
Logfile checking: Logwatch

LogWatch 6.0.2 (04/25/05) 

Processing Initiated: Thu Jul  7 10:13:34 2005
Date Range Processed: all
Detail Level of Output: 10
  Type of Output: unformatted
Logfiles for Host: host.example.com

------------------------------ DNSSEC Begin ------------------------
No Valid Signature received 6 times

Detail >= 5 log messages:
  Marking as secure 97 times
  Verified rdataset succeeded 97 times
  Attempted positive response validation 96 times
  Nonexistence proof found 20 times
  Attempted negative response validation 18 times
  Validation OK 2 times

------------------------------ DNSSEC End ------------------------

------------------------------ Resolver Begin ---------------------

Received validation completion event  171 times
  Validation OK  125 times
  Nonexistence validation OK received  46 times

------------------------------ Resolver End ----------------------

LogWatch End
DNSSEC-Aware Applications

• DNSSEC-Tools contains patches to:
  – Firefox
  – Thunderbird
  – Postfix, Sendmail, LibSPF
  – wget, lftp, ncftp
  – OpenSSH
  – OpenSWAN (opportunistic encryption)
  – Jabberd

• More details about DNSSEC applications later
DNSSEC Capable Firefox

About This Project

The goal of the DNSSEC-Tools project is to create a set of tools, patches, applications, wrappers, extensions, and plugins that will help ease the deployment of DNSSEC related technologies.

- Tool Descriptions and ScreenShots
- Download

To contact the project developers, please write the dnssec-tools-users AT lists.sourceforge.net mailing list or submit bugs to the bug database.

Project News

DNSSEC: Secure: 2  Insecure: 2  Errors: 1
DNSSEC Capable libspf2
DNSSEC Debugging Tools

• Dnspktflow
  – Graphical DNS data flow tracing

• Donuts
  – DNS Zone-file error checker (discussed previously)
Trace your queries: dnspktFlow
Documentation

• Available on project webpage http://www.dnssec-tools.org
• Step-by-step guide for DNSSEC operation using DNSSEC-Tools
• Step-by-step guide for DNSSEC operation using BIND tools
• Manual pages
• User Documentation
• Tutorials tailored towards the needs of particular types of adopters