DNS Security Tools (http://www.DNSSEC-Tools.org)

Russ Mundy
SPARTA, Inc.
<mundy@sparta.com>
DNSSEC-Tools

SPARTA is developing DNSSEC applications
- http://www.dnssec-tools.org/

Components:
- Applications, Utilities, ETC
- Infrastructure: DNSSEC Libraries, Perl Modules, ...
- Tools for managing DNSSEC Zones
- Educational Materials
Firefox detects validation failures
Sendmail+spfmilter
detecting validation failures
DNSSEC-Tools: Libraries

DNSSEC validating resolver 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
Zone Management Tools

• Zonesigner
  – Signs zones in one step
  – Defaults do the “right thing” most of the time

• Rollerd
  – Automatic Key-Rollover Daemon
  – Implements key-rollovers with proper timing

• Trustman
  – Trust Anchor Management Daemon
  – Client utility to watch zones for key rollovers
Zone Management Tools

• Utilities:
  – lskrf
  – expchk
Trace your queries: dnspktFlow
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.

Results: noclaim.ns.test.dnssec-tools.org:
- Rule Name: DNSSEC_SUB_NOT_SECURE
- Level: 3
- Error: sub-domain noclaim.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_ORGTTTL 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_RRSIG_SIGNER_NAME_MATCHES
  DNSSEC_NSEC_RRSIG_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_HAS_MATCHING_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
Check your logfiles: 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 ########################################################################
Use Mapper to view zone status (before)
Use Mapper to view zone status (after)
Documentation

• Step-by-step guide for DNSSEC operation using DNSSEC-Tools
• Step-by-step guide for DNSSEC operation using BIND tools
• Manual pages
• User Documentation
Developer Resources

- Test zone test.dnssec-tools.org
  - Contains many DNSSEC “errors” to test against
- Validator standard API to be published
- Developers guide to using the validator and resolver libraries – work in progress
Questions

?