Interoperability Tests Report for RFC2845 (TSIG)

Mohsen.Souissi@nic.fr

(6WIND, AFNIC, Euro6IX, G6)

IETF 57, Vienna

dnsext-wg

July 15th, 2003

Outline

- Introduction
- Goals and non goals
- Quick description of tests
- Results
- Conclusion

Introduction

- TSIG (Secret Key Transaction Authentication for DNS)

  is specified in RFC 2845

- It provides an authentication mechanism at the transaction level using shared secrets and one way hashing

- It can be used:
  - To authenticate dynamic updates as coming from an approved client
  - To authenticate responses as coming from an approved recursive name server
  - To authenticate zone transfers as coming from an authoritative name server

Goals of the Interop Tests

- RFC 2845 is currently in the ***"Proposed Standard"*** status
- In order to move it forward to the ***"Draft Standard"*** status:
  - Interop tests need to be performed
  - At least two independent implementations should be found interoperable
- An interop report is needed
  - Comprehensive list of tests performed with results
- When 2 implementations fail to interoperate with respect to a given test
  - A report is sent to implementers in order to determine the origin of the problem:
    - Specification error (broken protocol)
    - Implementation error (with respect to the spec)
    - Documentation (e.g. ambiguity ➔ different interpretations)

Non Goals of the Interop Tests

- To test full conformance of each implementation with respect to the specifications (RFC)
- To publish names of implementations tested
- To measure and compare performance of implementations (benchmarking)
- To give detailed explanations on the causes of failures (if any)

Who, where, when?

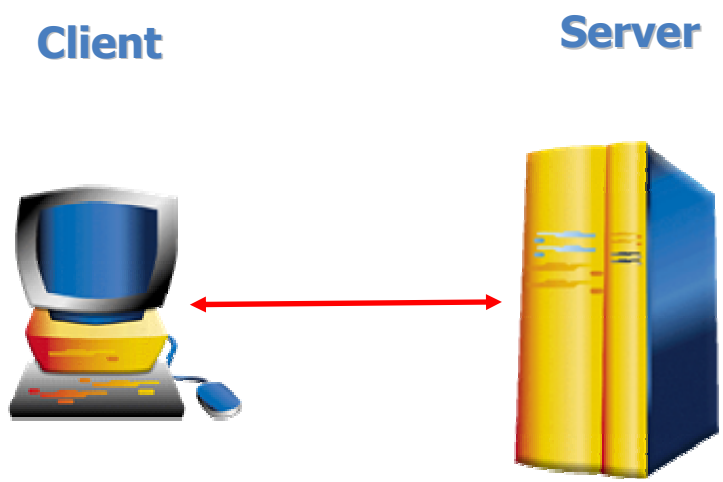
- Who?
  - 6WIND / Euro6IX
  - AFNIC
  - With the help of
    - Euro6IX Project (FT R&D, U Murcia)
    - G6
- Where?
  - AFNIC, Saint Quentin en Yvelines, France
- When?
  - June 17th, 2003

Categories of tests

- Client-Server (C-S):
  - involves one client and one server at a time
- Slave-Master (S-M):
  - involves two servers, one slave and one master
- Client-Forwarder-Server (C-F-S):
  - involves one client and two servers, the intermediate one acting as a "forwarding server"

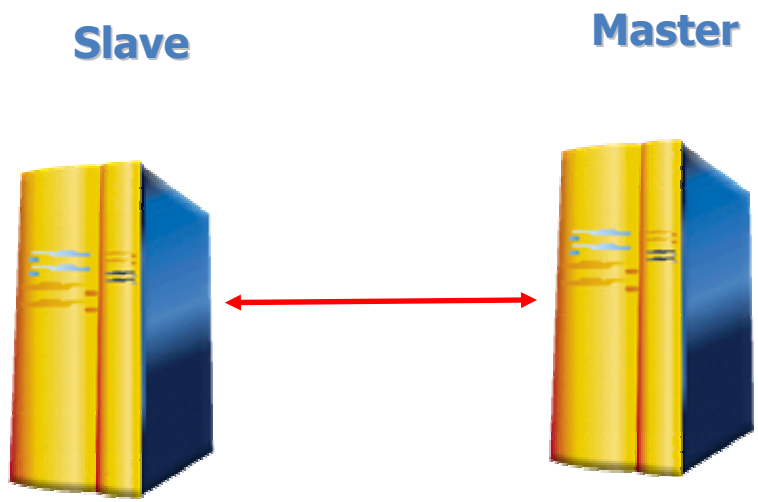
Client-Server tests

- OK (basic test) ➔ C1
- Errors:
  - BADKEY ➔ C2
  - BADTIME (early and late) ➔ C3.1, C3.2
  - BADSIG ➔ C4
- TSIG exclusive: (TSIG only) ➔ C5
- Not exclusive ➔ C6
- Truncation (TCP fallback) ➔ C7
- Multi-envelopes (OK and KO) ➔ C8.1, C8.2



Slave-Master tests

- OK ➔ S1
- Errors:
  - BADKEY ➔ S2
  - BADTIME (early and late) ➔ S3.1, S3.2
  - BADSIG ➔ S4
- TSIG exclusive ➔ S5
- Not exclusive ➔ S6
- Multiple envelopes (OK and KO) ➔ S7.1, S7.2



Client-Forwarder-Server tests

- C-F: NO KEY
  - C-S: NO KEY
    - F-S: GOOD/BAD KEY ➔ `F1.3, F1.4`
  - C-S: GOOD KEY
    - F-S: NO KEY ➔ `F1.1`
  - C-S: BAD KEY
    - F-S: NO KEY ➔ `F1.2`

- C-F: GOOD KEY
  - C-S: NO KEY
    - F-S: NO/GOOD/BAD KEY ➔ `F2.1, F.2.2, F.2.3`

- C-F: BAD KEY
  - C-S: NO KEY
    - F-S: NO/GOOD/BAD KEY ➔ `F3.1, F.3.2, F3.3`

Results

- Three client implementations: A, B, C. Two server implementations: X,Y
- In ***Client-Server*** category:
  - All tests were successful except for those related to truncation (C7) which partially succeeded and multi-envelopes (C8.[12]) which we failed to check
- In ***Slave-Master*** category:
  - All tests were successful by all possible Slave-Master combinations except for those related with multi-envelopes which we failed to check
- In ***Client-Forwarder-Server*** category (section 4.7):
  - Server implementations X and Y, configured as forwarding servers, do not accept to be bypassed by a client directly sharing a secret with the upstream server (failure of F1.1 and F1.2)
  - Tested C-F-S combinations partially interoperate for the remaining tests
  - Some misbehavior was reported to implementers. Patch received and applied ➔ results improved

Conclusion

- TSIG Interop tests were performed
- Full or partial interoperability has been found depending on the category of tests (C-S, S-M or C-F-S)
- Preliminary report at:

  http://w6.nic.fr/RFC2845/ *(dual stack!)*

- What's next?

- Questions/comments: rfc2845@nic.fr