Securing Security - DANE TLSA Monitoring

Patrick Koetter und Carsten Strotmann, sys4 AG

CREATED: 2023-10-20 FRI 08:52

DANE TLSA Monitoring

The need for monitoring

- Traditional SMTP-TLS usage is very forgiving, on errors the protocol switches to plain text communication (opportunistic TLS)
- With DANE, errors in TLS results in an hard error - the communication will fail
    - Mail will not be delivered and might bounce back to the sender

Things to monitor

- Operators of DANE secured mail services should monitor their setup for the following error conditions
  - Existence of a TLSA record
  - DNSSEC validation errors on the TLSA record
  - Number of TLSA records (to prevent TLSA records from accumulating after certificate rollover)

A Bash function to test DANE-SMTP (1)

- BASH function **`danesmtp`** (source: Viktor Dukhovni):

```
danesmtp() {
   local host=$1; shift
   local opts=(-starttls smtp -connect "$host:25" \
               -verify 9 -verify_return_error -brief \
               -dane_ee_no_namechecks -dane_tlsa_domain "$host")
   set -- $(dig +short +nosplit -t tlsa "_25._tcp.$host" | egrep -i '^[23] [01] [012] [0-9a-f]+$'
   while [ $# -ge 4 ]
   do
      opts=("${opts[@]}" "-dane_tlsa_rrdata" "$1 $2 $3 $4")
      shift 4
   done
   (sleep 1; printf "QUIT\r\n") | openssl s_client "${opts[@]}"
}
```

A Bash function to test DANE-SMTP (2)

- Usage:

```
# danesmtp mx01.posteo.de
verify depth is 9
CONNECTION ESTABLISHED
Protocol version: TLSv1.2
Ciphersuite: ECDHE-RSA-AES256-GCM-SHA384
Peer certificate: businessCategory = Private Organization, jurisdictionC = DE, jurisdictionST = B
Hash used: SHA512
Verification: OK
DANE TLSA 3 1 1 ...b86d75419e2f593e2ab08399 matched EE certificate at depth 0
Supported Elliptic Curve Point Formats: uncompressed:ansiX962_compressed_prime:ansiX962_compresse
Server Temp Key: ECDH, P-256, 256 bits
250 DSN
DONE
```

DANE Monitoring scripts

- The Monitoring scripts in the Github repository below can be used to implement basic DNS and DNSSEC monitoring checks for a monitoring system
    - https://github.com/cstrotm/dns-monitoring-scripts
    - https://github.com/cstrotm/dnssec-check
- The Bash-Function presented in the previous slides can be used as a starting point to implement DANE-SMTP checks in monitoring systems

End

Questions? Answers!