Securing the Last Hop

Ondrej Sury
IETF 81, Quebec City

Wire Security

- Between validating resolver and application
- “Unprotected AD bit is for debugging only”
- RFC 3655 says:
  - “A resolver MUST NOT blindly trust the AD bit unless it communicates with a recursive nameserver over a secure transport mechanism or using a message authentication such as TSIG [RFC2845] or SIG(0) [RFC2931] and is explicitly configured to trust this recursive nameserver.”
  - Applicable to stub/application resolver as well

The Trust

- In Resolver we trust
  - In the hotel
  - At the airport
  - At some random place with random DNS resolver
- Any resolver (and any configuration) received by DHCP
  - Any DHCP!

APIs

- The **getaddrinfo()** function is used to get a list of IP addresses and port numbers for host hostname and service servname.
  - No secure-wire information
  - No trust information
  - No AD bit

Questions for the WG

- Is there a problem to solve (or document)?
- Is this in the scope of DANE?
  - Or do we address this just by saying:
    - We need this but it needs to be solved elsewhere
- Not just our problem...
- Shove it elsewhere?
  - Existing working group (DNSEXT?)
  - New working group

Questions (cont...)

- Wire-security vs trust
  - Two problems or just one (“I trust thee” bit)
- What other options do we have?
  - For a wire-security?
    - TSIG, SIG(0), IPSec, VPN, “secure network”
  - For trust?
  - For APIs?
- How to bootstrap?
  - From rogue DHCP... :)