“secure” resolver wishlist

fits/starts

- concepts vs vocabulary – sorry :)
- sent to namedroppers oct2003
- no public follow up till…
- gieben-resolver-application-interface-00 apr2004
- and several independently crafted bits of code

shared views?

- one bit is not enough…
- local policy needs a grammar
- those pesky applications

pesky apps

- intelligent diagnostics
- auditing
- repeatable decisions

intelligent diagnostics

"The host you asked for exists, but is not cryptographically secure, so you can not visit it."

"The host you asked for exists, but the signature has expired, so you can not visit it."

"The host you asked for does not exist, and I can prove it."

"Your internet is broken, and I can not verify the existence of the host"

auditing

Sep 25 19:29:08 cassidy pluto[652]: "private-or-clear#0.0.0.0/0"[33] ...192.139.46.135===? #52: no RSA public key known for '192.139.46.135'; NXT verified.

Sep 21 09:57:59 abigail sshd2[674]: connection from "205.150.200.252", verified to be cassidy.sandelman.ottawa.on.ca with SIG X.
Sep 21 09:58:00 abigail sshd2[2449]: User mcr, coming from cassidy.sandelman.ottawa.on.ca, authenticated.

Received: from karoshi.com (vacation.karoshi.com [198.32.6.68] verified by SIG) by weblet.ip4.int (8.11.6/8.11.6) with ESMTP id h8PMcji22577 for <dns-vet@ep.net>; Thu, 25 Sep 2003 15:38:45 –0700

repeatable decisions

NFS mount request came from host X, which I can not presently verify with DNSSEC because a SIG three levels up expired, however, it has the same public key as last time, when it was considered good. So, I will complain a lot, but I'll let it through.

Any other classes of apps?

Considerations / Assumptions

Applications will drive the use of validation.

so… validation is –NOT- monolithic by end system or interface but per application.

end systems / interfaces may have any number of applications that use them.

some applications will only be “legacy” resolver aware.

DNS resolution and Chain Validation are fundamentally distinct/different actions that share some common elements.

Validator as Resolver on Steroids (ROS)

API / socket?

“coddle legacy apps”?

ephemeral or persistent?

bloat – size/speed tradeoffs

what/who are you? when were you made?

… more questions?

tribal warfare or defacto/dejura

Is this a DNS protocol issue? or… Is this reasonable to take to the IETF?

what is expected behaviour and where is it documented?

implementers each making their own choices will cause interoperability problems that will be difficult to diagnose.

if we do talk, in what forum should the discussion take place?

FIN?