ANIMA

&

Zero Touch Provisioning for NETCONF Call Home

draft-ietf-netconf-zerotouch

NETCONF Zero Touch

A technique to bootstrap a secure NETCONF connection between a newly deployed device and a deployment-specific Network Management System

Assumes device uses DHCP to obtain IP settings

- address, netmask, gateway, DNS servers, etc.

Use Cases

- Connecting to a remotely administered network
  - DHCP server administered by 3rd-party
  - Unlikely device will receive site-specific information
  - Device must reach out to network for initial configuration

- Connecting to a locally administered network
  - DHCP server can be customized
  - Device may receive some site-specific information
  - Device tries local information first, falling back to network otherwise

Solution In a Nutshell

- Device's factory default state includes logic to try to download a "Configlet" from a Configuration Server (a HTTP server)
- Device's pre-programmed list of well-known Configuration Server URLs can be augmented by a new DHCP option
- The Configlet specifies the required boot-image and contains an initial configuration, which is expected to configure a NETCONF Call Home connection
- Device may also download a boot-image from the Configuration Server, rebooting if necessary
- Configlet is signed by a chain of trust that the device can authenticate. Configlet may optionally be encrypted with device's public key
- Mutually-authenticated secure NETCONF Call Home connection, realized by device's IDevID and Configlet's settings

How it relates to ANIMA

- NETCONF Zero Touch is really about bootstrapping a device with an initial boot-image and a configuration that, in part, supplies public-keys for mutual authentication

- The configuration can be *anything*
  - Set public-keys, configure “anima” mode, etc.
  - It does NOT have to configure NETCONF Call Home

Potential Issues

- Assumes L3 and a DHCP server
- In order to prevent substitution attacks, Configlet must contain device's unique identifier (no option for reduced security). Configuration Server may need to get a signed Configlet in near real-time.
- For isolated networks (no Internet), deployments need a local Configuration Server (an HTTP server) and configure local DHCP servers with the Configuration Server's URL

Potential Remedies

- If reliance on DHCP is objectionable, alternates can be supported, so long as they result in a configured IP stack, including DNS
- DNS resolution not needed if URL encodes an IP address
- automate the Configlet signing and staging steps, to support deployments where device identifiers are not known until the last minute. (scan QCR off device)

Relationship to bootstrapping-keyinfra

- Overlap
  - Both drafts begin with device having an IDevID
  - Both drafts end with mutually authenticated trust
  - Both drafts have an L3 aspect

- Differences
  - KeyInfra can work at L2, before moving to L3
  - ZeroTouch more than just key distribution → config
    - KeyInfra supports follow-on interactions, but doesn't define any

Questions / Concerns / Suggestions ?