Secure Network Bootstrapping Infrastructure Proposal

Name

Secure Network Bootstrapping Infrastructure

Repo Name

snbi

Description

The Secure Network Bootstrapping Infrastructure (SNBI) project securely and automatically brings up an integrated set of network devices and controllers. Typically, operators must perform some manual key distribution process before secure communication is possible between a set of network devices. Instead, SNBI uses a zero-touch approach to bootstrapping that leverages manufacturer-installed IEEE 802.1AR certificates to secure even the initial communications. SNBI devices and controllers automatically discover each other, get an IP-address assigned, and establish secure IP connectivity. In addition, this discovery process reveals the physical topology of the network, exposes each type of a device (i.e. whether it is a regular network device or a controller), and assigns the domain for each device. This device type and domain information can also be used for initiating controller federation processes. As part of the SNBI project a basic infrastructure to host, run, and lifecycle-manage multiple network components/functions within a network device is created. These components/functions can include individual network element services, such as performance measurement, traffic-sniffing functionality, or traffic transformation functionality.

Scope

The scope of the SNBI project includes:

- *Secure bootstrapping:* Iteratively discover the connectivity between devices (network elements and controllers) and establish secure IP-connectivity between these devices. Each device in the network is automatically assigned an IP-address and basic IP-routing between the devices is established. As part of the bootstrapping process, a secure communication channel is created and certificates are distributed. Once established, devices and controller can reach each other and bring up control and management protocols. Examples may include Netconf or Openflow and their associated transport connections. Solution components are as follows:

Secure network bootstrapping – device component: The secure discovery service is created as a software package and integrated with the network container reference platform for the devices.

Secure network bootstrapping – controller components:SNBI Registrar: The registrar is the trusted entity/anchor for a network domain. It maintains the list of devices which belong to a domain. It decides (based on its policy rules) which devices are admitted to join the domain. The SNBI Registrar also offers certificate management (issue, renew, revoke) using a lightweight implementation of a certificate authority. Certificate management is fully contained in the SNBI solution, hence ease of use and out-of-the-box ínstall of the OpenDaylight solution are maintained.SNBI Plugin: The secure discovery service is created as a southbound plugin.

- *Foundation for hosting networking capabilities on forwarding elements/devices:* SNBI includes components on the controller and on forwarding elements. OpenDaylight so far supplies a framework to host functionality on the controller. The SNBI projects complements this with a reference environment for forwarding elements. This includes offering a portable foundation to run, package and lifecycle-manage network components /function on a variety of forwarding elements/devices - such as routers, switches, servers, etc. This includes supplying a set of base functionality to build portable functionality for forwarding elements. Furthermore, it includes capabilities for automatic system-level integration testing between forwarding elements and the controller. Secure bootstrapping can be built upon this portable foundation. As the portable foundation builds on container technology, its will be extendable to support additional orchestration and configuration management functions.

The figure below provides an overview of the different components of the SNBI project.

blocked URL

Technical solution details: The following section provides a high-level overview of how the SNBI is expected to operate. The SNBI incrementally adds devices to a Domain. The Domain could initially be formed by just a Controller serving as SNBI-Registrar (please also see the picture below). The following steps are followed in case a new device attaches to a Domain:

1. The new device discovers the Domain. This starts with a search for a SNBI-Registrar. Contact to the SNBI-Registrar will typically be supplied via a “domain edge device” which is already part of the Domain, has the SNBI active, and acts as a proxy for the SNBI-Registrar. Discovery will first try to locate a “domain edge device” on the local link using neighbor discovery, in case this fails, it will try to obtain an address using DHCP and

search for a registrar using DNS service discovery. If this is also not successful, it could search for a predefined, factory-provided global registrar using DNS. Note that the latter two methods already require some form of IP connectivity to the DNS server.

2. The new device presents its 802.1AR credentials to the discovered SNBI-Registrar. The message can be relayed by the “domain edge device” serving as proxy.
3. The SNBI-Registrar checks whether device belongs to the Domain. If true, invites the new device to join the “Domain” and provides it with a “device id”.
4. The new device validates the SNBI-Registrar signature in the invite message and, if valid, decides to join the domain.
5. After accepting the invite message, the new device generates a certificate signing request. It creates a public and private key.
6. The new device then initiates a “Boot strap request” message towards the registrar and provides a PKCS10, PKCS10_signature and the public key.
7. The SNBI-Registrar negotiates to enroll with a Certificate Authority (CA) using the SCEP protocol contained within the SNBI-Registrar component.
8. The result of the negotiation provides a “Domain certificate”, which is relayed from the SBNI-Registrar to the new device using a “Bootstrap response” message.
9. The device is now a member of the domain and will only repeat the discovery process if it is returned to factory default settings.
10. Once enrolled, the new device establishes a secure communication channel to the domain edge device, which connects it securely to the Domain and configures basic IP connectivity:

Create a loopback interface on the new device and assign it an address from an SNBI specific address prefix (e.g. combining the prefix with a hash of the device serial number and domain name).Establish a secure tunnel between the new device and the domain-edge device.Automatically configure a routing protocol (e.g. OSPF, RPL) over the newly established tunnel.Establish clock-synchronization between the newly added device and the domain by configuring NTP.Enable hop by hop service discovery mechanism, using mDNS to discover services like NTP Server, AAA Server, SBNI-Registrar.

blocked URL

The intent is to have all code match to evolving IETF drafts and standards. The following technologies are expected to be used from existing open source projects: NTP, AAA, Syslog, secure tunneling (e.g. IPsec), SCEP, mDNS, CA (Dogtag). Beyond these stable technologies, there is relevant IETF bootstrapping work in its infancy in the Homenet and NMRG working groups. Therefore full standards compliance is not possible today. As standardization solidifies, all SNBI-required code will be made compliant.

Resources Committed (developers committed to working)

- Anu Nair (anu.nair@ericsson.com)
- Balaji B L (blbalaji@cisco.com)
- Liming Wei (lwei@cisco.com)
- Vijay Anand R (vanandr@cisco.com)
- Y F Siu (ysiu@cisco.com)

Initial Committers

- Anu Nair (anu.nair@ericsson.com)
- Balaji B L (blbalaji@cisco.com)
- Liming Wei (lwei@cisco.com)
- Vijay Anand R (vanandr@cisco.com)
- Y F Siu (ysiu@cisco.com)

Vendor Neutral

The code base will be created as a part of the project. The new code base will have no vendor package names in code and no vendor branding present in code or output of build. In addition, no vendor branding will be present in documentation.

Meets Board Policy (including IPR)

Yes.

Presentations

Event	Date	Theme	Presenter	Deck	Notes
SNBI Overview	May/15/2014	SNBI overview for the TSC	Frank Brockners <fbrockne@cisco.com>, IRC: brockners, Balaji B L <blbalaji@cisco.com>	SNBI overview deck	