Status update on ANIMA WG

SACM WG IETF102

Toerless Eckert, Futurewei USA (tte@cs.fau.de)
07/24/2021

Slides at github.com/toerless/presenations/slides-ietf111-sacm-eckert-anima...
Background

The Autonomic Networking Integrated Model and Approach (ANIMA) working group develops and maintains specifications and documentation for interoperable protocols and procedures for secure automated network management and control of professionally-managed (*) networks.

• ANIMA as a good fit of SACM goals and a good platform for further SACM work ?!
• After ANIMA was formed, we did consult with SACM for alignment guidance
• And then we went away into producing our charter round 1 RFC and only recently charter round 2.
• Now we felt it was a good time to circle back to SACM updating on what we did and encourage further collaboration / input from SACM community

(*) ANIMA does not want to step on HOMENET
From NMRG to ANIMA

NMRG Autonomic Networks:
Self-X networks. X = configuring, healing, managing, optimizing, protecting, .... RFC7575/RFC7576

Network wide Intent based management

ASA – Autonomic Service Agents.
Distributed software modules embodying a decentralized or distributed function/service on network devices.

ANI - Autonomic Network Infrastructure
Common infra for ASA and secure automation of legacy networks
BRKI: Secure, zero-touch bootstrap/onboarding
ACP: Secure zero-touch network wide connectivity
GRASP: Secure zero-touch extensible signaling

Figure 1: Reference Model for an Autonomic Node from RFC7575 slightly enhanced
ANIMA Charter round 1 (ANI) published

Autonomic Networking Infrastructure (ANI)

May 2021  RFC-Editor Cluster 325, 420 pages

RFC8366: Validation use case 1: Stable Connectivity (23 pages)
RFC8368: BRSKI voucher  (24 pages)
RFC8990: GRASP – Generic Autonomic Signaling Protocol (55 pages)
RFC8991: GRASP API (29 pages)
RFC8992: Validation use case 2: Prefix Management (19 pages)
RFC8993: Autonomic Networking Reference Model (26 pages)
RFC8994: ACP – Autonomic Control Plane (128 pages)
RFC8995: BRSKI – Bootstrap Remote Key Infrastructures (116 pages)

Fig.1: Use-case example, Autonomous opening of champagne bottle
For Self Study: Autonomic Network according to ANIMA
RFC8993

Intent and Reporting
Network wide, abstract management

Autonomic Network (AN)

Autonomic Function N
ASA N

Autonomic Function 1
ASA 1
Autonomic Service Agent

GRASP
Generic Signaling

ACP - Autonomic Control Plane

BRSKI – Secure Bootstrap

ANI Autonomic Network Infrastructure

Network OS

Domain Certificate

Autonomic Network Infrastructure (ANI)

Secure GRASP messages

secure resilient zero-touch hop-by-hop channels

Autonomic Network (AN):
Intent based network management

Controller

Reporting/Telemetry/Analytics

EMS

Simple, legacy Management Tools

Domain Certificates

MSO OSS

ANI:
Secure, reliable and automatic IPv6 NOC connectivity,
Secure bootstrap, Zero touch service auto configuration
Domain wide (NOC and infrastructure) zero-touch certificates

NOC – Network Operations Center
OAM – Operation, Administration, Maintenance

© 2018, Huawei. Used with permission
ANI operator experience

**Day 1**: Wide area network physically plugged together, connected to NOC, no CLI configured on any router, controller/orchestrator did nothing.

**ANI/BRISKI** gave all devices automatically X.509 ANI domain certificates

**ANI/ACP** automatically establishes on every link a secure ACP tunnel and on ever node a VRF with network wide IPv6 connectivity ONLY for OAM by ASA or legacy NOC equipment, not for user traffic (in-band virtual network)

**ANI/GRASP** running across ANI/ACP provides service discovery for existing decentralized services e.g.: in NOC and common new signaling for ASA

No user packets will flow (nothing was configured). Unauthorized equipment can not connect, Attackers can not even eavesdrop ACP traffic on any link.

Manual / SDN / ASA provisioning/startup of config/services can commence

**Day 1...N**: Secure, Stable connectivity: Operator/Controller can configure any ANI device without out-of-band network. Misconfiguration of addressing, routing, security or other features can not disconnect NOC from ANI nodes, because ANI/ACP is not configurable (autonomous)

ACP will automatically adjust to new/failed links/nodes (ACP RPL routing protocol).

BRISKI/EST will automatically renew domain certificates

New ANI nodes can be added any time, impaired nodes can be revoked from ACP via their certificates.
How to bootstrap ANI

Only required config to get ANI running (example)

ansi registrar
domain-name ani.example.com
Ethernet 0
acp-connect
Register my cert with vendor MASAs

“NOC”
Mgmt Laptop Ethernet 0

Seed Router
ANI BRSKI/PKI Registrar and CA (example)
Bootstrap to ANI domain membership

Ensemble cast, *not the script*

- **Domain Registrar**
  - Drives/coordinates process

- **Pledge**
  - The new, to-become domain member device

- **Proxy**
  - Distributed Agent to give registrar connectivity to adjacent pledge

- **Manufacturer (MASA)**
  - Authorizes Registrar towards Pledge so Pledge will permit to be enrolled into domain

- **Voucher**
  - New digital artefact to indicate to Pledge that Registrar is authorized to control Pledge

- **Admission Control**
- **ACP Address allocation**
- **Certificate (signing)**
  - Rely on certificate authority (CA) Potentially a hierarchy.
For self-study: How does it really work – ANI (1)
For self-study: How does it really work - BRSKI (2)

- **Announce Registrar to all BRISKI Circuit Proxy agents via ACP GRASP**
- **Pledge powers on / connects to Proxy**
- **Pledge learns Proxy via DULL GRASP**
- **TCP: Pledge <-> Proxy <-> Registrar**
- **TLS: Pledge <--------> Registrar (BRISKI)**
- **Registrar now trusts PIC**
- **Pledge does not yet trust RDC**
- **Pledge request voucher to trust RDC**
- **Registrar claim pledge to get voucher from MASA**
- **Pledge now trusts RDC**
  - (EST) Pledge requests trust anchor to later authenticate domain peers
  - Pledge requests cert parameters to build its domain certificate
  - (EST) Pledge requests signing of domain cert
- **Pledge telemetry: I am enrolled!**
Where are we now

• Since Q2’ 2020 on 2\textsuperscript{nd} Charter
  • Added ASA work to charter
  • Added ANI enhancement
  • Pushed out Intent back to NMRG
    • NMRG nicely working on the research steps
    • But key ANIMA contributors busy with charter 1 until May.

• ANI: Bootstrap sees quite wide proliferation/adoption across IETF and industry (next slide)
  • Hackathon at IETF111, Also iot-onboarding / MUD adjacencies
  • Relatively little new code to write (on top of existing PKI, tool chains), but quite security critical
  • (Toerless) way too many different protocol preferences in different markets = many variations needed.
  • Try to keep a common framework/common security behavior
  • Key work items: “constrained” devices BRSKI / voucher, cloud-connected registrar

• ANI: ACP seeing little movement yet
  • Logical ? Bootstrap must first work
  • Pre-standard industry implementations
  • (Toerless) Complex to implement well in legacy router infrastructures (much easier with newer/containerized/virtualized infrastructures, or BMC

• Various prototype implementations exist
  • More implementations welcome
Bootstrap landscape / roadmap

https://github.com/anima-wg/enrollment-roadmap (somewhat stale)
What is next? ASA?!

Ongoing work in NMRG, then maybe ANIMA?

What distributed/decentralized services are of interest? especially also for security

We have seen many comprehensive, ambitious architectur proposals in ANIMA over the years

But ANIMA is in OPS, so we are primarily interested in stuff that can be operationalized (easily)
ANI with GRASP makes this easy and agile – including experimentation / prototyping

ANI and xtensions: Done/ongoing in ANIMA and especially bootstrap also in other groups

Figure 1: Reference Model for an Autonomic Node from RFC7575 slightly enhanced
Pragmatic considerations (1) (sorry, no eye candy)

• Application protocols with End-to-end encryption (TLS, QUIC)
  • Do often not use strong, automatically renewed and flexible PKI certificates but just TLS with username/password and Web PKI with their problematic Trust Anchor management.
  • Certificate management often seen as difficult by operators

• Just use ANI certificates ?!
  • Simply relying on ANI certificate could help to automate/use strong crypto for end-to-end applications
  • If existing ANI services are not sufficient, additional (higher layer) automation can be implemented as ASA
  • E.g.: additional role/authorization functionality for certificates via ANI/ASA so certificates become more functional
Pragmatic considerations (2) (sorry, no eye candy)

• Existing infrastructure services protocols are often not deployed with “security”
• Operationaly hard to do key management and bootstrap for the services.
  • NTP, DNS, SMTP, MacSec, routing protocols, “tftp”, IPFIX and several others
• When completely insecure protocols are run across ACP, their traffic is protected by ACP
  • Hop-by-hop authentication/encryption
• But many need their own, non-certificate credentials
  • And several should not run across ACP (OAM plane)
• ACP/GRASP ASA to the rescue
  • ASA does not need to worry about how to discover candidate protocol peers (link-local or ,network wide) whether to trust them, or how to come up with new messages – All done by ACP/GRASP
  • Simple to write distributed scripts (e.g.: TCL or python) to automate generation and provisioning of such keying material
  • Automating e.g.: securing of routing protocols wih dynamic keys could be maybe a < 100 lines of code script using GRASP API (TBD)
If networks where cars

SDN-Controller
SDN-Orchestrator
SDN-Developer
Data Analyst
Network operator
Security Expert

In-network intelligence

ANIMA

“self driving networks”
The End

Please engage with us (proposal, questions, suggestion) if you think this is useful for you! – anima@ietf.org